SI-STIN: A Smart Identifier Framework for Space and Terrestrial Integrated Network

Su Yao, Jianfeng Guan, Zhiwei Yan, and Ke Xu

Abstract

Currently, many hybrid satellite-aerial-terrestrial networks are under construction. The problem is how to coordinate heterogeneous communication networks and platforms to provide more effective services, which is seriously hindering the further development of networks. To mitigate this and other problems, a novel heterogeneous wireless network architecture named the Smart Identifier for Space and Terrestrial Integrated Network (SI-STIN) is designed. Based on the Smart Identifier Network (SINET), SI-STIN aims to solve the problem of the heterogeneous convergence of the integrated network layer, break through the triple binding of the traditional network layer design, and ultimately achieve high efficiency for resource integration and interconnection. The SI-STIN includes three layers and two domains: the smart pervasive service layer, dynamic resource adaption layer, and collaborative network component layer, and the entity domain and behavior domain, in which many separate identifiers and behavior descriptions are applied. Then the details, workflow, applications, and challenges of the STIN are presented. Experimental analysis verifies that the SI-STIN improves the performance in regard to network security and transmission efficiency and thus has great potential to satisfy various network demands.

Introduction

Currently, with the rapid development of network technology, methods of communication are rapidly changing. The requirements of global efficient communication services anytime and anywhere are becoming increasingly demanding. To meet these requirements, different types of communication systems are taken into consideration, such as satellite, space, and terrestrial integrated networks (mobile communication networks and the Internet). Satellite and space networks have the advantages of wide-scale geographical coverage and flexible network-construction, while traditional terrestrial networks have the advantage of being a mature technology with abundant resources. Therefore, the integration of these different networks could enhance the rate of resource utilization and realize support for abundant and massive services [1]. However, how to coordinate heterogeneous communication networks and platforms from terrestrial to space for providing more effective services is one of the most important research problems.

Compared to traditional terrestrial networks, the space and terrestrial integrated network (STIN) has different features, such as dynamic network topology, long distance between network nodes, vulnerable communication channels, and limited resources of space network nodes. As a result, many mature terrestrial network technologies are difficult to directly apply in the STIN.

The goal of the STIN is to achieve efficient information transmission and application sharing among various users and application systems of ground, sea, near-Earth space, and deep space. Based on significant differences of various types of network systems, including top-design of the network architecture and protocols, STIN could provide cross-network information sharing and application services for all types of end users from the space to the ground, only through key technologies, such as large-scale high-speed information transmission, dynamic space networking and routing, and network security.

Existing Solutions on the Space and Terrestrial Integrated Network

Recently, much research and many projects have been carried out to construct a new space terrestrial network. Within them, the Space and Terrestrial Integrated Network project [2] has been proposed based on the terrestrial network and expanded by a space and satellite network that covers the entire near-Earth space environment. This project is a major project of national science and technology toward 2030, and the goal of this project is develop a new infrastructure that integrates space and terrestrial networks [3].

Figure 1 illustrates the architecture of this project. From space to terrestrial, the architecture can be divided into three different parts. The first part is space-based backbone networks, which consist of deep-space detection satellites, remote sensing satellites, spy satellites, and other space-based backbone nodes near geosynchronous orbit. The space-based backbone networks mainly achieve backbone network interconnection, backbone network access, network management, and other functions. The second part is space-based access networks, which consist of space stations, aviation networks, unmanned aerial vehicles, and other low Earth orbit (LEO) satellite nodes in near-Earth space. These space-based access networks mainly realize the functions of the space-based Internet of Things, access network interconnections, mobile com-

Digital Object Identifier:
10.1109/MNET.2018.1800175

Su Yao and Ke Xu are with Tsinghua University; Jianfeng Guan is with Beijing University of Posts and Telecommunications; Zhiwei Yan is with China Internet Network Information Center.

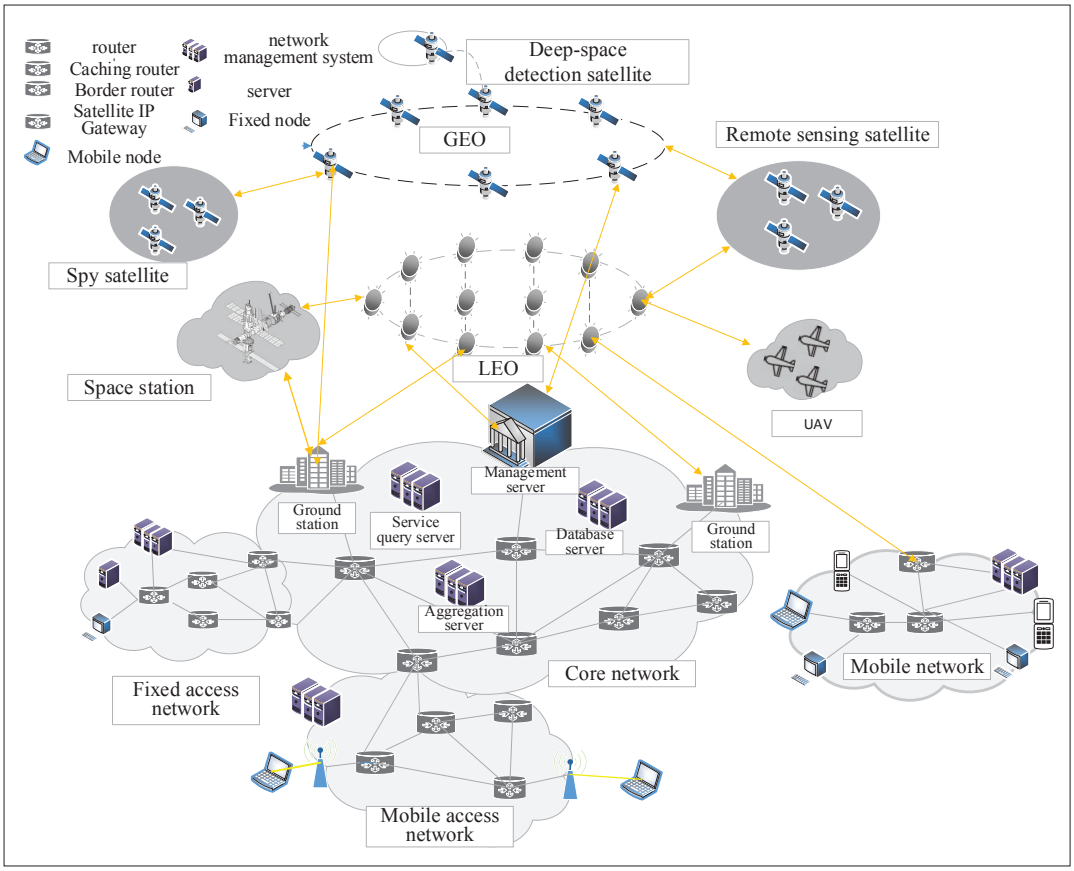

FIGURE 1. Architecture of the Space and Terrestrial Integrated Network project.

munications, and other functions. The last part is the ground-based network, which consists of fixed access networks, mobile access networks, mobile networks, ground stations, and different servers in the ground core network. The main function of the ground-based network is to interconnect networks, from space networks to terrestrial networks; interconnect the different ground networks; and provide maintenance control and application. This new infrastructure can provide a new solution for applications in marine, aviation, aerospace, and inclusive information systems as well as global commercial broadband communication.

In the meantime, scientists in America have constructed a STIN system that mainly consists of a geostationary Earth orbit (GEO) network complemented by LEO and global terrestrial networks [4]. However, the function of satellites mainly provides a bent-pipe signal transmission, which lacks data storage, forwarding, and networking. To realize space networking and integration of a universal network, a series of technical challenges need to be solved in the physical layer, data link layer, network layer, and transport layer. A unified network architecture design is significant for efficient integration and different networks' interconnection.

Recently, many research efforts focus on this topic. Kapovits *et al.* defined and presented software defined networking (SDN)-based reference architectures for providing assured quality end-to-end service over an integrated satellite/terrestrial network [5]. Ferrs *et al.* investigated how network functions virtualization (NFV) technologies can enhance the interoperability of the space networks and the deployment of services across space-terrestrial networks [6]. Also, Bertaux *et al.* provided a description of how SDN/NFV can enhance space network architecture for extending the range of applications of space network communication and achieving seamless integration with terrestrial networks [7].

Many research projects have been carried out to construct a new space terrestrial network. Within them, the Space and Terrestrial Integrated Network project has been proposed based on the terrestrial network and expanded by a space and satellite network that covers the entire near-Earth space environment.

These research works adopted SDN/NFV in the space-terrestrial scenario, but SDN/NFV technologies are still applied in the terrestrial part, and the space segment has little difference. Besides, there are still some important challenges. First, a centralized control structure will cause security problems because the control link can be attacked easily. Table 1 illustrates five different kinds of security issues associated with STIN architecture based on SDN/NFV. As shown in Table 1, the control layer and data layer are more likely to suffer an attack than other layers and interfaces. Second, the changing space network topology will bring transmission efficiency problems because the storage and processing capability of satellite nodes are limited and the management overhead is increased.

In this article, we propose a generic architecture named the smart identifier STIN (SI-STIN) for STIN based on the smart identifier network

Security issues	Layers or interfaces affected				
	Application layer	Interface between application layer and control layer	Control layer	Interface between control layer and data layer	Data layer
Unauthorized controller access			✓	✓	✓
Unidentified application	✓	✓	✓		
Controller hijacking			✓	✓	
Flooding attack between controller and switch			✓	✓	✓
Flooding attack on flow table of switch					✓

TABLE 1. Security issues associated with the STIN based on SDN/NFV framework.

(SINET) to achieve good efficiency, scalability, availability, and security. The SI-STIN aims to solve the problem of the heterogeneous convergence of the design of the integrated network layer of the STIN, including the space and terrestrial segments, break through the triple binding of the network layer design, and ultimately achieve high efficiency for resource integration and interconnection.

Architecture of SI-STIN

The original design of the Internet has exposed many shortcomings that can cause serious security issues and many other application problems. The source of these shortcomings is a series of "bindings," including resource-location binding (RLB), control-data binding (CDB), and user-network binding (UNB), which boost flexibility and self-adaptability of the TCP/IP-based Internet.

To decouple these bindings, many approaches have been proposed, such as SDN and NFV technologies [8]. However, it can only solve the problem of CDB. As a result, a novel Internet architecture named SINET was proposed [9]. The SINET architecture leverages service identifiers, behavior descriptions, and mapping mechanisms to provide services for consumers. This architecture achieves dynamic resource adaptation by perceiving service demands and network states. Consequently, the SINET improves the utilization of network resources and reduces energy consumption.

These observations motivated the design of the proposed SI-STIN. The reference model of the SI-STIN is shown in Fig. 2a. Different from current network architectures, the SI-STIN is vertically divided into three layers, namely, the smart pervasive service layer, the dynamic resource adaption layer, and the collaborative network component layer. Meanwhile, the SI-STIN is horizontally divided into two domains, namely, the entity domain and behavior domain. These logical units and interactions among them provide great support for smart cooperation within the SI-STIN. The main functions of these five logical units are as follows.

The smart and pervasive service layer plays a role as a project manager that is responsible for the identification, description, and management of different STIN services, including aviation management, maritime service, disaster relief, global mobile communication, anti-terrorism, and remaining stable.

The dynamic resource adaption layer of the SI-STIN plays a role as a work group leader, dynamically adapting network resources and configuring network families. This layer perceives service demands and network states to satisfy the service demands and improve the quality of experience. Each function group consists of a set of network components that have similar functions, such as a satellite communication network, maritime communication network, aeronautical communication network, mobile communication network and the Internet.

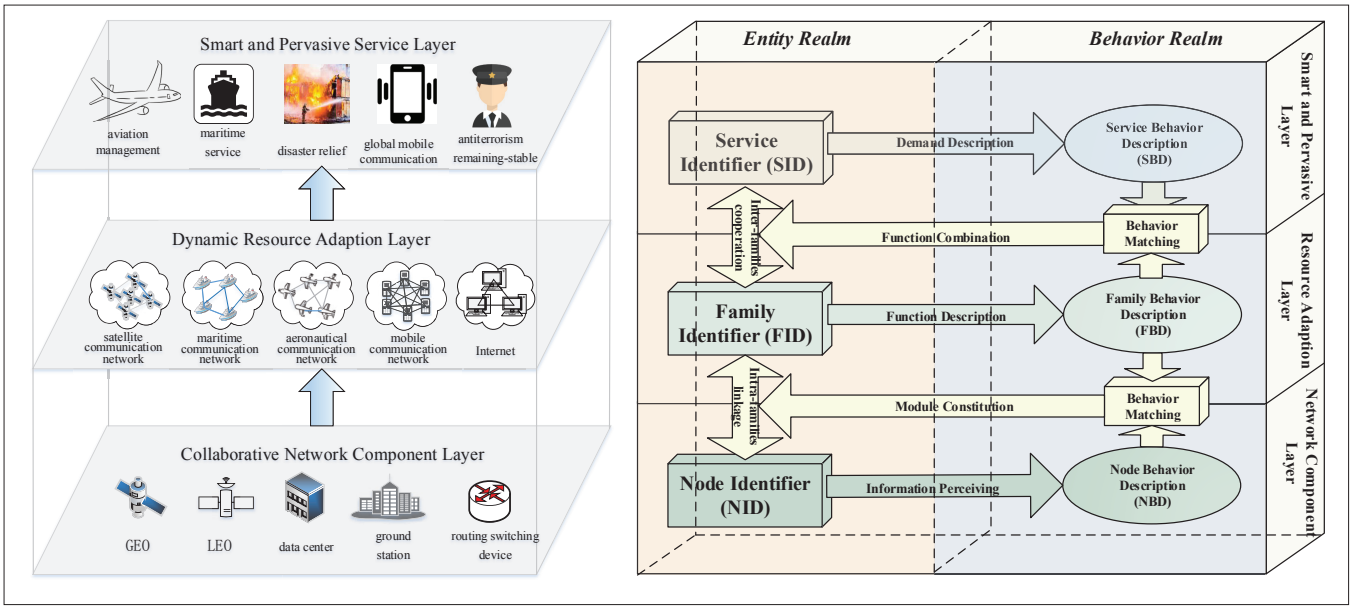

FIGURE 2. Overview of the SI-STIN: a) reference model of the SI-STIN; b) operational principles of SI-STIN.

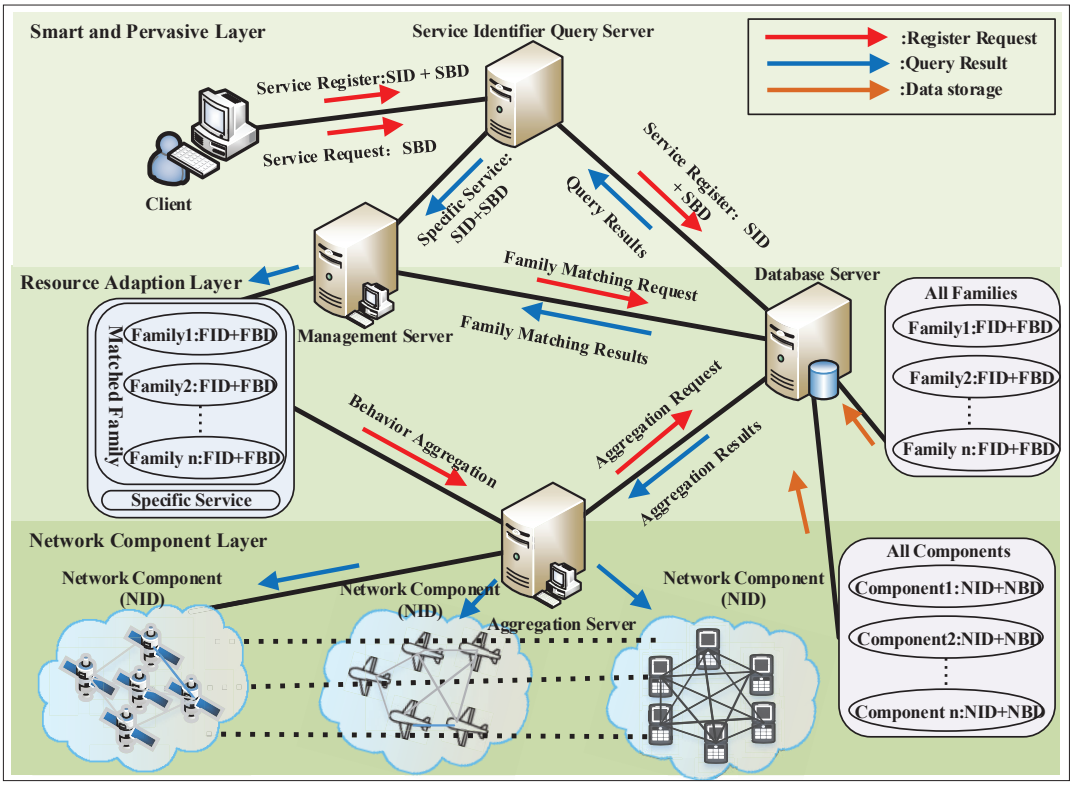

FIGURE 3. Operational workflow and example application of the SI-STIN.

The collaborative network component layer of the SI-STIN plays a role as a work member, which is responsible for the storage and transmission of data. This layer is also responsible for the behavior perception and behavior aggregation of network components, including GEOs, LEOs, data centers, ground stations, and routing switching devices.

The entity domain of the SI-STIN exclusively identifies entries in three layers, including service identifiers (SIDs, identifiers for STIN services), family identifiers (FIDs, identifiers for network resources) and node identifiers (NIDs, identifiers for network nodes).

The behavior domain of the SI-STIN describes the behavior of different entities in three layers, namely, service behavior description (SBD), family behavior description (FBD) and node behavior description (NBD). For instance, SBD includes the service type, service cache, provider signature, and so on; FBD includes the resources size, function, composition, capacity, and so on; and NBD includes the node function, power consumption, and so on.

The operational principles of the SI-STIN are shown in Fig. 2b. Between the smart and pervasive service layer and dynamic resource adaptation layer, the SI-STIN deploys behavior matching mechanisms and maps the SBD to the FBD to find the optimal network families for a smart service. Then the selected network families operate collaboratively based on the inter-family cooperation mechanism. The SI-STIN employs the behavior aggregation mechanism in the dynamic resource adaptation layer and collaborative network component layer. The behavior aggregation mechanism maps the FBD to the NBD to find the optimal set of network components. Then, based on the intra-family linkage mechanism, the network components in a network family cooperate. Through these mechanisms, the SI-STIN achieves dynamic resource adaption and satisfies the demands of pervasiveness and smartness.

Workflow and Example Application

The feasibility of network deployment and application must be considered when designing a new architecture for the STIN. The operational workflow and example application of the SI-STIN are shown in Fig. 3. We take satellite communication service as an example to illustrate the process. First, the communication operators register the SIDs and SBDs of the provided services at the service identifier query server (SIQS). The service consumer submits the SBD of the needed service to the SIQS. The SIQS looks for the candidate combinations of SID and SBD using the service identifier inquiry algorithm. Then the SIQS returns the results to the service consumer. The service consumer selects the SID and SBD based on its own preference. The selected SBD is matched with FBDs through the service identifier mapping mechanism to find the optimal network family. Then the FID and FBD of a network family can be confirmed. The behavior aggregation server aggregates the network components to the confirmed network family through the behavior aggregation mechanism. The selected SBD and NBDs within the chosen network family are analyzed to find the optimal network components through a network game algorithm. Finally, the service consumer acquires the service through the chosen network family and network components. Furthermore, if the service is popular, the service is stored in the memory module of the network component, and the corresponding SID and SBD will be stored in the memory sub-mod-

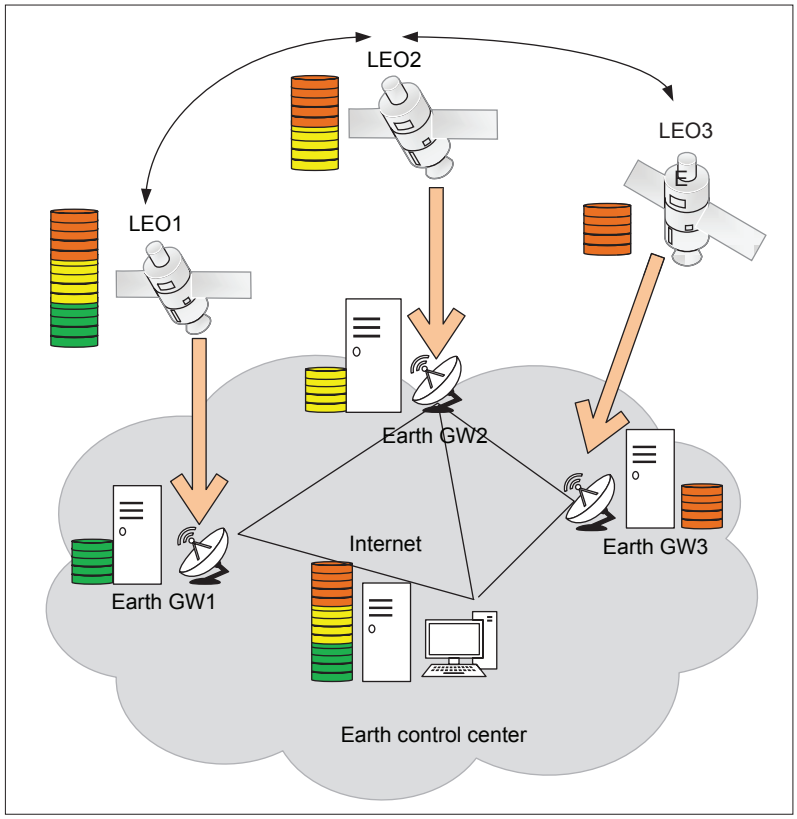

FIGURE 4. Network topology of the data transmission scenario.

Contact/idle	Duration	Rate	Delay	Jitter
LEO1->GW1	400 s	100 kB/s	7 ms	1 ms
Idle period	7 min			
LEO2->GW2	450 s	100 kB/s	8 ms	2 ms
Idle period	10 min			
LEO3->GW3	780 s	100 kB/s	7 ms	1 ms

TABLE 2. Parameters of the data transmission process.

ule. Consequently, other consumers can obtain the service from the nearest network component.

The SI-STIN has the potential for practical applications and can provide great benefits for various service demands. In this instance, two types of different cooperation approaches are proposed: inter-family and intra-family cooperation. Among different network families, the inter-family cooperation mechanism is used. This mechanism can be implemented by building a coalitional game approach. All related families make up a coalition. Each family in a coalition can decide whether to leave its current coalition or to join a new coalition, aiming to improve the quality of service. On the other hand, intra-family cooperation is used to interconnect the network components in one family. The selected components in the same family cooperate to finish each task. One available approach for the intra-family cooperation mechanism is to adopt the dynamic Bayesian game.

Performance Analysis and Experiments

In this section, we validate and evaluate the design of the SI-STIN through both analysis and experiments. We analyze the performance of the SI-STIN mainly in two aspects: network security and transmission efficiency.

To evaluate the SI-STIN's performance, a small-scale testbed platform is designed for experiments. In the traditional TCP-IP-based network architecture or SDN/NFV-based network architecture [6, 7], LEO satellites such as remote sensing satellites usually transfer large-scale data to the ground station. However, there is a limited contact time when a LEO passes through a ground station in one orbital cycle. The UK-DMC satellite [10] is used as an example, and its link speed is 1 Mb/s. Suppose the contact time between the a LEO and a ground station is 500 s; the maximum file size that the LEO can transfer is only 62.5 MB. Therefore, it is impossible for one LEO to transfer hundreds of single raw pictures during its contact window. Typically, two or more passes are needed to transfer one large data file. During each pass, parts of a file are transferred from the LEO to the Earth gateway first; then these parts are transferred to a control center for reassembly. When all of the parts of a file have been transferred, the complete image file is finished. In the SI-SINET architecture, each LEO satellite and Earth gateway is seen as one component. Therefore, the LEO satellites and Earth gateways make up one satellite function group. In this function group, the data transmission process only goes through one contact window.

The network topology of this testbed is shown in Fig. 4. This group function consists of seven components: three LEO satellite components, three Earth gateway components, and one control center component. A satellite toolkit (STK) is used to model the LEO link topology and characteristics to ensure the authenticity of the data. The parameters generated by an STK are described in Table 2. We use a CFDP program to transfer a 128 MB image file from the LEO to the Earth gateway. CFDP is configured with a 128 kB block of the Licklider Transmission Protocol (LTP), 32 kB Bundle Protocol, and Contact Graph Routing (CGR) protocol [11].

Figure 5a shows the comparison of the link speed between LEO satellites and Earth gateways. LTP starts the file transmission as soon as the link is available. In the traditional network, only one LEO satellite completes the whole file transmission process. Initially, the LEO transmits a 37 MB block of the image file to the Earth GW1. After a seven-minute break, the LEO establishes a connection with Earth GW2 and then transfers another 37 MB block of the file. Finally, after another 10 minutes of disconnection, the LEO establishes a connection with Earth GW3 and transfers the remaining block of the file. Ultimately, the Earth control center reassembles the blocks of the file from the GWs.

In the SI-STIN architecture, the communication process is quite different. The function group consists of three LEO satellites completing the file transmission process. Before file transmission, the whole file is divided into blocks and distributed to the different LEO satellites. Therefore, the whole file transmission can be seen as only one communication process. In fact, LEO1, LEO2, and LEO3 transmit blocks of the file synchronously. In the ideal

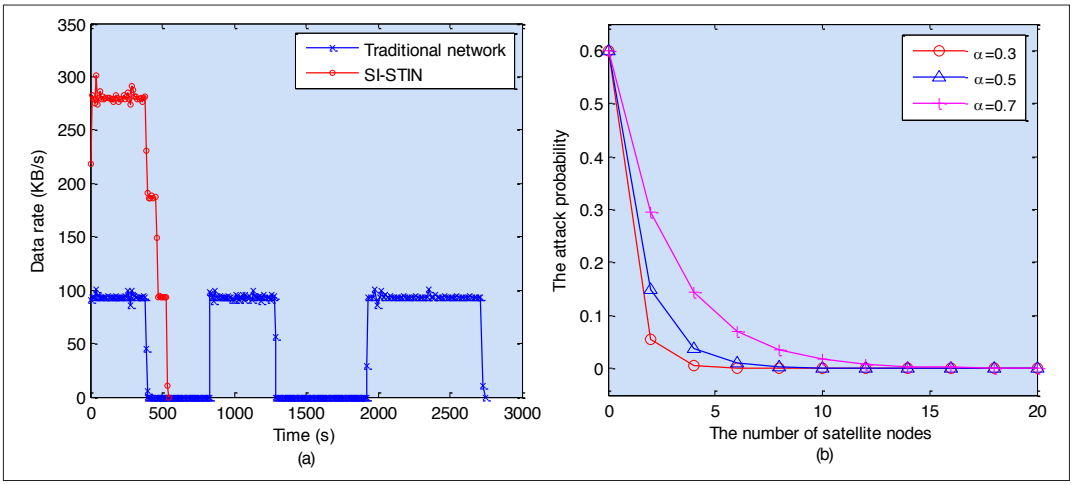

FIGURE 5. Evaluation results: a) file transmission process; b) attack probabilities in the SI-STIN architecture.

case, the link speed rate is the sum of these three links. After 400 s, the LEO1 satellite disconnects from GW1. Therefore, the maximum link speed rate is the sum of the LEO2 and LEO3 links. Then, after 50 s, the LEO2 satellite disconnects from GW2.Therefore, the link speed rate of the function group is the LEO3 link speed rate. The file transmission process using the SI-STIN architecture is shown in Fig. 5a. From Fig. 5a, we observe that the link speed in the SI-STIN is much larger than that of the traditional network. As a result, the time over which the whole file transmission process takes place is much shorter than that of the traditional network.

Since the satellite node is susceptible to a host of attacks, including data corruption, session hijacking, and eavesdropping, security is an important consideration in satellite communication network design. Space communication channels are open, which makes it easy for an unauthorized user to obtain signals and data. More seriously, any well-equipped adversary can send spurious commands to the satellite node and disrupt communication. As a result, the link between satellite nodes and ground stations could be invalidated. In the SI-STIN, although the attacker knows the NIDs of the components, he/she cannot know their corresponding locations, increasing the difficulty of an attack. Moreover, due to the collaboration of components in a family, an entire content can be provided by many potential nodes. The transmission path for a certain service may be dynamic, and other collaborative components will help the component avoid being attacked.

According to a survey by the Institute of Space Technology [12], 40 percent of satellite nodes were impacted by a host of attacks in 2014. With this ratio, we analyze the probability of one component being attacked in an SI-STIN. Figure 5b shows a comparison of attack probabilities in different numbers of network satellite nodes, where three different attack factors (α = 0.3, 0.5, 0.7) are considered. In this figure, it is observed that the attack probabilities decrease below 0.01 when the number of satellite nodes in a family increase to 15 because with the increment of the family scale, the number of available protection paths increase, and it is more difficult for an attacker to guess the accurate transmission path. This experiment shows that the SI-SINET is capable of enhancing security.

> Overall, the SI-STIN provides a promising space and terrestrial iIntegrated network blueprint, which is expected to integrate various innovations and applications, including all types of heterogeneous networks, ranging from space to terrestrial.

Opportunities and Challenges

Due to its novelty, flexibility, and robustness, the SI-STIN provides great opportunities to solve many challenging issues, such as high-speed transmission support, security issues, and energy saving. Overall, the SI-STIN provides a promising space and terrestrial integrated network blueprint, which is expected to integrate various innovations and applications, including all types of heterogeneous networks, ranging from space to terrestrial.

Although the SI-STIN has been deeply researched, there are still some challenges to overcome. The first challenge is to develop the high intelligence of the SI-STIN. In practical applications, there are many complex cases to be faced. For example, a family may undertake many intricate functions, and a component may belong to several families concurrently. Moreover, the function of a component may change as the environment changes. How to efficiently schedule and manage these families and components is a very challenging topic. A possible solution is to use the group selection algorithm [13] and advanced biological intelligence in the decision mechanisms [14].

Another large challenge is large-scale deployment of the SI-STIN. The current Internet architecture is occupied by multiple stakeholders and used by billions of users. Generally, they are not willing to make changes from the current Internet to a significantly different Internet architecture. An available approach is to establish many small-scale platforms for certain areas without drastically affecting existing services. Then the SI-STIN can be tested, validated, and extended step by

It is worth mentioning that the SI-STIN matches the overall design philosophy for a space and terrestrial integrated network. In the future, complex mechanisms and advanced applications will be further researched to make the SI-STIN more powerful and effective.

step before deploying the large-scale platform. Additionally, the security strategy design for the SI-STIN should be considered in the case of a different attack scenario [15].

Conclusion

This article proposes a theoretical model for a space and terrestrial integrated network, the SI-STIN. The SI-STIN adopts a novel architecture featuring three layers and two domains, in which many independent identifiers and behavior descriptions are used to solve the problems of coordinating different heterogeneous communication networks, from space to terrestrial. With this design, the detailed mechanisms, workflow, and applications are further introduced. Performance analysis and experiments show that the SI-STIN has many advantages in terms of the transmission efficiency and security issues. This article also states the opportunities and challenges of the STIN. It is also worth mentioning that the SI-STIN matches the overall design philosophy for a space and terrestrial integrated network. In the future, complex mechanisms and advanced applications will be further researched to make the SI-STIN more powerful and effective.

Acknowledgment

This research was supported in part by the National Key Research and Development Program (2018YFB0803405) and National Natural Science Foundation of China Grants 61802222, 61472212, 61825204, and 61402486, and a project funded by the China Postdoctoral Science Foundation (2018M641358). This work has also been supported by Huawei.

References

[1] K. Xu *et al.*, "A Tutorial on the Internet of Things: From a Heterogeneous Network Integration Perspective," *IEEE Network*, vol. 30, no. 2, Mar./Apr. 2016, pp. 102–08.
[2] M. Q. Wu *et al.*," Overall Framework Design of Space-Ground Integrated Information Network," *Satellite & Network*, vol. 3, 2016, pp. 30–36.
[3] W. Wu *et al.*, "Reflections on the Development and Construction of Space-Ground Integration Information Network," *Telecommun. Science*, vol. 12, 2017, pp. 3–9.
[4] Y. Vasavada *et al.* "Architectures for Next Generation High Throughput Satellite Systems," *Int'l. J. Satellite Commun. & Networking*, vol. 34, no. 4, 2016, pp. 523–46.
[5] Á. Kapovits *et al.*," Advanced Topics in Service Delivery Over Integrated Satellite Terrestrial Networks," *IEEE Advanced Satellite Multimedia Systems Conf. and the Signal Processing for Space Commun. Wksp.*, 2014, pp. 92–98.
[6] R. Ferrús *et al.*, "SDN/NFV-Enabled Satellite Communications Networks: Opportunities, Scenarios and Challenges," *Phys. Commun.*, vol. 18, 2016, pp. 95–112.
[7] L. Bertaux *et al.*, "Software Defined Networking and Virtualization for Broadband Satellite Networks," *IEEE Commun. Mag.*, vol. 53, no. 3, Mar. 2015, pp. 54–60.
[8] Xu K *et al.*, "Toward a Practical Reconfigurable Router: A Software Component Development Approach," *IEEE Network*, vol. 28, no. 5, Sept./Oct. 2014, pp. 74–80.
[9] H. Zhang *et al.*, "Smart Identifier Network: A Collaborative Architecture for the Future Internet," *IEEE Network*, vol. 30, no. 3, 2016, pp. 46–51.
[10] C. Caini and R. Firrincieli R. "Application of Contact Graph Routing to LEO Satellite DTN Communications," *IEEE ICC*, 2012, pp. 3301–05.
[11] R. Wang *et al.* , "Licklider Transmission Protocol (LTP)-Based DTN for Cislunar Communication," *IEEE/ACM Trans. Net.*, vol. 19, no. 2, 2011, pp. 359–68.
[12] S. Muhammad *et al.*, "A Survey Paper on Security Issues in Satellite Communication Network Infrastructure," *Int'l. J. Engineering Research & General Science*, vol. 2, no. 6, 2014, pp. 887–900.
[13] J. Guan *et al.*, "GBC-Based Caching Function Group Selection Algorithm for SINET," *J. Network and Computer Applications*, vol. 85, 2017, pp. 56–63.
[14] C. Dovrolis, "Evolvable Network Architectures: What Can We Learn From Biology," *ACM SIGCOMM CCR*, vol. 40, no. 2, 2010, pp. 72–77.
[15] S. Yao, J. Guan, and H. Zhang, "Survivable Strategy Set Design for Malicious Attack Propagation in NEMO Scenario," *EURASIP J. Wireless Commun. & Net.*, vol. 234, no. 1, pp. 1–10.

Biographies

Su Yao received his Ph.D. degree in communications and information systems from Beijing Jiaotong University, China, in January 2017. Currently he is doing postdoctoral research at Tsinghua University. His research interests include next generation Internet architecture and network security.

Jianfeng Guan received his Ph.D. degree in communications and information systems from Beijing Jiaotong University in January 2010. He is currently an associate professor with the Institute of Network Technology at Beijing University of Posts and Telecommunications, China. His current research interests include mobile IP, mobile multicast, and next generation Internet technology.

Zhiwei Yan received his Ph.D. degree from the National Engineering Laboratory for Next Generation Internet Interconnection Devices at Beijing Jiaotong University. He joined the China Internet Network Information Center in 2011 and is currently an associate professor at the Chinese Academy of Sciences. Since April 2013, he has been an invited researcher at Waseda University. He is active in IETF and published RFC 8191. His research interests include mobility management, network security, and next generation Internet.

Ke Xu received his Ph.D. from the Department of Computer Science & Technology of Tsinghua University, where he serves as a full professor. He has published more than 100 technical papers and holds 20 patents in the research areas of next generation Internet, P2P systems, the Internet of Things (IoT), and network virtualization and optimization. He is a member of ACM and has guest edited several special issues in IEEE and Springer journals.