

Space-Terrestrial Integrated Architecture for Internet of Things



ZHANG Gengxin, DING Xiaojin, QU Zhicheng

(Telecommunication and Networks National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: To realize the ultimate vision of Internet of Things (IoT), only depending on terrestrial network is far from enough. As a supplement and extension of terrestrial network, satellite network can offer powerful support to realize the depth and breadth of the coverage. However, existing satellite networks are usually designed for particular purposes. Moreover, traditional satellite networks and terrestrial networks are developed and operated separately, consequently they cannot meet the need of network flexibility required by IoT. In this paper, a space-terrestrial architecture is conceived for constructing a space-terrestrial based IoT (ST-IoT) system. Additionally, a reliable identification procedure, an integrated access and communication procedure, as well as a clustering cooperative transmission strategy are also presented.

Keywords: Internet of Things; system architecture; space-terrestrial integrated network

DOI: 10.12142/ZTECOM.202004002

<http://kns.cnki.net/kcms/detail/34.1294.TN.20201111.1431.003.html>, published online November 11, 2020

Manuscript received: 2020-09-25

Citation (IEEE Format): G. X. Zhang, X. J. Ding and Z. C. Qu, "Space-terrestrial integrated architecture for Internet of Things," *ZTE Communications*, vol. 18, no. 4, pp. 03 - 09, Dec. 2020. doi: 10.12142/ZTECOM.202004002.

1 Introduction

With the deployment of 5G networks and the development of the Internet of Things (IoT) technology, information transmissions have been expanded from people-and-people to people-and-things as well as things-and-things^[1]. Therefore depending on pure terrestrial network can hardly satisfy the depth and breadth of the coverage required by the Internet of Everything. Meanwhile, space information network (SIN)^[2-3] has received increasing research attention as a benefit of its ability of exploiting both satellite network and terrestrial network to expand the depth and breadth of the coverage.

There are two kinds of designs for SINs. First, space nodes

are supported by terrestrial network, which is the most mature architecture represented by Inmarsat, Intelsat, wideband global satcom (WGS)^[4-5], etc. Under this architecture, space nodes of SIN merely serve as transparent transmitting channel, and globally distributed terrestrial network will provide services by processing the receiving data. In this way, system complexity can be reduced by simplifying space equipment, and it is convenient for maintenance and upgrade. However, this architecture has a poor invulnerability since the core elements of SIN are deployed on the ground. As an alternative, space-based network, represented by Iridium and advanced extremely high frequency (AEHF)^[6-7], is an architecture to establish an independent SIN through inter-satellite links (ISLs). This

architecture highlights the SIN nodes' capabilities of processing, exchanging, and controlling. On the one hand, it enhances systems' invulnerability compared with the former architecture. On the other hand, the increasing capabilities may sharply raise the complexity of space equipment as well as the cost of construction and maintenance. Moreover, in Ref. [8], in order to decrease the delay and enhance the reliability, the authors designed a new IoT routing mechanism in the presence of small-world characteristics, and explored the reliability and delay models with the aid of Cayley graphs.

As a further development, space-terrestrial integrated network (STIN) has also been designed^[9], which can combine the advantages of the aforementioned two architectures. Within this framework, the space network is applied to realize global coverage and the terrestrial network takes charge of most managing and controlling functions. Differing from Ref. [9], an architecture of a space-terrestrial based IoT system is conceived in this paper. Moreover, the procedures of control plane for space-terrestrial based IoT (ST-IoT), reliable identification as well as integrated access and communication are designed.

The rest of this article is organized as follows. In section 2, we briefly introduce the whole system architecture design. In section 3, three procedures are proposed to satisfy system features. Section 4 concludes this article.

2 System Architecture

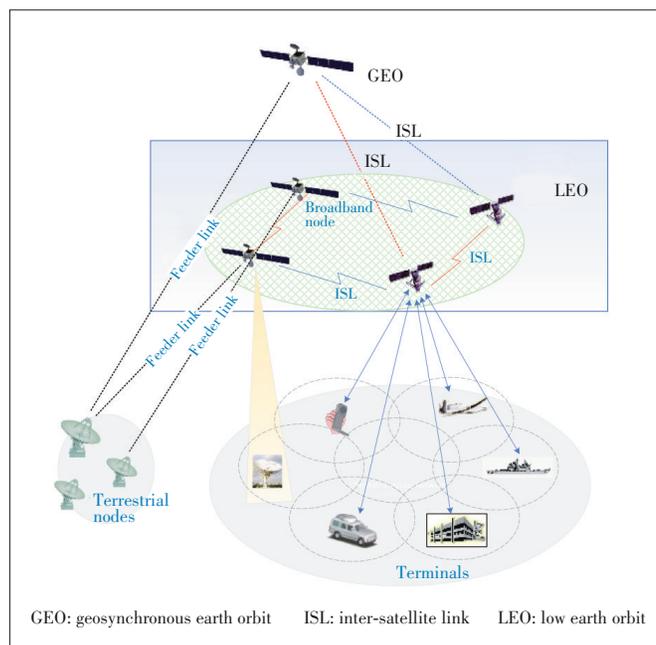
From Ref. [10], the architecture of space-based access network is shown in **Fig. 1**. According to this architecture, as satellite based IoT is the supplementary and extension of terrestrial IoT, the compatibility between two systems should be considered in architecture design. From the aforementioned background, a space-terrestrial integrated architecture is conceived for ST-IoT, which is depicted in **Fig. 2**, and can be used in the space-terrestrial integrated network^[10] and satellite Internet^[11]. The whole system consists of space backbone network (SBN), space access network (SAN), terrestrial access network (TAN) and core network (CN). To be noticed, from the aspect of space-terrestrial integration, ST-IoT shares the identical CN with the terrestrial system. Following of this section mainly focuses on illustrating the space part of the architecture.

In ST-IoT system, the space section aims at user addressing, access control and session management. Therefore, in Fig.2, core access and mobility management function (AMF) and session management function (SMF) have been extended into space part. Meanwhile, space system has unique resource allocation and management mechanisms, thus these two function nodes can be integrated with space-terrestrial integrated manage-control center (STIMCC). This integration is recognized as the terrestrial section of control plane (TSCP), i. e., space-terrestrial integrated control gateway

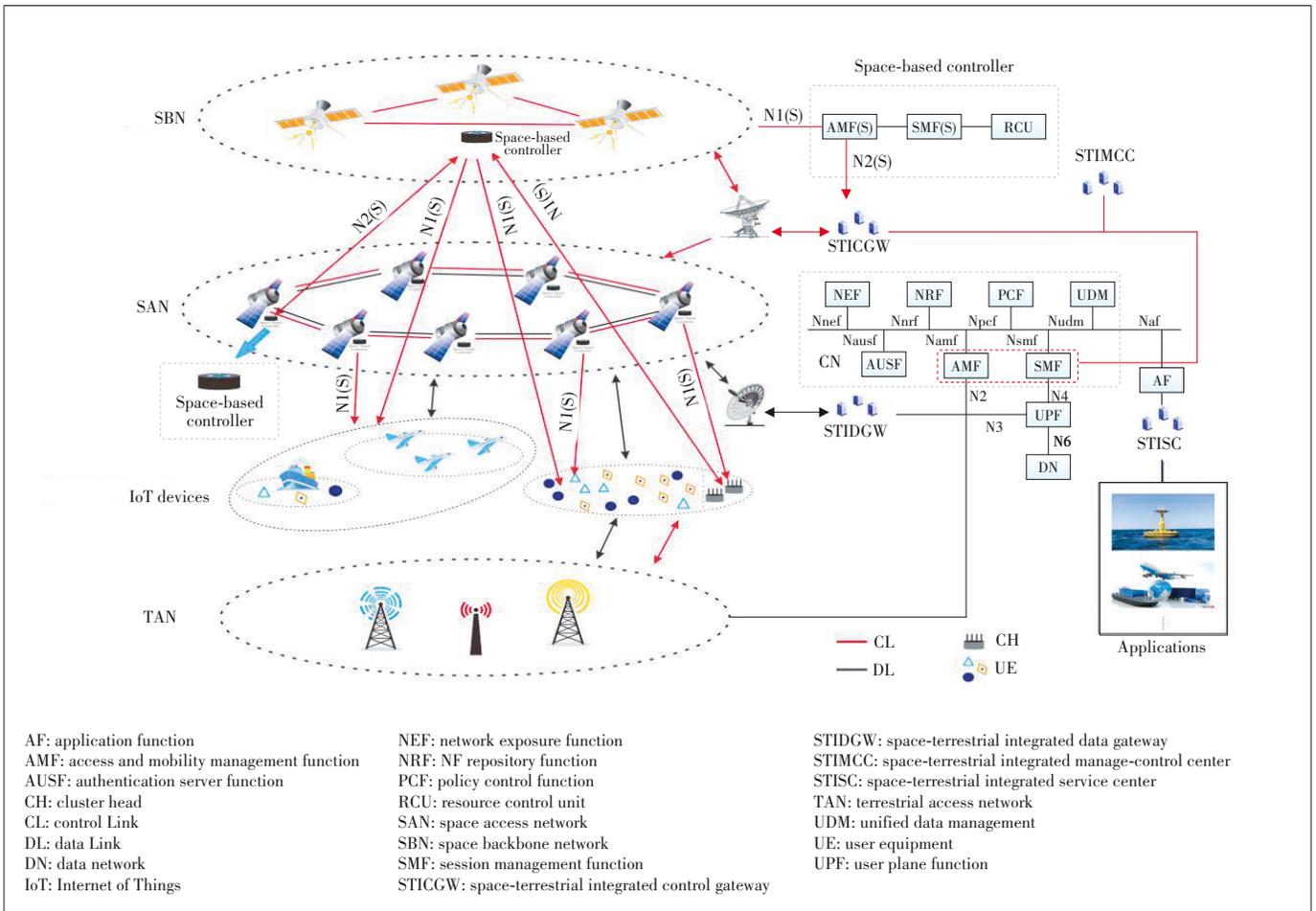
(STICGW), which aims to transmit CN control commands and space resource allocation commands to the space control plane (SCP). In this architecture design, SCP consists of both SBN and SAN nodes. In view of the platform ability, space-based controllers (SBC) deployed on SBN nodes mainly utilize the broadcasting beam on geosynchronous earth orbit (GEO) satellite to efficiently transmit control commands to the low earth orbit (LEO) satellite and IoT terminals within the coverage area. As the supplementary and back-up of the former kind of SBC, SBC deployed on SAN nodes focuses on hot-zone and areas that SBN cannot cover. As shown in Fig. 2, the N2(S) reference point (RP) is used to transmit control signals between two kinds of SBC, in order to perform resource allocation in SAN. Meanwhile, to match TSCP, SBC has on-board AMF and SMF, and receives resource control command through resource control unit (RCU).

Moreover, as shown in Fig. 2, for controlling IoT terminals, the N1(S) RP may be used to transmit access control and resource control information to the terminals. Meanwhile, parts of connection oriented (CO) IoT terminals can also utilize their N1(S) RP to make access request to SBC. When the request has been approved, the IoT terminal can initiate data transmission to the corresponding access node. In the data plane, data converged from SAN and TAN will be sent to CN via space-terrestrial integrated data gateway (STIDGW).

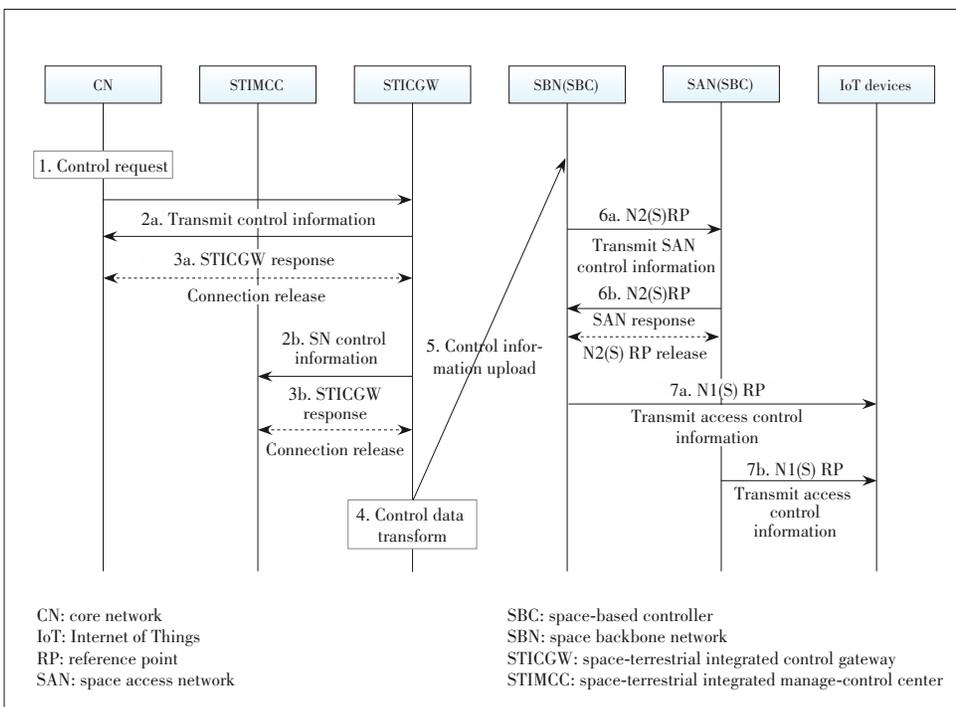
Then, we will introduce the procedures belonging to the space part. Specifically, the procedure of the control plane for ST-IoT is shown in **Fig. 3**. AMF and SMF of CN may be activated to transmit control information to STICGW, and STIMCC may be also utilized to transmit space resource control information to STICGW. The control information will be



▲ **Figure 1. Architecture of space based access network.**



▲ Figure 2. Conceived architecture for IoT.



▲ Figure 3. Procedure of control plane for space-terrestrial based IoT (ST-IoT).

converged and transformed in STICGW, and then transmitted to SBC via control link. Due to the current deployment limitation of STICGW, the control information will be transmitted to SBC on SBN nodes. While SAN nodes are flying across SBN coverage areas, SBC on SAN nodes will utilize N2(S) RP to receive control information. After that, SBCs belonging to different networks will operate predefined rules to transmit access control information via N1(S) RP to IoT terminals.

For IoT terminals, since several deployment areas like aerial, maritime and some remoted land locations are not covered by TAN, ter-

minerals in aforementioned areas can only transmit through SAN. When an area is covered by both TAN and SAN, IoT terminals can choose appropriate network according to factors like traffic requirements and device ability. The main features of IoT terminals are listed in **Table 1**.

3 Highly Efficient and Reliable Procedure Design

3.1 Reliable Identification Procedure Design

ST-IoT system faces numbers of challenges including massive access, lack of on-board and frequency resources. Due to these problems, it is significant to make sure that only certified terminals can get access to the system. Therefore, in this sub-section, an identification procedure is discussed, which is depicted in **Fig. 4**. The procedure is divided into five steps, which will be illustrated as follows.

Step 1: When users pay for registering their IoT terminals, the unified data management (UDM) function node in CN will send registration information to authentication server function (AUSF) via RP N13. After that, UDM and AUSF will report terminals' registration information to AMF(T) via RP N8 and N12, respectively.

Step 2: AMF(T) utilizes service key (SK) to encrypt registered user's key (UK) to generate encoded manage message (EMM), and then sends SK and EMM to SBC.

Step 3: AMF(S) in SBC will encrypt SK with control word

(CW) to generate encoded control message (ECM). CW is a group of random numbers used to encrypt data stream and to decode data in the receivers. Meanwhile, CW is also used to initiate the pseudorandom sequence generator (PRSG) to scramble the access control information (ACI), which mainly contains SAN nodes' condition, system parameters, and other control commands initiated from network side. It is generated by SBC and CN.

Step 4: SBC utilizes multiplexer to multiplex ECM, EMM and encrypted ACI into transmission stream. To be noticed, EMM will be penetrated into the stream every 6 - 8 seconds. To decode CW from ECM, terminals should be proven that they have been registered.

Step 5: At the receiver, IoT terminals use demultiplexer to demultiplex data stream, and use UK to decode encrypted EMM to achieve SK. Then, SK can be used to decode encrypted ECM, thus achieving CW. Finally, IoT terminals use CW to get full ACI and continue the follow-up operation.

3.2 Integrated Access and Communication Procedure

The common features of IoT traffic can be summarized as random access, high concurrency, and short burst. However, the wide coverage, long latency, high dynamic feature of LEO satellites will bring huge challenges to design ST-IoT transmission mechanisms. In ordinary access process, before traffic data transmission, numbers of operations should be finished by terminals. Under the restraints of LEO satellites, the access process has to satisfy the demands of low control

▼Table 1. IoT terminals features: (a) AN types; (b) Device types

(a)							
AN Type	Operation Mode		Operating Procedure		Corresponding Terminals		
SAN	ACIO		SBC broadcast access control information, IoT terminals access to SAN nodes via random access scheme		Regular IoT terminals deployed in aerial, maritime, remote areas; Low QoS demand terminals in hot-zone.		
	CO		IoT terminals initiate access request to SBC, SBC response request with specific resources (time, frequency, access node). IoT device transmit data to corresponding access node.		Converging cluster head terminals; High QoS demand terminals.		
TAN	IoT		Terminals in TAN coverage areas.				

(b)							
Device Type	Amount	Typical Application	Data Rate	Operating Mode	Traffic Feature	Typical Environment	AN node
Regular device	Large	Collecting, tracking	Low	ACIO/CO/TI	Short burst	Aerial, maritime, land	SAN/TAN/Cluster head
Converging cluster head terminals	Low	Converged collecting	High	CO	Long packet	Land	SAN
High QoS terminals	Low	Monitoring	High	CO/TI	Stream	Aerial, land	SAN/TAN
High security terminals	Low	Sensitive data transmission	Low	ACIO	Short burst	Sensitive areas	SAN

ACIO: access control information oriented
 AN: access network
 CO: connection oriented

IoT: Internet of Things
 QoS: quality of service
 SAN: space access network

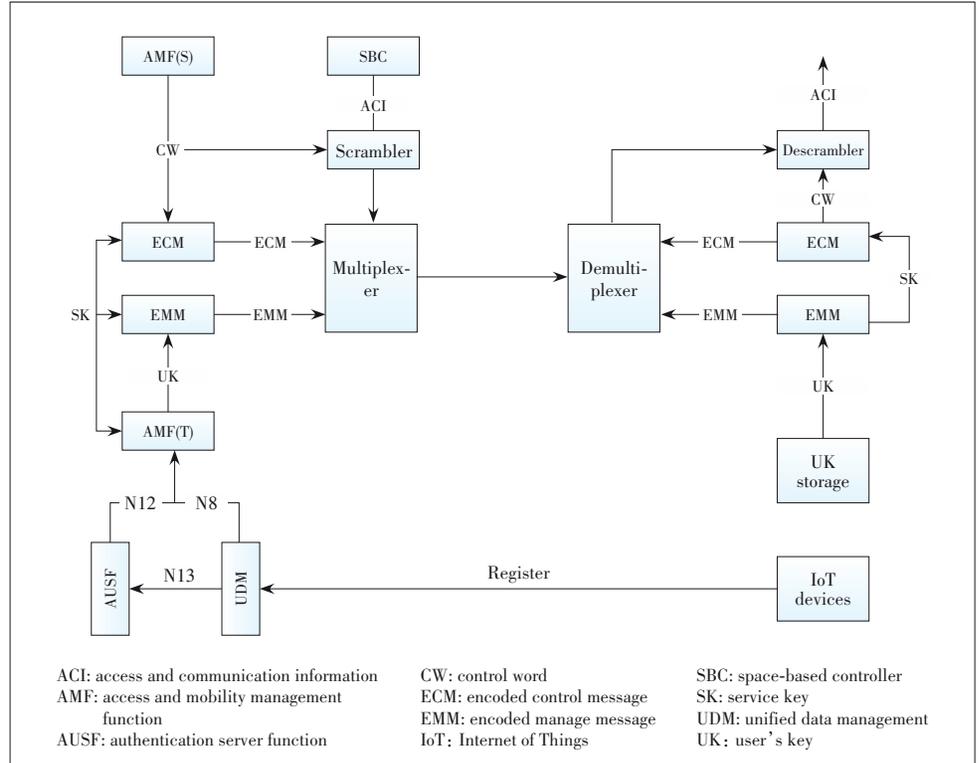
SBC: space-based controller
 TAN: terrestrial access network
 TI: terrestrial IoT

and less coordination. The most significant problem that ST-IoT faces is massive concurrent uplink access requests caused by wide coverage. According to aforementioned illustration, frequent interactive control mechanism does not satisfy the demand of ST-IoT system. Therefore, in this subsection, an integrated access and communication procedure is presented, which is depicted in **Fig. 5**. This procedure mainly focuses on massive regular IoT terminals, which have relatively low quality of service (QoS) requests and are insensitive to time-latency. At the beginning of the procedure, IoT terminals will be awakened by their built-in triggers and then turn into monitoring mode. Once a terminal receives ACI from an SBC (following the frame illustrated in Section 3.1), it will package its own ID with traffic data and then transmit the packed data to its corresponding SAN node. After these operations, the IoT terminal will immediately turn into sleep mode for saving energy purposes. User data will be converged and recovered in SAN earth gateway station (EGS), and then EGS, STIDGW and CN will finish the similar terrestrial IoT traffic procedure (3GPP Rel-13), where EGS represents terminals and STIDGW represents eNodeB.

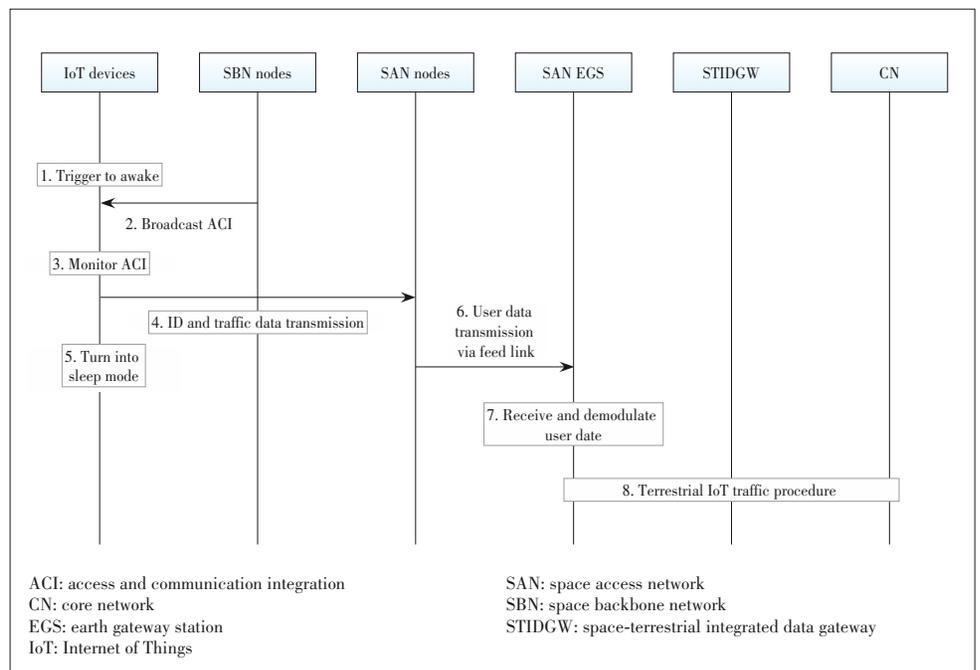
3.3 Clustering Cooperative Transmission Strategy

In ST-IoT system, SAN coexists with TAN, which means that multi-mode terminals can access both SAN and TAN in co-coverage areas, where TAN usually has higher access priority. However, when concurrent access requests exceed TAN's capacity, it is necessary to coordinate TAN and SAN in order to realize load balance between two networks. Considering the different deploying locations of terminals, the possible network coverage situation can be categorized as follows.

- (1) Multi-network coverage area, where network coordination is required to maintain concurrent access requests and ensure load balance between TAN and SAN;
- (2) Single-network coverage area, where IoT terminals will attempt to access in available network.

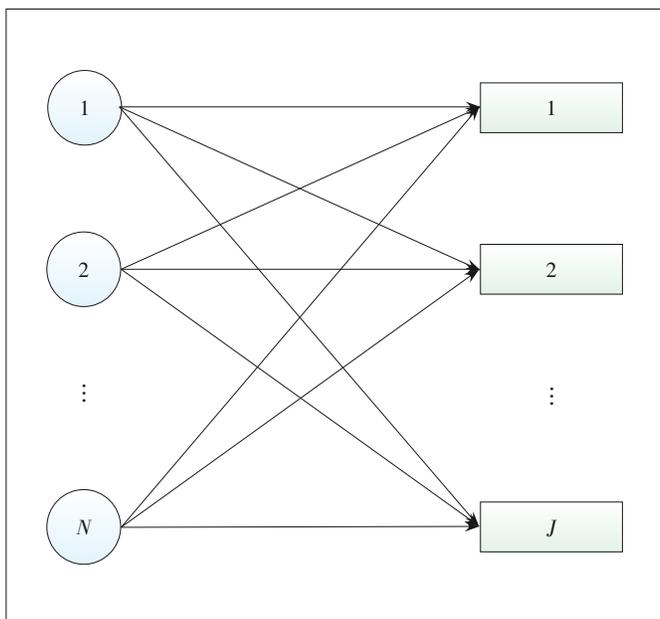


▲ Figure 4. Procedure of reliable identification.

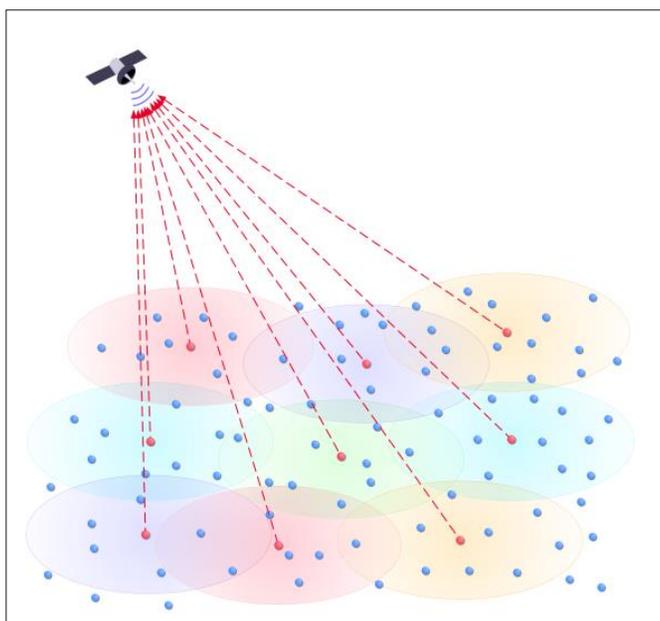


▲ Figure 5. Integrated flow of access and communication.

In the first case, assuming that at time t , there are N IoT terminals, and J available access networks, as shown in **Fig. 6**. Considering K factors (e. g., distance, number of terminals, channel state information, etc.), multiple attribute decision making^[12] can be utilized to perform the matching among IoT terminals and available networks. In the second case, a satellite-coverage-area, as shown in **Fig. 7**, due to the limitation of spatial resolution and frequency resources, IoT terminals within a single beam cannot avoid collisions in the presence of massive connections. To reduce colliding probability, a clustering transmission strategy is introduced in this section. This



▲ **Figure 6. Multi-terminal and multi-network matching.**



▲ **Figure 7. Clustering cooperative transmission strategy.**

strategy has two steps, namely cluster head election and terminals access.

It is necessary to clarify that the amount of cluster head within a single beam is up to C , which further divides the coverage area into C grids. Assuming that there are N IoT devices in grid m , the cluster head in this grid can be elected via the following function:

$$c_m = \arg \max_{i,i=1,2,\dots,N} f_m(h_i, n_i, e_i) \\ s.t. \quad e_i \geq 0.5E \\ n_i \leq D,$$

where c_m is the ID of elected cluster head node, and h_i, n_i , and e_i represent the link condition, node amount in coverage area, and battery level of node i , separately. Besides, E is the maximum energy of a node, and D is the node amount upper bound that a cluster head node can afford.

For cluster head election, link condition, battery level and node location are the essential factors to be considered. After cluster head election, IoT terminals will choose to access appropriate head, relying on the attributes of distance, node amount in coverage area, and link condition.

4 Conclusions

In this paper, we investigated a space terrestrial integrated network oriented IoT, where massive IoT terminals can access both the space network and the terrestrial network. We conceived a space terrestrial integrated architecture for supporting massive connections. Moreover, we also discussed some technical issues of ST-IoT, including reliable identification method, access and communication integrated flow, and clustering cooperative transmission strategy. To further improve the tolerable number of IoT terminals, more efforts should be devoted in both innovative fundamental theory and sophisticated experiments.

References

- [1] CHIEN W C, LAI C F, HOSSAIN M S, et al. Heterogeneous space and terrestrial integrated networks for IoT: architecture and challenges [J]. IEEE network, 2019, 33(1): 15 - 21. DOI:10.1109/mnet.2018.1800182
- [2] HU D, HE L, WU J. A novel forward-link multiplexed scheme in satellite-based internet of things [J]. IEEE Internet of Things journal, 2018, 5(2): 1265 - 1274
- [3] QU Z C, ZHANG G X, CAO H T, et al. LEO satellite constellation for Internet of Things [J]. IEEE access, 2017, 5: 18391 - 18401. DOI: 10.1109/access.2017.2735988
- [4] PAVARANGKON P, MURATA K T, OKADA M, et al. Bandwidth utilization enhancement using high-performance and flexible protocol for INTEL-SAT satellite network [C]//2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Vancouver, Canada: IEEE, 2016: 1 - 7

- [5] MORRIS E, LEVINE L, CMEYERS, et al. System of systems interoperability (SOSI): final report [R]. Pittsburgh, USA: Carnegie Mellon University, 2004. DOI: 10.1184/R1/6584534.v1
- [6] SCHROTH K, BURKHARDT N, CHE T-S, et al. IP networking over the AEHF MILSATCOM system [C]//IEEE Military Communications Conference (MILCOM). Orlando, USA: IEEE, 2012:1 - 6
- [7] BENZERROUK H, NGUYEN Q, FANG X X, et al. Alternative PNT based on Iridium next LEO satellites doppler/INS integrated navigation system [C]// 26th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS). Saint Petersburg, Russia, 2019: 1 - 10
- [8] JIANG Y N, GE X H, ZHONG Y, et al. A new small-world IoT routing mechanism based on cayley graphs [J]. IEEE Internet of Things journal, 2019, 6(6): 10384 - 10395. DOI:10.1109/jiot.2019.2938800
- [9] WANG P, ZHANG J X, ZHANG X, et al. Convergence of satellite and terrestrial networks: a comprehensive survey [J]. IEEE access, 2020, 8: 5550 - 5588. DOI:10.1109/access.2019.2963223
- [10] YAO H P, WANG L Y, WANG X D, et al. The space-terrestrial integrated network: an overview [J]. IEEE communications magazine, 2018, 56(9): 178 - 185. DOI:10.1109/mcom.2018.1700038
- [11] AZUA D Z, CALVERAS A, CAMPS A. Internet of satellites (IoSat): analysis of network models and routing protocol requirements [J]. IEEE access, 2018, 6: 20390 - 20411. DOI:10.1109/access.2018.282398
- [12] BISIO I, MARCHESE M. Satellite earth station (SeS) selection method for satellite-based sensor networks [J]. IEEE communications letters, 2007, 11 (12): 970 - 972. DOI:10.1109/lcomm.2007.071246

Biographies

ZHANG Gengxin received his bachelor, master and Ph.D degrees in 1987, 1990 and 1994 respectively, all from Department of Radio Communication Engineering, Nanjing Institute of Communication Engineering, China. He is currently a professor in Nanjing University of Posts and Telecommunications, China. His research interests include satellite communications, deep space communications and space information network, where he has headed several projects.

DING Xiaojin (dxj@njupt.edu.cn) received the Ph.D. degree in information and communication engineering from National Mobile Communication Research Laboratory, Southeast University, China. He is currently an associate professor in Nanjing University of Posts and Telecommunications, China. His research interests include space information network, cooperative communications, and physical-layer security.

QU Zhicheng received the B.S. degree in telecommunication engineering from Xi'an University of Posts and Telecommunications, China in 2010. He is currently pursuing the Ph.D. degree in satellite communication with the Institute of Satellite Communication, Nanjing University of Posts and Telecommunications, China. His research interests include physical and link layer issues for satellite communications and space information networks.