

# Integrated Architecture for Networking and Industrial Internet Identity

LU Hua<sup>1</sup>, LI Xiaolu<sup>2,3</sup>, XIE Renchao<sup>2,3</sup>, and FENG Wei<sup>4</sup>

(1. Guangdong Communications & Networks Institute, Guangzhou, Guangdong 510700, China;

2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;

3. Purple Mountain Laboratories, Nanjing, Jiangsu 211111, China;

4. Department of Information and Software Services, Ministry of Industry and Information Technology of People's Republic of China, Beijing 100846, China)



**Abstract:** Several excellent works have been done on the industrial Internet; however, some problems are still ahead, such as reliable security, heterogeneous compatibility, and system efficiency. Information-Centric Networking (ICN), an emerging paradigm for the future Internet, is expected to address the challenges of the industrial Internet to some extent. An integrated architecture for industrial network and identity resolution in the industrial Internet is proposed in this paper. A framework is also designed for the ICN-based industrial Network And Named Data Networking (NDN) based factory extranet with Software-Defined Networking (SDN). Moreover, an identity resolution architecture in the industrial Internet is proposed based on ICN paradigms with separate resolution nodes or with merging resolution and routing.

**Keywords:** ICN; NDN; industrial network; industrial Internet identity

DOI: 10.12142/ZTECOM.202001005

<http://kns.cnki.net/kcms/detail/34.1294.TN.20200317.1624.005.html>, published online March 18, 2020

Manuscript received: 2019-12-08

**Citation** (IEEE Format): H. Lu, X. L. Li, R. C. Xie, et al., "Integrated architecture for networking and industrial internet identity," *ZTE Communications*, vol. 18, no. 1, pp. 24 - 35, Mar. 2020. doi: 10.12142/ZTECOM.202001005.

## 1 Introduction

Recent advances in the integration of the Internet and the industry have attracted great attention. The industrial Internet [1] is a new industrial economic system that incorporates industrial production, advanced production technologies, internet information technologies, and other new technologies. The industrial Internet supports ubiquitous connection, flexible supply, and efficient allocation of manufacturing resources to satisfy the demands of manufacturing industry, such as digitalization, networking, and intelli-

gence. As a result, it reorganizes and optimizes the modes of industrial production, manufacturing, production organization, and service.

The industrial Internet includes industrial network, industrial platform, industrial security, and industrial internet identity. Although some excellent works have been done on these four aspects of the industrial Internet, a few major problems are still ahead, such as reliable security, heterogeneous compatibility, and system efficiency. In terms of security, network failures may have catastrophic consequences. Industrial networks communicate between sensors, actuators, and control centers, which needs ultra-high reliability. Encryption and other cryptographic techniques are often considered as a silver bullet to ensure security in the industrial Internet. A reliable data protection capability is essential for the industrial Internet; however, IP-based sender-driven end-to-end communi-

This work was supported in part by National Key Research & Development Project (Grant No. 2019YFB1804400) and the MIIT of China 2019 (Innovative Identification and Resolution System for Industrial Internet of Things). LU Hua and LI Xiaolu contributed equally to this work and are co-first authors of the article.

cations have fundamental security defects, introducing host-centric security mechanisms. In terms of heterogeneous compatibility, due to the lack of unified standards in industrial internet identity, manifold identity systems constitute the present situation of multi-system heterogeneity. Heterogeneous compatibility has become one of the main challenges to be addressed in the industrial Internet. In terms of system efficiency, the current industrial Internet system separates networking and identity resolution. The multi-layer architecture is not conducive to efficient information interaction and represents a large portion of infrastructure costs. A more flattening industrial Internet architecture is necessary to reduce the information loss in different system levels.

Information-Centric Networking (ICN) [2], an emerging paradigm for the future Internet, is expected to address the challenges of the industrial Internet to some extent. The key idea of the ICN is to replace the traditional host-based networking primitives with novel name-based ones. In the ICN, a content requester does not need to maintain the knowledge of specific hosts (that act as a content provider), and all networking operations are driven by content names without any references to host locators. ICN strictly names data packets according to its contents instead of its locations, which natively promotes content-based security mechanisms. Content naming also introduces name-based routing protocols, which can route paths according to content names directly. ICN provides an opportunity to integrate networking and identity resolution for the industrial Internet.

In this paper, we first propose an integrated architecture for industrial network and identity resolution in the industrial Internet. We present the framework designs of ICN-based industrial network architecture and Named Data Networking (NDN)-based factory extranet with Software-Defined Networking (SDN). We also address an identity resolution architecture in the industrial Internet based on ICN paradigms with separate resolution nodes or with merging resolution and routing.

The remainder of this paper is organized as follows. In Section 2, we comprehensively review the industrial Internet and ICN. In Section 3, we present an integrated architecture for industrial network and industrial internet identity. We conclude this paper in Section 4.

## 2 Overview of Industrial Internet and Information-Centric Networking

### 2.1 Industrial Internet

The industrial Internet is a service system based on mass data collection, convergence, and analysis for the demand of manufacturing industry, such as digitalization, networking, and intelligence. It is an industrial cloud network that supports ubiquitous connection, flexible supply, and efficient allocation of manufacturing resources. The ultimate goal of the industrial

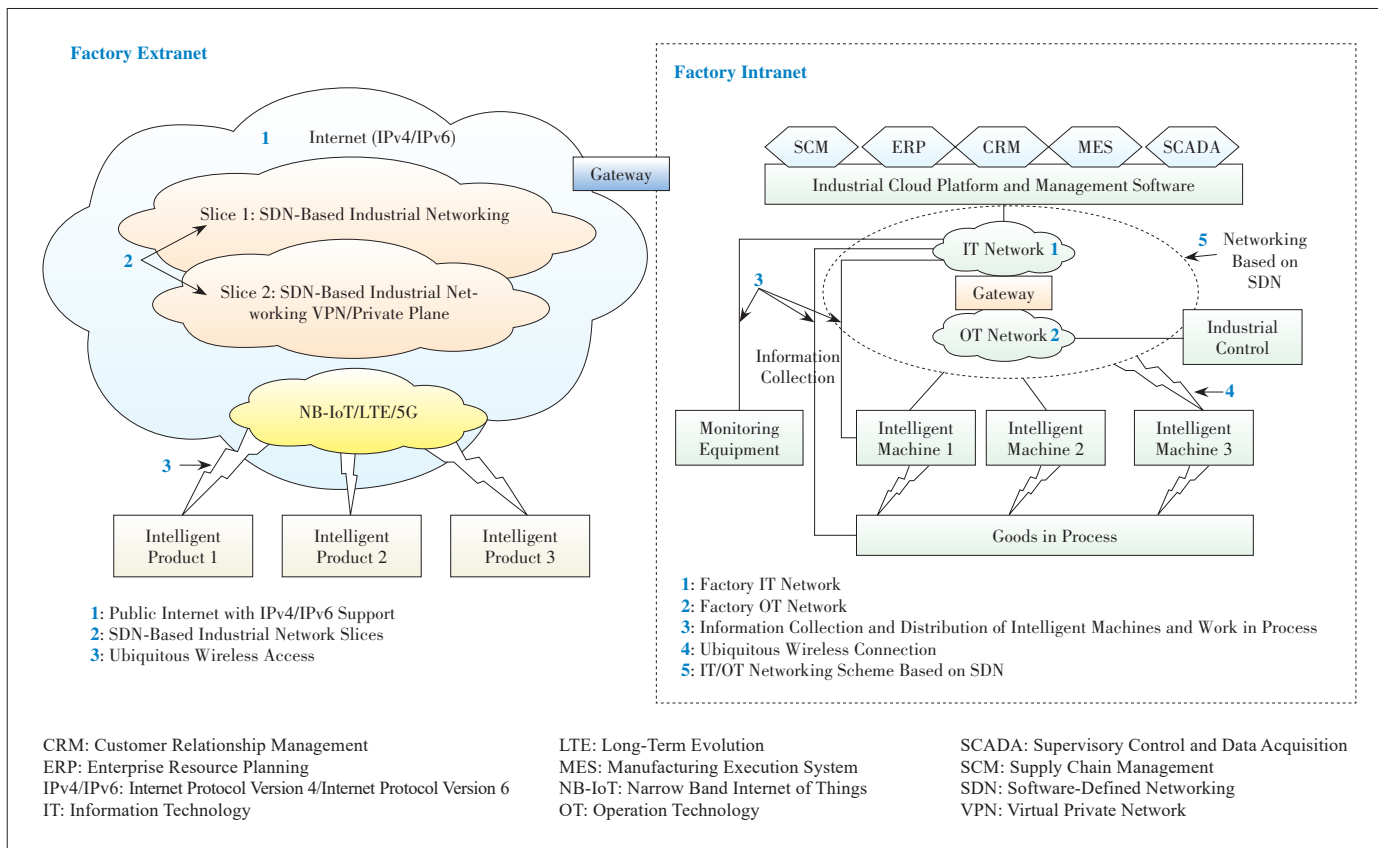
Internet is to realize enterprise intelligence, so as to build the powers of manufacturing and network. industrial Internet architecture consists of four main aspects: industrial network, industrial platform, industrial security, and industrial internet identity. Among them, we will introduce the industrial network and the industrial internet identity in detail.

#### 2.1.1 Industrial Network

The industrial network is an important foundation to realize the layout of the industrial Internet. It integrates the industrial production processes, the information communication technologies, and the basic elements of intelligent manufacturing systems. The industrial network interconnects people, machines, control systems, and information systems together. Its core is to connect the entire industrial system, break information isolation, and ensure the barrier-free data transmission between different devices and systems, thus forming an intelligent system. **Fig. 1** shows the overall architecture of the industrial network. We can divide the industrial network into a factory intranet and a factory extranet according to the deployment position. The factory intranet is deployed in factories and connects people, products, intelligent machines, industrial control and information systems. The factory extranet connects the enterprise, intelligent products, users, and service platforms, aiming at supporting various activities in a product lifecycle.

The factory intranet, according to the carried data, can be divided into Information Technology (IT) network and Operation Technology (OT) network. The IT network connects the information systems in enterprises, interconnecting with the control systems. The OT network interconnects the production control systems (including Distributed Control System (DCS), Fieldbus Control System (FCS), and Programmable Logic Controller (PLC)) and the machines (mainly servers on the device and sensors). The current factory intranet faces several obstacles, including the coexistence of multiple protocols and multiple transmission modes, the existing 5G technology unable to meet the requirements of wireless communication in the factory, the heterogeneous hierarchical access to enterprise data, the ossified network architecture, and the lack of customized services. In order to cope with the above issues, manifold solutions have been researched among the industry, academic, and standardization organizations.

In industry, China Academy of Information and Communications Technology (CAICT) and Huawei have jointly proposed MulteFire, 5G, and SDN/NFV solutions to transforming and constructing the factory intranet. China United Network Communications Co., Ltd. has applied industrial Passive Optical Network (PON) technology at the perception layer to provide wired network coverage for production line equipment and achieved wired and wireless integrated network coverage in the workshop through the wireless network bearer. ADLINK Technology has explored a future wireless factory



▲ Figure 1. The overall architecture of the industrial network.

model by using agile 5G industrial wireless technology.

In academia, GOGOLEV et al. [3] studied the integration scheme of industrial field equipment and embedded object linking and embedding OLE for Process Controls (OPC) Unified Architecture (UA) on Time Sensitive Networking (TSN). MANNWEILER et al. [4] outlined the favorable deployment scenario of 5G/TSN systems integrated under the industry 4.0 environment. NSAIBI et al. [5] proposed a solution to integrating TSN into the automation network and demonstrated its improvement and enhancement of delay performance in industrial Ethernet.

In standardization organizations, the Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), and other standardization organizations are committed to the transformation of the factory intranet. In order to solve the problem of hierarchical and heterogeneous access to industrial data, the OPC Foundation proposed a unified OPC architecture in 2008 to solve the problem of heterogeneous data connection. In order to meet the deterministic delay, the IEEE 802.1 working group has formulated and developed TSN-related standards, aiming to establish a “universal” time-sensitive mechanism for the Ethernet protocols [6], [7]. The IETF has developed the related standards for Deterministic Networking (DetNet) [8], which provides reliable network-lay-

er transmissions by providing data transmission with a certain range of delay, packet loss, and delay jitter.

The factory extranet connects users, data centers, factories, and upstream/downstream enterprises to facilitate enterprise cooperation, operation decision-making, and rapid deployment. The current factory extranet faces with such problems as the large granularity of network services and stiff adjustment, the inability of enterprises to provide edge computing power, and network security. In order to cope with these problems, many solutions have been researched among the industry, academic, and standardization organizations.

In industry, China Mobile and Huawei have introduced Software-Defined Wide Area Network (SD-WAN) controller into the factory extranet to separate the control and forwarding functions of network equipment, so as to build a Wide Area Network (WAN) with open business, flexible programming, and easy operation and maintenance for enterprise users. By building SD-WAN, Huawei could quickly distribute connection services and provide management in the cloud, making it more convenient for enterprise users to define new services and conduct network management. China United Network Communications Co., Ltd. has proposed an integrated application project of 5G industrial Internet automotive extranet transformation.

In academia, CHAUDHARY et al. [9] designed a multi-tribute secure communication model for the industrial Internet with SDN. LI et al. [10] proposed an adaptive transmission architecture for the industrial Internet based on SDN and edge computing and provided a coarse-grained transmission algorithm. To meet the processing requirements of enterprises for big data, the edge computing technology was used to provide enterprises with edge computing capacity and edge caching capacity in [11] and [12], so as to support industrial Internet applications and realize production monitoring, data processing, automatic decision-making, and automatic and rapid response to user demands.

In standardization organizations, the industrial Internet has become the focus of 3GPP R16. 5G network slices are constructed to meet different business operations. 5G edge computing accelerates the integration of industrial IT and OT networks, improves the performance of the industrial Internet such as high reliability and low delay, provides better security and user privacy, and optimizes resource sharing and user experience. The current standardization of 3GPP industrial Internet architecture mainly includes three aspects: new network architecture, enhanced network functions, and new networking mode [13] - [15].

### 2.1.2 Industrial Internet Identity

Identity resolution is a key hub to connect industrial elements and realize industrial data interchange, which is responsible for providing identification registration, management, analysis, and other services. The identity resolution system includes two parts: identity coding and identity resolution. The identity code is used as the "ID card" to identify the unique device; the identity resolution utilizes identification to uniquely locate and address the device. Currently, there are many identity resolution systems, such as Electronic Product Code (EPC) global [16], Object Identifiers (OID) [17], Handle [18], and UID [19].

We can divide the existing identity resolution systems into two categories, namely, the evolution schemes and the clean-slate schemes. The evolution schemes are still based on the Domain Name System (DNS) system, which overlay a set of identity services on top of the DNS technology and store the identity ID and the mapping associated with it. At present, OID, Ecode, and Global Standards One (GS1) belong to the evolution schemes. These schemes are conducive to deployment, but at the same time, they are secondary platforms grafted on DNS. All lookups need to go through DNS, which resulting in low resolution efficiency and heavy reliance on the operation of DNS system. In addition, some researchers believe that the expansion of DNS system should be more cautious due to the importance of DNS system.

The clean-slate schemes, such as Handle and UID, utilize fresh identity resolution technologies which are different from DNS. Specifically, Handle system is a popular identity resolu-

tion solution, which has gradually become the essential infrastructure promoting the fusion of the Internet, data, and artificial intelligence. Handle system has broad prospect and is able to effectively integrate information islands and implement cross-border information sharing, which is an indispensable technology to the future development. These identity resolution technologies are independent of the DNS system and are more suitable for industrial internet scenarios, but at the same time, the clean-slate identity resolution infrastructures need to be deployed, which are expensive and take a long time.

Identity resolution in the industrial Internet faces severe challenges in efficiency, heterogeneous compatibility, and security. The identity resolution system obtains the information addresses of objects (such as IP addresses) based on identification, and then the network routes information requests to the devices storing the information. The whole process of obtaining data needs to be completed by the cooperation with identity resolution system and the network routing system, which is complex and redundant to some extent, resulting in low efficiency of content retrieval. In addition, the data security needs to be considered in both systems, resulting in the difficulty of ensuring the whole system security. There are many heterogeneous identity resolution systems, causing conflicts between them. Without the compatibility of heterogeneous identities, it will be difficult to realize the interconnection between industrial Internet applications.

## 2.2 Information-Centric Networking

The ICN replaces the traditional address-centered network communication model with information naming centric ones to realize efficient information retrieval. The idea of ICN was first proposed by NELSON in 1979. Several countries around the world have started a series of ICN-related projects. We review the ICN from the following perspectives, including typical projects, naming mechanisms, and important features.

### 2.2.1 Typical Projects

The American academic community takes the lead in launching research projects on content-oriented network architectures, including Content-Centric Networking (CCN), NDN [20], Data-Oriented Network Architecture (DONA) [21], etc. The European Union has launched research projects on Network of Information NetInf, Publish-Subscribe Internet Technologies (PURSUIT)/Publish-Subscribe Internet Routing Paradigm (PSIRP), Point, etc. We will introduce DONA and NDN.

#### 1) DONA.

DONA, launched in 2006 and lasting for two years, is a data-oriented network architecture proposed by the Radiation (RAD) Laboratory at the University of California, Berkeley. The project comes up with a self-validating name and adds the capability of advanced caching. The architecture design also takes naming, name resolution, security, and routing into consideration. It expounds the basic functions, such as server se-

lection, mobility, multihoming, multicast, and session initialization. In the extended applications, DONA realizes content distribution, delay tolerant networks, access rules, and middleware. The name resolution mechanism of DONA is similar to DNS but not exactly the same. DONA designs a flat naming mechanism based on URL construction, which realizes the registration, publication, and acquisition of content. Furthermore, naming is used to solve the problems of persistence and reliability. The new self-verification approach simplifies the security model; and the name resolution method finding the path by name solves the validity problem. At present, the project has been completed, but its research results have laid the foundation for the subsequent designs of various ICN architectures.

2) NDN.

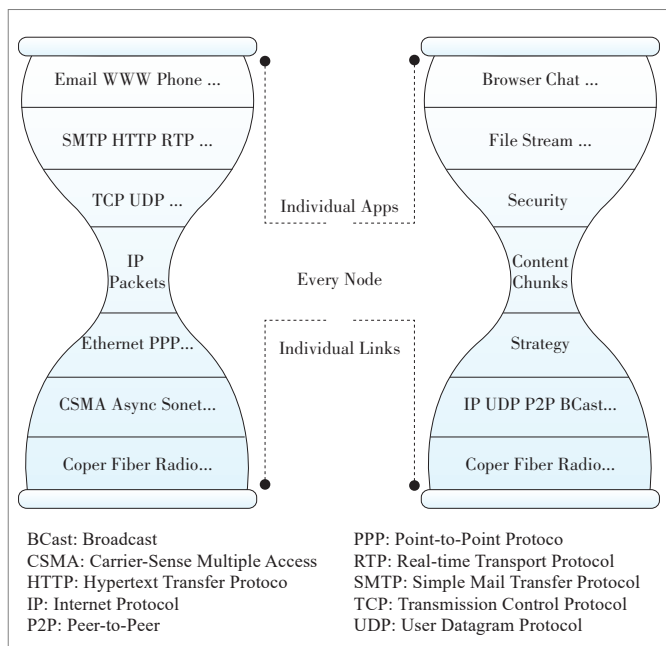
In 2009, JACOBSON of the PARC Research Center proposed CCN and launched the CCNx project. The NDN is an engineering project based on the idea of CCN. It was one of the research projects on the future Internet architecture announced by the Natural Science Foundation of the United States in August 2010. NDN tries to change the current host-based point-to-point communication architecture and realize the transformation to a new network architecture centered on named data. NDN shifts its focus from “the where” to “the what”, which focuses on the content that users and applications are interested on. NDN decouples the content from the protected hosts and directly protects the content, so as to expand the communication mechanisms fundamentally. With the name-based routing, NDN references the hourglass model of current IP network. As shown in Fig. 2, it places the con-

tent block instead of IP in the waist part and constructs the basic safety module by signature for all named data.

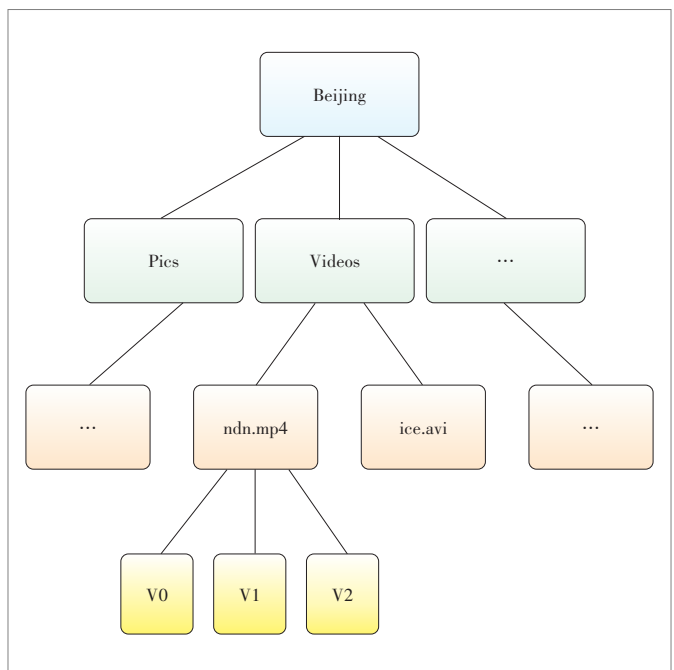
2.2.2 Naming Mechanisms

The naming mechanisms of ICN fall into two categories: hierarchical naming and flat naming. The typical representative of hierarchical naming is NDN, which is similar to URL with “/” as the separator. With hierarchical naming, network nodes can receive, recognize, and forward the received content based on longest prefix matching. At the same time, hierarchical naming is adopted to facilitate clustering of network nodes, which can merge similar items and facilitate search. For example, as shown in Fig. 3, to find /Beijing/videos/ndn.mp4/v1, NDN will first lookup /Beijing, since the data naming with the /Beijing prefix has been gathered together. The aggregation ability enables NDN to process massive data. It solves a part of the burden caused by naming, that is, the amount of content in the whole network is much larger than that of hosts, which makes the scale of content-oriented addressing larger than that of host-oriented ones. Nevertheless, hierarchical naming is generally less secure.

The typical representative of flat naming is DONA, which has the form of a  $P:L$ .  $P$  is the hash value of public key of the content provider;  $L$  is name tag, describing the content details, and the granularity of  $L$  can be control by the user. In addition, DONA supports naming formats of  $P:*$ , which can be used to verify that the prefix is used, and of  $*:L$ , which can be used to describe  $L$  contents or services provided by any content service provider. The naming of hash strings without semantics guarantees good stability and uniqueness, but at the



▲ Figure 2. Named data networking hourglass architecture with content chunks.



▲ Figure 3. Named data networking hierarchical naming example.

same time brings inconvenience in understanding and memory, and the name will change after the encryption algorithm is upgraded.

### 2.2.3 Important Features

ICN separates content from its location by virtue of its name-based routing, which greatly facilitates the transmission and forwarding of information. Therefore, ICN provides an efficient platform for content distribution. Compared with the traditional IP networks, its core features and advantages are as follows:

#### 1) Content naming.

NDN directly names the content, decouples the content and location information, and realizes name-based routing. On the other hand, since the address space of content naming is infinite, it can effectively solve the problem of IP address exhaustion in terms of a large number of terminals in the IoT environment.

#### 2) In-network caching.

Due to the decoupling of content from specific geographical locations brought by content naming, it is feasible to cache content copies in the network. The spatial resources of in-network caching can be used to exchange time benefits, reducing content response time and saving bandwidth.

#### 3) Mobility support.

ICN is a content-enabled request/response model, which eliminates the need to establish and maintain connections. Therefore, ICN is more suitable for mobility scenarios. When the request packet passes through the ICN router, the router will automatically record the track of the demand packet and return the data packet to the user according to the track. When the user moves, a new trajectory will be generated again, so there is no need to maintain the location information of the user in the network. Supporting the mobility of hosts solves the problem of efficiently transmitting mass information. Compared with end-to-end IP communications, ICN's connectionless communication provides a better foundation for seamless switching of mobility, and at the same time, in-network caching benefits for reducing content response latency.

#### 4) Network layer security.

ICN has taken security into consideration during its design. By directly protecting the content itself, the security mechanism of ICN is more robust than that of IP. In traditional IP networks, security depends on whether the host is trusted. If the host is not trusted, the information stored on the host is considered untrusted. However, the security of information is not necessarily related to the host where the information is stored. ICN directly implements security measures on information, so that the granularity of security policy can be coarse or fine.

As a result, ICN adopts information naming instead of the traditional address-centered network communication model,

so as to solve some inherent problems in IP networks and meet users' demand for massive information access. Introducing ICN to the Industry Internet can solve the problem of separating industrial network and industrial identity resolution. We design an integrated architecture for industrial network and identity resolution in the industrial Internet, to flat the overall industrial internet architecture, improve information retrieval efficiency, increase network scalability, and improve data security in the industrial Internet.

## 3 An Integrated Architecture for Industrial Network and Industrial Internet Identity

In this section, we describe the proposed integrated architecture for industrial network and industrial internet identity. The details of this architecture are described as follows.

### 3.1 ICN-Based Industrial Network Design

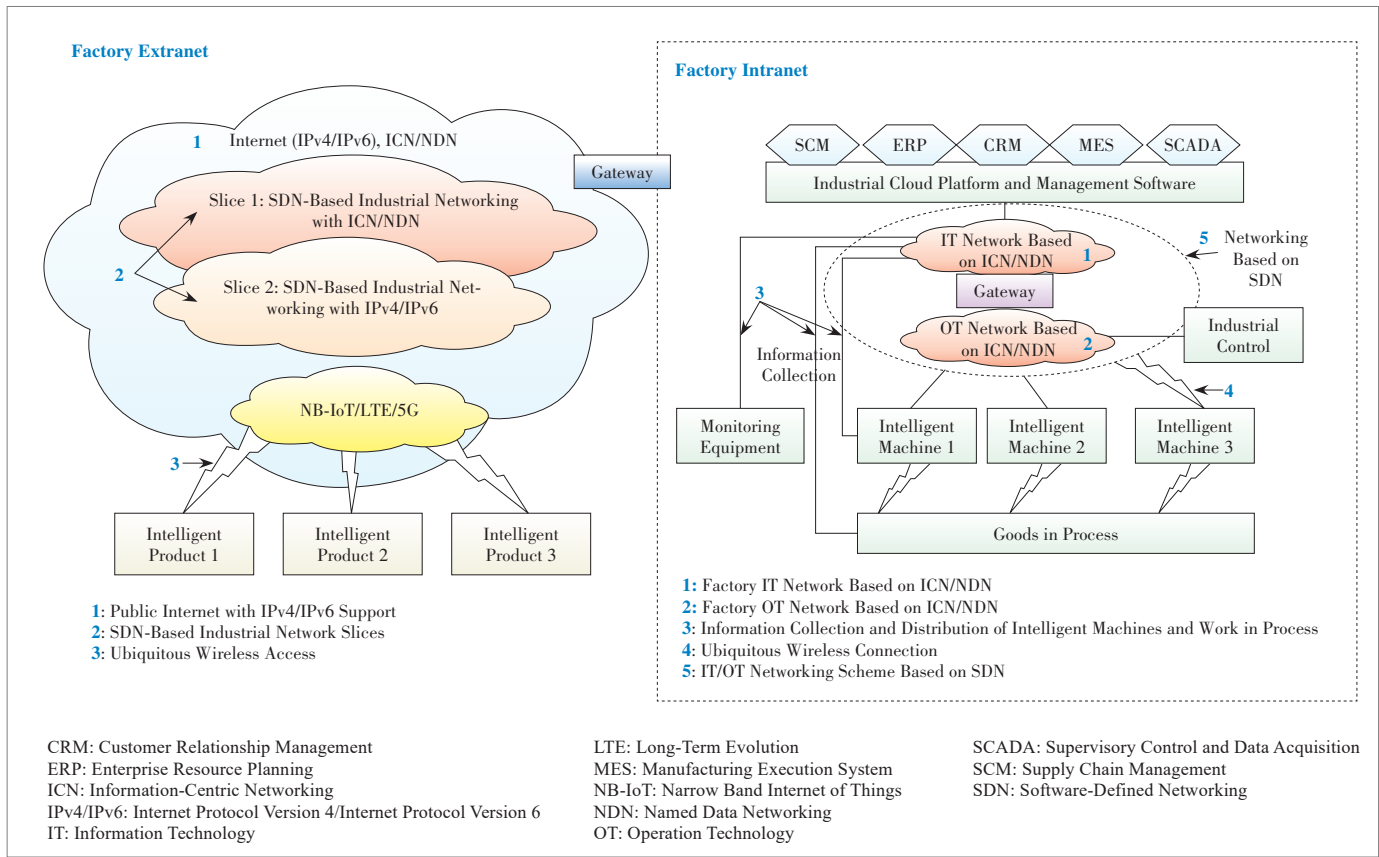
In order to meet the development of industrial network services, the networks need to guarantee efficient data transmission, flexible mobile access, convenient and differentiated demand, and industrial data security. It is urgent to introduce new network technologies to solve the problems including low utilization of network resources, redundancy and complexity of protocol, patchy security mechanism, and inflexible mobile access.

The data-centered ICN provides a solution to solve the above problems to some extent. ICN provides efficient content distribution, mobility support, and security support, bringing new opportunities for the development of industrial networks. In order to realize the deployment of ICN/NDN technology in the industrial network, we propose an overall framework design and a specific NDN-based factory extranet design with SDN.

#### 3.1.1 Framework Design

The overall framework design of ICN-based industrial network is shown in **Fig. 4**. Both factory intranet and factory extranet are ICN enabled. Moreover, we utilize SDN to manage and orchestrate both factory extranet and factory intranet, which resides in the threefold aspects. First, SDN can manage and orchestrate the high-dimensional and high-volume resources, especially the caching/computing/networking resources in ICN and large amounts of machines and equipment in the industrial Internet. Second, SDN can separate the control plane (routing protocol) from the forwarding devices to release more resources for processing and forwarding, so as to improve the network performance. Finally, SDN can provide network programmability to implement fresh information-centric schemes conveniently. As a result, it is convincing to implement the ICN-based industrial Internet in a software-defined architecture.

We take the factory extranet as an example. The factory ex-

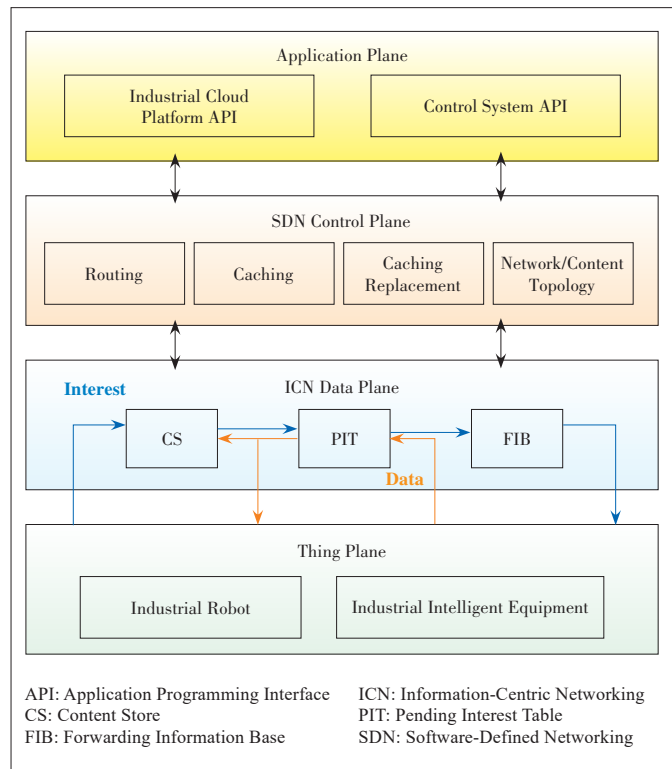


▲ Figure 4. A framework design of ICN-based industrial network.

trinet includes three main components. First, the public Internet supports the coexistence of IPv4/IPv6 and ICN/NDN. Due to the explosive growth of the number of industrial Internet terminals, the network based on IP addresses is unable to meet the needs of the industrial Internet. Therefore, ICN/NDN network mechanism is introduced to directly name the network content itself to solve problems such as insufficient IP addresses and difficult mobility support. Second, the network slices based on 5G or other network technologies are supported. Industrial networks can include multi-slice implementation of multi-protocol network configuration, such as SDN based IPv4/IPv6 industrial Internet slices and SDN based ICN/NDN industrial Internet slices. Third, ubiquitous wireless access is introduced. NB-IoT, LTE enhancement, 5G and other technologies are utilized to realize wireless access to various smart products.

### 3.1.2 NDN-Based Factory Extranet with SDN

Taking the representative NDN as an example, the specific deployment design of NDN-based factory extranet with SDN is shown in Fig. 5. Based on the characteristics of separating control and forwarding in SDN, we divide the NDN-based factory extranet architecture with SDN into four layers: the application plane, SDN control plane, ICN data plane, and thing



▲ Figure 5. The NDN-based factory extranet design with SDN.

plane.

#### 1) Application plane.

The application plane is responsible for interacting with the industrial internet cloud platform and control system and formulating network strategies which are implemented by the control plane. The application plane provides API interfaces to interact with the external environment and implements specific network functions by formulating network policies (such as load balancing, traffic scheduling, and resource allocation) to meet network performance requirements in different scenarios.

#### 2) SDN control plane.

The SDN control plane is responsible for the centralized control of the data plane devices. The SDN control plane holds the global topology of network nodes and contents within the network, uses the routing strategy to calculate the path, and installs the FIB table to the data plane devices. At the same time, the control plane grasps the caching strategies and caching replacement strategies, so as to carry out content caching under different requirements. The SDN control plane interacts with the application plane, providing the application plane with the underlying network information (e. g. , network traffic) and implementing the upper application's control instructions on the data plane devices.

#### 3) ICN data plane.

The ICN data plane, under the centralized control of the control plane, is responsible for packet forwarding and caching to quickly respond to content requests from the thing plane. Taking the NDN paradigm as an example, the content requests can be cached locally or routed through Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) tables in the form of Interest packets. The Data packages directly use the PIT table to return the content request nodes along the reverse paths of Interest packets, and at the same time, the local cache strategies are utilized to cache the content into CS. This process completes the content request and response.

#### 4) Thing plane.

The thing plane implements all devices accessing to the industrial Internet, such as industrial robots, industrial intelligent devices, and sensors. These devices act as network terminals, playing the role of content sources (collecting content) and/or content requesters for efficient content distribution and acquisition through the ICN data plane.

### 3.2 ICN-Based Identity Resolution in The Industrial Internet

Identity resolution in the industrial Internet needs to query the server addresses, which store product information using product identity, or directly query product information and related services. ICN/NDN is applied to the industrial Internet for identity resolution. We use content naming as the identification of products, components, and equipment. The name

resolution mechanism in ICN is used as the identity resolution scheme in the industrial Internet. ICN paradigms include the ICN architectures that implement name resolution and routing as independent functions (such as DONA, PURSUIT, SAIL, COMET, and MobilityFirst) and the ICN architectures that merge name resolution and routing functions (such as CCN and NDN) [22].

For the former paradigm, name resolution servers (called by different names) are organized hierarchically, and consumers and producers contact such servers to publish and subscribe to content in various ways. Consumers obtain the locations of publishers from name resolution servers and send their content requests to those locations to get the required content or services. Enabling the updates of name-to-address mapping is a non-trivial problem using hierarchical structures, spanning trees, or DHT-based organizations of servers.

For the later paradigm, NDN and CCNx merge name resolution and routing functions; in this way, routers are the fact name resolvers by establishing routes to name prefixes on a hop-by-hop basis. A major advantage of doing this is that it eliminates the complexity of designing and maintaining a network of name-resolution servers that replace the DNS. This merging of functionalities is supported by: 1) a name-based routing protocol operating in the control plane, which updates the entries in FIBs listing the next hops to known name prefixes, and 2) forwarding interests based on the Longest Prefix Match (LPM) between the Content Object (CO) name in the interest and a name prefix listed in the FIBs.

We design from these two types as follows.

#### 3.2.1 Identity Resolution Based on ICN with Separate Resolution Nodes

Name resolution in DONA is provided by specialized servers called Resolution Handlers (RHs).

There is at least one logical RH at each Autonomous Systems (AS). The multi-level identity resolution system in the industrial Internet can adopt DONA's multi-level RH architecture, including four levels: root node, national top-level node, secondary identity resolution node, and enterprise identity resolution node. When the identity resolution system in the industrial Internet is deployed by ICN with separate resolution nodes, the current network technology can still be used at the network layer and below, or ICN can be directly deployed at the network layer. When ICN is directly deployed in the industrial network layer, it can be used as both routing and identity resolution system, so as to realize the integrated design of identity resolution and routing.

As shown in **Fig. 6** the content provider needs to send the registration information to the identity resolution system to complete the registration (Fig. 6, step 1). The user queries the identity resolution system for the content provider that can provide the required content object. The identity resolution system finds the most appropriate content provider based on



the content identity name, which may be the registered content provider or the cache on the resolution node (Fig. 6, step 2). The content object is returned directly to the user along the reverse path (Fig. 6, step 3).

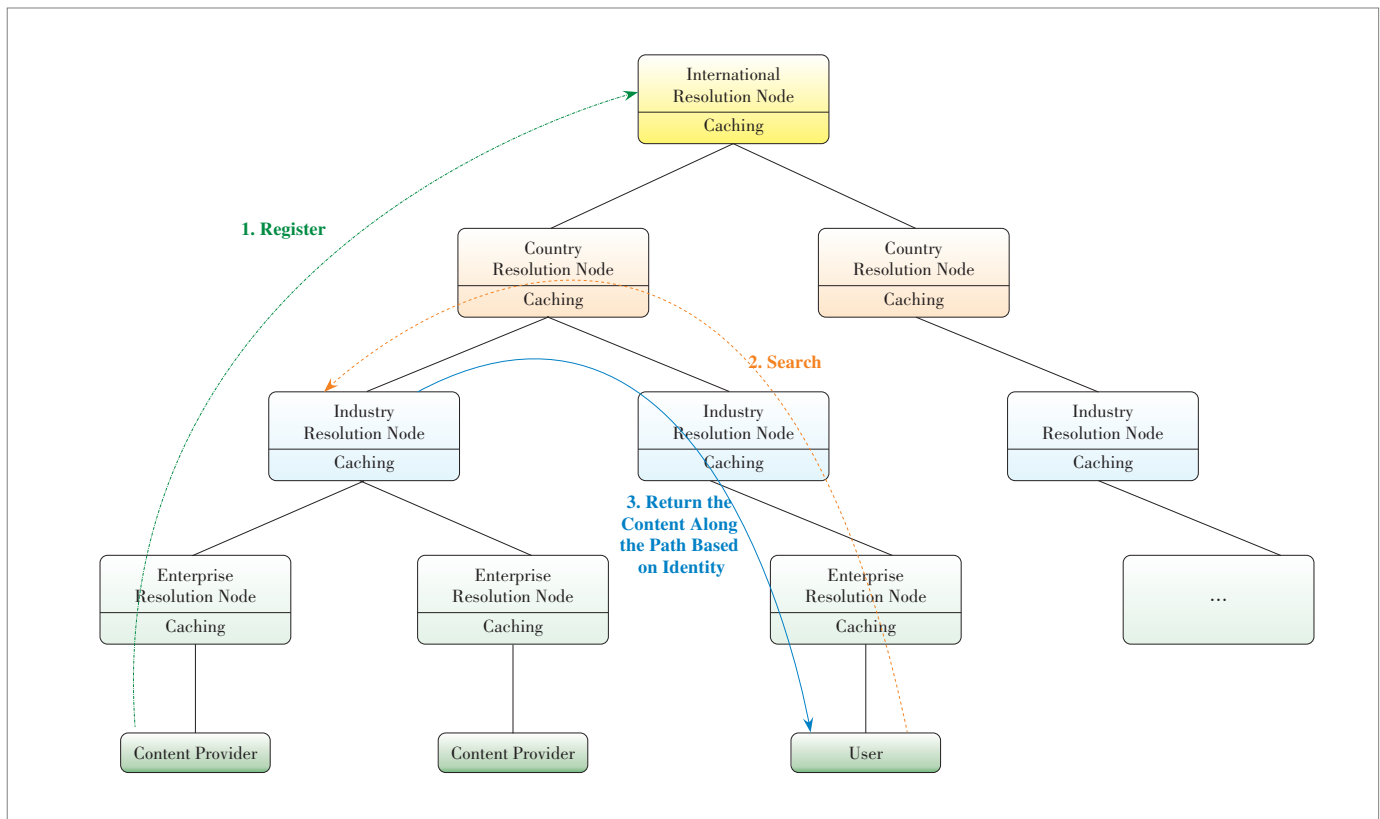
### 3.2.2 Identity Resolution Based on ICN with Merging Resolution and Routing

The NDN paradigm can directly merge the name resolution and routing. Specifically, NDN implements content name-based routing and forwarding based on name-based routing protocols without the need for a DNS server to query the server location. This characteristic of the NDN network provides an effective solution to integrate network routing and identity

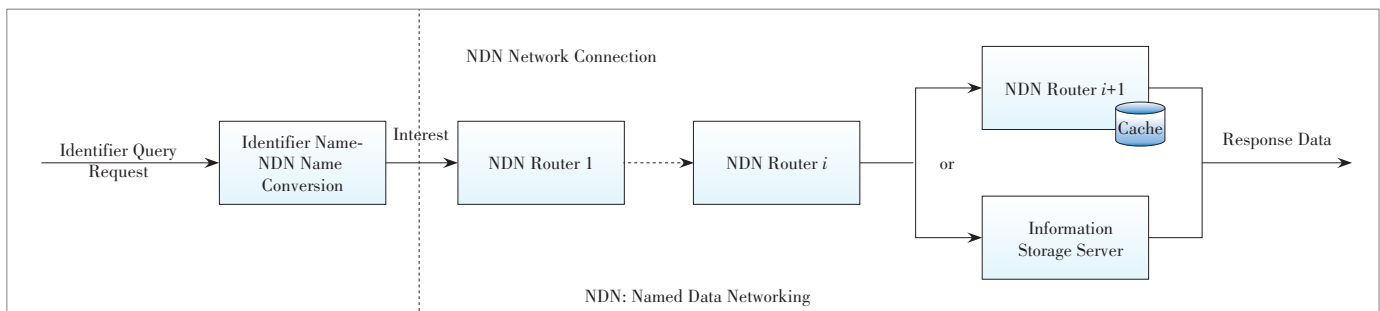
resolution. The merging architecture is shown in Fig. 7.

As shown in Fig. 7, the identifier name-NDN name conversion module is responsible for converting the queried identifier name into the naming format of NDN, that is, to obtain the NDN identifier name, so that the identifier query request can be forwarded in NDN. The NDN router is responsible for forwarding the interest packets and data packets, and stores the passing data packets into the local cache. The information storage server stores the identifier name, corresponding NDN identifier name, and its information.

The identifier query request first needs to be constructed as an interest packet conforming to the NDN naming format before accessing the NDN network, so that the interest packet



▲ Figure 6. Identity resolution and routing architecture based on data-oriented network architecture.



▲ Figure 7. Architecture of merging identity resolution and routing based on NDN.

can be forwarded in NDN. Until the NDN identifier name is found in the NDN router cache or the information storage server, the corresponding information data packet is returned to the identification query request node along the reverse path of the interest packet to complete the information query response.

The designs of the identifier name-NDN name conversion module and information storage server are as follows.

1) The identifier name-NDN name conversion module.

In order to integrate identity resolution and NDN networks, it is imperative to unify NDN naming and identifier names. Since NDN naming is hierarchical, and the existing identifier names include different parts; besides, both NDN naming and identifier names are variable-length naming, so NDN naming is very suitable for compatibility with a variety of identifier names.

Specifically, since each part of the NDN hierarchical naming is separated by “/”, while the delimiters of different identifier names are different, the identifier name-NDN name conversion module is responsible for unifying the various delimiters of identifier names as “/”. Besides, the NDN identifier name also uses the identification mechanism as the prefix to avoid conflicts between different identification systems. At the same time, it enhances the aggregation of the NDN identifier name and improves query efficiency. We have to note that the identifier name-NDN name conversion module is executed before the request packet accesses the NDN network, such as end devices.

We use OID as an example to describe the conversion process. The OID mechanism has OID numeric value, OID alphanumeric value, and OID Internationalized Resource Identifier (OID-IRI). For numeric values, different levels are separated by “.”, such as {2. 17. 2. 3} which is converted to NDN identifier name as /OID/2/17/2/3. For alphanumeric values, it is exemplified by {joint-iso-itu-t (2) registration-procedures (17) document-types (2) binary (3)}, which is converted to NDN identifier name as /OID/joint-iso-itu-t (2)/registration-procedures (17)/document-types (2)/binary (3). For OID-IRI, the example is /Joint-ISO-ITU-T/Registration-Procedures/Document Types/Binary, which is converted to NDN identifier name as /OID/Joint-ISO-ITU-T/Registration-Procedures/Document Types/Binary.

2) The information storage server.

Since the identifier name is uniformly converted by the identifier name-NDN name conversion module before accessing the NDN network, the registration of the identifier name in the information storage server should also include the converted NDN identifier name. Each record in the information storage server contains the identifier name, NDN identifier name, and information content.

**Fig. 8** shows the following workflow of the process of registration as well as the identifier query request and response in the proposed merging architecture.

1) Register and publish in the information storage server.

a) Register: When a new identifier name and its corresponding information content are to be registered and stored in the information storage server, the identifier names of all entries in the information storage server are searched for the identifier name to be registered. If it exists, it means that the identifier name already exists in the information storage server, thus updating the information content. If it does not exist, a new entry is added to the information storage server to record this identifier name and its information content. The NDN identifier name is also recorded, which is obtained according to the conversion rule in the identifier name-NDN name conversion module. Due to applying the same conversion rules, the NDN identifier name stored in the server is consistent with the NDN identifier name converted when the identifier query request is made. The registration entry of product 1 is shown in Fig. 8.

b) Publish: The information storage server publishes the locally stored NDN identifier name, so that the NDN network can perform routing and forwarding according to the NDN identifier name.

2) End device 1 requests an identifier query.

a) End device 1 gets the identifier name {2. 17. 2. 3} of product 1 and converts it to the NDN identifier name /OID/2/17/2 by local identifier name-NDN name conversion model. And then, it constructs an interest packet sending to the NDN network.

b) When the NDN router receives this interest, it processes and forwards the interest according to the standard NDN node processing model [20]. That is, it looks up in the local cache. If the corresponding data exists, it will return the data packet immediately; otherwise, it forwards this interest based on PIT and FIB.

c) The interest packet reaches the information storage server through R1 and R2. The information storage server searches the NDN identifier name. If it exists, the information storage server returns the data packet (/OID/2/17/2/3); otherwise, it discards the interest.

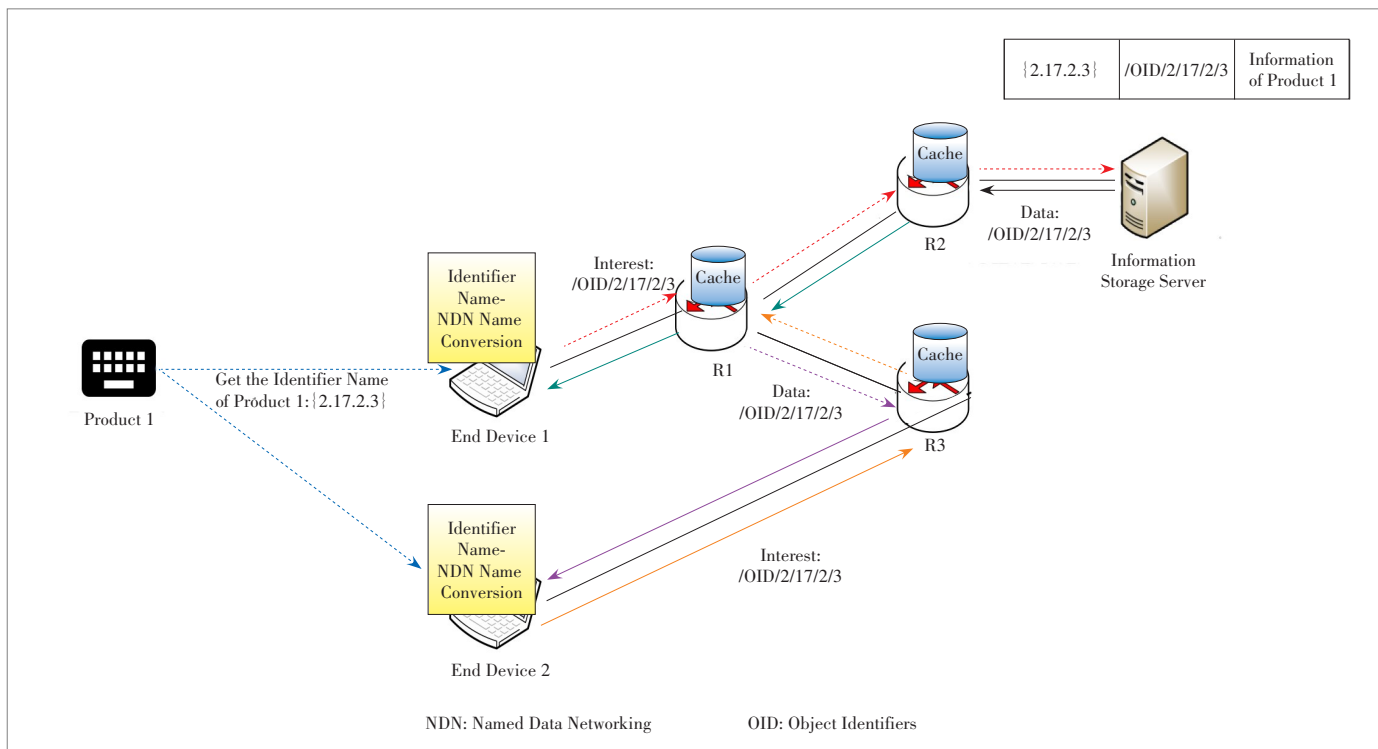
d) When the NDN router receives this data packet, it returns the data packet to end device 1 along the reverse way of interest according to the standard NDN node processing model [20], and caches this data packet according to the local caching strategies. The cached entry in the local cache contains /OID/2/17/2 and the information of product 1.

3) End device 2 requests the same identifier query.

a) End device 2 also requests to query the information of this product. It obtains the identifier name of product 1, and converts it to the NDN identifier name. It constructs an interest packet and sends the interest to the NDN network.

b) When this interest arrives at R1 via R3, because this product information is already stored in the local cache of R1, R1 can directly return the data packet (/OID/2/17/2/3).

c) The data packet is returned from R1 to end device 2 via R3, thus completing the identifier query request.



▲ Figure 8. The workflow of the merging architecture.

## 4 Conclusions

In this paper, we overviewed the industrial network, industrial Internet identity, and ICN. We presented an integrated architecture for industrial network and industrial Internet identity. We proposed the overall framework of ICN-based industrial network and NDN-based factory extranet with SDN. We also addressed the architecture of identity resolution in the industrial Internet based on ICN with separate resolution nodes or with merging resolution and routing. By introducing ICN into the industrial Internet, we realized the integration of industrial network and identity resolution system, flattening the overall architecture of the industrial Internet, improving the efficiency of information retrieval, network scalability, and data security.

## References

- [1] DUAN S H, GAO W, WANG J P. A Novel Network Control Architecture for Large Scale Machine in Industrial Internet [C]//IEEE International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI). Beijing, China, 2015: 229 - 232. DOI: 10.1109/iiki.2015.56
- [2] XYLOMENOS G, VERVERIDIS C N, SIRIS V A, et al. A Survey of Information-Centric Networking Research [J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 1024 - 1049. DOI: 10.1109/surv.2013.070813.00063
- [3] GOGOLEV A, MENDOZA F, BRAUN R. TSN-Enabled OPC UA in Field De-

vices [C]//IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). Turin, Italy, 2018: 297 - 303. DOI: 10.1109/etfa.2018.8502597

- [4] MANNWEILER C, GAJIC B, ROST P, et al. Reliable and Deterministic Mobile Communications for Industry 4.0: Key Challenges and Solutions for the Integration of the 3GPP 5G System with IEEE [C]//Mobile Communication-Technologies and Applications; 24. ITG-Symposium. Osnabrueck, Germany, 2019: 1 - 6
- [5] NSAIBI S, LEURS L, SCHOTTEN H D. Formal and Simulation-Based Timing Analysis of Industrial-Ethernet Sercos III over TSN [C]//IEEE/ACM 21st International Symposium on Distributed Simulation and Real Time Applications (DS-RT). Rome, Italy, 2017: 83 - 90. DOI: 10.1109/distra.2017.8167670
- [6] BRUCKNER D, BLAIR R, PSTANICA M, et al. OPC UA TSN-A New Solution for Industrial Communication [R]. B&R Industrial Automation, 2018
- [7] AL-GUMAEI K, SCHUBA K, FRIESEN A, et al. A Survey of Internet of Things and Big Data Integrated Solutions for Industrie 4.0 [C]//IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). Turin, Italy, 2018: 1417 - 1424. DOI: 10.1109/etfa.2018.8502484
- [8] IETF. Deterministic Networking Architecture: RFC 8655 [S]. 2019
- [9] CHAUDHARY R, AUJLA G S, GARG S, et al. SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment [J]. IEEE Transactions on Industrial Informatics, 2018, 14(6): 2629 - 2640. DOI: 10.1109/tii.2018.2789442
- [10] LI X M, LI D, WAN J F, et al. Adaptive Transmission Optimization in SDN-Based Industrial Internet of Things with Edge Computing [J]. IEEE Internet of Things Journal, 2018, 5(3): 1351 - 1360. DOI: 10.1109/jiot.2018.2797187
- [11] DATTA S K, BONNET C. MEC and IoT Based Automatic Agent Reconfiguration in Industry 4.0 [C]//IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). Indore, India, 2018: 1 - 5. DOI: 10.1109/ants.2018.8710126
- [12] UGWUANYI E E, GHOSH S, IQBAL M, et al. Reliable Resource Provisioning Using Bankers' Deadlock Avoidance Algorithm in MEC for Industrial IoT [J]. IEEE Access, 2018, 6: 43327 - 43335. DOI: 10.1109/access.2018.2857726
- [13] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Communication for Automation in Vertical

- Domains: TR 22.804 [S]. 2017
- [14] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for Cyber-Physical Control Applications in Vertical Domains: TR22.104 [S]. 2019
- [15] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security for 5GS Enhanced Support of Vertical and LAN Services: TR 33.819 [S]. 2020
- [16] BROCK D L. The Electronic Product Code (EPC) [R]. Cambridge, United States: Auto-ID Center White Paper MIT-AUTOID-WH-002, 2001
- [17] Orange SA. Object Identifier (OID) Repository [EB/OL]. (2020-01-05). <http://www.oid-info.com>
- [18] IETF. Handle System Overview: RFC 3650 [S]. 2003
- [19] MAEDA M. System and Method for Initially Configuring and Booting a Device Using a Device Identifier: U.S. Patent No. 7293168 [P]. 2007-11-06
- [20] 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
- [21] KOPONEN T, CHAWLA M, CHUN B G, et al. A Data-Oriented (and Beyond) Network Architecture [J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 181. DOI: 10.1145/1282427.1282402
- [22] GARCIA-LUNA-ACEVES J J, MIRZAZAD-BARIJOUGH M, HEMMATI E. Content-Centric Networking at Internet Scale through the Integration of Name Resolution and Routing [C]//3rd ACM Conference on Information-Centric Networking (ACM - ICN' 16). Kyoto, Japan, 2016: 83 - 92. DOI: 10.1145/2984356.2984359

### Biographies

**LU Hua** received his master's degree in information and communication from Jeonbuk National University, Republic of Korea. He is the director of the Network Technology Innovation Center of Guangdong Communication & Network Institute, China. He worked with ZTE Corporation and was engaged in the research and development of wireless base stations, core networks, bearer

networks, virtualization and other system products. He has 15-year experience of research and development of industrialization in baseband channel codec, voice codec, router, and virtualization. His research interests include new network architecture, software-defined networking, P4 programmable, and virtualization.

**LI Xiaolu** (lixiaolu@bupt.edu.cn) received her B.S. degree in telecommunication engineering from Beijing University of Posts and Telecommunications (BUPT), China in 2017. She is currently working toward her Ph.D. degree at the State Key Laboratory of Networking and Switching Technology, BUPT. Now she is visiting Carleton University, Canada as a visiting Ph.D. student. Her current research interests include future network architecture design, information centric networking, software defined networking, edge intelligence, and the industrial Internet.

**XIE Renchao** received his Ph.D. degree from the School of Information and Communication Engineering, BUPT in 2012. From July 2012 to September 2014, he worked as a postdoctoral researcher at China Unicom. From November 2010 to November 2011, he visited Carleton University as a visiting scholar. He is currently an associate professor with BUPT. His current research interests include future network architecture design, information centric networking, 5G networks, and the industrial Internet. He has published more than 30 journal and conference papers. He served on the Technical Program Committees (TPCs) of Chinacom 2016 and 2012 IEEE Vehicular Technology Conference (VTC)-Spring. He has also served for several journals and conferences as a reviewer, including IEEE Transactions on Communications, ACM/Springer Wireless Networks, the EURASIP Journal on Wireless Communications and Networking, Wireless Communications and Mobile Computing (Wiley), IEEE Communications Letters, 2011 IEEE GLOBECOM, and so on.

**FENG Wei** is a visiting scholar of University of Cambridge, United Kingdom. He is working at the Department of Information Technology Application and Software Services, Ministry of Industry and Information Technology of People's Republic of China. His research interest is the industrial Internet of Things.