Computers, Materials & Continua CMC, vol.64, no.1, pp.439-454, 2020

A Safe and Reliable Routing Mechanism of LEO Satellite Based on SDN

Chao Guo[1, *], Juan Guo[2], Chanjuan Yu[1], Zhaobin Li[1], Cheng Gong[3] and Abdul Waheed[4]

Abstract: Satellite networks have high requirements for security and data processing speed. In order to improve the reliability of the network, software-defined network (SDN) technology is introduced and a central controller is set in the network. Due to the characteristics of global perspective, control data separation, and centralized control of SDN, the idea of SDN is introduced to the design of the satellite network model. As a result, satellite nodes are only responsible for data transmission, while the maintenance of the links and the calculation of routes are implemented by the controller. For the massive LEO satellite network based on SDN, a state evaluation decision routing mechanism is proposed. The designed mechanism monitors the status of the entire network effectively and reduces the on-board load on the satellite network. The best routing decision is made under the comprehensive consideration of the current and historical status of each inter-satellite link between Low Earth Orbit (LEO) satellite network nodes. The calculation and storage requirements are controlled within a reasonable range. Based on the curve parameter transmission fuzzy encryption algorithm, a safe and reliable condition assessment decision routing mechanism (CADRM) is designed. It ensures that the personal information of the LEO satellite network can be transmitted safely and effectively. The experimental simulation results show the improvement of network throughput, the reduction of packet loss rate and the enhancing of network reliability.

Keywords: Route, LEO satellite, SDN, state assessment, inter-satellite link.

1 Introduction

The use of satellites is more cost-effective than terrestrial networks in realizing the full coverage and deep access to mountains, deserts, and oceans by future broadband IP networks. LEO satellite network has the advantages of low latency and large coverage

[1] Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing, 100070, China.

[2] Vocational and Technical College, Guilin University of Electronic Technology, Beihai, 536000, China.

[3] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, 100083, China.

[4] University of Management Technology, Lahore, 55300, Pakistan.

[*] Corresponding Author: Chao Guo. Email: guo99chao@163.com.

Received: 19 January 2020; Accepted: 05 April 2020.

area, which is of great significance in real-time communication of anyone at any time [Adnane, Foitih, Mohammed et al. (2018)]. In recent years, several LEO satellite constellations have been proposed and implemented in the world, such as the Starlink project proposed by SpaceX, the OneWeb program of the United States, the Hongyan constellation and the Hongyun project proposed by China Aerospace Science and Technology Corporation [Bin, Defeng, Xiao et al. (2018)]. In most cases, the LEO constellation has been proposed to form a mesh network through inter-satellite links between neighboring satellite nodes. On this basis, efficient and secure routing is the function of the future LEO satellite network as a terrestrial terminal accessing the backbone network in the global communication network.

The dedicated hardware infrastructure in satellite networks comes from different vendors and has different communication protocols. It imposes significant limitations on the reconfigurability and interoperability of satellite networks, leading to management complexity increase [Su, Lin, Zhou et al. (2015)]. Due to a large number of nodes in the network and the complex network deployment, it is difficult to control the distribution of data traffic and manage the network. The new network architecture of Software Defined Networking (SDN) [Liu, Wang, Chaudhry et al. (2018); Alvizu, Maier, Kukreja et al. (2017); Sato, Uchida and Shibata (2014)] separates the data layer from the control layer. The control layer monitors the entire network and performs a comprehensive analysis of the real-time information about network traffic distribution and node load. Based on this information, the optimal path can be calculated.

To realize real-time access to small power mobile terminals and seamless global coverage of satellite signals, more and more satellite nodes are deployed in the LEO satellite network. Therefore, the characteristics of the LEO satellite network and related problems are studied [Xiao, Cai, Wang et al. (2015)]. The routing algorithm has become an urgent problem. A safe and reliable condition assessment decision routing mechanism (CADRM) proposed in this paper makes routing decisions by considering the inter-satellite link-state based on queue length and packet loss rate. It improves network throughput, reduces packet loss rate, and enhances network reliability.

Satellites are expected to play an increasingly important role in providing broadband Internet services over long distances in an efficient manner. Future networks will consist mainly of hybrid ground nodes connected via satellite links. Security is an important issue in such networks. The curve parameter transmission fuzzy encryption algorithm is applied to generate a key s based on personal physiological characteristics. The personal data information that needs to be sent can be encrypted. It ensures the security of personal communication in the satellite IP network with low transmission reliability and security.

A state evaluation decision routing mechanism is proposed to implement the lowest possible computation and storage overhead. It achieves load balancing while considering the network history information. The key is generated by the fuzzy parameter encryption algorithm [Huang and Chao (2011)] proposed by the previous work. The algorithm is based on the classic biometric encryption technology of Fuzzy Vault [Juels and Sudan (2004)]. Instead of adding confusing points in the key generation process, the sinusoidal superposition curve is used to fit the curve containing the real points, and then the transmission is performed. Compared with the Fuzzy Vault encryption technology, the curve parameter transmission fuzzy algorithm greatly reduces the amount of data that the key generation needs to transmit. It obtains a real-time energy-saving lightweight satellite personal communication key generation scheme to improve the CADRM routing mechanism.

The rest of this paper is arranged as follows. Section 2 describes the related work. Section 3 introduces SDN, SDN-based satellite networks, and their frameworks. Section 4 introduces the routing algorithm for LEO networks. Section 5 introduces the transport encryption algorithm. Analysis and simulation results will be described and displayed in Section 6. Section 7 gives the conclusions and an outlook for future work.

2 Related work

SDN provides real-time network management and maintenance to improve the efficiency and stability of the network. Therefore, combining SDN with a new generation of LEO satellite networks [Arti and Jain (2017); Jia, Liu, Gu et al. (2017); Li, Zhou, Luo et al. (2016); Nazari, Du, Gerla et al. (2016); Zhang and Wang (2016)] can improve network performance effectively.

With the increase in the number of satellites, the topology change of the satellite network is accelerated, and routing calculation becomes more and more difficult. Some literature designed the routing algorithm based on virtual topology, which was widely used in the routing calculation of the LEO satellite network [Liu, Xu, Tang et al. (2016); Tan and Zhu (2014)]. The environment of the satellite network is different from the ground network. Factors such as transmission delay and load balance have been verified to affect the information processing efficiency of the satellite network. It is urgent to establish a safe, reliable and efficient routing mechanism to adapt to the unique network environment and provide an independent communication system without ground relay [Caini and Firrincieli (2012); Lu, Zhao, Sun et al. (2013)]. The packet Distributed Routing Algorithm (DRA) [Ekici, Akyildiz and Bender (2001)] proposed earlier was based on the polar-orbit LEO satellite network topological structure. DRA selected the load-balancing routing mechanism of the next-hop according to the measurement of the shortest transmission distance of the packet. However, due to the lack of network status and control information exchange between satellites, routing performance would decline rapidly when link congestion occurred. Compact explicit multi-path routing (CEMR) [Bai, Lu, Lu et al. (2005)] achieved the purpose of load balancing based on multi-path mechanism and queuing delay prediction. Unfortunately, the congestion state memory and queue delay of the next-hop node could not be transmitted through this mechanism, resulting in packet loss. Priority-based adaptive routing PAR and enhanced PAR [Korçak and Alagoz (2005)] use inter-satellite link history usage records and buffer information to make routing decisions. When forwarding packets, a PAR tended to select a low-utilization link for forwarding. The ad-hoc network was similar to the LEO satellite IP network in single-hop routing. Because of the high latency of the latter, the routing decision of the ad-hoc network was not applicable to LEO satellite network [Cruz-Sanchez, Staples, Schott et al. (2013)]. The routing mechanism proposed in this paper makes routing decisions by considering the inter-satellite link-state based on queue length and packet loss rate.

Satellites are vulnerable to a range of attacks, including eavesdropping, session hijacking, and data corruption [Dewangan and Sahu (2016)]. The problem of ensuring communication security is another issue that needs to be addressed in satellite networks. To maximize the achievable secrecy rate of the eavesdropped fixed-satellite service, [Du, Jiang, Zhang et al. (2018)] designed a cooperative secure transmission beamforming scheme. It was realized through the satellite's adaptive beamforming, artificial noise, and the cooperative beamforming of terrestrial Base Stations (BSs). [Roy-Chowdhury, Baras, Hadjitheodosiou et al. (2006)] looked at the performance problems arising in hybrid networks due to security additions like Internet security protocol (IPSec) or secure socket layer (SSL), and suggest solutions to performance-related problems. However, none of the schemes proposed in the above literature addresses user authentication or message integrity issues for group communication. In this paper, the curve parameter transmission fuzzy encryption algorithm is applied to encrypt the personal data information that needs to be sent. It ensures the security of personal communication in the satellite IP network with high transmission reliability and security.

3 System model

3.1 Software defined network

Software Defined Network (SDN) is a new type of network innovation architecture that is an implementation of network virtualization. Its core technology, OpenFlow, separates the control plane of the network device from the data plane, thus achieving flexible control of network traffic. SDN makes the network more intelligent as a pipeline and provides a good platform for innovation and applications of core networks. The deployment of the new network function in SDN only requires a centralized software upgrade at the control node, thereby implementing a fast and flexible customized network function. Besides, SDN architecture is also very open. It abstracts the entire network and provides users with a complete programming interface so that users can satisfy their customized network resources according to the upper-layer services and applications. The open and programmable characteristics of SDN brings the potential to break the monopoly of certain vendors on devices, protocols, and software. More people can participate in the research and development of network technology.

Fig. 1 shows the architecture of SDN. The SDN is divided into the data plane, control plane, and application plane from south to north. The data plane and the control plane communicate with each other using the SDN control data plane interface. The SDN Northbound Interface (NBI) is responsible for communication between the control plane and the application plane. NBI allows users to customize development according to actual needs. SDN is a dynamic, manageable, cost-effective, and adaptable architecture, seeking to be suitable for the high-bandwidth and dynamic characteristics of today's applications.

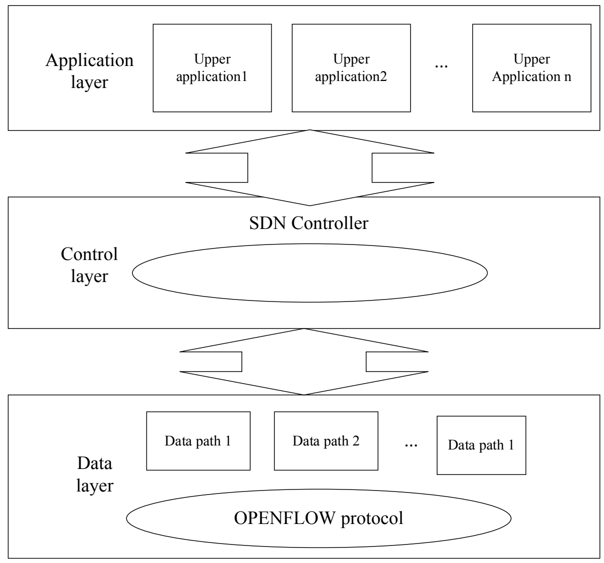

Figure 1: SDN framework

3.2 Satellite network based on SDN

There are several reasons why SDN architecture is suitable for satellite networks:

●In a satellite network, its topology is highly dynamic due to its fast speed. The use of SDN controllers can perform real-time and efficient calculations based on these topologies to enhance the stability of the network.

●SDN has a global perspective and can effectively manage regular and periodic satellite networks.

●Due to the hardware versatility and software programmable features of SDN, the cost of satellite network updates is greatly reduced.

●In the SDN architecture, the satellite node is only responsible for the data transmission, while the link maintenance and routing calculation are handled by the controller. The efficiency and reliability of network communication have been greatly improved.

●Based on the global perspective and centralized control of SDN, it provides a basis for real-time monitoring of the entire network and traffic monitoring of each node. It is beneficial to find the optimal transmission path to meets the communication requirements and save the bandwidth resources of satellite communication.

Therefore, combining SDN technology with a new generation of LEO satellite networks improves the flexibility of network monitoring and management [Lin, Liu, Zhou et al. (2014); Lin, Zheng, Zhou et al. (2015)].

Fig. 2 shows the SDN-based LEO satellite network framework. The Multi-layer satellite network structure includes multiple layers of LEO satellites at different heights. High-level satellites manage low-level satellites to achieve global coverage. Most LEO satellites are located in the data layer of the SDN network, which are based on the OpenFlow protocol and transmit data according to the controller's instructions. The ground control stations and some high-level LEO satellites are located in the control layer of the SDN network. Based on the complete network view, the controllers provide the best path for data transmission and real-time management of the network [Hui, Zhou, Xu et al. (2020)].

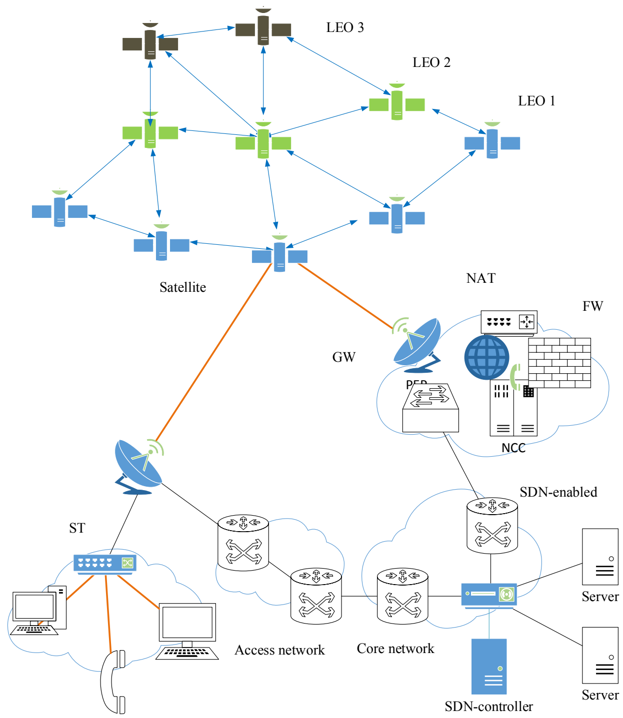

Figure 2: Satellite network framework based on SDN

4 State evaluation decision routing mechanism

Compared with the routing algorithm of traditional terrestrial cellular network, the routing algorithm of the LEO satellite network has more limitations, mainly in the following aspects:

●The nodes in the LEO satellite network run fast and have low orbital altitudes. Compared with other satellite networks, the network structure has a high speed dynamic change. Network topology and link state are updated frequently. As a result, the average end-to-end delay of data transmission is long and the system error rate is high.

●In the space environment, the chip used by the satellite node has better anti-radiation interference performance than the material used by the ground communication node. It limits memory capacity and the processing efficiency of the central processing unit.

●Satellites operate in space and are expensive to launch and recover. Repair after the damage is very difficult. The destruction of any satellite will have a great impact on the entire network communication and bring huge losses. Therefore, it is necessary to improve the robustness of the satellite network.

In order to improve the effectiveness of the LEO satellite communication network and the reliability of data transmission, the first problem to be solved is the routing problem. Because the satellite nodes in LEO satellite communication network are run fast in the orbit, the network topology is highly dynamic. The traditional routing algorithm for terrestrial mobile cellular networks is mainly used to calculate the fixed topology. Static topology is not suitable for LEO satellite network with dynamic network topology, so traditional routing algorithms cannot be directly applied.

The routing mechanism based on the SDN-based satellite network architecture is proposed. It makes routing decisions by considering the inter-satellite link-state based on queue length and packet loss rate. The relationship between these two parameters is expressed by a formula. The value is called as a state parameter θ_m . The queue length is defined as the buffer occupancy rate in a satellite time interval. The packet loss rate reflects the relationship between successful transmission and loss of data packets. In addition to considering the state θ_m of the current time interval, CADRM also considers the historical state. It reflects the continued use of the link and thus obtains a key-value routing factor K_m . When a packet arrives at the satellite via an inter-satellite link or a satellite-ground link and needs to be forwarded, the satellite will detect each K_m of the four inter-satellite links and find the minimum inter-satellite link as the next-hop path. Since K_m will continue to grow over time, it is difficult for satellites to provide sufficient resources of calculation and storage. A standardization process is proposed to limit K_m to an acceptable range.

4.1 Model establishment

Considering the simplified management of the polar orbit constellation and the advantages of global coverage design, the system model is built on the polar orbit constellation inter-satellite link under the framework of the SDN-based satellite network. Each satellite has four inter-satellite links that communicate with four neighbor nodes, two of which are intra-orbital links and the other two are inter-orbital links. A satellite has four independent buffers for four different directions of inter-satellite links, and there are four queues for each buffer.

In order to study the routing of satellite networks, Graph $G=(V,E)$ is used to establish a network model, where V denotes the satellite nodes and E denotes the inter-satellite links connecting different satellites. Each satellite node has a unique number 0 to n, and the satellite node can be represented as $v_i (i = 0,1,\ldots,n)$, $v \in V$. e_{ij} represents the inter-satellite link of the satellite v_i to v_j $(j = 0,1,\ldots,n)$, and e_{ji} denotes the opposite direction, $e \in E$.

4.2 The setting of status parameters

The key to the optimal link-state setting in CADRM is the buffer occupancy and packet loss in the actual operation of link during the current time interval. In order to apply CADRM to a variety of different satellite network systems, the parameters used primarily to express the relative performance of the inter-satellite links rather than the actual values. In the status parameter θ_m, m denotes the mth time interval. The length of the buffers may be different in different satellite systems, so a ratio of the actual length of the queue state is more appropriate for multiple systems. The length of the queue is defined as the ratio of the buffer occupancy O_q to the total buffer length L within current time interval. The packet loss rate is defined as the ratio of the lost packet R_l to the total transmitted packet R_{total}. Assuming that only packet loss due to link congestion is considered, the status parameter can be expressed as:

$$\theta_m = \frac{O_q}{L} + \frac{R_l}{R_{total}} \tag{1}$$

Since $\frac{O_q}{L}$, $\frac{R_l}{R_{total}} \in [0,1]$, then $\theta_m \in [0,2]$. Within the current time interval, the network runs without packet loss and buffer occupancy, $\theta_m = 0$; in the extreme case of all packet loss and buffer full occupancy, $\theta_m = 2$.

4.3 Routing factor settings

The primary purpose of the routing factor parameter K_m is to direct the satellite node to make appropriate routing decisions and indicate the performance of the current inter-satellite link. When a packet that needs to be forwarded arrives at the satellite node, the satellite selects the appropriate inter-satellite link as the next-hop path by looking up the routing table. Selecting the inter-satellite link not only depends on the current time interval link-state θ_m, but also needs to consider the past situation, because a good θ_m does not mean that the link is always in good condition.

The current time interval link state is more informative than the past state. To show that current data is more important than past data, an attenuation function d^m is proposed. d^m is an incremental function, multiplied by θ_m such that when m decreases, the result tends to 0. d^m has a range of $[0,1)$.

Assuming that the current time interval is m, K_m is derived from the following formula (2):

$$K_m = \sum_{s=0}^{m} d^{m-s}\theta_s \tag{2}$$

It should be noted that limited satellite resources cannot withstand huge overhead. It includes calculating d^m from the first time interval of the system startup and calculating the product and power during each interval.

It can be seen from Eq. (3) that Eq. (2) is an iterative process:

$$K_m = \theta_m + d\sum_{s=0}^{m-1} d^{m-1-s}\theta_s = \theta_m + dK_{m-1} \tag{3}$$

After the iterative process of Eq. (3), K_m equals the sum of θ_m and dK_{m-1}, and the memory overhead is only used to store these three parameters. Therefore, the requirements for satellite computing and storage capacity will be greatly reduced.

Over time, K_m will gradually increase and may reach the storage limit. To solve this problem, the following normalization process is used. This process limits K_m to a certain range $0 \le K_m \le 1$.

Multiply $\frac{1}{1+d}$ by the formula (2) to get:

$$K_m = \sum_{s=0}^{m} \frac{d^{m-s}}{(1+d)^{m-s+1}}\theta_s \tag{4}$$

Let $\frac{d}{1+d} = \varepsilon$, compare formula (3), get normalized K in the equation K_m:

$$K_m = (1\text{-}\varepsilon)\theta_m + \varepsilon K_m \tag{5}$$

Among them, ε satisfies $\begin{cases} \varepsilon < 1-\varepsilon \\ 0 < \varepsilon < 1 \end{cases}$ and solves $\varepsilon \in \left(0, \frac{1}{2}\right)$.

4.4 Direction estimation process

After the above processing, the satellite node can select the optimal link for the routing request. But the destination node is likely to be in the opposite direction of the current node. In order to complete the routing decision of the destination node selection direction, the direction estimation process will eliminate the link that generates the loop. This process divides the network into four regions and centers on the current node. In both cases the destination node location is excluded by the routing area: 1) in the area; 2) at the junction of the two areas. Only inter-satellite links within or at the intersection are selected as alternative paths, regardless of other links. The mesh network and the modified symmetric inter-satellite link LEO network are suitable for this process.

This method not only avoids loop generation but also avoids the case where the selected optimal routing factor link does not point to the destination node. The opposite direction means that more jumps are needed to the destination node. Due to the long delay caused by multiple strips, those links are not superior to the “forward link” in the area.

Considering that the routing decision occurs in node v_i, its neighbor nodes are arranged clockwise in the upper, right, lower, and left directions, and the destination node is v_d.

Definition 1: The area (direction) is the routing area of v_i when the following formula is satisfied.

$$Direction=\begin{cases} Upper\ left,\ \ x_d-x_i>0, y_d-y_i>0 \\ Lower\ left,\ \ x_d-x_i>0, y_d-y_i<0 \\ Lower\ right,\ \ x_d-x_i<0, y_d-y_i<0 \\ Upper\ right,\ \ x_d-x_i<0, y_d-y_i>0 \end{cases} \tag{6}$$

Given the coordinates $v_i:(x_i,y_i)$, $v_d:(x_d,y_d)$, the optional inter-satellite link ISLs is $E=\{e_{ih},e_{ij},e_{ik},e_{il}\}$. The direction estimation process is proposed on the basis of definition 1. When v_i is in the upper left of the region, $E=\{e_{ih},e_{ij}\}$; when v_i is in the lower left of the region, $E=\{e_{ij},e_{ik}\}$; when v_i is in the lower right of the region, $E=\{e_{ik},e_{il}\}$; when v_i is in the upper right of the region, $E=\{e_{il},e_{ih}\}$, returns the value of E. The above is the process of selecting an optional link obtained by routing decision when the route request is sent on the node v_i.

5 Curve parameter transmission fuzzy encryption algorithm

On the basis of establishing the state evaluation decision routing mechanism, taking into account the trend of personal communication applications in the development of low-orbit satellite IP networks in the future. Meanwhile, the transmitted data information is encrypted in order to ensure personal communication security. In this paper, a fuzzy parameter encryption algorithm is used to generate a key s based on personal physiological characteristics, and s is used to encrypt the personal data information that needs to be sent. This ensures the security of personal communications in satellite IP networks with low transmission reliability and security.

First, assume that the key s is a 128-bit random number, and input s into a checksum calculation module to calculate the check value. The check value is then concatenated at the end of the key s to form a modified cipher. Here, the CRC-16-CCITT with a polynomial of 0×1021 is used, as in Eq. (7). In this test, the CRC-16 lookup table algorithm is used.

$$x^{16}+x^{12}+x^{5}+1$$

(7)

From here on, all operations will be performed in the Galois field with a base of 65536, GF (2^{16}). The corrected password s' is divided into (8+1) values a, that is $s'=a_0\ \&\ a_1\ \&\cdots\&\ a_8$, and these values are set as coefficients of the polynomial $p(x)$, and the highest order is 8, that is, $p(x)=a_0x^8+a_1x^7+\cdots+a_7x+a_8$. After the formation of $p(x)$, the user's physiological characteristic values are used to calculate the real point (x,y), and several random confusion points are added so that the fitted curve can be prevented from being too close to the original polynomial curve. Then, using the sinusoidal superposition polynomial to fit these real points and the confusion points to obtain a curve $f(x)$ and store its parameters, the parameter of the curve is that the vault needs to be transmitted. The receiver receives the vault transmitted by the sender, combines the possessed user biometric value x', calculates (x', y') according to $f(x')$, and finally decrypts the decrypted key according to Lagrangian interpolation and CRC.

6 Performance analysis

In the SDN-based satellite network system, the topology of the satellite network changes frequently. Therefore, the computational efficiency of the routing algorithm, the network convergence rate and the communication performance of the network after the network topology changes can be improved. The paper compares the packet loss rate and throughput of the CADRM and CEMR, PAR and Dijkstra shortest path routing algorithms proposed in this paper. In addition, in order to verify the effectiveness of the fuzzy algorithm for curve parameter transmission on the CADRM routing mechanism, a comparison is made with the simulation of the Fuzzy Vault scheme. The network packet loss rate should be controlled within a certain range during normal transmission. Throughput is the maximum rate that a device can accept without frame loss. The test method is: sending a certain number of frames at a certain rate in the test and calculating a frame transmitted by the device under test. If the number of frames sent is equal to the number of received frames, the transmission rate is increased and retested; if the frame is received Less than the transmission frame, the transmission rate is reduced and retested until the final result is obtained. The throughput test results are expressed in bits per second or bytes per second.

The Compressed Multipath Routing (CEMR) algorithm utilizes the Hash coding technique to compress the path information to reduce routing overhead. Based on the formal method (PAR), the problem of the automatic generation of sorting algorithms is studied. The Dijkstra algorithm is used to find the shortest path between two points in the graph, or to specify the shortest path from one point to all other points, which is essentially a greedy algorithm.

The simulation parameters are shown in Tab. 1. In the experiment, to fully reflect the difference in the performance of various mechanisms, all links are set to be error-free links. During the simulation, the average packet size is set to 1 KB, and the delay of all links is set to 20 ms. Each ISL buffer is set to 200 kb to store 200 packets.

Table 1: Simulation parameters

Number of tracks	6
Number of satellites per track	11
Satellite height	780 km
Cross-slit ISLs	No
Number of links	2 in-rail +2 rail
ISL bandwidth	25 Mb/s
ISL buffer size	200 packets

As shown in Fig. 3, compared with the shortest route routing algorithm of CEMR, PAR and Dijkstra, the CADRM proposed in this paper has the lowest packet loss rate. The better performance of CADRM than CEMR and PAR is due to the historical information of the inter-satellite link, and Dijkstra only looks for the shortest path without considering the link load balancing problem. The simulation results show that as the number of terminal transmissions increases, the satellite node buffer is gradually occupied, and the system packet loss rate will continue to increase.

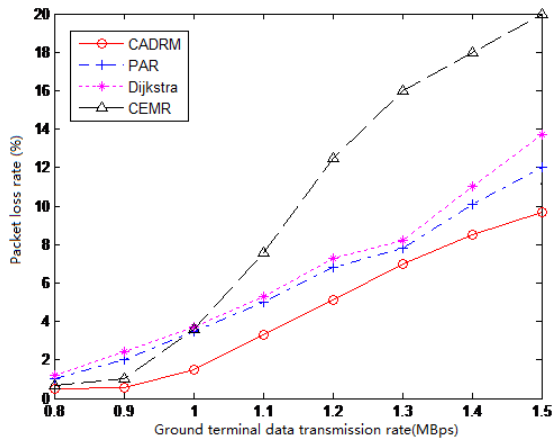

Figure 3: Packet loss rate under different transmission rates

As shown in Fig. 4, experimental simulations show that CADRM achieves the best performance in total throughput in the four routing mechanisms. It can be seen that the total throughput has the same trend concerning the packet loss rate.

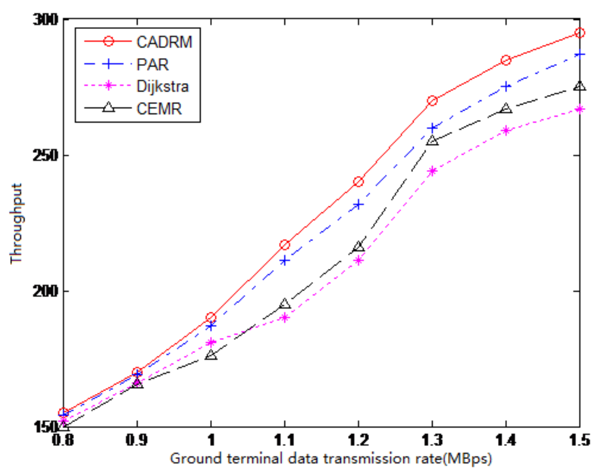

Figure 4: Throughput at different transmission rates

The fuzzy key binding (Fuzzy Vault) algorithm was proposed by Juels et al. [Juels and Sudan (2004)], and its biggest feature is its ambiguity. In the Fuzzy Vault algorithm scheme, the main idea is to hide the key to be protected in the polynomial coefficient, and then use the biometric as the variable of the polynomial to obtain the corresponding polynomial value, and generate a large number of hash points not on the polynomial, forming Vault. At the time of decoding, the real feature points are separated from the vault, and then the encryption key is reconstructed by a polynomial.

In order to verify the effectiveness of the curve parameter transmission fuzzy algorithm on the CADRM routing mechanism, nine feature points are taken as an example for experimental verification. Experiments were carried out with 100 sets of physiological characteristics as experimental data, and the success rate of decryption of the Fuzzy Vault scheme and curve parameter transmission fuzzy scheme was compared. The recovery success rate of the original method is about 79%, while the experimental result of the method is about 85%. The success rate is slightly higher. In terms of the amount of data transmitted, 15 coefficients are finally generated according to the algorithm encryption phase. The data is transmitted by the method, regardless of the user data of the LEO satellite network. Similarly, the receiver can accurately restore the original data of the sender based on the data plus the user's feature information. As shown in Fig. 5, the amount of data generated by the Fuzzy Vault solution will increase significantly as the number of original data increases.

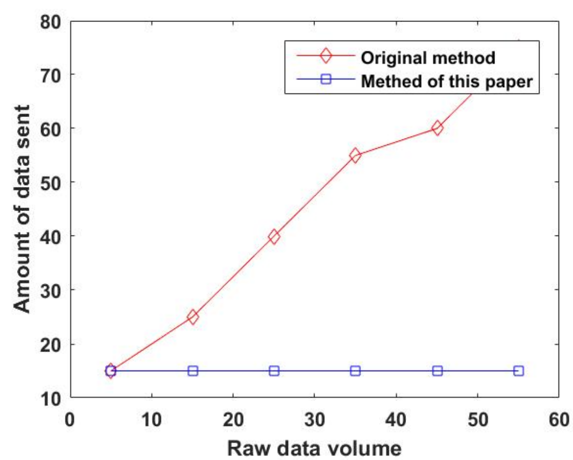

Figure 5: Send data comparison

Therefore, in terms of the amount of data sent and the power consumption of transmission, the method is more resource-saving than the amount of data transmitted by the Fuzzy Vault. According to the amount of data transmitted, the Fuzzy Vault is more resource-saving and suitable for personal communication security of the LEO satellite network.

7 Conclusion

Considering a large number of satellite network nodes, a satellite network architecture based on SDN is proposed. Then, according to the current and historical link conditions reflected by routing factors, a state evaluation decision routing mechanism is proposed to balance the impact of link state. Each satellite processes routing requests, and the routing area is limited to the minimum number of hops. On this basis, the fuzzy parameter encryption algorithm is used to improve the security performance of the routing mechanism. It provides support for secure personal communications without terrestrial relays. The simulation results give the optimal ratio of current and historical link states. The proposed algorithm not only reduces the packet loss rate but also improves the maximum throughput and communication security.

Of course, the algorithm can be applied to other satellite constellations with ISLs. The next step is to extend the algorithm to the rosette satellite constellation through experimental verification. Besides, there are still some problems with dealing with the scalability of the coordinator and how to integrate heterogeneous networks operated by different entities. The next step is to focus on making breakthroughs in these areas.

Acknowledgement: We gratefully acknowledge anonymous reviewers who read drafts and made many helpful suggestions.

Funding Statement: This work is supported by Fundamental Research Funds for the Central Universities of China (328201911) , C. G. (Chao Guo), the Open Project Program of National Engineering Laboratory for Agri-product Quality Traceability, C. G. (Chao Guo), Beijing Technology and Business University (BTBU) No. AQT-2018Y-B4, C. G. (Chao Guo), Higher Education Department of the Ministry of Education Industry-university Cooperative Education Project, C. G. (Chao Guo), and Education and Teaching Reform Project of Beijing Electronic and Technology Institute, C. G. (Chao Guo).

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

References

Adnane, A.; Foitih, Z. A.; Mohammed, M. A. S.; Bellar, A. (2018): Real-time sensor fault detection and isolation for LEO satellite attitude estimation through magnetometer data. *Advances in Space Research*, vol. 61, no. 2, pp. 1143-1157.

Alvizu, R.; Maier, G.; Kukreja, N.; Pattavina, A.; Cavazzoni, C. (2017): Comprehensive survey on T-SDN: software-defined networking for transport networks. *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2232-2283.

Arti, M. K.; Jain, V. (2017): Relay selection based hybrid satellite-terrestrial communication systems. *LET Communications*, vol. 11, no. 17, pp. 2566-2574.

Bai, J.; Lu, X.; Lu, Z.; Wei, P. (2005): Compact explicit multi-path routing for LEO satellite networks. *HPSR. Workshop on High Performance Switching and Routing*, pp. 386-390.

Bin, Y. I.; Gu, D. F.; Xiao, C.; Kai, S. (2018): Integrating BDS and GPS for precise relative orbit determination of LEO formation flying. *Chinese Journal of Aeronautics*, vol. 31, no. 10, pp. 88-97.

Caini, C.; Firrincieli, R. (2012): Application of contact graph routing to LEO satellite DTN communications. *IEEE International Conference on Communications*, pp. 3301-3305.

Cruz-Sanchez, H.; Staples, G. S.; Schott, R.; Song, Y. Q. (2013): Operator calculus approach to minimal paths: precomputed routing in a store and forward satellite constellation. *IEEE Global Communications Conference*, pp. 3431-3436.

Dewangan, N., Sahu, N. (2016): Simulation of current security scenario in satellite data networks using OMNET++. *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3297, no. 287, pp. 20827-20834.

Du, J.; Jiang, C.; Zhang, H.; Wang, X.; Ren, Y. et al. (2018): Secure satellite-terrestrial transmission over incumbent terrestrial networks via cooperative beamforming. *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1367-1382.

Ekici, E.; Akyildiz, I.; Bender, M. (2001): A distributed routing algorithm for datagram traffic in LEO satellite networks. *IEEE/ACM Transactions On Network*, vol. 9, no. 2, pp. 137-147.

Lin, F.; Liu, Q.; Zhou, X.; Xiong, K. (2014): Towards green for relay in InterPlaNetary internet based on differential game model. *Science China Information Sciences*, vol. 57, no. 4, pp. 1-9.

Lin, F.; Zheng, Y.; Zhou, X.; Lü, X. (2015): DMMF: dominant and max-min fair allocation in satellite network. *China Communications*, vol. 12, no. 2, pp. 149-154.

Hui, H.; Zhou, C.; Xu, S.; Lin, F. (2020): A novel secure data transmission scheme in industrial Internet of things. *China Communications*, vol. 17, no. 1, pp. 73-88.

Huang, Q.; Chao, G. (2011): Efficient key cryptography based on body area networks. *IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, pp. 171-174.

Jia, M.; Liu, X.; Gu, X.; Guo, Q. (2017): Joint cooperative spectrum sensing and channel selection optimization for satellite communication systems based on cognitive radio. *International Journal of Satellite Communications & Networking*, vol. 35, no. 2, pp. 139-150.

Juels, A., Sudan, M. (2004): A fuzzy vault scheme. *Proceedings IEEE International Symposium on Information Theory*, pp. 408.

Korçak, Ö., Alagoz, F. (2005): Analysis of priority-based adaptive routing in satellite networks. *2nd International Symposium on Wireless Communication Systems*, pp. 629-633.

Li, T.; Zhou, H.; Luo, H.; Qi, X.; Yue, Y. (2016): Using SDN and NFV to implement satellite communication networks. *International Conference on Networking and Network Applications*, pp. 131-134.

Liu, Y.; Xu, W.; Tang, F.; Kuang, L.; Yang, Y. (2016): An improved multi-path routing algorithm for hybrid LEO-MEO satellite networks. *IEEE Trustcom/BigDataSE/ISPA*, pp. 1101-1105.

Nazari, S.; Du, P.; Gerla, M.; Hoffmann, C.; Capone, A. (2016): Software defined naval network for satellite communications (SDN-SAT). *MILCOM IEEE Military Communications Conference, Baltimore*, pp. 360-366.

Liu, P.; Wang, X.; Chaudhry, S. R.; Javeed, K.; Ma, Y. et al. (2018): Secure video streaming with lightweight cipher present in an sdn testbed. *Computers, Materials & Continua*, vol. 57, no. 3, pp. 353-363.

Roy-Chowdhury, A., Baras, J. S.; Hadjitheodosiou, M.; Papademetriou, S. (2006): Security issues in hybrid networks with a satellite component. *IEEE Wireless Communications*, vol. 12, no. 6, pp. 50-61.

Sato, G., Uchida, N., Shibata, Y. (2014): Performance evaluation of software defined and cognitive wireless network based disaster resilient system. *Ninth International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 406-409.

Su, J.; Lin, F.; Zhou, X.; Lu, X. (2015): Steiner tree based optimal resource caching scheme in fog computing. *China Communications*, vol. 12, no. 8, pp. 161-168.

Tan, H.; Zhu, L. (2014): A novel routing algorithm based on virtual topology snapshot in LEO satellite networks. *IEEE 17th International Conference on Computational Science and Engineering*, pp. 357-361.

Lu, Y.; Zhao, Y.; Sun, F.; Li, H.; Wang, D. (2013): Dynamic fault-tolerant routing based on FSA for LEO satellite networks. *IEEE Transactions on Computers*, vol. 62, no. 10, pp. 1945-1958.

Zhang, Y.; Wang, Y. (2016): SDN based ICN architecture for the future integration network. *16th International Symposium on Communications and Information Technologies*, pp. 474-478.