sensors

MDPI

Communication

Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack

Yan Zhang [1], Yong Wang [1,2], Yihua Hu [1,2,*], Zhi Lin [1,2], Yadi Zhai [1], Lei Wang [1,2], Qingsong Zhao [1,2], Kang Wen [1] and Linshuang Kang [1]

[1] College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China
[2] Anhui Province Key Laboratory of Electronic Restriction, Hefei 230037, China
* Correspondence: skl_hyh@163.com

Abstract: Low Earth orbit satellite constellation networks (LSCNs) have attracted significant attention around the world due to their great advantages of low latency and wide coverage, but they also bring new challenges to network security. Distributed denial of service (DDoS) attacks are considered one of the most threatening attack methods in the field of Internet security. In this paper, a space-time graph model is built to identify the key nodes in LSCNs, and a DDoS attack is adopted as the main means to attack the key nodes. The scenarios of two-satellite-key-node and multi-satellite-key-node attacks are considered, and their security performance against DDoS attacks is also analyzed. The simulation results show that the transmission path of key satellite nodes will change rapidly after being attacked, and the average end-to-end delay and packet loss are linearly related to the number of key-node attacks. This work provides a comprehensive analysis of the security performance of LSCNs under a DDoS attack and theoretical support for future research on anti-DDoS attack strategies for LSCNs.

Keywords: LSCNs; DDoS; space-time graph model; security performance; anti-DDoS

check for updates

Citation: Zhang, Y.; Wang, Y.; Hu, Y.; Lin, Z.; Zhai, Y.; Wang, L.; Zhao, Q.; Wen, K.; Kang, L. Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack. *Sensors* **2022**, *22*, 7286. https://doi.org/10.3390/s22197286

Academic Editors: Zhiyong Feng, Weiwei Jiang and Yafeng Zhan

Received: 11 August 2022
Accepted: 22 September 2022
Published: 26 September 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Low Earth orbit (LEO) satellite constellation networks have attracted people's attention due to their benefits of low latency and extensive coverage [1–9]. Countries around the world have proposed LEO constellation plans, showing their ambition to join the "space race" of satellite networks. A number of studies about satellite communication systems have begun both domestically and internationally as a result of the significant advancement in LEO satellite communication technology. LEO satellite constellations such as OneWeb, Kupier, and Starlink are the most prevalent [10–12]. The most developed low Earth orbit satellite constellation network (LSCN) system at the moment is SpaceX's Starlink satellite network.

Compared to terrestrial networks, LSCNs have periodicity and regularity. However, although these characteristics bring convenience to the research of LSCNs, they also make LSCNs extremely vulnerable to several types of threats and attacks [13]. For instance, an adversary can take advantage of the LSCN's global coverage to turn its advantages into vulnerabilities and manipulate ground users to form botnets to launch DDoS attacks from multiple locations. This kind of attack threat has been regularly exploited in terrestrial networks and has caused significant damage, and it is quite likely to be used to attack LSCNs in the future.

Due to frequent link switching, the network topology also changes accordingly. How to obtain the information of key network nodes has become one of the important research directions of many scholars in satellite network security. Wei et al. [14] conducted an evaluation based near the center of the rapid assessment of the importance of satellite network nodes. The study indicated that the results of this method of assessment are more reasonable. To improve the survivability of LSCNs, Wang et al. [15] utilized time-cumulative

graph techniques (C-TVG) to compute the betweenness centrality of each node in the graph in the modeling network but only considered betweenness centrality. Considering the differences in inter-layer connectivity relationships, Xu et al. [16] proposed the dynamic supra-adjacency matrix (DSAM) temporal network model to measure the importance of satellite nodes. Finally, experimental simulations of the Iridium and Orbcomm constellations demonstrated that the DSAM method has a relatively accurate recognition rate and high stability.

At present, there are relatively few studies on satellite network security, especially the DDoS attack [17–20]. The latest research progress on LSCN DDoS attacks was the first volumetric DDoS attack against next-generation LSCNs: ICARUS [21]. The Starlink constellation was simulated to study single-link and multi-link DDoS attacks. Single-link attacks were divided into attacking uplinks, downlinks, and inter-satellite links; multi-link attacks were based on the calculation and analysis of all links of the satellite Internet between two regions and attacks on the bottleneck link that connect the two regions so as to achieve regional communication blocking. Domestic research on satellite network security mainly focuses on DDoS protection and detection. Aiming at protecting satellite Internet from DDoS attacks, Guo et al. [22] proposed a blockchain-based distributed collaborative entrance defense (DCED) framework, with which network traffic characteristics can be recorded and aggregated at the entrances of satellite Internet. The results show that the framework can accurately identify attack traffic in 1500 ms, and the framework is more effective than other similar DDoS methods.

However, there is little research on the security performance of LSCNs at present, which greatly limits the comprehensive development of LSCNs. Therefore, the space-time graph model is firstly used to determine the key nodes in the satellite network, a DDoS attack is used as the main means to attack the key nodes in the link, and the security performance of the entire satellite network against DDoS attacks is analyzed. Finally, the co-simulation in the scenario is confirmed. It has certain reference value for analyzing the security of LSCNs.

In the following sections, we first introduce related works on satellite key-node identification and satellite network DDoS attacks. Section 2 describes the methods used. Next, the simulated scenario and the parameter settings are given in Section 3. Section 4 analyzes the security performance of LSCNs after being attacked. Finally, we provide the conclusions.

2. Materials and Methods

2.1. Space-Time Graph Model

Studying the identification of key nodes in a satellite network is the basis of network vulnerability analysis, and it is also an important step in attacking LSCNs with DDoS. As a spatial information network, LSCNs are dynamic and connected, and traditional static graph models cannot model their highly dynamic network topology. Therefore, the concept of topology snapshot was formally proposed. Suppose there are N satellite nodes in a satellite network, $V = \{v_1, v_2, .., v_N\}$ represents the set of all satellite nodes. Divide the satellite network into time slots $\{1, 2, \ldots, T\}$ with the same interval in a period; then, in the time slot t, the network topology of the satellite can be expressed as $G^t = \{V^t, E^t\}$. In this time slot, V^t represents the set of all satellite nodes, and E^t represents the set of all links. So the set of satellite network topology snapshot sequences can be represented by $\{G^1, G^2, \ldots, G^T\}$. However, there is no end-to-end path between some node pairs in the snapshot, and the network topology composed of topological snapshot sequences is not connected.

In order to solve the connectivity problem, we transform the satellite network topology snapshot sequence $\{G^1, G^2, \ldots, G^T\}$ into a space-time graph model $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ [23,24]. In the space-time graph model, the satellite network is divided into $T + 1$ layers, the satellite nodes of each layer are $V = \{v_1, v_2, .., v_N\}$, and so the entire space-time graph contains $N \times (T + 1)$ nodes. Each adjacent layer can be connected by a space link and a time link. If a directed link $\overrightarrow{v_i^t v_j^t} \in E^t$ exists, a space link $\overrightarrow{v_i^{t-1} v_j^t} \wedge (i \neq j)$ will be added between

the adjacent layers, indicating that the node v_i can send data to v_j during time period $[t-1, t)$. The red path represents the space-time path for data sent from node v_2 to reach node v_5 through 4 time slots. Compared with other models, the space-time graph model can analyze the topology of a satellite dynamic network from the time dimension and space dimension and identify the key nodes in the constructed network. The space-time graph model is shown in Figure 1.

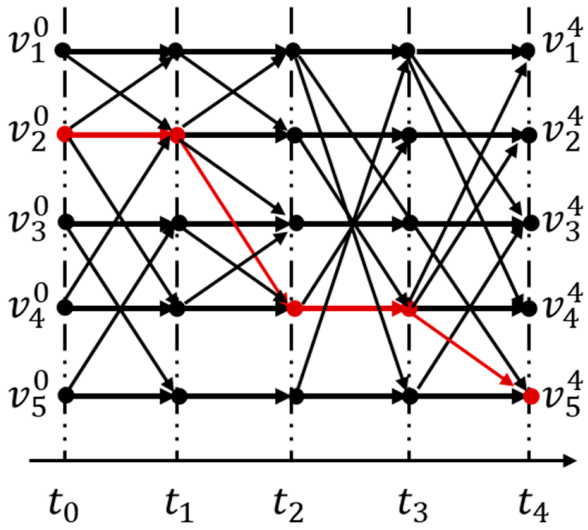

Figure 1. Space-time graph model.

2.2. Distributed Denial of Service (DDoS) Attacks

Denial of service (DoS) is an attack method that employs network protocol weaknesses to consume target resources and prevent victim hosts or network services from operating normally. However, because of the assault's sluggish tempo and restricted attack area, the adversary is unable to initiate a large-scale flood. DDoS is a scaled-up version of a DoS attack. The principle is that hackers hijack a large number of normal hosts to make them puppet hosts and send flood packets to the server to consume network resources and link bandwidth. The DDoS assault is currently regarded as the most dangerous attack method in the area of Internet security. The adversary can use the asymmetry of resources to generate large amounts of attack traffic, which eventually leads to a server crash. Figure 2 illustrates the DDoS attacks on LSCNs. The specific manifestations are as follows:

- Generate a lot of useless data, blocking satellite communication and making the attacked host unable to respond to user requests normally;
- Utilize the flaws in the network protocol of the attacked host to send repeated service requests repeatedly so that the attacked host cannot process the normal requests of users in time;
- Utilize the flaws of the attacked host's Internet to repeatedly send malformed attack data, thus occupying most of the host's memory and crashing the host.

The satellite network is characterized by decentralized users and a high degree of node autonomy, and the trust mechanism between nodes has become a major network security risk, especially for DDoS attacks, which have natural vulnerabilities. The study of DDoS attacks on LSCNs is still in its early stages at the moment. Similar to the terrestrial Internet, LSCNs are mainly subject to the following four popular DDoS attacks [20,25]:

- ICMP Flood: This attack sends a large number of ping packets to the victim in a short period of time and uses the method of exhausting the victim's resources to achieve the purpose of paralyzing the server so that it cannot continue to work normally;
- TCP SYN Flood: This attack captures the defect of the TCP three-way handshake and four-way teardown protocol and initiates many false SYN connection request packets

to the target host, which continuously occupies the resources of the target host and eventually causes the network to be paralyzed;

- UDP Flood: This attack sends a large number of UDP packets to the victim in a short period of time, making the victim overloaded and unable to undertake normal transmission work, exhausting the resources of the target host;
- HTTP Flood: This attack floods normal services in the network by sending malformed HTTP protocol packets, which can cause more damage without high rates.

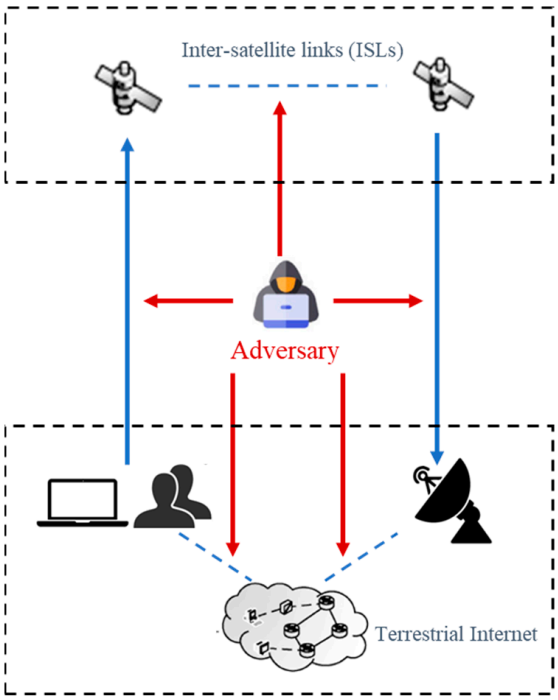

Figure 2. DDoS attacks on LSCNs.

3. Platform Design and Simulation

3.1. Simulation Tools

The LSCN security performance simulation platform is jointly implemented by STK, NS3, and Exata. Exata is a network simulation tool developed by Scalable Networks Technologies (SNT). Compared with QualNet, the performance of Exata has been further improved, with the advantages of parallel distributed simulation, real-time semi-physical simulation, and high-precision large-scale simulation. The packet-level simulation is carried out through NS3, and the importance of key satellite nodes in the region to the regional network is studied and analyzed. For LSCN network communication, DDoS attack deployment, and network-wide data analysis, Exata is utilized as a platform for network simulation. STK is used to generate the orbital information and data of the LEO and import them into Exata.

3.2. Orbit Parameter Settings

During the whole process, we set the satellite orbit inclination to 42° and the satellite orbit altitude to 335 km on STK. We select the network communication between A and B to implement an LSCN DDoS attack and analyze its security performance against DDoS attacks. After calculation, a total of 207 ground co-track satellites are selected to pass through the area within 10 s, and the simulation area is a rectangular area of about 8544 km × 4589 km. The orbit parameter information and 2D simulated scene are shown in Table 1 and Figure 3.

Table 1. Orbit parameter information.

Parameter	Value
Orbit type	Circular
Altitude	335 km
Inclination	42.0 deg
RAAN	0 deg
Number of tracks	10
Number of satellites	207
Regional area	8544 × 4589 km^2

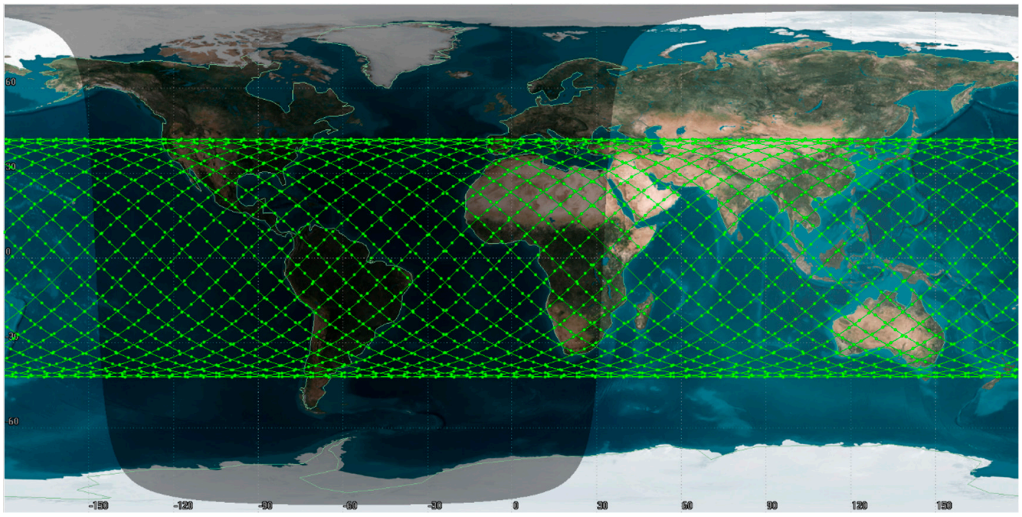

Figure 3. Simulated satellite 2D scene.

3.3. Interface Configuration

We use STK to establish a common-track satellite constellation that returns to the ground. Since the logical positions of the satellites in the constellation are relatively static within the time slice, as long as the relative positions of the satellites remain unchanged, the antenna can achieve communication as long as the antenna is kept aligned. The set antenna gain is 60 dB. We enable the QualNet interface in STK to configure the interface of the LEO satellite constellation and adopt the Open Shortest Path First routing protocol (OSPFv2) and distance−vector routing protocol (Bellman-Ford).

3.4. DDoS Attack Model Parameter Configuration

Since there is no Exata interface in STK that can be used directly, according to the use documents of the two simulation software programs, their joint simulation can realize interoperability by using the QualNet interface in STK and the AGI Satellite Toolkit Interface in Exata. The attack method chosen in this paper is a basic attack in Exata, and the data rate is set to 100 pkts/s. Layer transmission protocol (CBR) application between satellite No.207 and satellite No.66 is established. The application transmission start time is 1 s, the end time is 3600 s, the data of each packet is 2047 bits, the transmission interval is 1 s, and the routing strategy is the shortest-path strategy. According to the constructed space-time diagram key-node identification model, the key nodes of the entire satellite network are generated through the NetworkX and MATLAB tools, using node degree centrality and average betweenness centrality as indicators, and the importance of key nodes in the AB regional network is sorted. Finally, satellite No.67 and satellite No.119 are selected as the key nodes of the link, which are the targets of this simulation. On Exata, No.208, No.209, and No.210 node devices are set up to simulate a DDoS attack launched by the botnet on the No.67 satellite, while No.211, No.212, and No.213 are bots that launch attacks on the No.119 satellite.

4. Result and Discussion

In order to better verify the attack effect, this simulation attacked two satellite key nodes and multiple satellite key nodes under the OSFPv2 protocol and Bellman-Ford protocol, respectively, and analyzed the security performance of LSCNs after being attacked.

4.1. Two-Satellite-Key-Node Attack

Figure 4 shows the change in the transmission path of key satellite nodes No.119 and No.67 under the OSFPv2 protocol after the DDoS attack. The yellow * indicate the attacked satellite-key-node. The blue solid line represents the attack on the key node by the botnet host, the green solid line represents the original transmission path of the two satellites, the green dotted line represents the path change after being attacked, and the arrowheads represent the path direction (same as other Figures). Under normal transmission, the number of packets received by satellite No.66 is 3579. After attacking the key nodes of both satellites at the same time, the applied transmission link changes rapidly, while the number of packets received by satellite No.66 is 3483, which results in a low packet loss rate. As shown in Figure 5, under the Bellman-Ford protocol, after the attack, the number of packets received by satellite No.66 is 3539, which only has a certain impact. The average end-to-end delay under a two-satellite-key-node attack scenario is shown in Figure 6. It can be seen that only attacking two key satellite nodes of the whole local satellite network under the OSFPv2 protocol has little impact on its network security performance.

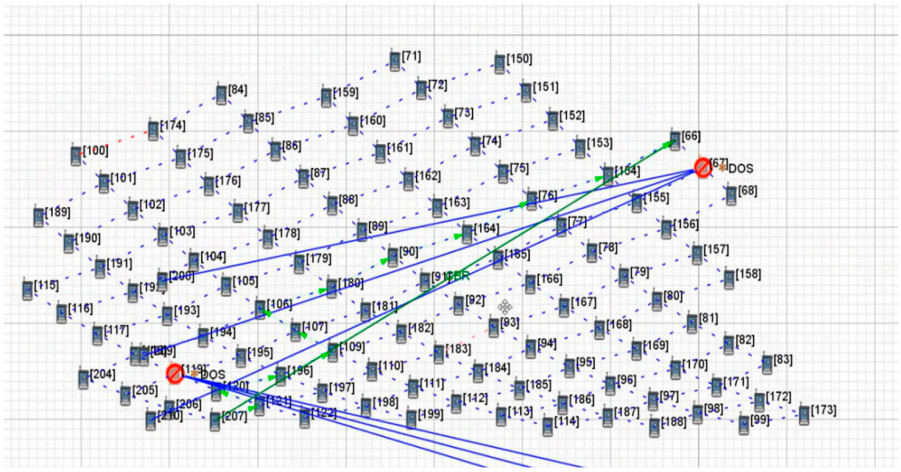

Figure 4. Two-satellite-key-node attack scenario under OSPFv2 protocol.

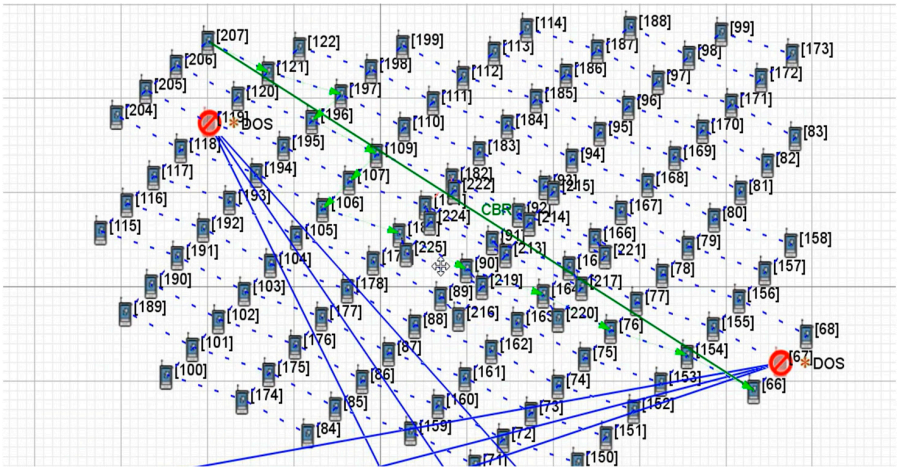

Figure 5. Two-satellite-key-node attack scenario under Bellman-Ford protocol.

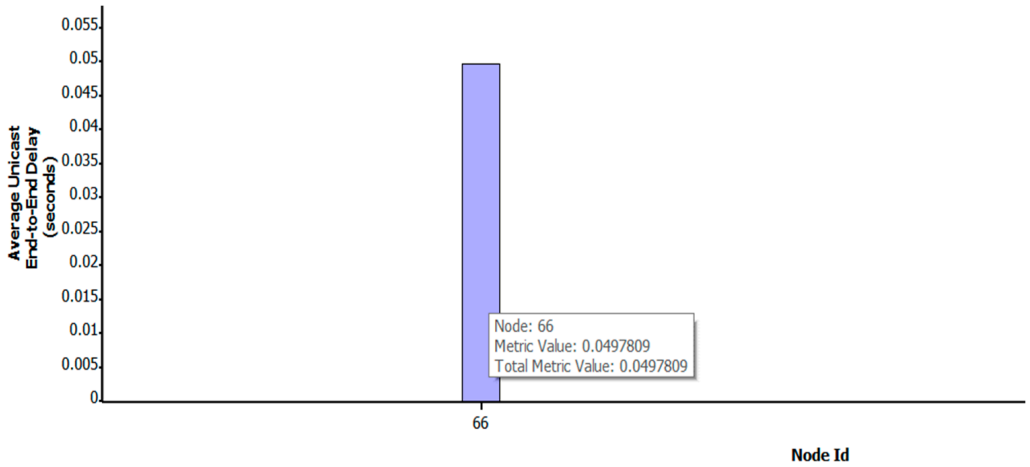

Figure 6. Average end-to-end delay under two-satellite-key-node attack scenario.

4.2. Multi-Satellite-Key-Node Attack

In order to verify the relationship between the number of key nodes and the attack effect, according to the ranking results of key nodes' importance, the network security performance of several satellite key nodes under the OSFPv2 protocol after being attacked is analyzed.

As shown in Figures 7 and 8, when DDoS attacks are applied to four key satellite nodes No. 121, No. 120, No. 119, and No. 67, the LSCN can still communicate by changing its satellite links. Although its communication links have changed, the number of satellite nodes that the path passes through remains the same, and so its communication propagation delay has no significant change.

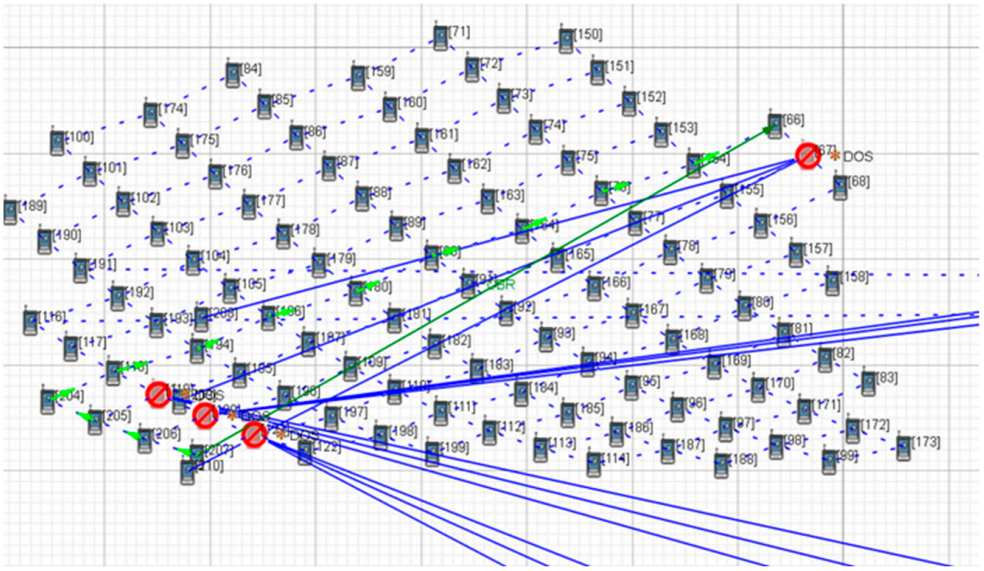

Figure 7. Four-satellite-key-node attack scenario.

As shown in Figures 9–11, when the key nodes of satellites No.121, No.120, No.119, No.194, and No.67 were attacked, the number of nodes increased after the link path was changed. Figure 11 clearly shows that with the increase in the number of key nodes attacked, the propagation delay also increases gradually, from the initial 0.049 s to 0.087 s. In addition, the number of data packets decreases to 3519, and the attack effect becomes more and more obvious.

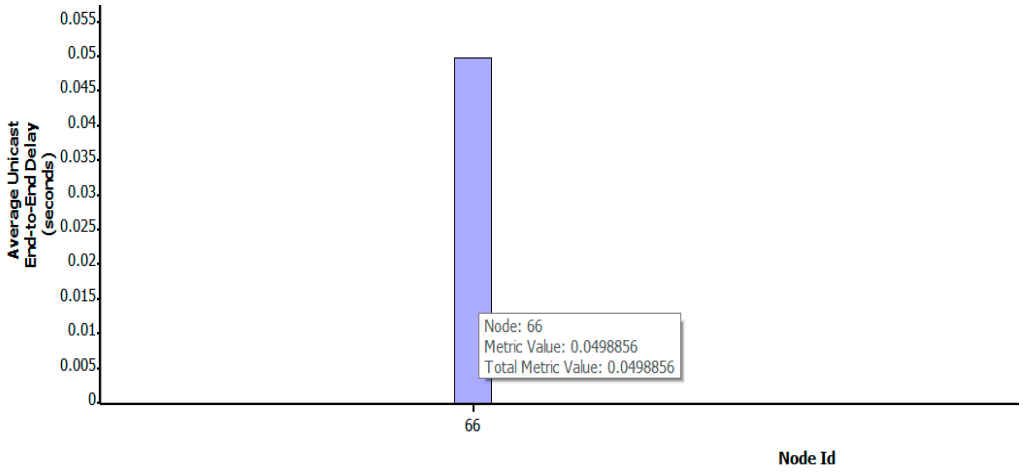

Figure 8. Average end-to-end delay under four-satellite-key-node attack scenario.

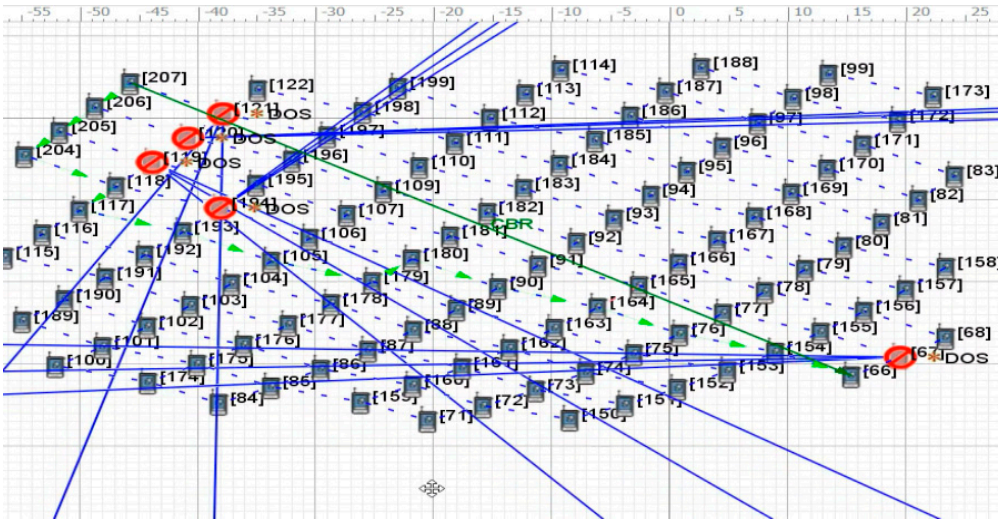

Figure 9. Five-satellite-key-node attack scenario.

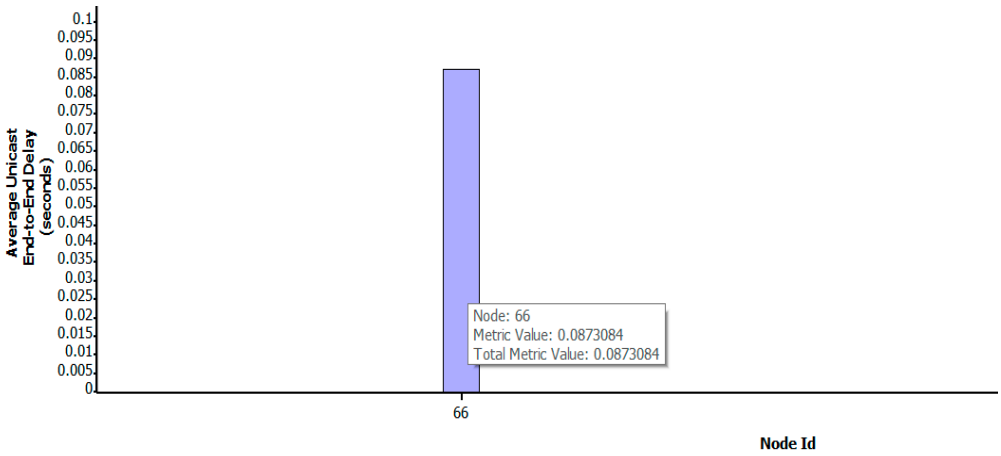

Figure 10. Average end-to-end delay under five-satellite-key-node attack scenario.

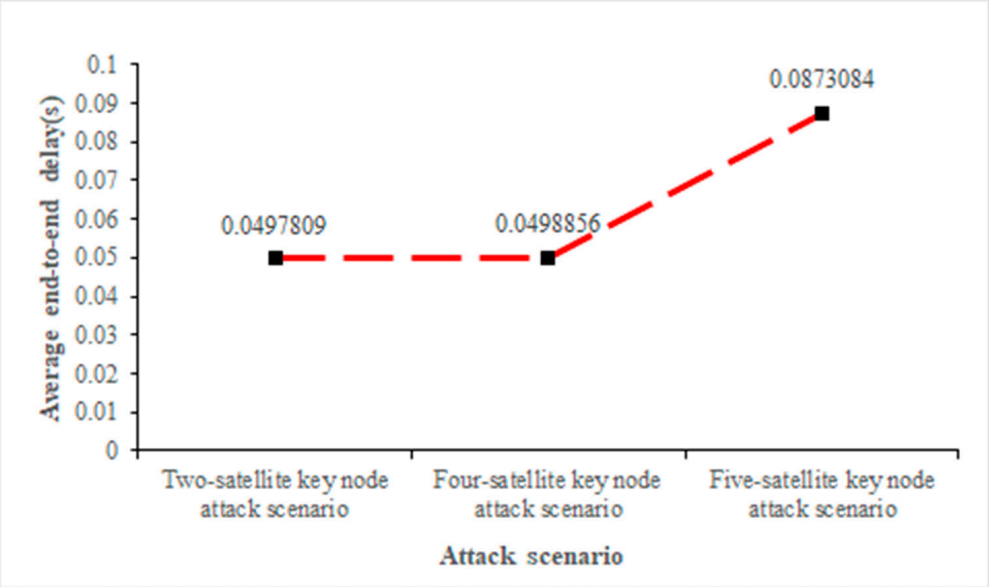

Figure 11. Average end-to-end delay under three attack scenarios.

We continued to verify the relationship between the number of key nodes and the attack effect and continued to carry out DDoS attacks on 10 key nodes and 12 key nodes of the network. The findings demonstrate that when the number of key nodes of attacked satellites increases, the transmission delay between satellites increases, which is proportional to the number of attacked satellites. When the number of attacked satellites reaches 12, the latency rises to 0.1003 s. However, the packet loss rate hardly changes, which may be the reason why the satellite quickly switches the backup link after being attacked.

5. Conclusions

As a key strategic field in the information age, the LEO satellite constellation is facing increasingly serious network security problems. In this paper, the space-time diagram model is proposed to identify the key nodes in the LEO satellite constellation, and a DDoS attack is adopted as the main means to attack the key nodes. The attack effects of two-satellite key nodes and multi-satellite key nodes are verified, and the security performance of the whole satellite network against a DDoS attack is analyzed, which is of great significance to effectively deal with LSCN attacks.

Author Contributions: Writing–original draft preparation, Y.Z. (Yan Zhang), Y.W. and Y.Z. (Yadi Zhai); writing–review and editing, Z.L., K.W. and L.K.; supervision, Y.H.; funding acquisition, Y.W., Q.Z. and L.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the National Natural Science Foundation of China (62201592, 61901490, and 61671454), the Research Plan Project of NUDT (ZK21-33), the Young Elite Scientist Sponsorship Program of CAST (2021-JCJQ-QT-048), and the Macau Young Scholars Program (AM2022011).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. An, K.; Lin, M.; Ouyang, J.; Zhu, W.P. Secure transmission in cognitive satellite terrestrial networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 3025–3037. [CrossRef]
2. An, K.; Liang, T.; Zheng, G.; Yan, X.; Li, Y.; Chatzinotas, S. Performance limits of cognitive-uplink FSS and terrestrial FS for Ka-band. *IEEE Trans. Aerosp. Electron. Syst.* **2019**, *55*, 2604–2611. [CrossRef]

3. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS aided hybrid satellite-terrestrial relay networks: Joint beamforming design and optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [CrossRef]
4. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. SLNR-based secure energy efficient beamforming in multibeam satellite systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, 1–4. [CrossRef]
5. Lin, Z.; Lin, M.; de Cola, T.; Wang, J.B.; Zhu, W.P.; Cheng, J. Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks. *IEEE Internet Things J.* **2021**, *8*, 11123–11134. [CrossRef]
6. Lin, Z.; Lin, M.; Wang, J.B.; de Cola, T.; Wang, J. Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 657–670. [CrossRef]
7. Lin, Z.; Lin, M.; Champagne, B.; Zhu, W.P.; Al-Dhahir, N. Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 251–255. [CrossRef]
8. Lin, Z.; Lin, M.; Champagne, B.; Zhu, W.P.; Al-Dhahir, N. Secure beamforming for cognitive satellite terrestrial networks with unknown eavesdroppers. *IEEE Syst. J.* **2021**, *15*, 2186–2189. [CrossRef]
9. Lin, Z.; Lin, M.; Wang, J.B.; Huang, Y.; Zhu, W.P. Robust secure beamforming for 5G cellular networks coexisting with satellite networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 932–945. [CrossRef]
10. Zhu, Q.Y.; Tao, H.C.; Cao, Y.H.; Li, X.H. Laser Inter-Satellite Link Visibility and Topology Optimization for Mega Constellation. *Electronics* **2022**, *11*, 2232. [CrossRef]
11. Boley, A.C.; Byers, M. Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth. *Sci. Rep.* **2021**, *11*, 10642. [CrossRef] [PubMed]
12. Inigo, D.P.; Cameron, B.G.; Crawley, E.F. A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. *Acta Astronaut.* **2019**, *159*, 123–135. [CrossRef]
13. Zhu, H.; Chen, S.Y.; Li, F.H.; Wu, H.; Zhao, H.Q.; Wang, G. User random access authentication protocol for low earth orbit satellite networks. *J. Tsinghua Univ. (Sci. Technol.)* **2019**, *59*, 1–8. [CrossRef]
14. Wei, D.B.; Qin, Y.F.; Kong, Z.X. The important node assessment method of satellite network based on near the center. In Proceedings of the 2016 IEEE International Conference on Network and Information Systems for Computers (ICNISC), Wuhan, China, 15–17 April 2016; pp. 103–107. Available online: https://ieeexplore.ieee.org/document/7945959 (accessed on 20 July 2022).
15. Wang, S.Q.; Zhao, Y.J.; Xie, H. Pkn: Improving survivability of leo satellite network through protecting key nodes. In Proceedings of the 15th International Conference on Emerging Networking EXperiments and Technologies, Orlando, FL, USA, 9 December 2019; pp. 7–8. [CrossRef]
16. Xu, R.; Di, X.Q.; He, X.W.; Qi, H. Evaluation method of node importance in temporal satellite networks based on time slot correlation. *J. Wireless Com. Network.* **2021**, *188*, 188. [CrossRef]
17. Tu, Z.; Zhou, H.C.; Li, K.; Li, M.; Tian, A.T. An energy-efficient topology design and DDoS attacks mitigation for green software-defined satellite network. *IEEE Access.* **2020**, *8*, 211434–211450. Available online: https://ieeexplore.ieee.org/document/9268145 (accessed on 22 July 2022). [CrossRef]
18. Di, A.O.; Ruisheng, S.; Lan, L.; Yueming, L. On the large-scale traffic DDoS threat of space backbone network. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 27–29 May 2019; pp. 192–194. Available online: https://ieeexplore.ieee.org/document/8819476 (accessed on 22 July 2022).
19. Li, C.J.; Sun, X.C.; Zhang, Z. Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. *IEEE Access.* **2021**, *9*, 113558–113565. Available online: https://ieeexplore.ieee.org/document/9514547 (accessed on 23 July 2022). [CrossRef]
20. Usman, M.; Qaraqe, M.; Asghar, M.R.; Ansari, I.S. Mitigating distributed denial of service attacks in satellite networks. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3936. [CrossRef]
21. Giuliari, G.; Ciussani, T.; Perrig, A.; Singla, A.; Zurich, E. ICARUS: Attacking low earth orbit satellite networks. In Proceedings of the 2021 USENIX Annual Technical Conference (USENIX ATC 21), Virtual, 14–16 July 2021; pp. 317–331.
22. Li, Y.J.; Li, H.W.; Lv, Z.Z.; Yao, X.K.; Li, Q.R.; Wu, J.P. Deterrence of Intelligent DDoS via Multi-Hop Traffic Divergence. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 13 November 2021; pp. 923–939. [CrossRef]
23. Li, F.; Chen, S.Y.; Huang, M.S.; Yin, Z.Y.; Zhang, C.; Wang, Y. Reliable topology design in time-evolving delay-tolerant networks with unreliable links. *IEEE Trans. Mobile Comput.* **2014**, *14*, 1301–1314. Available online: https://ieeexplore.ieee.org/document/6871429 (accessed on 25 July 2022). [CrossRef]
24. Huang, M.S.; Chen, S.Y.; Li, F.; Wang, Y. Topology design in time-evolving delay-tolerant networks with unreliable links. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 5296–5301. Available online: https://ieeexplore.ieee.org/document/6503962 (accessed on 26 July 2022).
25. Guo, W.; Xu, J.; Pei, Y.K.; Yin, L.G.; Jiang, C.X.; Ge, N. A Distributed Collaborative Entrance Defense Framework against DDoS Attacks on Satellite Internet. *IEEE Internet Things J.* **2022**, *9*, 15497–15510. Available online: https://ieeexplore.ieee.org/document/9777763/ (accessed on 26 July 2022). [CrossRef]