Identifier Management of Industrial Internet Based on Multi–Identifier Network Architecture

WANG Yunmin[1,2], LI Hui[1,2], XING Kaixuan[1], HOU Hanxu[3], Yunghsiang S. HAN[3], LIU Ji[1], and SUN Tao[4]

(1. Shenzhen Graduate School, Peking University, Shenzhen, Guangdong 518055, China;
2. Pengcheng Laboratory, Shenzhen, Guangdong 518000, China;
3. School of Electrical Engineering and Intelligentization, Dongguan University of Technology, Dongguan, Guangdong 523808, China;
4. The Network and Information Center of Shenzhen University Town, Shenzhen, Guangdong 518055, China)

Abstract: The industrial Internet realizes intelligent control and optimized operation of the industrial system through network interconnection. The industrial Internet identifier is the core element to accomplish this task. The traditional industrial Internet identifier resolution technologies depend excessively on IP networks, and cannot meet the requirements of ubiquitous resource-restraint Internet of Things (IoT) devices. An industrial Internet identifier resolution management strategy based on multi-identifier network architecture is proposed in this paper, which supports content names, identities, locations, apart from the traditional IP address. The application of multiple types of identifiers not only solves the problem of IP addresses exhaustion, but also enhances the security, credibility, and availability of the industrial Internet identification resolution system. An inter-translation scheme between multiple identifiers is designed to support multiple identifiers and the standard ones. We present an addressing and routing algorithm for identifier resolution to make it convenient to put our strategy into practice.

Keywords: identifier resolution; industrial Internet; inter-translation; multiple identifier; routing and addressing

1 Introduction

The industrial Internet is an intelligent closed loop driven by data and integrated by Information Technology (IT) and Operational Technology (OT). The identifiers of the industrial Internet will spread the hosts in the traditional Internet to resources such as goods, information, machines, and services, and extend the IP addresses to a heterogeneous, off-site, and refined information set [1]. The identifier resolution system consists of an identifier coding system and a resolution system [2]. The identifier code is the identity card of the machine or the goods, and the resolution system uses the identifiers to locate and query the machine or the goods uniquely. Identifier resolution is the premise of the supply chain system, the production system, the complete lifecycle management, and the intelligent service. Identifier resolution provides a technical support on unified network layer for cross-industry/inter-disciplinary industrial Internet platforms and enables intelligent association of heterogeneous devices

and services from different vendors. Similar to the Domain Name System (DNS) in the traditional Internet, the industrial Internet identifier resolution system is the gateway to the entire industrial Internet, as shown in **Fig. 1**. Besides, it is the basis for the interconnection of the whole industrial Internet.

The identifier resolution system is an essential part of the industrial Internet architecture, and also a nerve hub supporting the interconnection of the industrial Internet [3]. Flexible identifier differentiation and information management of the entire network resources are achieved by assigning each product, component, machine, or device or digital intellectual property copyright a unique "identity card". Industrial Internet identifier resolution refers to the unique positioning and relevant information query of machines, goods, and digital knowledge products. At the same time, the global supply chain system and enterprise production system can be accurately connected.

IP protocol is the backbone protocol of contemporary Internet connection. In the meantime, various universal industrial Internet identifier resolution systems, such as Handle [4], Object Identifier (OID) [5], Ubiquitous ID (UID) [6], and Global Standard 1 (GS1) [7], are also designed and running upon the IP architecture [8]. However, the industrial Internet often contains many resource-constrained devices, which have smaller memory, limited computing power, and energy. Sensors and actuators often raise communication requirements in industrial applications that are critical for business and safety. Besides, the design concept of the IP model is based on a host-to-host communication mode, which will become a bottleneck to deal with high traffic and high bandwidth environment.

Moreover, regarding the particular application scenarios, identifier authentication, Quality of Service (QoS) assurance, and the network efficiency are not supported by the current Transmission Control Protocol / Internet Protocol (TCP/IP) protocol stack. In the future, the integration of terrestrial Internet and satellite-based space Internet is a possible technical requirement of the industrial Internet [9].

This paper proposes an Internet identifier resolution management system based on the multi-identifier network architecture. It eliminates the malpractice and hidden dangers of excessive concentration on IP network management and control. The main contributions of this paper are listed as follows:

1) We propose a hierarchical network architecture with manageable and controllable trust and privacy protection that supports multiple identifier routing and addressing. The core of this network is that the network inherently supports multiple network identities for simultaneous routing and addressing, and assists users to access the new network system in mul-
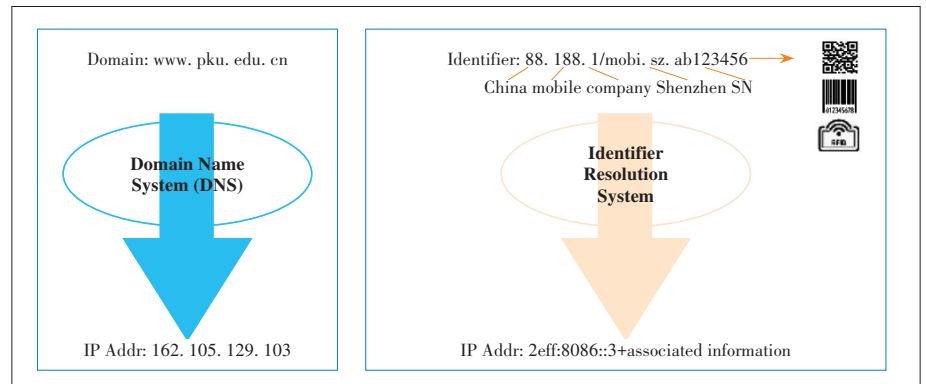
▲Figure 1. An Industrial Internet identifier.

tiple ways seamlessly. The identity of the user is integrated with the content published on the network, which can ensure the regular operation and management of the network. At the same time, the hierarchical signature scheme with high security and low complexity is introduced to ensure that the network data content cannot be tampered and stolen, which dramatically improves the security, credibility, and availability of the whole network.

2) We present the inter-translation schemes for multiple identifiers in order to solve the problem that multiple network identifiers and multiple standard identifiers inevitably coexist.

3) An addressing algorithm is designed to speed up the lookup process of the identifier's name, which makes our proposal more convenient to be put into practice.

The remainder of this paper is outlined as follows. Section 2 provides background and related work. We describe in detail the design essentials of the autonomously controllable multiple identifier systems for the industrial Internet in Section 3. Inter-translation of multiple network identities is presented in Section 4, and addressing algorithms for large scale identifier space are proposed in Section 5. Section 6 concludes the paper.

2 Related Work and Background

2.1 National Industrial Internet Identifier Resolution System

The national industrial Internet identifier resolution system of China is designed with three levels: international root nodes, national top nodes, and secondary nodes, besides recursive resolution nodes along with all these levels, as shown in **Fig. 2**. By the end of 2018, five national top-level nodes of identifier resolution in Beijing, Shanghai, Guangzhou, Wuhan, and Chongqing were put into operation, fully supporting various identifier systems. By the end of 2019, 47 secondary nodes had been set up, and the number of identifier registrations has reached 915 million, with 785 pertinent enterprises [10].

The national top-level nodes act as the foundation, which continuously improve the system functions and capabilities

based on the established plan and gradually build the network infrastructure of the identifier and resolution system of open integration, unified management, interconnection, security, and reliability. The secondary nodes are the graspers, a number of which have been playing their roles in pioneering new approaches [11]. They are built to promote the integrated innovation application of industrial Internet identifier resolution. Lastly, industrial applications are the purpose of identifier resolution. It can encourage the application demonstration in many industries such as aviation and machinery vehicles, and gradually build the identifier resolution industry ecology.

2.2 Named Data Networking

Named Data Networking (NDN), a content-based future network architecture, was proposed ten years ago [12], [13]. NDN replaces host-addressed IP packets with named data as a new narrow waist of the hourglass protocol stack. Each data object has a hierarchy name that is used as a unique identifier in the application context that publishes and consumes the data. In order to request a data object, an interest is sent with a prefix of the data name. The NDN forwarder forwards the interest packet towards the location where the data may be located. Each forwarder along the path records the interest and its incoming interface in the local Pending Interest Table (PIT). When a matched packet is found either in the forwarder's cache or from the original producer, the packet will be returned to the requester along the reverse path recorded in the PITs of the nodes. A copy of the data packet will be stored in their local caches after forwarding to satisfy the future requirements for the same data request. The data packet has an encrypted signature generated by its producer, together with the name of the signing key, which allows data consumers to verify the provenance of the received data regardless of its source. Compared with the traditional IP network, it is more suitable for the demand of industrial Internet content and has the po-

tential to solve the problems and challenges of the industrial Internet on the network layer. Specifically, for the industrial Internet, NDN is superior to IP in security, mobility, scalability, and quality of service [14].

However, NDN only supports the content network identifier, so the solution for constructing an industrial Internet identifier based on NDN also has significant drawbacks in its unbound name length and publish-subscribe data acquisition model. NOUR et al. propose a hybrid name scheme for heterogeneous devices [15] and recent advances in how to exploit NDN for IoT scenarios are surveyed in [16].

Therefore, it is urgent to construct a multi-identifier future network model in which identifier serves as the content center. The data exchange between nodes is based on identity, content, service, ground space location, besides the IP address of the endpoint. Content-centric networks increase efficiency for content delivery, especially when the content is stored in multiple nodes, and content providers or content requesters are in the process of moving.

# 3 Autonomously Controllable Multi-Identifier Architecture for Industrial Internet

3.1 Multiple Identifier Management

This proposal dispenses the dependence of the traditional industrial Internet and IP networks, based on a multi-identifier future network architecture. The system breaks through the current dilemma of IP single identifier and centralized management. It constructs an industrial Internet identifier service platform based on the voting-based consortium blockchain [17], and supports network addressing and routing with multiple identifiers and parallel coexistence, including identity, content, service, location, and IP address, as shown in **Fig. 3**. The dilemma of unilateral monopoly is broken in the centralized management of domain names of the IP system [18].

1) Name. Name is a hierarchical string that is used to identify each resource in the network. In order to support the addressing process of content name directly, the multi-identifier network nodes have a forwarding information table with a name as the key to record the corresponding forwarding port information. The data transmission is performed in a user-driven manner: the content requester puts the content name into an interest message and sends it to the network; the routing node records the arrival port of this interest message in the PIT and queries the Forwarding Information Table (FIB) [19]; The mes-
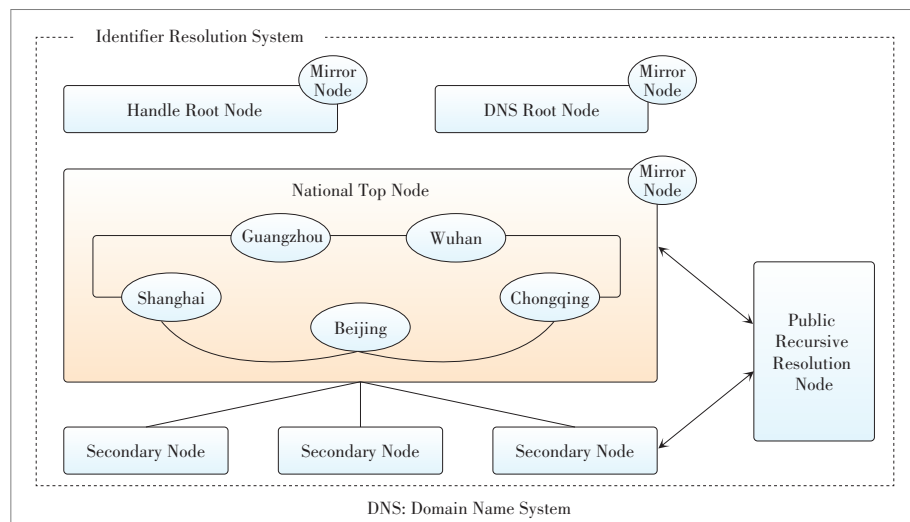
▲Figure 2. The national Industrial Internet identifier system of China.
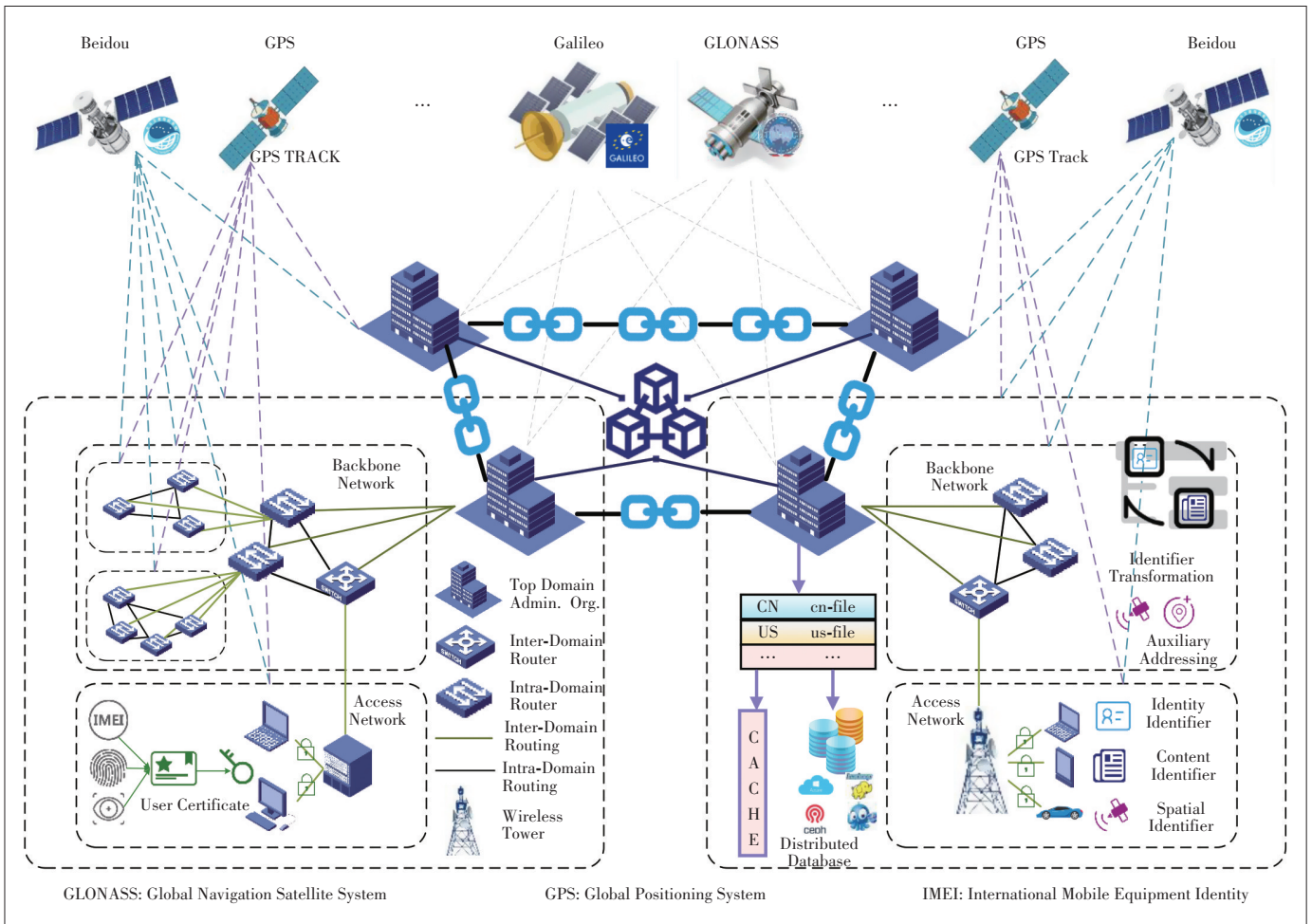
▲Figure 3. Multi-identifier future network architecture.

sage is forwarded until it reaches a holder of the content; by querying the pending interest table, the packet containing the requested content will be traced back to the requester along the arrival path of the interest message; the name-oriented addressing process will decouple the data itself from the specific location of the data, which provides more flexibility to the network system.

2) Identity. The identity is used to identify a user locally or globally. The favorite identity identifiers include the public key, the user's ID, the International Mobile Equipment Identity (IMEI) code of the mobile phone, the email address, and other various identities, besides biometrics information such as the face, fingerprint, pupil, and voice. The behaviors of users on the network, including the issuance and access to network resources, will be subject to the specific authority determined by their identity, and each behavior can be traced back to the identity information of the user.

3) Location. The location information can not only represent the geographical location in the real sense, but also represent the virtual location in the abstract space, such as the mathematical coordinates acquired by the nodes after map-

ping the network into the geometric space. The addressing process for spatially geographical location is that the multi-identifier network nodes calculate the geometric distance between each neighbor and the destination, and the smallest one is greedily selected as the forwarding object. And global navigation satellite system (GNSS), such as Galileo in EU, Beidou in China, Global Positioning System (GPS) in USA, Global Navigation Satellite System (GLONASS) in Russia are supported in our system, as shown in Fig. 3.

3.2 Identifier Registration and Request

The network supports routing and addressing with multiple types of identifiers, including the identity identifier, content identifier, spatial location identifier, and IP address identifier. The content identifiers of all resources in the network are bound to the identity identifier of the publisher. After a user logs into the network, the spatial location identifier and the accessed network resources will be recorded in the network supervision node of blockchain for security supervision and data protection.

The identifier registration steps are as follows.

Step 1 is resource content registration. The network node receives the resource content registered by the user. At the same time, it adds the identity identifier of the content publisher and the spatial location identifier according to the location of the node where the content is stored.

Step 2 is network node authentication. After receiving the identifier registration request transmitted by the user, the network node will review the content and its user information, register the resource identifier, and then register the generated identifier to the upper-level domain and add the local identifier prefix.

Step 3 is identifier registration request transmission. After receiving the identifier registration request, the upper-level network node transmits its registration identifier message to the controller of the located domain, for subsequent authentication and registration operations based on the predefined data transmission protocol.

Step 4 is identifier verification. After receiving the identifier registration request from the subordinate network domain, the network node in the top-level domain will verify the data of the request and return the corresponding confirmation signal to the original application node. The distributed storage scheme ensures that all registered identifiers cannot be tampered with. The original identifier information will be stored on the distributed database of the top-level domain. After a predefined time, corresponding database synchronization will be carried out within the entire network to confirm that the resource identifier information between the respective top-level domains is equivalent and unified.

The network resource requesting steps are as follows.

Step 1 is inquiry request. Transmitting a query request to the nearest network node.

Step 2 is local identifier data query. When the nearest multi-identifier network node receives the request sent by the user, it will distinguish the identifier type according to the identifier of the query. If it is an IP address, it will go on with the traditional DNS query process. Otherwise, if it is an identity or content identifier, then it will query the forwarding table. If the identifier content recorded in the forwarding table already exists in the local database, the corresponding identifier content will be returned, otherwise Step 3 will be executed.

Step 3 is requesting query transmission. When there is no corresponding identifier contained in the local database, the query request will be uploaded to the upper-level network node. After receiving the query request, the upper-level network node will query the identifier following Step 1 to Step 2. If the corresponding identifier content is queried, it will be returned to the low-level network node; otherwise, the query request is subsequently transmitted to the upper-level network node recursively until the top-level domain network node.

Step 4 is identifier query, verification, and interworking. After the top-level domain nodes find the relevant registered identifier, it will automatically issue the relevant shortest path according to the dynamic topology of the existing network. The related multi-mode network nodes on the forwarding path in the network will receive a new forwarding path table and establish a data transmission path through multi-hop routing; if the nodes in the top-level domain do not find the corresponding identification and query other network identification information corresponding to the identification in the database, proceed to Step 5.

Step 5 is the identifier request distribution. The network node in the top-level domain will distribute the query request to the specified network domain according to the original identifier and the first prefix after the identifier is converted, until the lowest-level network node specified by the query request is locally queried. If the corresponding identifier content is found successfully, it is delivered to the query requester; otherwise, the query error information is returned.

4 Inter-Translation of Multiple Network Identities

When a piece of content is registered and published on a multi-identifier network, the name content can be bound with multiple identifiers, such as identity, content, location information, and IP address. Therefore, there is a need for multiple identifiers to be commonly addressed. In addition, the identifiers in the industrial Internet should be application-oriented and record the product information. On the other hand, it should support addressing and routing. Due to the diversity of the applications, it is difficult to establish a global hierarchical naming scheme that is suitable for all applications.

Therefore, on the multi-identifier-based industrial Internet service platform, multiple network identifiers and multiple standard identifiers coexist. A globally unique namespace needs to be established, as well as a unique namespace for each application. The multi-identifier translation table is utilized to establish an Inter Translation Table (ITT) and interoperability mechanism with existing common identifiers.

4.1 Translation Process Between Name and Identity

In order to maintain a secure network environment, we bind the name of the content to the identity of its original publisher, and use a valid extension to identify network resources in the following mode: $/UniqueID_A/SubID_A/Name/Sig(Name,PrK_A)$. $UniqueID_A$ is the globally unique identifier of the publisher A, and no collision occurs; it will generate the public-private key pair of the user. $SubID_A$ is the secondary identifier when the content is published, because the same user in the network may have multiple identities. *Name* is the hierarchical content name and $Sig(Name, PrK_A)$ is the signature of the content name signed by A. Before the content is received by the user or cached at the intermediate routing node, its signature must be verified to ensure its legitimacy based on the security mechanism described above. As a result, any resource in the

network can be traced back to its original publisher, which guarantees the regulatory nature of the publishing behavior and the security of network transmission. Under this representation, an identifier can be regarded as a particular form of extension names, that is, those with empty content names. Therefore, we use the prefix tree data structure to support storage and query operations on names and identities.

Under this representation method, identity can be regarded as a special form of extension name, that is, when the content name is empty, we use the prefix tree as a data structure to support the storage and query operations of names and identities (**Fig. 4**).

4.2 Translation of Location, Name, and Identity

As mentioned above, each user corresponds to a uniquely real or virtual spatial location identifier. In order to reduce the routing delay, we set the location identifier of the name in a network to the nearest node location holding the corresponding content of the name, which is calculated and distributed by the upper control node. **Fig. 5** shows the transformation sequence with the following four steps.

1) A resource request is issued with a particular identifier.

2) The multi-identifier system performs queries based on the identifier type. If the request is issued with traditional domain names, DNS is queried directly. If it is an IP address and exists in the identification Inter-translation Forwarding

Table (IFB), mutual translation is performed; otherwise, the agent accesses traditional IP networks. If it is other type of identifiers such as an NDN identifier, or an identity identifier, the content identifier is first queried in the Content Store (CS), Pending Interest Table (PIT) and inter-translation forwarding table. If it exists, an inter translation is performed; otherwise, go to Step 3.

3) If the identifier does not exist in the current domain, the multi-identifier system will recursively query up to the top domain.

4) If there is no such identifier information in the top-level domain, the query will be performed according to the specific lower-level domain of the identifier information, until the bottom-level domain specified by the identifier, and the corresponding result will be returned if it exists. Otherwise, a query error message is returned.

# 5 Addressing Algorithm for Large-Scale Identifier Space

In order to meet the needs of distributed storage, classification, addressing and forwarding services of ultra-billion-level industrial Internet identifier, a hierarchical distributed storage strategy is proposed to study the hyperbolic addressing routing mathematical model and the fusion Hash Prefix Tree (HPT) algorithm. The index expansion problem of the forwarding table has to be solved and the forwarding strategy optimized to improve the success rate of the addressing route.

We designed a FIB composed of a hash table and a prefix tree [20], where the hash table is used to support fast lookups, and the prefix tree is used to store logical relationships between names. The main structure of FIB is demonstrated in **Fig. 6**.

In the hash table, the name (such as /C1/C4/C5) is used as the key. Moreover, the pointer to the node in the prefix tree is used as the value. Thus, the fast retrieval of forwarding information from name to tree is realized.

The edge in the prefix tree represents a name component (such as /C1). On the other hand, each node represents a splicing of all components in the path from the requester node to the root node. The node stores the forwarding information corresponding to the name, the corresponding category of the table item, and the pointer used to maintain the tree structure. Because the name
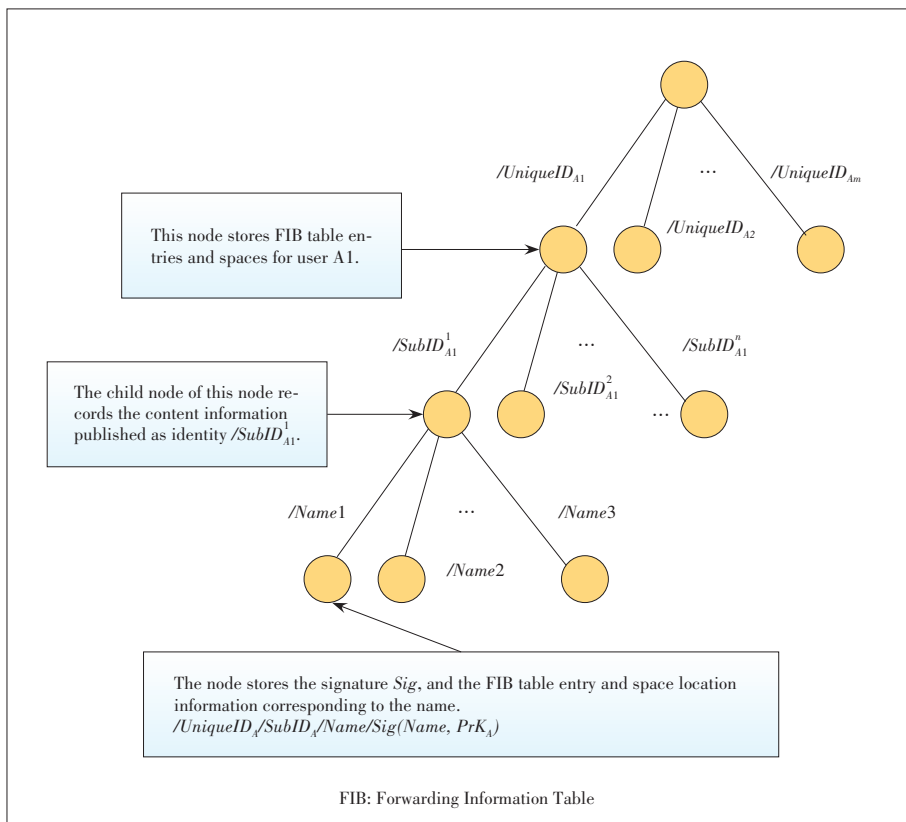
▲Figure 4. Multiple identifiers forwarding architecture using prefix tree structure.

WANG Yunmin, LI Hui, XING Kaixuan, HOU Hanxu, Yunghsiang S. HAN, LIU Ji, and SUN Tao
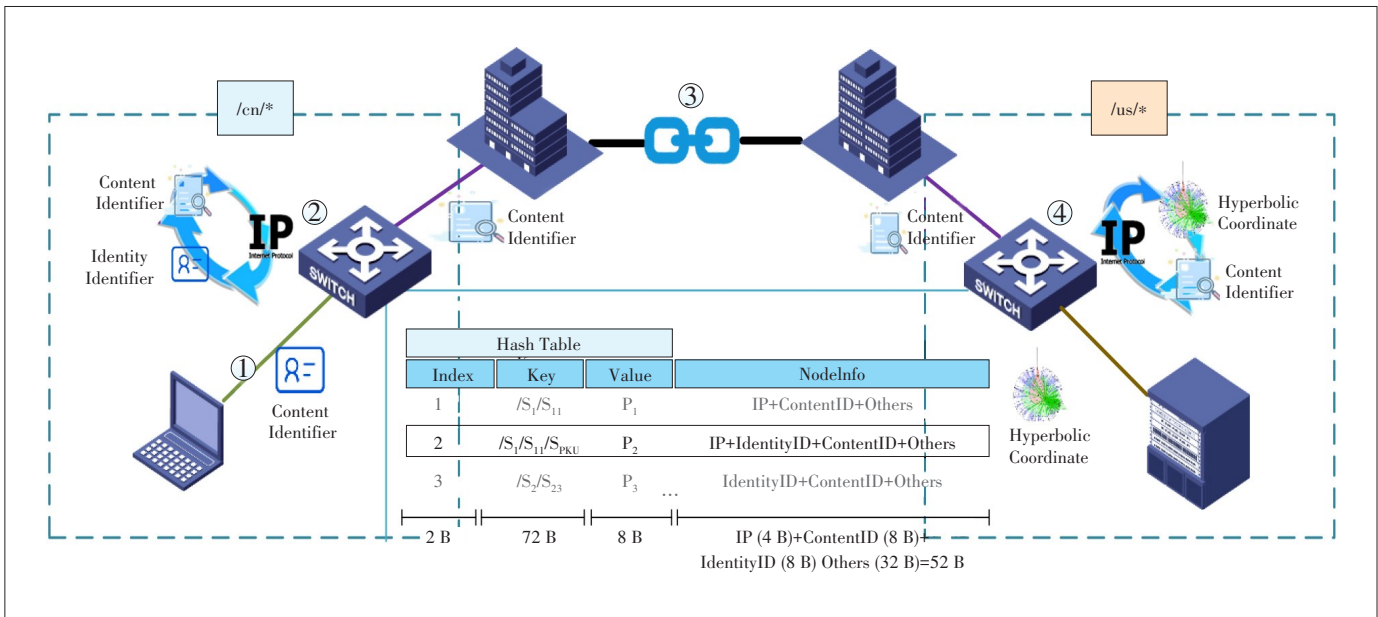
▲Figure 5. The translation process of location, name, and identity.
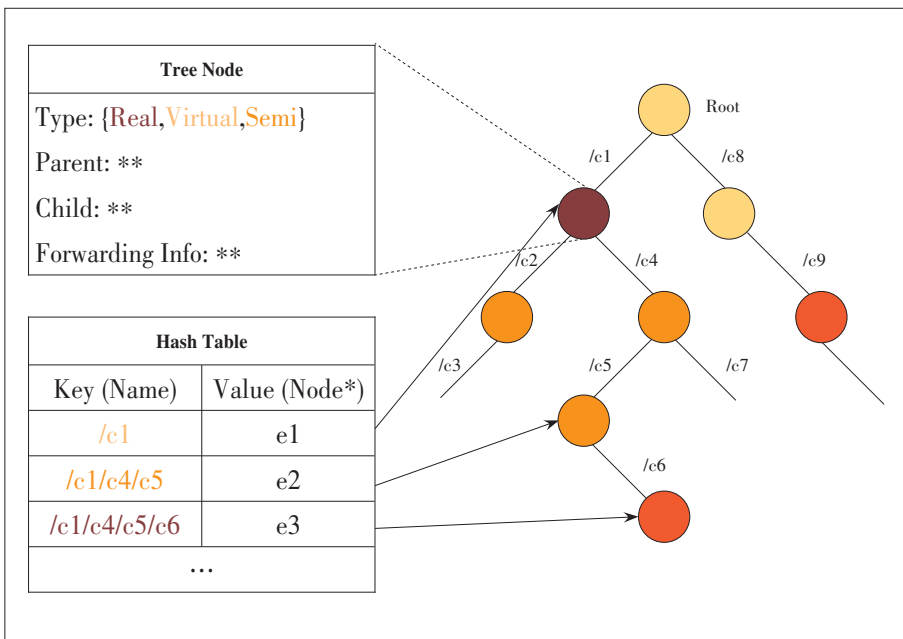
▲Figure 6. Hybrid fowarding information table of hash table and prefix tree.

realized by traversing the whole table without the help of tree structure.

2) The backtracking process is speeded up in the search algorithm. Each node in the tree has only one parent node, the process of backtracking does not need to query and match names or components, so it achieves a faster search speed.

3) It facilitates the removal of the obsolete unreal table items in time, that is, the leaf nodes with non-real types. In the process of table algorithm, as long as all kinds of leaf nodes are real, unnecessary table items can be cleaned up.

6 Conclusions

The ubiquitous industrial Internet makes it a challenge to design a suitable identifier resolution system. In this paper, an industrial Internet identifier resolution management strategy based on multi-identifier network architecture is proposed, which supports content name, identity, service, and location, besides the traditional IP address. Identification management is also included in our proposal, such as identification registration and request and data addressing and forwarding. The inter-translation scheme and address algorithm proposed in this paper show a better performance in the identification resolution management of the industrial Internet.

does not need to be recorded repeatedly in the tree, the introduction of tree structure will only bring limited additional storage overhead.

The prefix tree is introduced for the following three purposes:

1) The categories of non-real table items are modified conveniently in a dynamic environment. For example, if "/C1" is inserted into FIB, all virtual table items prefixed with "/C1" need to change their categories into semi-virtual ones. For the diversity of the NDN identifier, this modification can only be

References

[1] QIN W, CHEN S Q, PENG M G. Recent Advances in Industrial Internet: Insights and Challenges [J]. Digital Communications and Networks, 2020, 6(1): 1 – 13. DOI: 10.1016/j.dcan.2019.07.001

[2] YANG Z, ZHANG D, LI J, et al. Identifier Technology in Industrial Internet [J]. Telecommunications Science, 2017, 33(11): 134 – 140, DOI: 10.11959/j. issn.1000-0801.2017296

[3] CHEN W. Intelligent Manufacturing Production Line Data Monitoring System for Industrial Internet of Things [J]. Computer Communications, 2020, 151: 31 – 41. DOI: 10.1016/j.comcom.2019.12.035

[4] HANDLE.NET (Ver. 9) Technical Manual [EB/OL]. (2019‑07‑26) [2019‑11‑28]. http://hdl.handle.net/20.1000/113

[5] SOUSA P, SILVA A R, MARQUES J A. Object Identifiers and Identity: a Naming Issue [C]//IEEE International Workshop on Object Orientation in Operating Systems. Lund, Sweden, 1995: 127 – 129.DOI: 10.1109/iwoos.1995.470569

[6] CenterU. I.. Ubiquitous Code: Ucode2009 [EB/OL]. (2009-07-28) [2019-12-01]. http://www.uidcenter.org

[7] GS1 Data Excellence Inc. GS1: The Global Language of Business [EB/OL]. [2019-01-12] (2020-01-02). https://www.gs1.org

[8] REN Y, XIE R, ZENG S, et.al. Survey of Identity Resolution System in Industrial Internet of Things [J]. Journal on Communications, 2019, 40(11): 138 – 155. DOI: 10.11959/j.issn.1000-436x.2019238

[9] SISINNI E, SAIFULLAH A, HAN S, et al. Industrial Internet of Things: Challenges, Opportunities, and Directions [J]. IEEE Transactions on Industrial Informatics, 2018, 14(11): 4724 – 4734. DOI: 10.1109/tii.2018.2852491

[10] LIU D. Promote the Integrated Development of 5G and Industrial Internet [R]. World 5G Convention, 2019

[11] LI H, QI Z. Thinking on Secondary Node Construction of Industrial Internet Identifier Resolution [J]. Information and Communications Technology and Policy, 2019, 296(02): 68 – 72. DOI: CNKI: SUN: DXWJ.0.2019-02-019

[12] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking Named Content [C]//ACM Conference on Emerging Networking Experiments and Technologies. Rome, Italy, 2009: 1 – 12. DOI: 10.1145/1658939.1658941

[13] ZHANG L X, AFANASYEV A, BURKE J, et al. Named Data Networking [J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66 – 73. DOI: 10.1145/2656877.2656887

[14] SHANG W T, BANNIS A, LIANG T, et al. Named Data Networking of Things (Invited Paper) [C]//2016 IEEE First International Conference on Internet‑of‑Things Design and Implementation (IoTDI). Berlin, Germany, 2016: 117 – 128. DOI: 10.1109/iotdi.2015.44

[15] NOUR B, SHARIF K, LI F, et al. A Unified Hybrid Information-Centric Naming Scheme for IoT Applications [J]. Computer Communications, 2020, 150: 103 – 114. DOI: 10.1016/j.comcom.2019.11.020

[16] ARSHAD S, AZAM M A, REHMANI M H, et al. Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT) [J]. IEEE Internet of Things Journal, 2019, 6(2): 2128 – 2158. DOI: 10.1109/jiot.2018.2873343

[17] LI H, HAN Y X, LI G X, et al. Prototype and Testing Report of a Multi-identifier System for Reconfigurable Network Architecture Under Co‑Governing [J]. SCIENTIA SINICA Informationis, 2019, 49(9): 1186 – 1204. DOI: 10.1360/n112019-00070

[18] DIB O, BROUSMICHE K L, DURAND A, et al. Consortium Blockchains: Overview, Applications and Challenges [J]. International Journal on Advances in Telecommunications, 2018, 11(1): 51 – 64.

[19] YI C, AFANASYEV A, WANG L, et al. Adaptive Forwarding in Named Data Networking [J]. ACM SIGCOMM Computer Communication Review, 2012, 42 (3): 62. DOI: 10.1145/2317307.2317319

[20] LI Z, XU Y P, ZHANG B C, et al. Packet Forwarding in Named Data Networking Requirements and Survey of Solutions [J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1950 – 1987. DOI: 10.1109/comst.2018.2880444

Biographies

WANG Yunmin received his B.Sc. from Tianjin University, China in 2000. Now, he is a Ph.D. candidate at School of Electronics Engineering and Computer Science, Peking University, China. His research interests include future network architecture and the industrial Internet.

LI Hui (lih64@pkusz.edu.cn) received his B.Eng. and M.S. degrees from Tsinghua University, China in 1986 and 1989 respectively, and Ph.D. degree from The Chinese University of Hong Kong, China in 2000. He is now a full professor of the Shenzhen Key Lab of Information Theory and Future Network Architecture, Future Network PKU Lab of National Major Research Infrastructure, Shenzhen Graduate School, Peking University, China. His research interests include future network architecture, cyberspace security, blockchain technology, and distributed storage systems.

XING Kaixuan is a postgraduate student at Shenzhen Graduate School, Peking University, China. His research interests include new architectures and new generations of information communication technology.

HOU Hanxu received his B.Eng. degree in information security from Xidian University, China in 2010, and Ph.D. degrees from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2015 and from the School of Electronic and Computer Engineering, Peking University, China. He is now an assistant professor with the School of Electrical Engineering & Intelligentization, Dongguan University of Technology, and honorary postdocter of the Department of Computer Science and Engineering, The Chinese University of Hong Kong. His research interests include erasure coding and coding for distributed storage systems.

Yunghsiang S. HAN received his Ph.D. degree from the School of Computer and Information Science, Syracuse University, USA in 1993. He is currently with the School of Electrical Engineering and Intelligentization, Dongguan University of Technology, China. He has also been a chair professor with Taipei University, China since 2015. He is an IEEE Fellow in error-control coding, wireless networks, and security.

LIU Ji is the director of the information office at Shenzhen Graduate School, Peking University, China. His research focuses on new network architecture.

SUN Tao is the director of The Network Information Center of Shenzhen University Town. His research interests include blockchain and cyberspace security.