Insight Into the Architecture and Technology of Smart Identifier Networks

Zhibo Fan*[a]

[*] Corresponding author: 2547837532@qq.com

[a] School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan, Hubei 430081, China

Abstract: The traditional Internet adopts a host-centric data transmission mode, and data are repeatedly transmitted between different computers, resulting in vast network traffic and low transmission efficiency. With the rise of the information-centric content sending mode, the traditional Internet has been unable to meet growing business needs. In this context, smart identifier networks have been proposed as next-generation Internet architectures and were initially applied in the industrial Internet, Internet of things and other fields. As the research direction of future network architecture, smart identifier networks are currently mainly deployed in the field of industrial manufacturing. It still needs to explore efficient applications on the Internet of Vehicles, Space-Earth Integration Networks, data centers and other scenarios to meet the needs of current new business in the short term, fundamentally solve the shortage of network architecture in the long term and supply a good development environment for future identification applications.

Keywords: Smart Identifier Network, Computer Network, Future Internet Architecture, Identifier Networking, Next-generation Networking

1 Introduction

Traditional network architecture has many shortcomings in security, mobility and energy consumption due to the network characteristics of triple binding (control and data binding, user and network binding, resource and location binding), which seriously hinders its further development. To solve the above challenges, governments around the world have started future network research projects. The National Science Foundation (NSF) launched the GENI program in 2005 and the FIND program in 2006. NSF published the FIA program in 2010, launched the US IGNITE program and CNS program in 2012, and launched the FIA-Next Phase program in 2014 to design the Next Generation Internet. In 2018, the United States and the European Union launched the EU-US collaboration on the NGI program, which aims to strengthen cooperation and strategic partnership in the field of next-generation Internet to promote common development [1]. SINET (smart identifier network) was proposed by the National Engineering Laboratory of Next Generation Internet Interconnection Equipment of Beijing Jiaotong University, aiming to solve the triple binding problem fundamentally and overcome the limitations of the existing Internet.

A smart identifier network is a new network architecture that realizes the triple separation of "identity and location separation", "control and forwarding separation", and "resource and location separation" through "three layers and two domains" and can flexibly and dynamically

ITEI 2023, November 24-26, Zhengzhou, People's Republic of China

DOI 10.4108/eai.24-11-2023.2343580

compose network security services to meet users' complex and diverse security service requirements. In multiple experimental tests, SINET has been shown to improve performance in many aspects compared to traditional network architectures, and because of its overall design concept of future Internet architecture, it can be compatible with existing facilities [2]. In terms of meeting the needs of growing businesses in the short term, SINET has been proven to be more efficient than traditional network architectures. SINET has been applied to communication and data transmission in high-speed railway networks due to its advantages in mobility support and multidimensional resource cooperation. To meet the challenges of heterogeneous network integration and effective differentiated routing faced by satellite networks, SINET realizes the integration and routing optimization of satellite and ground networks by decoupling the identity and location information of the network and terminal [3].

As an important research direction of the next generation Internet, there is no comprehensive review of smart identifier networks in the literature. This paper aims to summarize main concepts and key technologies of SINET, analyze the relevant network architectures, and introduce typical application scenarios of SINET and corresponding challenges and opportunities. Compared with previous review papers, this paper presents the latest and most comprehensive research progress of smart identifier networks.

The rest of this paper is organized as follows. Section 2 provides an overview of SINET. Section 3 analyzes relevant network architectures. Section 4 summarizes the key technologies of SINET. Section 5 introduces typical application scenarios of SINET. Section 6 analyzes the challenges and opportunities faced by SINET.

2 Overview of sinet

The smart identification network creatively proposes a "three-layer, two-domain" system architecture (Fig. 1) through the triple separation of "identity and location separation", "control and forwarding separation" and "resource and location separation". The "three layers" are the smart service layer (SSL), the resource adaptation layer (RAL) and the network component layer (NCL). The smart service layer is responsible for service identification, description, search, and dynamic matching; the resource adaptation layer is responsible for sensing service requirements from the smart service layer, and the network resource status of the network component layer dynamically adapts network resources; the network component layer is responsible for data storage and forwarding, as well as behavior perception and clustering functions. The "two domains" refer to the entity domain (ED) and the behavior domain (BD). The entity domain is responsible for identifying execution units such as network services, network groups, and functional components; the behavior domain is responsible for dynamically characterizing the attribute characteristics of network services, network groups, and functional components.

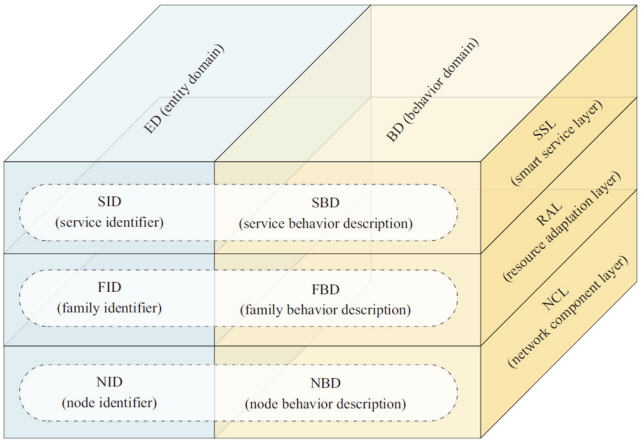

Figure 1 The architectural design of smart identification network [3].

In the smart identifier network, the entity domain uses the Service ID (Service ID, SID) to mark the service to realize the "separation of resources and locations" of the service; the family ID (Family ID, FID) is used to mark the functional modules of the network family, and the component identification (Node ID, NID) marks network components to realize the "separation of control and forwarding" and "separation of identity and location" of the network; the behavior domain uses Service Behavior Description (Service Behavior Description, SBD) to represent the characteristics of service identifiers in the entity domain; Family Behavior Description (FBD) is used to characterize the salient features of group behavior; and Node Behavior Description (NBD) is used to further describe the topology and function of network components.

3 Related architectures

3.1 Software defined networking

Software Defined Networking (SDN) was proposed in 2008, which achieves efficient and flexible network management and control with separated network control and data planes [4]. The SDN architecture defined by the Open Network Foundation (ONF) includes the infrastructure layer, the control layer, the application layer and the interface between each layer, which is shown in figure2. The infrastructure layer is responsible for the forwarding and processing of data packets and the network equipment operational state management. The control layer is responsible for controlling and managing the infrastructure layer. And the application layer provides network services and business requirements [5]. In the SDN architecture, infrastructure, controllers and applications are not limited to existing software, hardware, virtualization or physical form. Its core technology, OpenFlow, enables the separation of the control plane and forwarding plane of network switching/routing devices, and the controller calculates and issues forwarding/routing rules uniformly in the network. SDN has changed the traditional IP network structure and realized the centralized control of network logic, but it has not changed the traditional TCP/IP layered model and packet forwarding mode.

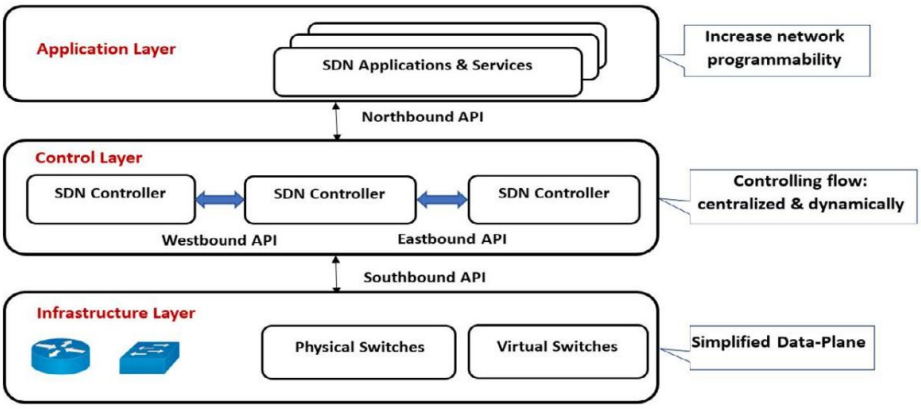

Figure 2 The schematic diagram of SDN layers [4].

3.2 Network function virtualization

The European Telecommunications Standards Institute (ETSI) established the NFV Industry Specification Group (Industry Specification Group, ISG) in 2012. Network function virtualization (NFV) is a new type of network technology which aims to change the way network operators build networks through IT virtualization technology. While reducing capital and operating expenses, virtualization technology deploys network functions in the form of software to enhance network flexibility and dynamically provide services on demand. The NFV architecture released by ETSI NFV ISG includes Network Function Virtualization Infrastructure (NFVI), Virtualized Network Function (VNF), and Network Function Virtualization Management and Orchestration (NFV M&O), as shown in figure 3. NFVI is responsible for virtualizing hardware resources and providing virtual resources to VNF; VNF corresponds to the network nodes of traditional networks and is responsible for data forwarding and storage based on pure software deployment; NFV M&O is responsible for the management tasks of virtualization, including orchestration and life cycle management of physical or software infrastructure resources, while interacting with external operation/business support systems, integrating NFV into the existing network management environment. A VNF forms a network service (network service, NS) by linking with other VNFs or physical network functions. In end-to-end service, according to the resource requirements and remaining resources of the NS, appropriate VNF placement and link selection meet user service needs and key decisions for the efficient use of infrastructure resources [6].

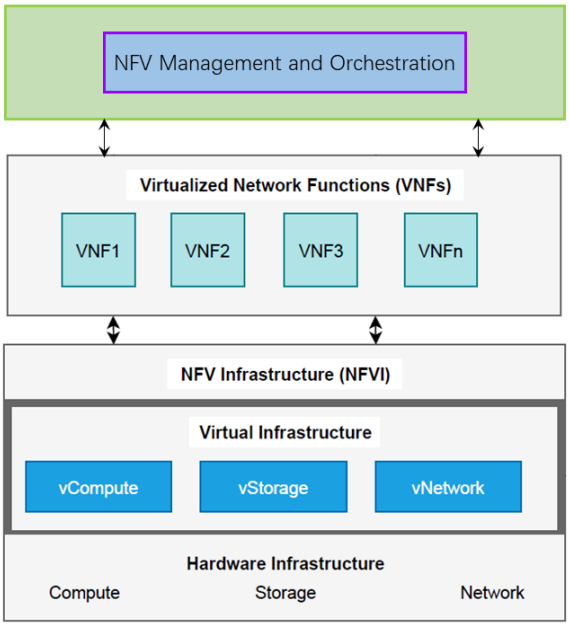

Figure 3 ETSI NFV architectural framework

3.3 Network function chains

Network providers deploy service functions (service functions, SFs), such as firewalls, intrusion detection systems, and WAN accelerators, while providing network services [7]. Network function chains (NFC) are a group of network functions arranged in a certain order. The deployment of NFC needs to rely on dedicated hardware devices, which is not only expensive but also brings a series of efficiency problems due to the need to be coupled with the network topology during application [8]. With the development of NFV, the deployment of SF can rely on standard servers that support virtualization. With the support of SDN, NFC can be decoupled from the network topology and deployed in the network in the form of VNF to form a VNF chain [9]. The SFC structure defined by the IETF SFCWG is mainly divided into network domains and NFV infrastructures that support SFC chains. Data packets are classified and encapsulated when passing through the service domain entrance of the network domain and matched to different services. After the path is processed by various SF combinations. In NFV, there are two mappings: virtualization of physical resources and integration of virtual resources. The first mapping virtualizes the physical resources that can be provided by the infrastructure into corresponding virtual resources, and in the second mapping, the virtual resources are combined with the available resources. Service resources are matched, integrated and allocated to corresponding VNFs.

3.4 Information centric networking

The "host-centric" design mode of the traditional network architecture makes the information transmission process have to rely on the end-to-end connection between the hosts. With the development of the information network, many problems have been exposed in the binding of

information and location in the traditional network architecture [10]. The emergence of Information Centric Networking (ICN) is precisely to decouple this binding and convert the "host-centric" that users do not care about into "information-centric", and information can be located in any location of the network, but the information content has a unique name. Figure 4 shows the evolution of ICN since Cheriton first introduced it in 1999 while solving name-based routing in the Translation Relay Internet Architecture Integrated Active Directory (TRIAD) architecture. When the user needs to obtain certain information, the network retrieves the content according to the information name, and since ICN starts from the information itself, it can implement a customized encryption mechanism for the information content according to the needs [11]. There is a cache mechanism in the ICN node, and the transmission resources are cached according to the node cache selection algorithm, making full use of network storage resources and reducing the problem of repeated transmission of the same content by similar network devices.

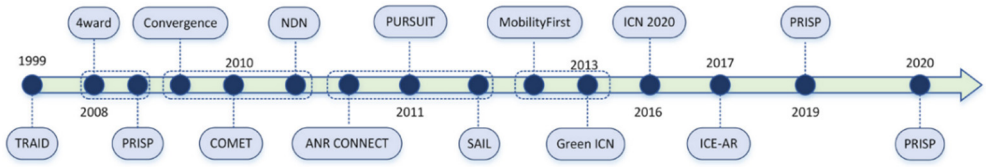

Figure 4 Timeline of ICN evolution over the past few decades

4 Key technologies of sinet

4.1 Security

With the application and development of smart networks, network access devices are increasing exponentially, making it easier for attackers to attack the network through access devices, posing a huge challenge to network security [12]. Due to its special service mechanism, SINET has a certain resistance to network attacks such as DNS spoofing attacks, IP address spoofing attacks, DDoS attacks, and link flooding attacks that are common in traditional networks [13]. However, attackers may still search for new attack methods by analyzing the basic structure of SINET, causing SINET's network core to crash, request invalidation, data leakage and other security issues, creating new network security threats to SINET. Constructing a security mechanism compatible with SINET and exploring the network security of SINET are the key technologies of SINET.

The core network is composed of mapping servers and core switching routers. The mapping relationship between access identifiers (Access IDentifier, AID) and routing identifiers (Routing IDentifier, RID) is controlled by the mapping system to prevent network attacks, while users in the access network. The way the access router connects to the core network has security issues and is vulnerable to attacks. An AID shuffling mechanism is designed to ensure individual rationality, budget balance and authenticity [14]. Figure 5 shows the basic architecture of identifier network and AID shuffling mechanism. The optimal solution is obtained with the minimum computational complexity, the maximum number of successes is achieved, and the dynamic identifier allocation problem is effectively solved.

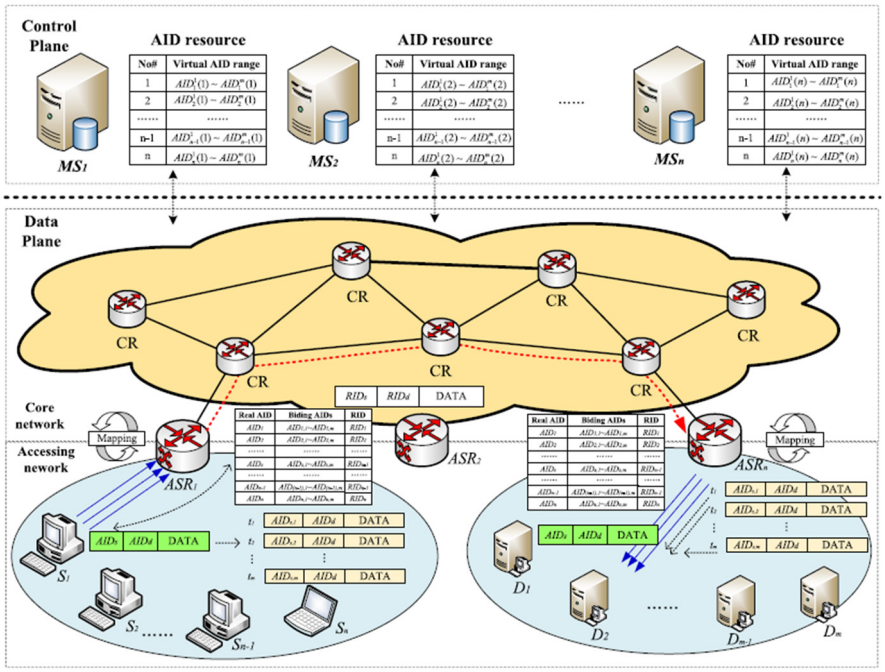

Figure 5 The architectural design of identifier network and its AID shuffling mechanism [14].

Existing network authentication mechanisms have security risks due to excessive reliance on network-specific certificate systems and affect network performance [15]. A security authentication mechanism based on MDINet is proposed by using a combined public key cryptosystem [16]. A set of authentication mechanisms are designed, and while meeting the needs of future networks, it has an insignificant impact on ordinary communication. Because of the complexity of traditional authentication operations in the early implementation of a railway intelligent collaborative network, a new chaotic random number generator was designed in [17], which can adapt to different programs by changing the length of the one-time password. The authentication mechanism uses lightweight identity authentication to overcome its own shortcomings while replacing the existing identity authentication with complex handshakes and a large amount of redundancy. It is not only suitable for fast mobile scenarios with short session connection life cycles but also for communication resources. Scenarios with limited and compromised connectivity.

The emergence of 5G networks has brought potential network security threats to massive terminal connections entering the Internet and is seriously affecting the security barriers. However, existing security protection solutions are too singular to isolate threats, and other reasons cannot effectively eliminate hidden dangers. A comprehensive investigation and summary of existing security solutions are conducted in [18], proposed a multidimensional fine-grained control (multidimensional fine-grained control, MFC) framework, and constructed a complete set of MFC authentication through the setting of wireless environment parameters. The prototype system modifies the system kernel while testing the superiority of the framework

and deepens the concept of "service classification" in further optimization, which has a considerable reference for the "information-centered" SINET network.

4.2 Caching

As a new type of future network architecture, SINET's "information-centric" design concept is different from the existing "host-centric" network, and it may be difficult to adapt to the current mainstream caching mechanism. However, with the emergence of large-scale access devices, the occurrence of duplicate traffic has increased. How to make reasonable use of the network cache, improve user experience, and reduce network pollution makes the cache mechanism for SINET a key design technology.

Due to the "information-centered" design concept and the realization of "separation of resources and location" and "separation of data and control", SINET has two major features in the caching mechanism: (1) Uniquely name the network service content and cache it in among some network components of SINET; (2) SINET can not only perceive the status of data cache and link throughput in real time but also control the storage of the cache system through the resource manager. These two characteristics make the performance of the cache mechanism designed for SINET surpass the current mainstream cache mechanisms such as Greedy, LCE, LCD, ProbCache and Random. Based on this, [19] proposed a crowd-based collaboration cache (C2Cache), which dynamically creates and perfects the cache function cluster by sensing the actual topology of the network and executes the maximum benefit caching algorithm in units of clusters. This can effectively improve the cache hit rate.

With the advent of the Internet of Things era, the connection between the Internet and people's lives has been further strengthened, Internet users have continued to increase, and global IP traffic has shown explosive growth. Based on a large-scale access convergence network, [20] proposed a "proximity" caching mechanism, which unicasts hotspot content to a large-scale access convergence router (Access Convergence Router, ACR) at the edge of the core network and then multicasts. The content cached by ACR is dynamically distributed to users to realize "integration of storage and transmission", and the separation of users and forwarding makes it easier to realize "the smallest world network". As a new network architecture, SINET also needs to consider the caching mechanism.

Internet of Vehicles poses a huge challenge to content distribution due to its high intermittent connection characteristics and the need to consider the universality of the wireless environment of the network. Aiming at the network content distribution scenario in the highway scenario, [21] proposes a content caching and retrieval strategy based on heat perception applied to vehicle ad hoc networks and proposes a novel popularity calculation method. Two retrieval modes switched according to the popularity level value and an active caching mechanism to deal with the peak value of the requested content are proposed. Based on this, SINET can design a corresponding high-speed session caching mechanism to cope with content distribution scenarios under different conditions.

Although the caching mechanism based on the "user-centered" design in the traditional network architecture is not suitable for SINET, its achievements over the years are still of reference significance for the caching mechanism of SINET. The delayed caching mechanism has received attention. Mobile edge caching reduces end-to-end latency by storing files in base stations. [22] proposes a greedy content placement algorithm based on large-scale mobile

network cooperative caching, which achieves (1-1/e) optimality; in addition, specific maximum cluster size constraints are given. The algorithm can reduce the file transfer delay by an average of 45%.

5 Typical application scenarios

5.1 Internet of things

The Internet of Things (IoT) network architecture is composed of information sensing devices such as infrared sensors, radio frequency identifiers (RFIDs), laser scanners, and GPS/Beidou locators, aiming at connecting any item to the Internet through the network, realizing the exchange and communication of information, completing the intelligent identification, positioning, tracking, monitoring and management of items through the Internet, and emphasizing that all objects (including people and machines) linked to the Internet have unique addresses and communicate through wired or wireless networks. The Internet of Things will have a huge impact on many aspects of human production and life. Whether it is industrial production, logistics transportation or daily life, the use of Internet of Things devices is growing rapidly.

The smart identifier network was initially applied to the Internet of Things. And the IoT identity modeling and identity addressing was a typical challenge [23]. Table1 shows the classified IoT identity addressing and Internet addressing. Ning et al. also discussed a series of challenges in applying the smart identifier network to the Internet of Things, including ease of use, semantics, exchangeability and selective perception in modeling, intelligent, decentralized and precise addressing services, security and privacy [23]. Liu et al. proposed a new variable-length identifier (variable-length identifier, VLI) solution for interconnected IoT networks, which aims to effectively support flexible identifier fields [24]. After the base VLI header, one or more extension headers can be added if desired. Each extension header contains a fixed-size identifier field. Depending on the combination of multiple identifier fields, IoT nodes can easily implement, parse and support variable length identifiers. Experimental results show that VLI can effectively reduce processing delay compared with fixed-length identification schemes.

Table 1 Classification and comparison of IoT Identity Addressing

Essential Method	Internet Addressing	IoT Identity Addressing
IP and URI	DNS	ONS
E.164 and URI	ENUM	
Low power and IPv6	N/A	6LoWPAN
URN	URN	Handle System
URI and XML	Web Service	
Intelligent Addressing	Search Engine, Semantic Understanding, Knowledge/Relationship Graph	

5.2 Integrated satellite-terrestrial network

To expand the coverage of the Internet of Things, including areas that are difficult to cover by ground networks, thereby providing ubiquitous connections and bringing more people a smarter life, telecom operators and related communication companies are looking for global solutions

based on the Internet of Things. Comprehensive solutions are covered. The working areas of logistics, solar energy, oil and gas extraction, offshore monitoring, agriculture, environmental monitoring, mining and other industries cannot be covered by terrestrial cellular networks. The presence of wide-area IoT is critical for network communication in these remote areas where terrestrial cellular networks cannot cover or have low connectivity. From this perspective, satellite technology that can be integrated with the existing terrestrial Internet of Things is a feasible method. Satellites will therefore play a special and important role in the IoT ecosystem, covering remote geographic areas where terrestrial networks are unavailable or inaccessible, such as on remote land (forests, deserts, etc.) and at sea. Satellites and 5G networks are showing a trend of integrated development [25]. The development of satellites and 5G technologies has laid the foundation for integration. As a supplementary extension, satellite communications have enhanced the capabilities of 5G networks. Satellites have extended the spatial dimension of ground networks. Satellites can achieve high reliability and high secure global coverage communications. Therefore, the complementarity between satellite communications and terrestrial 5G communications is greater than competition, and the integration of the two is the future development trend.

The smart identifier network was initially verified in the star-earth fusion network. Yao et al. designed a new heterogeneous wireless network architecture called SI-STIN, which applied space and ground integrated network intelligence identifiers [26]. And they analyzed and verified the performance of SI-STIN in terms of network security and transmission efficiency, and it has great potential in meeting various network requirements. Based on the idea of a smart identifier network, a network architecture called SAT-GRD was proposed, which aims to realize the efficient integration of satellite and ground networks. Specifically, SAT-GRD separates the identity and location of hosts and networks [27]. Then, it isolates the host from the network and further divides the entire network into a core network and an edge network. This makes SAT-GRD more flexible and scalable to achieve heterogeneous network convergence and avoid problems caused by IP address semantic overload. And they implemented a proof-of-concept prototype of SAT-GRD and confirmed its feasibility.

6 Research challenges and opportunities

In this section, we discuss the research challenges and opportunities facing smart identifier networks. The discussion in this section mainly summarizes the deficiencies in the existing research to inspire more follow-up research.

(1) Security Challenge

The naming mechanism in the smart identifier network may be analyzed and targeted by attackers. In the smart identifier network, service content is replicated in the network, which can reduce network load and service retrieval delay. However, this kind of content duplication makes the service content farther away from the control scope of the service producer and cannot be effectively verified and controlled. Faced with this security challenge, future research on smart identifier networks needs to conduct in-depth research on service content encryption mechanisms, user identity authentication, and service access authentication.

(2) Routing Challenge

Routing and forwarding are especially important functions of smart identifier networks. An excessively large routing table will occupy the resources of the router, resulting in the inability to respond to legitimate user requests in a timely manner, thereby reducing the overall performance of the smart identifier network. In the face of routing challenges, future research on intelligent identification networks needs to consider routing protocols based on quality-of-service perception, efficient cache placement strategies and cache replacement strategies to improve the cache hit rate of service content.

(3) Deployment Challenge

The future Internet is a complex system that includes multiple network architectures and various network scenarios, such as the industrial Internet and satellite Internet. In such a complex network environment, a large number of users and devices make the large-scale deployment of smart identifier networks difficult. In the face of deployment challenges, future research on smart identifier networks needs to consider how to realize the perception of service resources and network resources under large-scale networks and realize the efficient transmission of service content.

7. Conclusion

In this paper, we present a recent survey of smart identifier networks, including related architectures, key technologies, and typical application scenarios. The related architectures covered in this paper include SDN, NFV, NFC, and ICN. These architectures are inspiring or enabling the development of smart identifier networks. Then, we discuss the key technologies, including security and caching. These key technologies help to boost the applications of smart identifier networks in the Internet of Things and satellite-terrestrial integrated networks. While smart identifier networks are promising for the future Internet, challenges still exist, and research opportunities are discussed in this paper to overcome these challenges and inspire follow-up studies.

References

[1] Huang T., Liu J., Huo R, et al. (2014) Survey of research on future network architectures. Journal of Communications. 2014, 35 (8): 184-197.

[2] Zhang, H., Quan, W., Chao, H. C., & Qiao, C. (2016). Smart identifier network: A collaborative architecture for the future internet. IEEE network, 30(3), 46-51.

[3] Zhang, H., Feng, B., & Tian, A. (2022). A systematic review for smart identifier networking. Science China Information Sciences, 65(12), 1-13.

[4] Aldaoud, M., Al-Abri, D., Awadalla, M., & Kausar, F. (2023). Leveraging ICN and SDN for Future Internet Architecture: A Survey. Electronics, 12(7), 1723.

[5] Jiang, W., Zhan, Y., Zeng, G., & Lu, J. (2022). Probabilistic-forecasting-based admission control for network slicing in software-defined networks. IEEE Internet of Things Journal, 9(15), 14030-14047.

[6] Adoga, H. U., & Pezaros, D. P. (2022). Network function virtualization and service function chaining frameworks: A comprehensive review of requirements, objectives, implementations, and open research challenges. Future Internet, 14(2), 59.
[7] Jiang, W. (2022). Graph-based deep learning for communication networks: A survey. Computer Communications, 185, 40-54.
[8] Jiang, W. (2022). Cellular traffic prediction with machine learning: A survey. Expert Systems with Applications, 201, 117163.
[9] Pattaranantakul, M., Vorakulpipat, C., & Takahashi, T. (2023). Service Function Chaining security survey: Addressing security challenges and threats. Computer Networks, 221, 109484.
[10] Rafique, W., Hafid, A. S., & Cherkaoui, S. (2022). Complementing IoT Services Using Software Defined Information Centric Networks: A Comprehensive Survey. IEEE Internet of Things Journal.
[11] Jiang, W., He, M., & Gu, W. (2022). Internet Traffic Prediction with Distributed Multi-Agent Learning. Applied System Innovation, 5(6), 121.
[12] Zhi T, Liu Y, Zhou H, et al. Research Progress and Security Analysis of the Service Mechanism in Smart Identifier Network, ACTA ELECTRONICA SINICA, 2021 49(8): 1653-1664.
[13] Jiang, W. (2022). Internet traffic matrix prediction with convolutional LSTM neural network. Internet Technology Letters, 5(2), e322.
[14] Guan, J., Zhang, Y., Yao, S., & Wang, L. (2019). AID shuffling mechanism based on group-buying auction for identifier network security. IEEE Access, 7, 123746-123756.
[15] Jiang, W. (2022). Internet traffic prediction with deep neural networks. Internet Technology Letters, 5(2), e314.
[16] Cheng, Y., Gao, S., & Hou, X. (2022, December). A Secure Authentication Mechanism for Multi-Dimensional Identifier Network. In 2022 International Conference on Networking and Network Applications (NaNA) (pp. 163-168). IEEE.
[17] Xu, T., Gao, D., Dong, P., Foh, C. H., Zhang, H., & Leung, V. C. (2019). Improving the security of wireless communications on high-speed trains by efficient authentication in SCN-R. IEEE Transactions on Vehicular Technology, 68(8), 7283-7295.
[18] Ai, Z., Liu, Y., Chang, L., Lin, F., & Song, F. (2019). A smart collaborative authentication framework for multidimensional fine-grained control. IEEE Access, 8, 8101-8113.
[19] Li H., Quan W., Cheng N., Zhang H., & Shen X. (2018). Crowd-based collaboration caching mechanism in smart identifier network. Chinese Journal on Internet of Things, 2(4), 5-13.
[20] Lan J., Wang P., Shen J., et al (2017). Research on push cache of large-scale converging access convergence networks. Chinese Journal on Internet of Things, 1(1), 50-54.
[21] Quan, W., Liu, Y., Jiang, X., & Guan, J. (2016). Intelligent popularity-aware content caching and retrieving in highway vehicular networks. EURASIP Journal on Wireless Communications and Networking, 2016(1), 1-10.
[22] Zhang, S., He, P., Suto, K., Yang, P., Zhao, L., & Shen, X. (2017). Cooperative edge caching in user-centric clustered mobile networks. IEEE Transactions on Mobile Computing, 17(8), 1791-1805.
[23] Ning, H., Zhen, Z., Shi, F., & Daneshmand, M. (2020). A survey of identity modeling and identity addressing in Internet of Things. IEEE Internet of Things Journal, 7(6), 4697-4710.
[24] Liu, G., Quan, W., Cheng, N., Zhang, H., & Shen, X. (2020). VLI: Variable-length identifier for interconnecting heterogeneous IoT networks. IEEE Wireless Communications Letters, 9(8), 1146-1149.
[25] Jiang, W. (2023). Software defined satellite networks: A survey. Digital Communications and Networks.
[26] Yao, S., Guan, J., Yan, Z., & Xu, K. (2019). SI-STIN: A smart identifier framework for space and terrestrial integrated network. IEEE Network, 33(1), 8-14.

[27] Feng, B., Zhou, H., Li, G., Li, H., & Yu, S. (2016, May). SAT-GRD: An ID/Loc split network architecture interconnecting satellite and ground networks. In 2016 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.