SADA: SDN Architecture Based Secure Dynamic Access Scheme for Satellite Network

Dong Yan(✉), Ming Gu, Luyuan Wang, and Xiongwen He

Institute of Spacecraft System Engineering CAST, Beijing 100094, People's Republic of China
yandong200@163.com

Abstract. In view of the characteristics of limited resources and insufficient security guarantee capability of satellite network nodes, this paper proposes a secure dynamic access scheme for satellite network based on SDN architecture. By adopting SDN architecture, the operation efficiency of the network system can be effectively improved. The access process is divided into two stages. In the first stage, node reputation is confirmed to ensure the network security. In the second stage, resource aware dynamic access is performed to improve the network QoS guarantee capability. Finally, the performance of the algorithm is verified by simulation experiments, which proves the advantages of the algorithm in data transmission success rate.

Keywords: Satellite Network · SDN Architecture · Node Reputation · Dynamic Access

1 Introduction

Satellite network has the characteristics of wide coverage, no influence of natural conditions on the ground, simple and flexible access. It can be efficiently applied to rescue, weather prediction, resource detection, environment and disaster monitoring. It is considered to be an important part of the next generation Internet by many researchers and also a space infrastructure to be actively developed and constructed.

Satellite networks can be divided into backbone nodes and access nodes according to node different functions. Among them, backbone nodes are usually composed of GEO/MEO satellites in high and medium orbits, and their responsibilities are mainly to process information exchange and transmission, while access nodes are usually composed of LEO satellites in low orbit to realize real-time information transmission and other functions. With the development of satellite network, the types and application types of access nodes are becoming more abundant, and the requirements for network service quality are becoming higher. Currently, the common network access and application mode, which relies on the ground system to plan in advance and reserves access bandwidth and processing resources, is relatively simple, but its fixed and inflexible manner makes it difficult to provide more efficient access methods and better service

R. Li et al. (Eds.): MOBILWARE 2022, LNICST 507, pp. 177–185, 2023.
https://doi.org/10.1007/978-3-031-34497-8_15

quality assurance. Meanwhile, with the continuous increase of access users, it will also greatly increase the complexity of ground planning.

At present, researchers have conducted some research on the access methods of satellite networks and propose a variety of schemes [1–3]. Most of these schemes still give advance connection planning. Although the bandwidth utilization efficiency and processing delay of the link slot are improved to a certain extent, the current state of the backbone node and the security performance of the access node are not considered. When the current load of the newly established backbone node is heavy, the connection state may be unstable, the processing and switching capacity may be reduced, and even the service may not be provided. When the security of the access node is not confirmed, it may lead to malicious behavior in the network, affect the performance of the whole network, and in some serious cases, cause network interruption. In view of these problems, this paper proposes SDN architecture based secure dynamic access scheme for satellite network, called SADA, which can authenticate the security of network access nodes and avoid the impact of network performance due to the overload of management nodes in the network.

The rest of this paper is organized as follow: the second part introduces the related work, the third part introduces the dynamic access mechanism in detail, the fourth part evaluates the performance of the algorithm through simulation experiments, the fifth part is the conclusion.

2 Related Work

Chen et al. [4] studied the routing technology based on the double-layer satellite network structure and proposed satellite grouping and routing protocol (SGRP). By using the relative position relationship between high and low orbit satellites, the low orbit access satellites are divided into several groups, and high orbit satellites corresponds to an access group. They collect and exchange the link delay, and calculate the routing table according to the shortest path principle. When the relative position relationship between the high and low orbit satellites changes, the grouping relationship will also change. At this time, a new group will be generated. The satellite network topology within the time when each packet has not changed can be considered as unchanged. This method is mainly applied to the scenario where the network connection relationship is relatively stable, and does not pay attention to the state of the network node itself and the scenario of dynamic access.

The distributed QoS routing algorithm (DQA) proposed by Xu et al. [5] takes into account the status of satellite nodes and can avoid the overload of nodes to a certain extent. When calculating and planning the routing table, it optimizes the two performance parameters of network delay and link utilization, which can reduce the network congestion probability. However, the algorithm is only designed according to specific limited QoS parameters, which limits the applicability of the algorithm, and does not consider the security of nodes, which may lead to network security risks.

Zhu et al. [6, 7] designed a network control architecture combining master controller and slave controller according to the idea of SDN. In this method, the users on the earth surface are divided into fixed logical areas, and each area corresponds to a corresponding

slave controller, which realizes the sub network division of the satellite communication network. The functions of the two controllers are different. The slave controller is responsible for collecting the network and node status information of the corresponding subnet and uploading it to the master controller. The master controller manages the satellite communication network topology according to the global network state and calculates the routing path between multiple subnets. The satellite only realizes the functions of information transmission, routing and forwarding to minimize the requirements on the on-board processing capacity.

The secure dynamic access mechanism of satellite network based on SDN architecture proposed in this paper uses SDN controller to master the global information of satellite network, which can obtain the real-time status of network nodes. The mechanism in this paper realizes adaptive dynamic access with intelligent selection method of network access with multiple QoS parameters. At the same time, the reputation model of satellite network nodes is designed to evaluate the security of access nodes, so as to avoid nodes with poor security from joining the network and affecting the network performance. Through this method, the newly added access nodes can be prevented from connecting to some high load backbone nodes, and the network security performance can be guaranteed, which can effectively solve the problems in the above research.

3 SDN Architecture Based Secure Dynamic Access Scheme for Satellite Network

3.1 SADA Network Model

SDN is a new network control architecture with decoupling advantage and forwarding function. In recent years, it has received more attention from researchers. By separating control and data and combining programmable control manner, it can realize flexible control and centralized management of the network. For the satellite network, the control plane node is responsible for collecting the node state information, authenticating the identity of the new access node, and completing the calculation, generation and distribution of the key. The data plane node no longer needs to have powerful computing and storage performance to complete complex tasks, but only needs to focus on basic tasks such as data forwarding. This remarkable feature of SDN technology is suitable for satellite network scenarios with severe resource constraints, which can effectively reduce node overhead and ensure more stable and efficient operation of satellite networks.

The control plane needs to complete the functions of node identity authentication, key calculation and distribution, node state collection, routing calculation, etc., and needs powerful basic performance. Therefore, most SDN researches are placing the control plane nodes on the ground. Although the ground node as the control plane can have more powerful basic capabilities, it may lead to insufficient timeliness of key control information due to the inability to realize global ground station construction. It is difficult to adapt to the higher real-time and dynamic requirements of the future satellite network. In this paper, a SDN satellite network model with master-slave controller structure is proposed, which is called SADA model. Taking the double-layer satellite network scenario composed of GEO-LEO as an example, a two-level structure control

plane is designed. The master controller is located on the ground, and its main functions are key generation and distribution, node state storage and analysis, routing calculation and other complex tasks according to specific algorithms. The slave controller node is located at the high orbit satellite node, and more than three GEO nodes can basically achieve full coverage of the low earth orbit satellites operating in the middle and low latitudes. They also maintain relatively stable and continuous communication with the master controller. As the backbone node in the network, it mainly completes new node discovery, node status collection and sending to the master controller. The slave controller nodes obtain the network operation rules from the master controller and sent to the data plane node. Compared with the traditional satellite node, the slave controller node usually has higher basic performance, so it can also ensure higher work efficiency when realizing the controller function. As an access node, the data plane node completes the routine data collection, distribution and transmission tasks after network access request and obtaining the control plane access authentication. The Fig. 1 of SADA model is shown as follows.

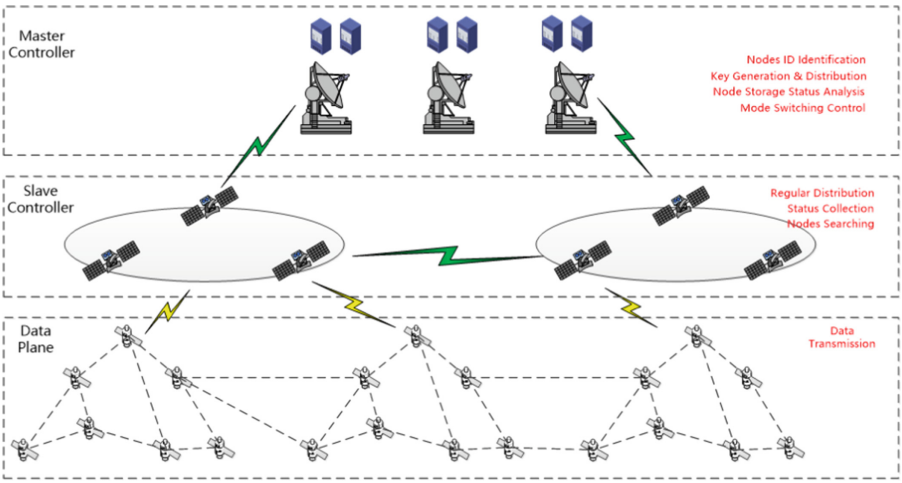

Fig. 1. SADA Model Figure

3.2 Dynamic Access Mechanism of Satellite Network

The current satellite network access methods mainly improve the bandwidth utilization efficiency and processing delay, but less consider the problems of limited resources and service capacity of satellite nodes and the security of access nodes, which makes it difficult to ensure the security of satellite network access and subsequent operation, data transmission efficiency and flexible management of the network.

Based on the dynamic access model of satellite network with two-level SDN control structure designed above, this paper intends to design from the following aspects: firstly, it proposes a node reputation evaluation strategy, analyzes the behavior of the access

node by collecting the network data of the access node, and then dynamically adjusts its network access capability according to the obtained reputation evaluation value to provide support for ensuring network security. Then, a load aware dynamic access mechanism for backbone nodes is proposed to avoid network congestion and high packet loss rate during satellite network access.

A. Reputation Evaluation

Reputation is used to express the credibility of an individual in group interaction. The main objectives of the reputation evaluation method designed in this paper include three main points. It can provide reliable information to determine whether a node is trusted. It can give priority to ensuring access requests of nodes with good reputation. It can limit response or even no response to the access request of the bad node. Reputation [8] is described as: the reputation of an entity refers to the expectation of its future behavior based on the observation of other entities or the information of its historical behavior at a given time and context. This definition emphasizes the contextual relevance of reputation, and explains that reputation occurs in the interaction between different entities, and also explains the continuity of node reputation and the relevance of future behavior. In 2004, S. Ganeriwal and M.B. Srivastava designed a reputation evaluation model BRSN [9] for the application scenario of wireless sensor networks with limited resources. The model uses Bayes formula to fit the reputation distribution and beta distribution, and obtains the conclusion that the reputation of the node follows the beta distribution, which can calculate the expected value of the beta distribution to obtain the trust value of the node. BRSN model performs fitting analysis on reputation distribution and beta distribution, and it is known that beta distribution can conveniently describe reputation distribution.

$$R_{\mathrm{kn}} = B(\alpha_{kn} + 1, \beta_{kn} + 1) \tag{1}$$

R_{kn} represents the reputation distribution of node k with respect to node n, α_{kn}, β_{kn} means the number of normal behaviors and the number of abnormal behaviors obtained by the node K with respect to the node n respectively.

SADA reputation model makes use of BRSN reputation method, and improves the specific application environment of satellite network. The reputation behavior of nodes is divided into data generation behavior, data transmission behavior and data response behavior. Data generation behavior mainly refers to the nodes, which are the source of data, actively initiates network attacks and other malicious behaviors, such as DDoS attacks and black hole attacks. Data transmission behavior attack mainly refers to whether there are malicious behaviors such as data discarding and content tampering in the process of routing exchange and data forwarding. The data response behavior mainly refers to the malicious behavior which causes no respond normally to the protocol requests of the control plane node or other nodes of the data plane, resulting in the interaction failure. When applying the SADA reputation model to calculate the reputation value of a node, it is necessary to combine the specific application scenarios and assign different weights according to the degree of influence of their behavior. The calculation method of the reputation value of node k to node n can be obtained:

$$C_{kn} = \begin{cases} W_s \times C_{kn-s} + W_t \times C_{kn-t} + W_r \times C_{kn-r} - m \times \Delta C & \text{(firstaccess or malicious actions before)} \\ W_s \times C_{kn-s} + W_t \times C_{kn-t} + W_r \times C_{kn-r} + \Delta C & \text{(no malicious actions before)} \end{cases} \tag{2}$$

$$W_s + W_t + W_r = 1 \tag{3}$$

$$C_{kn-s/t/r} = E(R_{kn}) = E(B(\alpha_{kn} + 1, \beta_{kn} + 1)) = \frac{\alpha_{kn} + 1}{\alpha_{kn} + \beta_{kn} + 2} \tag{4}$$

C_{kn} represents the reputation value of node k for node n. W_S, W_t and W_r respectively represent the influence weight of data generation behavior, data transmission behavior and data response behavior in the application scenario, and $C_{kn\text{-}s}$, $C_{kn\text{-}t}$ and $C_{kn\text{-}r}$ respectively represent the reputation value of data generation behavior, data transmission behavior and data response behavior, ΔC represents the control change amount. $C_{kn\text{-}s/t/r}$ represents the special behavior reputation, which is the statistical expectation of the reputation distribution. It can be expressed by $E(R_{kn})$. Any kind of abnormal behavior will cause β_{kn} to add 1, and each normal behavior will cause α_{kn} to add 1.

The calculation of reputation value takes the historical behavior of the node as an important measurement element, and takes the time period of each access to the network as the calculation cycle. When calculating the reputation of this cycle, the reputation of the first two cycles needs to be considered. Therefore, when calculating the reputation value, there are two cases. The first case is that the access node accesses the network for the first time or has a malicious behavior before. When calculating the reputation value of this cycle, the control change amount is reduced to punish. M represents the number of cycles in which the malicious behavior occurred before, and can be taken as 0, 1, 2. In the second case, the access node has not had any malicious behavior before, and the control change amount can be additionally rewarded when calculating the reputation value of the current cycle. Set the minimum reputation threshold C_0 and the normal threshold C_1. When the reputation value of a node is less than C_0, the node is prohibited from joining the network. When the reputation value of a node is greater than C_1, the node is fully allowed to join the network. When the reputation value of a node is between C_0 and C_1, the node's access request is permitted with the ratio of p. p is set according to the application scenario.

B. Resource Aware Dynamic Access Mechanism

The traditional satellite access methods mainly consider coverage and connection time. However, with the continuous demand of space applications for QoS guarantee capability, the traditional methods have been difficult to meet the needs of user applications. Due to the limited resources of the satellite network nodes, when the nodes handle the high load state, large packet loss is likely to occur. This may affect the normal communication of the satellite network and even threatens the network security. In this paper, a node load aware dynamic access mechanism is designed, which focuses on the real-time load state of the satellite while improving the utilization efficiency of satellite resources. During the access process, the dynamic access selection is made by evaluating the current load state of the backbone nodes, so as to avoid the excessive load of the satellite network nodes and ensure the secure and stable operation of the satellite network.

SADA designs a multi metric parameters dynamic access mechanism, and selects the node CPU utilization rate, the signal-to-noise ratio and the connection service time as the access metric parameters for dynamic access processing, which can be replaced with the application scenario. When an access node wants to join the network, the backbone node

makes dynamic access selection according to its current performance and connection status with the access node.

$$R_{kn} = \mathrm{A}\frac{c_{\max} - c}{c_{\max} - c_{\min}} + B\frac{10^{\frac{s}{10}}}{10^{\frac{s_{\max}}{10}}} + \mathrm{C}\frac{t_{remain}}{t_{\max}}. \tag{5}$$

$$\mathrm{A} + \mathrm{B} + \mathrm{C} = 1 \tag{6}$$

R_{kn} represents the probability value of the current access to the satellite network. c represents the current CPU utilization value. C_{max} and c_{min} are two thresholds, which can be called upper threshold and lower threshold. s represents the signal-to-noise ratio of the satellite, and s_{max} represents the maximum value of the signal-to-noise ratio. T_{remain} is the coverage time that the satellite to be accessed can provide, t_{max} is the maximum coverage time that a single satellite can provide. A, B and C are the weights of the three parameters. Set the minimum threshold R_{min} for dynamic access. If R_{kn} is less than R_{min}, it indicates that the current access resources are insufficient and the current access is rejected. Otherwise, dynamic probabilistic network access is performed according to the calculated R_{kn}.

C. Satellite Network Security Dynamic Access Mechanism

The satellite network secure dynamic access process is divided into two stages. In the first stage, the node reputation is confirmed. When the slave controller nodes receive the access request of the data plane node, it is necessary to confirm the reputation of the access node, besides conventional ID identification, key authentication etc. With the method proposed in the paper, the reputation value of the access node is obtained according to its reputation behavior. A threshold value is set for the reputation value of the node accessing the network. The process can start the second stage, only when the minimum value of the network access reputation is met. Otherwise, the control plane rejects the node accessing the network. In the second stage, resource aware dynamic access is performed. The control plane node judges the current access resource status of the backbone node according to the resource aware dynamic access mechanism in this paper, and calculates the access probability to perform network dynamic access. If the current access resource status is insufficient to meet the node's efficient access and subsequent high-quality network services, the access request is rejected.

4 Performance Evaluation

In order to verify the performance of SADA, this section selects one of the most representative QoS algorithms DQA to compare the performance of the end-to-end transmission success rate of satellite nodes. The end-to-end transmission success rate of satellite nodes is one of the most important network performance indicators, which can reflect the rationality of network architecture, access and transmission strategy, and QoS guarantee capability.

The experiment topology in this section is composed of 3 GEO satellites and 66 LEO satellites. The LEO satellites consist of 6 orbital planes, 11 satellites in each orbital plane. On the basis of this topology, 3–5 access nodes are set as malicious nodes, and the

destination nodes are randomly selected. The paths between them can be called malicious paths. Set the packet loss rate of intermediate nodes passed by a single malicious path as 0.7, the packet loss rate of intermediate nodes passed by two malicious paths as 0.6, the packet loss rate of intermediate nodes passed by three or more malicious paths as 0.5, and the packet loss rate of intermediate nodes not passed by malicious paths as 0.9. Compare the data transmission capability that different algorithms can guarantee when facing different numbers of malicious nodes. In order to ensure the authenticity and effectiveness of the test, 100 tests are conducted for each test condition, and the average value is taken to finally obtain the data transmission success rate under this condition.

Figure 2 shows the impact on the DQA data transmission success rate in the face of different numbers of malicious nodes, and Fig. 3 shows the performance comparison of SADA and DQA in the transmission success rate.

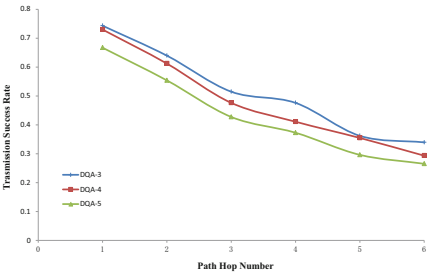

Fig. 2. Data transmission success rate of DQA under different conditions

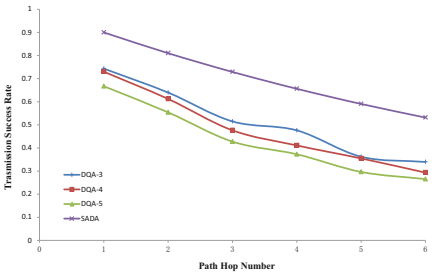

Fig. 3. Transmission success rate of SADA and DQA

It can be seen from the experiment results in Fig. 2 that the transmission success rate will decrease with the increase of the number of malicious nodes. It is not difficult to see from the test results in Fig. 3 that the algorithm performance of SADA is better than that of DQA. The main reason is that SADA's reputation evaluation and resource aware dynamic access mechanism can effectively prevent malicious nodes from joining the network, avoid the overload of network nodes, and improve the network QoS guarantee capability.

5 Conclusion

SADA is a secure dynamic access mechanism of satellite network based on SDN architecture. The method mainly consists of the following parts: 1) SDN architecture is adopted to separate the data plane from the control plane. The control plane is divided into a master controller on the ground and a slave controller on the space part, effectively improving the operation efficiency of the network system. 2) Reputation evaluation comprehensively evaluates the current and historical network reputation behavior of a node, and responds to the network access request of a node, supplies limited response or no response according to the obtained reputation value of the node, so as to ensure the security of the network. 3) The mechanism of resource aware dynamic access selects typical performances that affect network access and operation, and conduct dynamic probabilistic network access, which can avoid overload of network nodes and improve

network QoS guarantee capability. Finally, the simulation results show that SADA has a better performance in data transmission success rate.

References

1. Papapetrou, E., Karapantazis, S., Dimitriadis, G.: Satellite handover techniques for LEO networks. Int. J. Satell. Commun. Netw. **22**(2), 231–245 (2004)
2. Papapetrou, E., Pavlidou, F.: QoS handover management in LEO/MEO satellite systems. Wirel. Pers. Commun. **24**(2), 189–204 (2003)
3. Chowdhury, P.K., Atiquzzaman, M.: Handover schemes in satellite networks: state-of-the-art and future research directions. IEEE Commun. Surv. Tutor. **8**(4), 2–14 (2006)
4. Chen, C., Ekici, E.: A routing protocol for hierachical LEO/MEO satellite IP networks. ACM Wirel. Netw. J. **11**(4), 507–521 (2005)
5. Xu, H., Wu, S.: A distributed QoS routing based on ant algorithm for LEO satellite network. Chinese J. Comput. **30**(3), 361–367 (2007)
6. Fan, Z., Wu, H., Xu, J., et al.: An optimization algorithm for spatial information network self-healing based on software defined network. In: Proceedings of the 12th International Conference on Computer Science and Education (ICCSE), New York, pp. 369–374 (2017)
7. Li, Y., Teng, Q., Kong, Z., et al.: Design of spatial information network routing strategy based on SDN architecture. Spacecr. Eng. **28**(5), 54–61 (2019). (in Chinese)
8. Hu, N., Zou, P., Sun, P.-D.: Reputation-based collaborative management method for inter-domain routing security: reputation-based collaborative management method for inter-domain routing security. J. Softw. **21**(3), 505–515 (2010). https://doi.org/10.3724/SP.J.1001.2010.03479
9. Saurabh. G., Laura, K., Srivastava, B., et al.: Reputation-based framework for high integrity sensor networks. ACM Trans. Sensor Netw. **4**(3), 15 (2008)