



Editorial: Special Topic on Domain Name and Identifier of Internet: Architecture & Systems



Guest Editor

LI Hui is a full professor of the Shenzhen Graduate School, Peking University (PKU), China. He received his B. Eng. and M. S. degrees from School of Information Engineering, Tsinghua University, China in 1986 and 1989 respectively, and Ph. D. degree from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2000. He was the director of Shenzhen Key Lab of Information Theory & Future Internet Architecture and director of PKU Lab of China Environment for Network Innovations (CENI), National Major Research Infrastructure. He proposed the first co-governing future networking “Multi-Identifier System (MIN)” based on blockchain technology and has implemented its prototype on the real operators’ network in the world, and the project “MIN: Co-Governing Multi-Identifier Network Architecture and Its Prototype on Operator’s Network” has received the award of World Leading Internet Scientific and Technological Achievements by the 6th World Internet Conference in 2019. His research interests include network architecture, cyberspace security, distributed storage, and blockchain.

Domain name and identifier are the identity representation of each subject in the packet data network, which are the identity certificates of an organization or individual in the computer network. It is the registration and identification method of each subject, as well as the basis for network operators to charge users for service management. In fact, a country’s entire collection of individual domain names and identifiers constitutes the country’s virtual cyberspace, just as the global collection of domain names constitutes the global cyberspace under IP network. Domain name and identifier are in fact the objective embodiment and existence of virtual cyberspace. The so-called security of cyberspace is the security of the contents and devices of each domain name or its corresponding IP address in the space. Therefore, how to define the structure of domain name and identifier string and how to construct the allocation, registration, resolution and service management system of domain name and identifier are the most basic matters for the reliable, stable and safe operation of packet data networks. How to manage the whole lifecycle of domain name or identifier is related to the sovereignty of each country’s cyberspace and is also fundamental to the security of each country’s cyberspace.

The extension of the IPv4 network system swept the world at a speed that its inventors could not have anticipated, becoming the most important global infrastructure of the current information age. However, there are two major defects in the traditional IP Internet system. One is that the IP address and domain name are centrally managed by a single organization.

The other is that the IP architecture does not have any guarantee scheme for network security and service quality. Decades of tinkering have proved impossible to cure.

The network itself is expanding the scale and dimension of its virtual space boundaries. The evolution of the Internet has experienced several stages, from a professional file information communication network used in scientific circles in the initial period to a consumer e-commerce network everyone could access, then to a physical interconnection network supporting automatic car driving, and finally to the value created network-industrial Internet emerging in recent years. It can be seen that network technology has indeed become the most important living and production infrastructure of human society. It is spawning hundreds of billions of domain names and identifiers for objects and data. Accordingly, its requirements on the reliability, security and service performance of the identification system are getting higher and higher.

Like the revolution of the earth around the sun, the existence of global packet data network has become an indispensable objective force in human society. We can only correct its deficiencies or defects in the course of its development or quietly replace them with new architecture without affecting the human society. This special issue is focused on the network architecture of the domain name or identifier and its system, around its evolution, security design and risk analysis model, specific industry application examples; eight papers are organized to introduce the current research trends and progress. Two of the papers discuss the gradual improvement of the traditional Domain Name Service (DNS) architecture and the architecture transformation; two papers discuss the combining of future network architecture to build industrial Internet identifier system; two papers discuss the traditional risk analysis model of IP network domain DNS and the

security design of identifier system for industrial Internet; the last two papers introduce the development of identification system for the industrial Internet and its concrete applications in different industries.

In response to the international community about the decentralization and the multilateral co-governing of Internet domain name and identifier management system, based on the proof of vote consensus algorithm of consortium blockchain, the first paper entitled “Prototype of Multi-Identifier System Based on Voting Consensus” proposes a network architecture for multiple kinds of identifiers, which is compatible with the domain name and able to be deployed over the current IP network, and has been verified on a large-scale operator’s network.

Object traceability based on Radio Frequency Identification (RFID) is an important capability of the Internet of Things (IoT). GS1 Electronic Product Code (EPC) global network was a de-facto standard in RFID technology, which was developed from EPC network architecture. The inefficiency of the EPC network was caused by the distributed storage of unrelated data and the access control mechanism of discovery service. The second paper entitled “Advanced EPC Network Architecture Based on Hardware Information Service” proposes an enhanced solution to alleviate the challenges and improve the performance of the original EPC network architecture.

The host end-to-end system characterized by host IP address cannot meet the demands of the industrial Internet centered on data and services. The third paper entitled “Integrated Architecture for Networking and Industrial Internet Identity” proposes an overall framework of Information-Centric Networking (ICN)-based industrial network and Named Data Networking (NDN)-based factory extranet with Software Defined Networking (SDN). Introducing ICN into the industrial Internet facilitates the integration of industrial network and identity resolution system, flattens the overall architecture of the industrial Internet, and improves the efficiency of information retrieval, network scalability, and data security. The ubiquitous industrial Internet makes it a challenge to design a suitable identifier resolution system. The fourth paper entitled “Identifiers Management of Industrial Internet Based on Multi-Identifier Network Architecture” proposes an architecture to support multiple kinds of identifiers for the Industrial internet, including content name, identity, and location, besides the traditional IP address. The exhaustion problem of IP addresses may be solved, and the security, credibility, and availability of the industrial Internet system are enhanced with the application of multiple types of identifiers. A multi-identifier translation table is designed to establish an inter-translation scheme between multiple identifiers. An identifier addressing and routing algorithm is also presented to make it convenient to

put the strategy into practice.

The security of domain name and identification system is the guarantee of reliable network operation. The fifth paper entitled “Risk Analysis of Industrial Internet Identity System” provides a detail and deep risk analysis of the current identity system represented by the domain name system and object identifier. According to the characteristics of the industrial Internet identity system, four open ecosystem planes are proposed, and a corresponding risk analysis view is established for various planes. Three defensive lines were proposed to establish the identity credit system. Security issue should be considered at the beginning of the design stage, and corresponding regulations should be setup to direct the system implementation. The sixth paper entitled “Security Risk Analysis Model for Identification and Resolution System of Industrial Internet” proposes an innovative security risk analysis model, which can help control risks at the initial stage of industrial Internet construction, provide guidance in the early design stage, and promote the healthy and sustainability of industrial identification and resolution system.

The last two papers are about the development and application of identifier system in industries. The seventh paper entitled “Construction and Application of Identifier Resolution in Automotive Industrial Internet” introduces the industrial ecosystem of the automobile industrial Internet built by Foton Motor Inc. This identifier resolution system facilitates continuous innovations, improving the design and manufacturing capabilities of the enterprise, the car ecosystem and the car life. Besides, it will not only enhance the stickiness of car customers and expand the influence and appeal of companies among users, but also promote product upgrading.

The industrial Internet technology will become more and more popular in different industries, and give birth to solution providers. The eighth paper entitled “Application of Industrial Internet Identifier in Optical Fiber Industrial Chain” is contributed by such a high-tech solution firm—Jiangsu ZTT LINK Ltd. It adapts the identifier system as a bridge to connect the information islands in the industry. It uses data to build a technology application ecosystem based on the identifier resolution system, and develops several application objects and application scenarios of the industrial Internet identifier. As an example, its application into the optical fiber manufacturing industry has brought higher efficiency and lower cost.

The guest editor would like to thank the editorial office of *ZTE Communications* for their continuous support throughout the submission and review processes. The guest editor would also like to thank all the authors for contributing to this special issue and thank the reviewers for their timely and professional review of these papers.