An Energy-Efficient Topology Design and DDoS Attacks Mitigation for Green Software-Defined Satellite Network

ZHE TU, HUACHUN ZHOU, KUN LI, MAN LI, AND ALETENG TIAN

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, Beijing 100044, China

Corresponding author: Huachun Zhou (hchzhou@bjtu.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFA0701604, in part by the National Natural Science Foundation of China (NSFC) under Grant 61802014 and Grant U1530118, and in part by the National High Technology of China (863 Program) under Grant 2015AA015702.

ABSTRACT As the continuous in-depth research of sixth generation (6G) technology, the satellite networks in the Space-Air-Ground Integrated Network (SAGIN) have received more and more attention. However, since satellite nodes have the characteristics of limited resources and dynamic link switching, it is important to effectively save energy in satellite networks. In this paper, we focus on how to make Software-Defined Satellite Networks (SDSN) more energy efficient. First, we propose an energy consumption model for satellite networks. Based on this model, we put forward an improved network topology generation algorithm, which can comprehensively consider the link switching energy consumption and the inter-satellite link energy consumption. Then, considering the huge energy consumption caused by abnormal traffic in the satellite network, we propose a DDoS mitigation mechanism in the satellite network, aiming to reduce the extra energy consumption generated by processing abnormal traffic in the satellite node. Finally, through performance evaluation, the proposed network topology generation algorithm and DDoS attack mitigation strategy can effectively reduce network energy consumption.

INDEX TERMS Energy-Efficient, SDSN, topology design algorithm, DDoS mitigation strategy.

I. INTRODUCTION

With the start of the research on the sixth generation (6G) of mobile communication technology in wireless networks, the Space-Air-Ground Integrated Network (SAGIN) [1], which integrates the terrestrial network, aerial network [2], ocean network [3] and satellite network, has received more and more attention as an important research direction in future 6G networks. However, compared with the nodes in terrestrial networks, aerial networks, and ocean networks, the satellite nodes in the satellite networks have limited resources such as link resources, communication resources, storage resources, and computing resources [4]. Therefore, it is urgent to develop a green satellite network. By separating the data plane from the control plane, the Software-Defined Network (SDN) decouples the data forwarding function from the control function. While the SDN architecture greatly increases the flexibility and controllability of the network, it can also comprehensively and effectively utilize the resources of the network [5]. Therefore, Software-Defined Satellite Network (SDSN) that combines SDN with the satellite networks has become a trend [6].

Compared with the traditional satellite network, SDSN greatly improves the utilization efficiency of satellite resources by its global view of the network and its ability to comprehensively control satellite network resources [7], [8]. SDSN can be regarded as a green satellite network to some extent. Nevertheless, SDSN still has some non-negligible energy losses, such as frequent inter-satellite link switching [9] and excessive processing of abnormal traffic. Therefore, reducing energy consumption that can not be ignored in satellites is an effective way to promote SDSN to be more green and energy-saving. To build an energy-efficient software-defined satellite network, this paper focuses on how to reduce the additional energy consumption caused by frequent link switching and abnormal traffic processing.

We first focus on how to reduce energy consumption due to frequent link switching. In the satellite networks,
the dynamic change of the relative position between satellite nodes makes the inter-satellite laser links need to be switched dynamically. Frequent link switching will make satellite nodes consume more energy, which brings great challenges to the satellite nodes that lack power resources. Therefore, reducing the number of inter-satellite link switching is an effective way to reduce satellite energy consumption. However, there is a contradiction between the link switching energy consumption and link energy consumption. On the one hand, reducing the number of inter-satellite link switching means extending the duration of the inter-satellite links, which will increase the energy consumption of the inter-satellite links. On the other hand, the shorter duration of the inter-satellite link will inevitably lead to frequent switching of the satellite network links, resulting in large energy consumption of link switching. Therefore, it is important to find a new topology generation algorithm for SDSN that can fully consider the above two types of energy consumption.

Then, we concentrate on how to mitigate the abnormal traffic in the satellite networks. By reducing the abnormal traffic, the energy consumption caused by processing the extra abnormal traffic can be greatly reduced. DDoS attacks are one of the major security threats that the current networks (especially satellite networks with limited resources) need to deal with [10], [11]. In SDSN, the abnormal traffic generated by DDoS attacks, while occupying satellite node processing resources, also has a great impact on the storage and forwarding of normal traffic. This not only reduces the overall utilization of the satellite network but also increases the energy consumption of the network. Hence, it is necessary to find an intelligent mitigation strategy to suppress the abnormal traffic generated by DDoS attacks while ensuring the forwarding of normal traffic, to improve the overall satellite network security and resource utilization.

Thus, in this paper, we present a new satellite network topology generation algorithm and an intelligent elimination strategy for DDoS attacks in satellite networks, aiming to improve network utilization, reduce network energy consumption, and achieve the purpose of green communications. In our previous work, we proposed a satellite network topology generation algorithm (DCTG algorithm) based on the link weights [12]. Based on the DCTG (Degree Constrained Topology Generation) algorithm, we have improved the satellite network topology generation algorithm so that it can consider comprehensively the switching energy consumption and energy consumption of the inter-satellite link. Besides, based on the Deep Reinforcement Learning (DRL) algorithms, we propose an intelligent mitigation strategy that can alleviate abnormal traffic caused by DDoS attacks in the SDSN. Using this intelligent mitigation strategy in the SDSN can not only prevent the normal traffic from being affected by the abnormal traffic, but also reduce the energy consumption of satellite nodes while improving the security of the satellite networks.

The contributions of this paper are summarized as follows:

- We designed a satellite network topology generation algorithm that can consider not only the characteristics of satellite links, but also the energy consumption caused by inter-satellite links and the link switching.
- We proposed an intelligent mitigation strategy based on the Deep Reinforcement Learning, which can effectively mitigate the abnormal traffic caused by DDoS attacks in SDSN. By training and verification, it proves that the proposed mitigation strategy can greatly reduce the energy consumption of satellite nodes.

The rest of the paper is organized as follows. In Section II, We first review the related works about SDSN and the network topology generation methods. Then, we review various methods and strategies for mitigating DDoS attacks in the network. In Section III, we present the framework of green SDSN. Then, in section IV, we present the improved topology generation algorithm based on the DCTG algorithm. In Section V, we put forward the intelligent mitigation strategy for DDoS attacks. Then we analyze the simulation results in Section VI. Finally, In Section VII, we sum up the paper and present our future work.

II. RELATED WORKS

In this section, we review the related work from three aspects: SDSN, topology generation algorithm, and the methods to mitigate DDoS attacks.

A. SOFTWARE-DEFINED SATELLITE NETWORK

Recently, many researchers have focused on SDSN. However, most researchers focus on network architecture design, for example [13], [14] and [15]. Based on SDN and Network Function Virtualization (NFV), Li et al. [13] proposed a software-defined framework SERvICE for Integrated space-terrestrial satellite Communication, which can achieve flexible satellite network traffic engineering and fine-grained QoS guarantee. Feng et al. [14] proposed a flexible architecture HetNet for heterogeneous satellite-terrestrial networks, which greatly enable network flexibility. Based on the software orchestration mechanism, Zhang et al. [15] proposed an end-to-end hybrid satellite-terrestrial network under two main scenarios of sparse and ultra-dense networks for different types of users with various QoS requirements. However, the above research focuses more on architectural design, and there is no in-depth research on energy consumption and security in SDSN.

B. TOPOLOGY GENERATION ALGORITHM

Different from the terrestrial network topology with the static network topology, the satellite network topology has the characteristics of dynamic time-varying. Therefore, how to generate topology in the satellite network has become an important issue for many researchers.

There are many algorithms for generating satellite network topology. In particular, Zhang et al. [16] put forward a shortest path algorithm for mobile satellite
communication networks. Using the improved shortest path algorithm, the satellite network topology can be generated while the satellite nodes are visible to each other. Chang et al. [17] investigated the topological design for the Low-Earth Orbit (LEO) satellite network. By modeling the LEO satellite network as a Finite State Automaton (FSA) based on the regularity of orbit movement, the near-optimal topology can be obtained through a simulated annealing algorithm. To generate the most cost-effective satellite network topology, Lillian et al. [18] proposed a unified mathematical framework using a two-stage stochastic programming formulation which has the advantage of incorporating uncertain traffic demand into the network design. For the Time-Division Inter-Satellite Link Topology Generation (TDILTG) problem, Chu et al. [19] put forward a mathematical model to formulate the TDILTG problem. Besides, [19] also proposed a very effective deterministic constructive algorithm to solve this problem.

Unfortunately, none of the above topology generation algorithms take into account the energy consumption of link switching and inter-satellite links. Therefore, to obtain a green SDSN topology, it is important to find a topology generation algorithm that comprehensively considers energy consumption.

C. METHODS TO MITIGATE DDoS ATTACKS

DDoS attacks make normal users unable to use the network by exhausting the server resources or filling up network bandwidth resources, which brings huge challenges to network security [20]. From another perspective, the network or server attacked by DDoS needs to spend more resources to provide services to normal users. Therefore, finding a method that can mitigate DDoS attacks can not only improve the security of the network, but also save the energy consumption of the network. The existing DDoS mitigation methods can be roughly divided into two parts.

The first part is to focus on the framework or mechanism design of the network. By designing a new architecture or mechanism, the network can be mitigated against DDoS attacks. Using NFV-based domain networks, Bahman et al. [21] proposed a collaborative DDoS defense mechanism named CoFence, which allows domain networks to help each other in handling a large volume of DDoS attacks through resource sharing. Yan et al. [22] proposed a multi-level DDoS mitigation framework (MLDMF) to defend against DDoS attacks for IIoT, which includes the edge computing level, fog computing level, and cloud computing level. Besides, Christos et al. [23] proposed a novel framework for the analytical modeling and optimal mitigation of distributed link-flooding attacks.

The second part is to mitigate DDoS attacks by using traditional methods [24], [25] or machine learning methods [26], [27]. In particular, with the rise of machine learning, more and more scholars are focusing their research on using machine learning methods to mitigate DDoS attacks. Shideh et al. [26] used a machine learning method, Vector Machines (SVM) to detect DDoS attacks. Obaid et al. [27] evaluated a few machine learning techniques to detect and block the DDoS attack in an SDN network, such as J48, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (K-NN). The results showed that J48 performs better than the other evaluated algorithms.

Most of the above-mentioned mitigation strategies for DDoS attacks are based on the terrestrial network, which can not be directly used in time-varying satellite networks. Although the security of satellite networks is higher than that of terrestrial networks, once the satellite network is attacked by DDoS, the damage caused will be extremely large. On the other hand, dealing with abnormal traffic caused by DDoS attacks makes satellite nodes need to spend a lot of meaningless energy consumption. Therefore, it is urgent to find a new mitigation strategy for DDoS attacks which can be used in satellite networks.

III. THE FRAMEWORK OF GREEN SDSN

In the previous research work of our team, a lot of researches on Software-defined Satellite Networks have been carried out ([13], [14], etc.). Besides, a software-defined space-ground integrated network prototype system based on the OpenStack platform was built. Therefore, in this section, based on previous research work [28], we propose a green software-defined satellite network framework from the perspective of energy saving, aiming to reduce the energy consumption of software-defined satellite networks. In addition, we also put forward two specific and effective implementation methods for how to implement a green software-defined satellite network.

As shown in Figure 1, the framework of green software-defined satellite network can be divided into four layers: forwarding layer, control layer, management layer, and intelligent layer. Following the idea of the hierarchical division of satellite nodes in [13], the satellite nodes in the satellite network are composed of GEO (Geosynchronous Earth Orbit), MEO (Medium Earth Orbit), and LEO satellites. Therefore, according to the function of satellite nodes in the satellite network, we can divide different satellite nodes into four different layers in the green SDSN framework. The satellite entities in the forwarding layer are composed of MEO and LEO satellites, while the entities in the control layer, management layer, and intelligent layer can be composed of different or the same GEO satellites.

Besides, We deploy many modules with different functions to the satellite entities at each layer of the green SDSN framework. As the core module in the forwarding layer, the information collection module (ICM) is responsible for collecting information such as the link status, node load, and energy consumption of satellite nodes. In the management layer, the topology awareness module (TAM) perceives the satellite network topology at that moment from the information collected by the ICM, and the information processing module (IPM) aggregates all the collected satellite network states into a high-dimensional tensor, which is used for the modules in the intelligent layer to formulate corresponding
energy-saving strategies. There are two main modules in the intelligent layer. The model prediction module (MPM) selects the green energy-saving strategy neural network model suitable for the moment and scenario based on the real-time satellite network topology information uploaded by the TAM. The DDoS mitigation model (DMM) is a specific manifestation of the neural network model selected by the model MPM, it formulates specific green and energy-saving DDoS mitigation strategies based on the network status information uploaded by the management layer. Besides, the SDSN controller at the control layer is responsible for receiving the green strategies by the intelligent layer, converting it into instructions that can be executed by the software-defined satellite switch, and sending it to each satellite node in the forwarding layer.

As shown in the right part of Figure 1, we have given an example to show in detail the common operation mechanism between MPM and DMM. After the MPM receives the topology information uploaded from the management layer, it selects the corresponding neural network model DDPG (Deep Deterministic Policy Gradient) for the satellite network topology at that moment. The DDPG algorithm in the DMM model can formulate specific energy-saving strategies based on the collected network status information, and then deliver them to the SDSN controller through the northbound interface. The detailed description of the DDPG algorithm will be explained in Section V-C.

Based on the proposed framework of green software-defined satellite network, we design two green energy-saving methods for software-defined satellite network. Firstly, we put forward a green satellite network topology generation algorithm, which can generate the satellite network topology with the minimum energy consumption by calculating the link switching energy consumption, data transmission energy consumption, and the inherent energy consumption of satellite nodes within a period time of the satellite network. Then, We design a DDoS attack mitigation mechanism for SDSN. This mechanism can use the trained DDoS mitigation agents to detect and block DDoS attacks in satellite networks in a timely manner, and can significantly reduce the extra energy consumption caused by forwarding abnormal traffic.

### IV. IMPROVED TOPOLOGY GENERATION ALGORITHM

In this section, we focus on the improved topology generation algorithm in SDSN. For the sake of clear description, we make the definition of the parameters in Table 1.

| Parameters | Definition |
|------------|------------|
| $D_s$      | The duration of the time slice-based network. |
| $D_b$      | The duration of the time block-based network. |
| $W_s$      | The link weight matrix of the time slice-based network. |
| $W_b$      | The link weight matrix of the time block-based network. |
| $X_s$      | The potential connection matrix in time slice-based network. |
| $X_b$      | The potential connection matrix in time block-based network. |
| $L_b$      | The link connection matrix in time block-based network. |
| $w_{ni, n_j}$ | A binary variable indicates whether the link $(n_i, n_j)$ exists in time block-based network. |
| $Q$        | The total energy consumption in a period of SDSN. |
| $Q_s$      | The total energy consumption in time slice-based network. |
| $Q_b$      | The total energy consumption in time block-based network. |
| $Q_1$      | The energy consumption for switching from the previous topology to the current topology. |
| $Q_2$      | The energy consumption of the link in time block-based network. |
| $Q_3$      | The inherent energy consumption of satellite nodes. |

### A. NETWORK MODEL WITH ENERGY CONSUMPTION

In our previous work [12], we modeled the satellite network at a certain time slice based on the link weights. On the basis of the link weights, we put forward a satellite network topology generation algorithm (DCTG algorithm) under the degree constraints. However, the proposed algorithm can not reflect the energy consumption of the satellite network. Therefore, we put forward the improved algorithm based on the DCTG algorithm, so that it can comprehensively consider the energy consumption caused by the handover and the inter-satellite link in SDSN.

Since the SDSN has the characteristics of predictable and periodic, we can model a period of SDSN as an undirected graph $G = \{V, E, D, W, Q\}$ based on the theory of Graph.
V and E represent the set of satellite nodes and potential inter-satellite links in the SDSN, respectively. D represents the duration of a period of the satellite network. W is a matrix representing the link weight of the satellite network, and Q represents the total energy consumption in a period of SDSN. Also, due to the high-speed movement between satellites, the inter-satellite links will handover frequently. So we can divide the satellite network into multiple time slices. In each time slice, the topology of the satellite network is static, and the network can be modeled as \( G_s = \{ V_s, E_s, D_s, W_s, Q_s \} \). In a period of SDSN, the satellite network can be expressed as being composed of \( m \) time slice-based networks, as shown in (1). \( G_s^j = \{ V_s^j, E_s^j, D_s^j, W_s^j, Q_s^j \} \). \( G_s^j \) represents the \( j \)-th time slice-based network.

However, the method of dividing the satellite network into time slice-based network based on the handover of the inter-satellite is obviously inappropriate. On the one hand, this method will cause a large number of invalid time slices with an extremely short duration. On the other hand, this method will cause huge energy consumption of link switching.

Therefore, we use another method to model SDSN. We divide the satellite network in a period into multiple time block-based network, and the network can be characterized by the model \( G_b = \{ V_b, E_b, D_b, W_b, Q_b \} \) at each time block. As shown in (1), SDSN can be represented as a network composed of \( m \) time block-based networks. \( G_b^j \) represents the \( j \)-th time block-based network. \( G_b^j = \{ V_b^j, E_b^j, D_b^j, W_b^j, Q_b^j \} \). The time block-based network is composed of one or more time slice-based networks, as shown in (2). \( G_b^j \) and \( G_b^j \) represent the \( j \)-th time slice-based network and the \( j \)-th time block-based network, respectively.

The relationship between the network \( G \) in a period, the time block-based network \( G_b \), and the time slice-based network \( G_s \) can be characterized as follows.

\[
G = \{ G_s^1, \ldots, G_s^j, \ldots, G_s^m \} = \{ G_b^1, \ldots, G_b^j, \ldots, G_b^m \} 
\]

\[
G_b^j = \{ G_b^{j,1}, G_b^{j,1+1}, \ldots, G_b^{j,m} \} \quad (1) 
\]

\[
1 \leq i \leq n, \quad 1 \leq j \leq m 
\]

\[
1 \leq k_j-1 + 1 \leq k_j \leq n 
\]

\[
k_0 = 0, \quad k_m = n \quad (2) 
\]

Equation (1) ensures that the SDSN model can be fully characterized by the time slice-based network model set and the time block-based network model set. Equation (2) indicates that the time block-based network is composed of one or more time slice-based networks. Equation (3) - (5) are the constraints of (2).

\[
D_b^j = D_b^{j,1+1} + D_b^{j,1+2} + \ldots + D_b^{j,1+2} \quad (3) 
\]

Besides, the relationship between the duration of the time block-based network \( D_b^j \) and the time slice-based network \( D_s^j \) can be characterized as (6). The duration of the time block-based network is the sum of the duration of the time slice-based networks it contains. The constraints of (6) are the same as those of (2).

### B. PROBLEM FORMULATION

In the following, we formulate the energy consumption problem of a period of SDSN as an ILP optimization problem.

In order to better measure the energy consumption of SDSN, the parameter \( X \) that characterizes the potential connection matrix should be introduced. The potential connection matrix \( X \) is a \( N \times N \) matrix with a diagonal of 0, which is composed of \( x_{n_1,n_2} \). \( N \) represents the number of the satellite nodes in the satellite network. \( n_1 \) and \( n_2 \) are integer pairs from 1 and \( N \), and \( n_1 \) is not equal to \( n_2 \). If two satellites are visible, \( x_{n_1,n_2} = x_{n_2,n_1} = 1 \), otherwise, \( x_{n_1,n_2} = x_{n_2,n_1} = 0 \).

\( X_s \) and \( X_b \) represent potential connection matrix in time slice-based and time block-based networks, respectively. The relationship between \( X_s \) and \( X_b \) can be expressed by (7), and \( X^j_s \) and \( X^j_b \) represent the \( j \)-th potential connection matrix in time slice-based network and the \( j \)-th potential connection matrix in time block-based network respectively. The constraint of (7) is (3) - (5).

\[
X^j_s = \{ X^j_s^{k_j-1+1}, X^j_s^{k_j-1+2}, \ldots, X^j_s \} 
\]

\[
= X^j_s^{k_j-1+1} \cap X^j_s^{k_j-1+2} \cap \ldots \cap X^j_s \quad (7) 
\]

In each time block, based on the DCTG algorithm proposed in the previous work [12], we can generate the network topology of this time block according to the link weight \( W_b \). We assume the inter-satellite link topology generated by DCTG algorithm can communicate in both directions. The link connection of the topology generated by DCTG algorithm can be represented by \( N \times N \) matrix \( L_b \), which is composed of \( l_{n_1,n_2} \). If the inter-satellite link exists, \( l_{n_1,n_2} = l_{n_2,n_1} = 1 \), otherwise, \( l_{n_1,n_2} = l_{n_2,n_1} = 0 \).

It can be inferred in [30] that the power equation of the inter-satellite laser link can be presented as (8).

\[
P_t = \frac{8P_r}{\pi \frac{d}{R_t R_r} \lambda^2} \quad (8) 
\]

\( P_r \) and \( P_t \) represent the received power and transmit power of the inter-satellite laser links, respectively. \( R_t \) and \( R_t \) represent the transmitting antenna diameter of the receiver and the transmitter. \( \lambda \) represents the wavelength of the transmitted laser. \( d \) represents the distance between two satellites.

In the inter-satellite laser link, the minimum power that the signal can be received by the satellite receiver is defined as \( P_{t_{min}} \). Therefore, the minimum transmission power \( P_{t_{min}} \) required by the normal communication of the inter-satellite link can be calculated by (8). We use \( P_t \) and \( P_t \) to represent the working power of the satellite receiver and receiver respectively. Besides, to simplify the calculation, we take the minimum transmitting power \( P_{t_{min}} \) as the working power \( P_t \) of the satellite transmitter.

For the inter-satellite link \( l_{n_1,n_2} \), the power of the transmitter on satellite \( n_1 \) can be expressed as \( P_{t_{n_1}} \), and the power of the
receiver on satellite \( n_2 \) can be expressed as \( \tilde{P}_{b}^{2} \). The power of the receiver in the network can be expressed as a \( N \times N \) matrix \( P_{R} \) composed of \( \tilde{P}_{R} \), and the transmitter power in the network can be expressed as a \( N \times N \) matrix \( P_{T} \) composed of \( \tilde{P}_{T} \). Therefore, in SDSN, the total energy consumption \( P \) generated by the transmitter and receiver can be expressed as the sum of the transmitter power \( P_{T} \) and the receiver power \( P_{R} \). In \( j \)-th time block, \( P_{b}^{j} \) represents the average received and transmitted power \( P \) of the network. Similarly, \( P_{R}^{j} \) and \( P_{T}^{j} \) represent the average power of transmitter and receiver in time block \( j \). The \( P_{b}^{j} \) can be represented as (9).

\[
P_{b}^{j} = P_{R}^{j} + P_{T}^{j} \quad (9)
\]

The energy consumption \( Q_{b}^{j} \) of the satellite network in time block \( j \) can be divided into \( Q_{b}^{j1} \), \( Q_{b}^{j2} \) and \( Q_{b}^{j3} \). Therefore, we can represent the total energy consumption \( Q_{b}^{j} \) of the satellite network in time block \( j \) as follows.

\[
Q_{b}^{j} = Q_{b}^{j1} + Q_{b}^{j2} + Q_{b}^{j3} \quad (10)
\]

\( Q_{b}^{j1} \) represents the energy consumption for switching from the previous topology to the current topology, and \( Q_{b}^{j2} \) indicates the energy consumption of the current link topology. \( Q_{b}^{j3} \) indicates the inherent energy consumption of satellite nodes, which is independent of the topology. \( Q_{b}^{j1} \), \( Q_{b}^{j2} \) and \( Q_{b}^{j3} \) can be represented by (11) - (13), respectively.

\[
Q_{b}^{j1} = Q_{h} \times \sum_{i \leq n_1 < n_2 \leq N} (L_{b}^{j-1} \oplus L_{b}^{j})_{N \times N} \quad (11)
\]

\[
Q_{b}^{j2} = D_{b}^{j} \times \sum_{i \leq n_1 < n_2 \leq N} (P_{b}^{j-1} \odot L_{b}^{j})_{N \times N} \quad (12)
\]

\[
Q_{b}^{j3} = D_{b}^{j} \times \sum_{n_1 = 1}^{N} \tilde{Q}_{n_1} \quad (13)
\]

\( D_{b}^{j} \) indicates the duration of the time block-based network in \( j \)-th time block, and \( Q_{h} \) and \( \tilde{Q}_{n_1} \) respectively represent the energy consumption of the inter-satellite link handover once and the inherent energy consumption of the satellite per second. \( L_{b}^{j} \) represents the generated topology link connection matrix \( L_{b} \) in time block \( j \).

\( (L_{b}^{j-1} \oplus L_{b}^{j})_{N \times N} \) represents the link matrix for switching from the previous time block to the current time block, and \( (P_{b}^{j-1} \odot L_{b}^{j})_{N \times N} \) represents the power matrix of the satellite networks, \( \oplus \) is the logical operation of XOR, and \( \odot \) is the Hadamard product.

The objective of the optimization model is to minimize the energy consumption of the period of SDSN while satisfying other constraints. The formulations are shown in the following:

Objective:

\[
\min \sum_{j=1}^{m} Q_{b}^{j} \quad (14)
\]

The constraint of (14) is (3) - (5).

---

Algorithm 1 DCTG Algorithm

**Input:** The link weight matrix \( M \), the degree constraint matrix \( \{d_{n_1}, d_{n_2}, \ldots, d_{n_j}, \ldots\} \).

**Output:** The topology matrix \( L \) of degree constrained SDSN.

1: initial set \( V_{i} \) and \( V_{f} \), Initial matrix \( L \), initial \( i \) = 0
2: \textbf{while} \( i \leq \text{len}(M) \) \textbf{do}
3: \quad choose \( M[i] \) which represent link \( x_{n_1n_2} \)
4: \quad initial \( d_{n_1}, d_{n_2} = \emptyset \)
5: \quad if both \( d_{n_1}, d_{n_2} \neq \emptyset \) then
6: \quad\quad if \( n_{1} \) or \( n_{2} \) not in set \( V_{i} \) then
7: \quad\quad\quad \( \tilde{d}_{n_1} = d_{n_1} - 1, \tilde{d}_{n_2} = d_{n_2} - 1 \)
8: \quad\quad\quad put \( n_{1} \) or \( n_{2} \) in set \( V_{i} \)
9: \quad\quad end if
10: \quad\quad if no closed loop in set \( V_{i} \) then
11: \quad\quad\quad update \( V_{F} \) use \( V_{F} \), update \( d_{n_1}, d_{n_2} \) use \( \tilde{d}_{n_1}, \tilde{d}_{n_2} \)
12: \quad\quad\quad put \( x_{n_1n_2} \) in matrix \( L \)
13: \quad\quad end if
14: \quad\quad if All the \( d_{l} \) in the closed loop \( == 0 \) then
15: \quad\quad\quad update set \( V_{i} \) use \( V_{f} \)
16: \quad\quad\quad else
17: \quad\quad\quad\quad update \( V_{f} \) use \( V_{f} \), update \( d_{n_1}, d_{n_2} \) use \( \tilde{d}_{n_1}, \tilde{d}_{n_2} \)
18: \quad\quad\quad\quad put \( x_{n_1n_2} \) in matrix \( L \)
19: \quad\quad\quad end if
20: \quad\quad end if
21: \quad\quad else
22: \quad\quad continue
23: \quad\quad end if
24: \quad\quad \( i++ \)
25: \quad end while

---

C. ALGORITHM

Based on the optimization target represented in the above subsection, we put forward the improved topology generation algorithm as follows. The core of the algorithm is to generate an energy-efficient SDSN topology. The proposed algorithm can not only comprehensively consider the link states, but also can minimize the total energy consumption of the network in a period.

We first review the DCTG (Degree Constrained Topology Generation) algorithm proposed in our previous work. We defined the degree of the satellite as the number of laser link connections for satellite nodes. The core of the algorithm is to generate a topology that maximizes the link weight of the overall network according to the link weight without violating the degree constraint. The pseudocode of the DCTG algorithm is shown in Algorithm 1.

\( M \) is a link weight matrix composed of link weight \( w_{n_1n_2} \) from large to small, the set \( V_{i} \) and \( V_{f} \) respectively represent the temporary vertex set and the final vertex set of the generated topology. \( d_{n_1}, d_{n_2} \) respectively represent the degree of satellite node \( n_1 \), and \( \tilde{d}_{n_1}, \tilde{d}_{n_2} \) are temporary variables that characterize the degree constraints of satellite \( n_1 \) and \( n_2 \). In order to avoid independent closed loops in the final topology, we use \( d_{l} \) to
Algorithm 2: The Improved Topology Generation Algorithm

**Input:** $G = \{G_1^1, \ldots, G_s^2, \ldots, G_s^n\}$.

**Output:** The topology in each time block $G_b^t$, which can minimize the total energy consumption of the SDSN in a period.

1: initial
2: while $G' \neq G$ do
3: initial $Q'$, $L'$
4: generate $\hat{G}$, $\hat{G} = \{G_1^1, \ldots, G_b^t, \ldots, G_b^n\}$
5: if $\hat{G}$ in $G'$ then
6: break
7: else
8: put $\hat{G}$ in $G'$
9: for $G_b^t$ in $\hat{G}$ do
10: Based on DCTG algorithm, the topology $L_b^t$ can be generated by $X_b^t$ and $W_b^t$
11: put $L_b^t$ in $L'$
12: calculate $P_b^t$, $D_b^t$, $Q_b^2$, $Q_b^3$
13: if $j = 1$ then
14: $Q_b^{1i} = 0$
15: else
16: calculate $Q_b^{1i}$
17: end if
18: calculate $Q_b^j$
19: $Q' + = Q_b^j$
20: end for
21: end if
22: put $\{Q', L'\}$ in set $Z$
23: end while
24: The subset $L$ matching the minimum $Q$ is the optimal topology generated.

Mitigating DDoS attacks can save energy in the satellite networks. Then, we propose a mechanism to Mitigate DDoS attacks. Besides, we present the Deep Reinforcement Learning (DRL) algorithm used in the DDoS mitigation strategy. Finally, we discuss how to deploy the DDoS mitigation strategy in SDSN.

### A. ENERGY SAVING BY MITIGATING DDoS ATTACKS

In Section IV, we propose an Improved topology generation algorithm. The satellite network topology generated by this algorithm can effectively reduce the additional energy consumption caused by frequent link switching. In addition, there is another aspect of energy saving that is worth discussing, that is, energy saving by mitigating DDoS attacks in the satellite networks.

It can be inferred in the [31] that the equation of the energy per bit $E_b$ in the satellite networks can be presented as (15).

$$E_b = S \times [B \log_2 (1 + \frac{S}{n_0 B})]^{-1} \quad (15)$$

$S$ is the average power of the transmitted signal (in watts), $B$ is the bandwidth of the inter-satellite link (in hertz), and $n_0$ is a constant characterizing the unilateral power spectral density of Gaussian white noise, respectively.

Therefore, if the total number of bits of normal traffic $b_n$ and DDoS attack traffic $b_a$ transmitted in the satellite network can be known respectively, the energy consumption $E_t$ generated by data transmission in the satellite network can be expressed as (16). $E_b^n$, $E_b^a$ represents the energy expended by the satellite node to transmit one bit of normal traffic and one bit of DDoS attack traffic, respectively.

$$E_t = b_n E_b^n + b_a E_b^a \quad (16)$$

It can be seen from the above equation (16) that mitigating the DDoS attack traffic in the satellite network can effectively reduce the energy consumption of the satellite nodes. Consequently, in the following sub-sections, we focus on how to effectively mitigate the DDoS attacks in the satellite network.

### B. THE MECHANISM TO MITIGATE DDoS ATTACKS

In recent years, machine learning is playing an increasingly important role in the current network. The combination of machine learning technology and satellite networks has received more and more attention.

In Section III, we propose a framework of the Green SDSN network. To mitigate DDoS attacks in a timely and effective manner, we deploy the DMM model to detect and block DDoS attacks in the intelligent layer. Based on the framework of green SDSN as shown in Figure 1, we propose the mechanism to mitigate DDoS attacks in the satellite networks, as shown in Figure 2. Specifically, the mitigation mechanism can be divided into three stages: the monitoring stage, attack confirmation stage and attack mitigation stage.
FIGURE 2. The mechanism to mitigate DDoS attacks in the green SDSN.

1) MONITORING STAGE
In the monitoring stage, the ICM module in the forwarding layer sends the status of the satellite network (satellite load, link load, node resource utilization, energy consumption, etc.) to the IPM module which is deployed in the management layer. The IPM module judges whether the satellite network (node) is under attack based on the collected information. If the module detects that the satellite network may be attacked, the mitigation mechanism enters the second stage, the attack confirmation stage. Otherwise, if the module detects that the network is secure, it will continue to be in the monitoring stage.

2) ATTACK CONFIRMATION STAGE
The IPM module in the management layer locates the attacked satellite in the SDSN according to the network state information collected by the ICM module. However, due to the dynamic characteristics of the satellite networks, even if the satellite node that may be attacked is found, the attack mitigation strategy cannot be implemented immediately. It is necessary to know the topology of the network at this moment. Therefore, the TAM module is deployed in the management layer. Using the collected information uploaded by the forwarding layer, the TAM module can obtain the entire topology of the SDSN at this time block.

Subsequently, the IPM module summarizes all the collected information about this potentially attacked node under this topology and aggregates it into a high-dimensional state information tensor. It should be noted that the high-dimensional state information tensor should include all the traffic information of other satellite nodes to the potential attacked satellite.

3) ATTACK MITIGATION STAGE
The attack mitigation stage can be divided into two steps. The first is to generate a DDoS mitigation strategy, and the second is to implement the mitigation strategy.

In the first step, the MPM module deployed in the intelligent layer selects the neural network model suitable for this exact time block-based network based on the network topology information uploaded by the management layer. Then, the DMM model generates the DDoS mitigation strategy for the boundary satellite nodes according to the high-dimensional state information tensor and the selected neural network model.

In the second step, using the interface between the intelligent layer and the control layer, the mitigation strategy can be successfully delivered to the control layer. The controller which is the main entity in the control layer generates the executable action on the basis of the mitigation strategy, and delivers the executable action to each satellite node in the forwarding layer through the southbound interface of the SDN. Subsequently, the nodes in the forwarding layer can alleviate the abnormal traffic caused by DDoS attacks in the network based on the delivered executable action.

At this point, the attack mitigation stage is over, and the mechanism to mitigate DDoS attacks will enter the monitoring stage again to continuously monitor the abnormalities in the satellite network.

C. THE DRL ALGORITHM IN MITIGATION STRATEGY
Deep reinforcement learning (DRL) is a Machine Learning (ML) algorithm that combines deep learning and reinforcement learning. It integrates the perception ability of deep learning and the decision-making ability of reinforcement learning. Deep reinforcement learning has become more and more popular because it can solve sequential decision problems.

DDPG algorithm [32] is a kind of deep reinforcement learning algorithm. The framework of the DDPG algorithm has been shown in the right part of Figure 1. Compared with the well-known DRL algorithms such as Deep Q-Learning and SARSA (State-Action-Reward-state-Action) algorithm, the DDPG algorithm can make decisions on continuous action space, so it is very suitable for making corresponding decisions for mitigating DDoS attacks in SDSN.

DDPG algorithm is a combination of Actor-Critic architecture and Deep Q-Network (DQN) algorithm. More precisely, DDPG is an actor-critic, deterministic policy gradient, off-policy algorithm. Based on the actor-critic architecture, the neural network in DDPG can be divided into two parts: actor-network and critic-network. The actor-network is used to adjust the policy parameters, and the critic-network evaluates the policy function of the actor-network evaluation on the basis of the time difference error. What’s more, because of the idea of the DQN algorithm, both the actor-network and the critic-network can be divided into the online network and the target network. The critic-network consists of target network...
\(Q(s, \mu(s|\theta^\mu))|\theta^Q\) and online network \(Q(s, a|\theta^Q)\). Similarly, the actor-network consists of target network \(\mu'(s|\theta^\mu')\) and online network \(\mu(s|\theta^\mu)\). \(s\) and \(a\) represent the states and actions, respectively. \(Q^\pi\) represents the weight of network \(\xi\), and \(\xi\) can be \(\theta^\mu\), \(\theta^Q\), \(\theta^G\) or \(\theta^\mu\). In addition, the DDPG algorithm also uses experience replay. It can collect the state transition samples in the environment through the exploration strategy, and store the samples in the replay buffer. At each subsequent update, the Small batches are sampled uniformly from the replay buffer. This method can effectively improve the utilization of data and break the association between data.

1. **States**\((s)\): States represents a state information tensor with high-dimensional characteristics, which is uploaded by the IPM module in the management layer. The states of the network at time \(t\) can be expressed as \(s_t\).

2. **Action**\((a)\): Actions represents the strategy made by the DMM model deployed in the intelligent layer at time \(t\). Specifically, the mitigation strategy indicates the mitigation degree of the traffic from the boundary satellites to the attacked satellite. The mitigation strategy is a matrix of numbers between 0 and 1, where 0 means that the traffic is completely discarded, and 1 means that the traffic is allowed to pass completely. After the controller deployed in the control layer receives the mitigation strategy generated by the DMM model, the controller generates an executable action and sends it to the satellite nodes. By executing the action, the states of the network changes to \(s_{t+1}\).

3. **Reward**\((r)\): Rewards represents the value obtained after executing the action when the network is in state \(s_t\). In this section, Rewards is used to evaluate the effectiveness of DDoS mitigation strategies. Specifically, reward indicates the proportion of normal traffic in the attacking node or the entire satellite network after the DDoS mitigation strategy eliminates abnormal traffic. Then, we can express Rewards as the following equation.

\[
\text{reward} = \begin{cases} 
-1, & l_t > u_{\text{max}} \\
1, & l_t \leq u_{\text{max}}, \lambda_a < \eta \varepsilon_a \\
\lambda_a - \varepsilon_a, & \text{else}
\end{cases}
\]

\(l_t\) represents the load of the satellite or entire satellite network at time \(t\), and the \(u_{\text{max}}\) indicates the maximum satellite load or entire satellite network load that the satellite or satellite network can normally provide services. \(u_{\text{max}}\) can be a value artificially defined based on experience. \(\varepsilon_a\) represents the percentage of normal traffic contained in the SDSN network or the percentage of normal traffic reaching the attacked satellite node before the mitigation strategy is executed. Similarly, \(\lambda_a\) represents the proportion of the normal traffic in the network or the proportion of the normal traffic reaching the attacked satellite node after implementing the mitigation strategy. In addition, in order to make the trained model make the mitigation strategy that has the least impact on the normal traffic, we set parameter \(\eta\) in the model training stage to correct the model. \(\eta\) is a constant from 0 to 1 that can be set by the network administrator. When \(\lambda_a\) is less than \(\eta \varepsilon_a\), we think that the training direction of the model for this round is wrong, and the reward value is \(-1\).

The DDoS mitigation agent uses the above reward formula as the optimization target to mitigate DDoS attacks. If the current network load or node load \(l_t\) is greater than the maximum load boundary \(u_{\text{max}}\) that can be tolerated, then the reward value is \(-1\). It means that the DDoS mitigation agent should try to avoid the situation where the network or satellite cannot provide normal services. If the current load \(l_t\) is less than the maximum load boundary \(u_{\text{max}}\), and the \(\lambda_a\) will be less than \(\eta \varepsilon_a\), the value of reward is still \(-1\). It means that the strategy made by the DDoS mitigation agent should have as little impact on the normal traffic as possible, to avoid the situation where the proportion of the normal traffic \(\lambda_a\) after the strategy is made is much smaller than the proportion of the normal traffic \(\varepsilon_a\) before the strategy is made. Excluding the above two situations, what remains is the goal of continuous optimization needed by the DDoS mitigation agent. This is to allow the agent to mitigate DDoS attacks as much as possible while executing the mitigation strategy, thereby continuously increasing the proportion of the normal traffic in the network.

In the DDPG algorithm, the structure of the neural network, the learning rate of the neural network, and the update rate between the actor and the critic-network have a great impact on the performance of the DDPG algorithm, which indirectly affects the performance of the DDoS mitigation model. So, in Section VI-B, we evaluate the above three performance parameters to build a better performance DDoS mitigation model.

### D. DETAILS OF DEPLOYING MITIGATION STRATEGIES

Since the satellite networks are different from the traditional terrestrial networks, deploying mitigation strategies in the SDSN still requires some additional considerations. In this subsection, we will describe some details of deploying the DDoS attack mitigation strategies in SDSN.

First of all, by taking advantage of the global view of the controller in the SDSN, the DMM model and the controller of the SDSN can be deployed on the same satellite node. This method can not only save the extra overhead caused by the inter-satellite module communication, but also enable the DMM model to make fast decisions based on the network status. Furthermore, considering that the satellite network has the characteristics of time-varying, the satellite deploying the controller and related modules should be selected as far as possible to establish long-term inter-satellite links with other satellites in the SDSN. This deployment method enables the controller and related modules to obtain the status of the satellite network at all times and can make decisions based on the network status to improve the security of the SDSN.

From another perspective, although the satellite network has a higher level of security than the terrestrial network, the satellite network still has the potential to be attacked. Moreover, once the satellite network is attacked, the damage caused by it will be particularly huge. Considering that most of the existing terrestrial networks communicate with
the satellite networks through terrestrial gateways, and the satellite networks do not have a complete security mechanism similar to the terrestrial networks. If the terrestrial gateways are controlled by the attackers, the security of the satellite networks will be greatly reduced. Therefore, the proposed DDoS mitigation strategy works on the edge satellite nodes of the satellite network and improves the security of the satellite network by mitigating the abnormal traffic entering the satellite network on the boundary satellite nodes.

In addition, most of the current DDoS mitigation strategies in the terrestrial networks are based on packet-level traffic. Since the satellite networks have many characteristics that are different from the traditional terrestrial networks, the use of packet-level DDoS mitigation strategies in the satellite networks will cause many problems. On the one hand, the amount of the data collected based on the packet-level traffic is particularly huge, which is not only detrimental to the transmission of the network states information between modules, but also satellite nodes’ rapid decision-making based on network states information. On the other hand, because the processing resources in the satellite networks are very scarce, processing huge amounts of packet-level traffic is a huge overhead for satellite nodes. Therefore, it is important to find a new method to collect the network states information at the boundary satellites in the SDSN. Compared with the packet-level traffic collection method, the flow-level traffic collection method can greatly reduce the amount of data to be collected while retaining the characteristics of the network traffic. It is a good way to mitigate the flow-level traffic in the DDoS mitigation strategy.

We present an example of deploying mitigation strategies in SDSN, which is shown in Figure 3. First, In the monitoring stage, the IPM module on the controller monitors the states of the entire satellite network by collecting flow-based network status information uploaded from each satellite node. Then, in the attack confirmation stage, the IPM and TAM modules locate the satellite node under attack based on the collected information. In the third stage, the controller formulates specific attack mitigation strategies based on the current network status and distributes them to the satellite border gateway.

VI. EVALUATION
In this section, the performance of the improved topology generation algorithm and the mitigation strategy for DDoS attacks are discussed. First, we evaluate the proposed improved topology generation algorithm and generate an experimental topology based on the algorithm. Then, we verify the performance of the DDoS mitigation strategy based on the topology which is generated by the improved topology generation algorithm.

A. THE PERFORMANCE OF THE IMPROVED TOPOLOGY GENERATION ALGORITHM

1) EVALUATION DESIGN
In order to evaluate the algorithm more realistic and meaningful, several assumptions need to be explained in advance.

- The design of the satellite network topology generation algorithm is carried from the perspective of the network administrator. It is assumed that the network administrator already knows the motion rules of the satellites and the visibility between the satellite nodes at the beginning of the topology design.
- It is assumed that the energy consumption of various parts of the satellite node, such as switching energy consumption, inter-satellite link energy consumption, and inherent energy consumption of the satellite, are known at the beginning of topology design.
- It is assumed that all satellites have the same performance and parameters, including the structure and the inherent energy consumption, except for the different distances from the orbit to the ground.

The satellite constellation in [32] was chosen to design the SDSN network to make this evaluation more representative and universal. Overall, this satellite network is composed of LEO, MEO, and GEO satellites. To be specific, the satellite network includes 66 LEO satellites, 10 MEO satellites, and 3 GEO satellites. Three GEO satellites are deployed in the same satellite orbit, while MEO satellites are deployed in two different orbits, with 5 MEO satellites deployed in each orbit. Besides, LEO satellites are deployed in 6 orbits, with 11 LEO satellites deployed in each orbit. The specific satellite network constellation parameters can be seen in Table 2.

We present an example of deploying mitigation strategies in SDSN, which is shown in Figure 3. First, In the monitoring stage, the IPM module on the controller monitors the states of the entire satellite network by collecting flow-based network status information uploaded from each satellite node. Then, in the attack confirmation stage, the IPM and TAM modules locate the satellite node under attack based on the collected information. In the third stage, the controller formulates specific attack mitigation strategies based on the current network status and distributes them to the satellite border gateway.

VI. EVALUATION
In this section, the performance of the improved topology generation algorithm and the mitigation strategy for DDoS attacks are discussed. First, we evaluate the proposed improved topology generation algorithm and generate an experimental topology based on the algorithm. Then, we verify the performance of the DDoS mitigation strategy based on the topology which is generated by the improved topology generation algorithm.

A. THE PERFORMANCE OF THE IMPROVED TOPOLOGY GENERATION ALGORITHM

1) EVALUATION DESIGN
In order to evaluate the algorithm more realistic and meaningful, several assumptions need to be explained in advance.

- The design of the satellite network topology generation algorithm is carried from the perspective of the network administrator. It is assumed that the network administrator already knows the motion rules of the satellites and the visibility between the satellite nodes at the beginning of the topology design.
- It is assumed that the energy consumption of various parts of the satellite node, such as switching energy consumption, inter-satellite link energy consumption, and inherent energy consumption of the satellite, are known at the beginning of topology design.
- It is assumed that all satellites have the same performance and parameters, including the structure and the inherent energy consumption, except for the different distances from the orbit to the ground.

The satellite constellation in [32] was chosen to design the SDSN network to make this evaluation more representative and universal. Overall, this satellite network is composed of LEO, MEO, and GEO satellites. To be specific, the satellite network includes 66 LEO satellites, 10 MEO satellites, and 3 GEO satellites. Three GEO satellites are deployed in the same satellite orbit, while MEO satellites are deployed in two different orbits, with 5 MEO satellites deployed in each orbit. Besides, LEO satellites are deployed in 6 orbits, with 11 LEO satellites deployed in each orbit. The specific satellite network constellation parameters can be seen in Table 2.

We present an example of deploying mitigation strategies in SDSN, which is shown in Figure 3. First, In the monitoring stage, the IPM module on the controller monitors the states of the entire satellite network by collecting flow-based network status information uploaded from each satellite node. Then, in the attack confirmation stage, the IPM and TAM modules locate the satellite node under attack based on the collected information. In the third stage, the controller formulates specific attack mitigation strategies based on the current network status and distributes them to the satellite border gateway.

VI. EVALUATION
In this section, the performance of the improved topology generation algorithm and the mitigation strategy for DDoS attacks are discussed. First, we evaluate the proposed improved topology generation algorithm and generate an experimental topology based on the algorithm. Then, we verify the performance of the DDoS mitigation strategy based on the topology which is generated by the improved topology generation algorithm.

A. THE PERFORMANCE OF THE IMPROVED TOPOLOGY GENERATION ALGORITHM

1) EVALUATION DESIGN
In order to evaluate the algorithm more realistic and meaningful, several assumptions need to be explained in advance.

- The design of the satellite network topology generation algorithm is carried from the perspective of the network administrator. It is assumed that the network administrator already knows the motion rules of the satellites and the visibility between the satellite nodes at the beginning of the topology design.
- It is assumed that the energy consumption of various parts of the satellite node, such as switching energy consumption, inter-satellite link energy consumption, and inherent energy consumption of the satellite, are known at the beginning of topology design.
- It is assumed that all satellites have the same performance and parameters, including the structure and the inherent energy consumption, except for the different distances from the orbit to the ground.

The satellite constellation in [32] was chosen to design the SDSN network to make this evaluation more representative and universal. Overall, this satellite network is composed of LEO, MEO, and GEO satellites. To be specific, the satellite network includes 66 LEO satellites, 10 MEO satellites, and 3 GEO satellites. Three GEO satellites are deployed in the same satellite orbit, while MEO satellites are deployed in two different orbits, with 5 MEO satellites deployed in each orbit. Besides, LEO satellites are deployed in 6 orbits, with 11 LEO satellites deployed in each orbit. The specific satellite network constellation parameters can be seen in Table 2.

We present an example of deploying mitigation strategies in SDSN, which is shown in Figure 3. First, In the monitoring stage, the IPM module on the controller monitors the states of the entire satellite network by collecting flow-based network status information uploaded from each satellite node. Then, in the attack confirmation stage, the IPM and TAM modules locate the satellite node under attack based on the collected information. In the third stage, the controller formulates specific attack mitigation strategies based on the current

| Orbit   | Orbit height | Orbit inclination | Number of satellites |
|---------|--------------|-------------------|----------------------|
| GEO     | 36000 KM     | 0                 | 9*3                  |
| MEO     | 10390 KM     | 45                | 2*5                  |
| LEO     | 780 KM       | 90                | 6*11                 |

TABLE 2. The parameters of space network.
such as visibility, relative distance, and the relative position between satellites, and then carried out subsequent performance evaluation experiments based on these basic data.

In order to reduce the computational complexity, we only select a satellite in each satellite orbit that can fully characterize the motion characteristics of the orbit as the satellite node in the topology generation algorithm. In the end, we chose a small satellite network consisting of 1 GEO satellite, 2 MEO satellites, and 6 LEO satellites to evaluate the performance of the topology generation algorithm. In addition, we screened the data generated by the STK tool during the 24-hour simulation satellite network, and randomly selected the data of about one hour (3878 seconds) for the satellite network topology design.

In this performance evaluation, the constraint degree of satellites $d_{nj}$ is set as 3. The wavelength of the transmitted laser $\lambda$ is set to $1.55 \times 10^{-6} m$, and the transmission antenna diameter of the transmitter $R_t$ and the receiver $R_r$ are both set to 0.5m. Considering that both the transmitter and the receiver will cause signal loss, the loss of the antenna $\eta$ is set to 0.8. The energy consumption of power $Q_h$ is set to 5 J. The power of the receiver $P_r$ in each satellite node is set to 5 W. For ease of calculation, the value of $\pi$ is set to 3.14. In addition, in the satellite simulation with a time of 3878 seconds, as all the 9 satellite nodes were in continuous operation, no single satellite was dormant without link connection. Therefore, the inherent energy consumption $Q_h$ of the satellite nodes was not taken into account when calculating the energy consumption of the overall satellite network.

The minimum receiving the power of transmitter $P_{min}^r$ is the key parameter in the topology generation algorithm of the satellite network. Therefore, in the next section, we will evaluate the performance of the satellite network topologies generated under different topology generation strategies with different minimum receiving power.

2) EVALUATION OF IMPROVED TOPOLOGY GENERATION ALGORITHM

In this section, the improved topology generation algorithm is evaluated by comparing the topology generation algorithm based on the proposed minimum energy consumption strategy with the topology generation algorithm based on several other strategies. We designed several scenarios with the different minimum signal received power $P_{min}^r$ to evaluate the topology generation algorithm. In each scenario, we use the topology generation algorithm to design the topology of the satellite network with the minimum signal receiving power $P_{min}^r$ of the satellite nodes of $1mW, 15mW,$ and $50mW$ respectively. Using the formula (8) - (14) and the improved topology generation Algorithm 2 proposed in Section IV-C, the total energy consumption of the SDSN network can be calculated, and the satellite network topology with the lowest energy consumption can be generated. The energy consumption of the entire SDSN network from 0 to 3878 seconds calculated by the topology generation algorithm under different strategies can be shown in Figure 5 and Table 3.

Four strategies, Min_Sw, Max_Sw, Max_Power, and Avg_Power applied to the topology generation algorithm are selected to compare with the minimum energy consumption strategy Min_Power proposed in this paper. Min_Sw and Max_Sw respectively represent the total energy consumption of the satellite topology generated by the two strategies of the least switching times and the most switching times. Max_Power and Min_Power represent the total energy consumption of the satellite network when choosing the highest total energy consumption strategy and the lowest total energy consumption strategy to generate the satellite topology, respectively. Avg_Power represents the average total energy consumption of the topologies generated based on different energy consumption strategies.

It can be seen from Figure 5 that the topology generation algorithm based on the lowest energy consumption proposed

| Power (J) | $P_{min}^r$ | 1mW  | 15mW  | 50mW  |
|-----------|------------|------|-------|-------|
| Min_Sw    | 185056.311 | 194944.668 | 219665.361 |
| Max_Sw    | 231417.533 | 239362.999 | 259226.662 |
| Min_Power | 185056.311 | 194895.475 | 219361.585 |
| Max_Power | 232772.251 | 245421.840 | 304261.132 |
| Avg_Power | 220712.237 | 229280.825 | 230702.294 |
in this paper is significantly better than other topology generation algorithms in terms of the total energy consumption of the satellite network. And it can be seen clearly that the total energy consumption of the satellite network topology generated by the improved topology generation algorithm is lower than that of the satellite network topology generated by the strategy of minimum switching times Min_Sw and maximum switching times Max_Sw. When the lowest signal receiving power is 1 mW, 15 mW and 50 mW, the total energy consumption of the satellite network topology generated by the improved topology generation algorithm is 20.67%, 20.59%, and 27.9% lower than the total energy consumption of the topology generated by the highest energy consumption strategy. In addition, the total energy consumption of the satellite network generated based on the algorithm proposed in this paper can be reduced by 16.15%, 15%, and 12.5% compared to the average total energy consumption Avg_Power of all possible satellite topologies generated under the three minimum received power scenarios.

From the above evaluation results, it can be concluded that the improved topology generation algorithm proposed in this paper can consider both the switching energy consumption and the link energy consumption. Using the topology generation algorithm proposed in this paper, the green and energy-efficient satellite network can be effectively constructed.

B. THE PERFORMANCE OF THE DDoS MITIGATION STRATEGY

In the previous section, by evaluating the improved topology generation algorithm, it can be verified that the obtained satellite network topology can effectively reduce the energy consumption of the satellite network. Therefore, based on the energy-saving satellite network topology generated in the performance of the improved topology generation algorithm, we evaluate the energy-saving performance of the DDoS mitigation strategy in this section, aiming to reduce the extra energy consumption of the satellite network due to processing abnormal DDoS attack traffic. The performance of the DDoS mitigation strategy can be evaluated in two parts: evaluation design and evaluation result analysis.

1) EVALUATION DESIGN

The satellite network topology generated by the topology generation algorithm based on the minimum energy consumption strategy is shown in Figure 6 for the evaluation of the DDoS mitigation strategy. Figure 6(a) shows the change of the connection between the GEO satellite, LEO satellites, and the MEO satellites in the satellite network within 0-3787 seconds. Figure 6(b) shows the experimental topology of evaluating the DDoS mitigation strategy model in the first time block.

Since the GEO satellites have a wide coverage area and can establish long-term inter-satellite links with LEO and MEO satellites. The controller in the SDSN network can be deployed on the GEO satellites. LEO and MEO satellites, as transponders in SDSN networks, perform store-and-forward functions. In addition, GEO satellites only have the control function in the SDSN network and do not participate in the forwarding of traffic, so in Figure 6(b), only MEO satellites and LEO satellites that perform store-and-forward functions are shown.

In Figure 6, we number the satellite nodes in the DDoS mitigation strategy evaluation scenario. Number 1 to 11 are the terrestrial nodes connected to the SDSN network. Number 12 and 13 are the MEO satellite nodes, and number 14-19 are 6 LEO satellite nodes that serve as access gateways to the satellite network. The node number 11 serves as a server node and provides services for other ground nodes. The ground nodes numbered 1-10 connect to the satellite network through the LEO satellites, and send traffic to the server node numbered 11 through the satellite network. In this scenario, the satellite network only carries the traffic for communication between ground nodes 1-10 and the server node 11.
In this evaluation scenario, the DDoS mitigation strategy model is deployed on the LEO satellite nodes on the border of the satellite network and the server node 11. In the server node 11, the DDoS mitigation strategy model collects the traffic from the ground nodes 1-10 and identifies the collected traffic. If it is confirmed that the server node is under DDoS attacks from the ground node, the DDoS mitigation mechanism in the server node enters the next stage, the DDoS attack mitigation stage. Specifically, on the access gateways of the satellite network, mitigate the DDoS attacks, and reduce the entry of DDoS flows into the satellite network. In this way, subsequent attacks on the server node caused by DDoS attack flows and extra energy consumption caused by DDoS attack flows on the gateways of the satellite network can be avoided.

2) DDoS MITIGATION MODEL
Since the shortage of resources on the satellite nodes, collecting packet-level data will result in excessive data volume, making it impossible to quickly analyze and distinguish DDoS attack traffic. In the server node 11, we aggregate the traffic sent from the ground node to the server node and analyze the flow-level traffic. The aggregation of flow features can make the amount of collected data smaller, and it is also conducive to quickly respond to DDoS attacks.

With reference to the features of DDoS traffic in the CICDDoS2019 dataset, we selected 13 traffic features that characterize DDoS attacks for the training of the DDoS mitigation model, as shown in Table 4.

We used the OMNeT++ simulation tool and the TensorFlow framework to train the DDoS mitigation model. During the model training, the proportion of ground nodes sending normal flow and ground nodes sending abnormal flow was set as 3:2, that is, 6 ground nodes send normal flow and 4 ground nodes send abnormal flow. The ground nodes that generate abnormal traffic are randomly selected, and the ground nodes are randomly selected to generate abnormal traffic during an episode of DDoS mitigation model training.

We select the DDPG algorithm as the core algorithm in the DDoS mitigation model and obtain the rewards and the new status of the satellite network through the interface with the OMNeT++ simulation tool. At the beginning of DDoS mitigation model training, the state of the network is random select, so in order to make the model learn all the states of the network as much as possible, we set the number of model training to 100000 times.

The input state of the DDoS mitigation model is the flow collected from the ground nodes at the server node, and the action of the model is the suppression degree of the different flows at the LEO satellite node at the boundary gateway of the SDSN network. If the model judges that the flow if normal traffic, then the normal traffic will not be suppressed or as little as possible at the boundary gateway. If the DDoS mitigation model judges that the flow is abnormal DDoS attacks, the DDoS attacks are suppressed in the boundary gateway of the satellite network. The reward obtained during DDoS mitigation model training is the change in the proportion of normal traffic reaching the server node before and after the DDoS mitigation strategy is deployed.

3) EVALUATION RESULT ANALYSIS
In this section, we evaluate the performance of the DDoS mitigation model.

First, we analyze the training stage of the DDoS mitigation model. After the DDoS mitigation model is trained for 100,000 times, we take the average reward value of 1000 training times and the average proportion of normal traffic to draw the training results. The proportion of normal traffic is the ratio of the proportion of normal traffic arriving at the service node after the deployment of the mitigation strategy to the total number of arrived traffic, while the reward value can be calculated by formula (17) given in Section V-C. The training results of the DDoS mitigation model can be shown in Figure 7(a) and (b). Figure 7(a) and (b) respectively represent the changes in the reward value during the DDoS mitigation model training stage and the proportion of normal traffic after the DDoS mitigation strategy is deployed.

It can be seen from Figure 7(a) that the reward value increases with the increase in the number of training steps. Similarly, in Figure 7(b), the proportion of normal traffic also increases as the number of training steps increases. It can be seen that the DDoS mitigation model can gradually improve the performance of the model with the increase of training times. At the beginning of the training, since the DDoS mitigation model did not learn enough about the characteristics
TABLE 4. The traffic features of the collected DDoS attacks.

| Number | Feature                          | Signification                                      |
|--------|---------------------------------|----------------------------------------------------|
| 1      | SrcNode                         | The source address of the flow                     |
| 2      | DstNode                         | The destination address of the flow                |
| 3      | SrcPort                         | The source port number of the flow                 |
| 4      | DstPort                         | The destination port number of the flow            |
| 5      | TTL                             | The packet lifetime of the flow                    |
| 6      | FlowRatio                       | The rate of flow                                   |
| 7      | FlowInterval                    | The interval of flow                               |
| 8      | FlowProtocol                    | The protocol number of the flow                    |
| 9      | AvePacketLength                 | The average packet length of the flow              |
| 10     | AvePacketHeaderLength           | The average packet header length of the flow       |
| 11     | AvePacketSize                   | The average packet size (bit) of flow              |
| 12     | AveBitRatio                     | The average bit rate of the flow                   |
| 13     | FlowPacketRatio                 | The packet rate of the flow (number of packets forwarded per unit time) |

of attack traffic and normal traffic, it was not able to quickly distinguish attack traffic from normal traffic and cannot implement the right mitigation strategies for attack traffic. However, with the continuous learning of traffic characteristics, the DDoS mitigation model can distinguish between normal traffic and abnormal traffic and can adopt suppression strategies for abnormal traffic to improve the proportion of normal traffic. When the number of training times reaches a certain level, the DDoS mitigation model will eventually converge. The reward value representing the change in the proportion of normal traffic after deploying the DDoS mitigation strategy finally converges to 0.664, and the proportion of normal traffic arriving at server node 11 after deployment of DDoS mitigation strategy converges to 0.9972.

Then, we calculate and analyze the change in energy consumption in the training stage of the DDoS mitigation model. First of all, we set the parameter values in the energy calculation formula (15). The $S$ representing the average energy of the transmitted signal is set as 5W, the intersatellite link bandwidth is set as 1 GHz, and the unilateral power spectral density of Gaussian white noise is set as $1 \times 10^{-10} W/Hz$. The energy cost of forwarding a unit bit of data $E_b$ can be calculated as $8.8 \times 10^{-10} J/bit$. Therefore, by using the number of packet bits collected at server node 11 and the Formula (16), we can calculate the energy consumption of normal and abnormal traffic. Figure 8 shows the energy consumption changes of several kinds of traffic before and after the DDoS mitigation model generation the mitigation strategy. IN_Total_Traffic, IN_Abnormal_traffic, and IN_Normal_traffic respectively represent the initial total traffic energy consumption, abnormal traffic energy consumption, and normal traffic energy consumption in the satellite node. OUT_Total_Traffic, OUT_Abnormal_traffic, and OUT_Normal_traffic represent the total traffic energy consumption, abnormal traffic energy consumption, and normal traffic energy consumption on the satellite node after the deployment of DDoS mitigation strategy.

As can be seen from Figure 8, the performance of the DDoS mitigation model gets better and better as the number of training steps increases. From the perspective of the energy consumption of data packets forwarded by satellite nodes, the DDoS mitigation model will not affect the forwarding of normal traffic too much. As the number of training steps increases, the models’ identification of abnormal traffic will become better. Therefore, it can be seen from Figure 8 that the energy consumption of forwarding abnormal traffic gradually decreases as the number of training steps increases, and eventually tends to near zero.

In addition, we also analyze and compare the influence of the parameters in the DDPG algorithm of the model on the DDoS mitigation model performance. We train DDoS mitigation models with different neural network structures and parameters and get the DDoS mitigation model after 100,000 training. Then, we use the same validation dataset consisting of 10,000 validated input traffic to evaluate DDoS
mitigation models with different neural network parameters. We take the average energy consumption of the 10,000 traffic forwarded by satellite nodes after the DDoS mitigation strategy is deployed as the evaluation index. Figure 9, Figure 10, and Figure 11 respectively represent the performance of the DDoS mitigation model under different parameters. initial_input represents the initial traffic in the validation dataset.

Figure 9 shows the impact of different neural network structures in the DDPG algorithm on the performance of DDoS mitigation strategies. The energy consumption of initial traffic without DDoS mitigation strategy was compared with that of DDoS mitigation model with LSTM (Long Short-Term Memory) [35], DENSE [36], GRU (Gated Recurrent Unit) [37] and BRNN (Bi-directional Recurrent Neural Network) [38] neural network structures. The parameters of the above neural networks are only shown in the difference of the structure of the neural network, and the number of neurons, the number of layers of the neural network and the activation function are all the same.

It can be seen that the mitigation model composed of a Dense structure has the worst performance. This model does not alleviate abnormal traffic but suppresses normal traffic in the network. The neural network of the LSTM structure slightly suppresses the traffic, but the effect is not good, and it cannot suppress the DDoS traffic well. The model consists of GRU and BRNN structure can suppress abnormal traffic well without affecting normal traffic in the network. The neural network structure of BRNN has the best mitigation effect on abnormal traffic, reducing the energy consumption of the satellite node’s forwarding by 72.77%, and the energy consumption of processing abnormal traffic is reduced by 98.3%.

Next, we compare the performance of the DDoS mitigation model at different learning rates and different update rates of the neural network, as shown in Figures 10 and 11. LR1, LR2, LR3, and LR4 represent learning rates of 0.0001, 0.001, 0.01, and 0.1. Tau1, Tau2, Tau3 and Tau4 represent neural network update rates of 0.0001, 0.001, 0.01 and 0.1. From Figure 10, it can be seen that after selecting a suitable neural network structure of the DDPG algorithm, the learning rate has a relatively small impact on the DDoS mitigation model. When the learning rate in the neural network is set to 0.001, the comprehensive performance of the DDoS mitigation model is the best. It can reduce the energy consumption generated by the satellite node forwarding abnormal traffic by 98.93% while only affecting 17.72% of the normal traffic forwarding.

Similarly, it can be seen from Figure 11 that the performance of the DDoS mitigation model is the best when the neural network update rate is 0.001. It can effectively suppress 99.59% of abnormal traffic and reduce the energy consumption of satellite nodes. It should be noted that when the update rate increases to 0.01 or 0.1, the performance of the model goes back to a significant decline. This is because although increasing the update rate parameter of the neural network can improve the speed of model training, the negative effect is that the stability of the model will be reduced, which may make the model converge to the local optimal value without sufficient perception of traffic features.

VII. CONCLUSION AND FUTURE WORK

In this paper, we propose an energy consumption model for satellite networks. Based on this model, we propose an improved network topology generation algorithm. This algorithm can comprehensively consider the link switching energy consumption and the inter-satellite link energy consumption. Then, in order to reduce the extra energy consumption due to network attacks, we propose a DDoS attack mitigation mechanism. Subsequently, based on deep reinforcement learning (DRL), we put forward the DDoS mitigation strategy for the constantly changing satellite networks. Finally, through performance evaluation, the proposed network topology generation algorithm and DDoS attack mitigation strategy can effectively reduce network energy consumption.

For future work, we plan to use more artificial intelligent technologies to explore more methods to build an energy-efficient and secure Satellite-Terrestrial Integrated Network.
KUN LI received the B.S. degree in telecommunications engineering from Beijing Jiaotong University (BJTU), China, in 2018, where he is currently pursuing the Ph.D. degree in information and communication engineering. He joined the National Engineering Laboratory for Next Generation Internet Interconnection Devices, BJTU. His main research interests include the architecture of next-generation internet, network service management, network security, satellite networks, and mobile internet.

MAN LI was born in Puyang, Henan, China, in 1997. She received the B.S. degree in communication engineering from Henan University, Kaifeng, China, in 2018. She is currently pursuing the Ph.D. degree with the School of Electronic Information Engineering, Beijing Jiaotong University, Beijing, China, with a focus on the cyber security, next generation internet, and flow detection.

ALETENG TIAN received the B.S. degree in telecommunications engineering from Beijing Jiaotong University, Beijing, China, in 2018, where he is currently pursuing the Ph.D. degree in information and communication engineering with the National Engineering Laboratory for Next Generation Internet Interconnection Devices. His current research interests include the areas of software-defined networking, network function virtualization, mobile edge caching, and satellite networks.