

## Views &amp; Comments

## Networking Automation and Intelligence: A New Era of Network Innovation

Hongke Zhang<sup>a,b,#</sup>, Wei Quan<sup>a,#</sup><sup>a</sup> National Engineering Laboratory for Next Generation Internet Technologies, Beijing Jiaotong University, Beijing 100044, China<sup>b</sup> Research Center of Networks and Communications, Peng Cheng Laboratory, Shenzhen 518000, China

The origin of the Internet can be traced back to the late 1960s. As the progenitor of the Internet, the Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switching network, with the main goal of enabling access to remote computers and exchanging data among several authorized computers. Over the latest decade, the Internet has achieved massive development, with billions of devices (including phones, computers, and even sensors) now easily connecting to it. Forecasts from IHS Markit show that the number of connected Internet of Things (IoT) devices increases annually by 12% on average and will surge to 125 billion by 2030 (Fig. 1(a)); furthermore, global data transmissions will increase annually by 50% on average in the next 15 years [1]. However, this rapid trend greatly increases the network complexity. Due to a lack of automation, current networks are facing unprecedented challenges in terms of network management and operations efficiency, which cannot be ignored [2].

The emerging applications also place various demands on the network infrastructure. For example, the high-speed railway (HSR) requires a network to support its high mobility (e.g., 350 km·h<sup>-1</sup>, Fig. 1(b)), the industrial IoT requires extra-low latency (e.g., below 1 ms), and military communication requires extra-high security and reliability. These demands coexist yet sometimes seem to be contradictory. For example, to improve security, cryptographic computing and complex authentication can be introduced. Without any doubt, complex computing will increase the transmission latency. In fact, it is difficult to expect any single unintelligent network to be reliable, flexible, expandable, secure, and cost-effective. This means that the network must have intelligent capacities and be capable of automatically performing a series of balancing actions.

### 1. Networking automation and intelligence

The concept of networking automation and intelligence provides a promising roadmap to cope with upcoming network requirements and ever-growing challenges. In fact, the idea of a network with intelligence is not new. As early as 2003, Professor David D. Clark from Massachusetts Institute of Technology (MIT)

proposed building a so-called *knowledge plane* for the Internet and analyzed the main challenges of doing so [3]. With funding from the National Basic Research Program of China (973 Program), we pointed out that such a network should be full of intelligence and involve collaboration in order to meet various new service requirements according to automatic flexible identifier mapping [4,5]. Professor Jiangxing Wu from National Digital Switching System Engineering & Technological R&D Center (NDSC), an academician of the Chinese Academy of Engineering, also proposed a polymorphic smart network (PINet) architecture to support multiple full-dimensionally definable network modals [6,7]. This prospective research played a foundational role in the development of network automation and intelligence.

In the last few years, networking automation and intelligence have attracted a great deal of research interest in the industry. Intent-based networking (IBN), proposed by Cisco, focuses on changing the way in which networks are managed, by abstractly expressing an intention as a specific management rule. Autonomous driving networking (ADN) and intent-driven networking (IDN), promoted by Huawei, aim to automatically validate, deploy, and optimize network functions based on the user's intention by decoupling network control logic. Juniper has also presented a vision of a self-driving network, which can measure and control in an automated manner [8]. Similarly, the zero-touch network (ZTN) promoted by the European Telecommunications Standards Institute (ETSI) Zero Touch Network and Service Management (ZSM) group is defined as having automation capacities, including specific upgrades based on configured services, automatic service placement, and service motion [9]. Knowledge-defined networking (KDN) has been put forward and is generally supported by mainstream companies, such as Broadcom, Cisco, Intel, and Nippon Telegraph & Telephone (NTT) [10,11]. We believe that networking automation is the most important and promising direction for network development thus far. Table 1 [3–11] lists the main research in this field.

### 2. Challenges and functional capabilities

Thanks to the aforementioned efforts, remarkable progress has been made in promoting further innovation in network

# These authors contributed equally to this work.

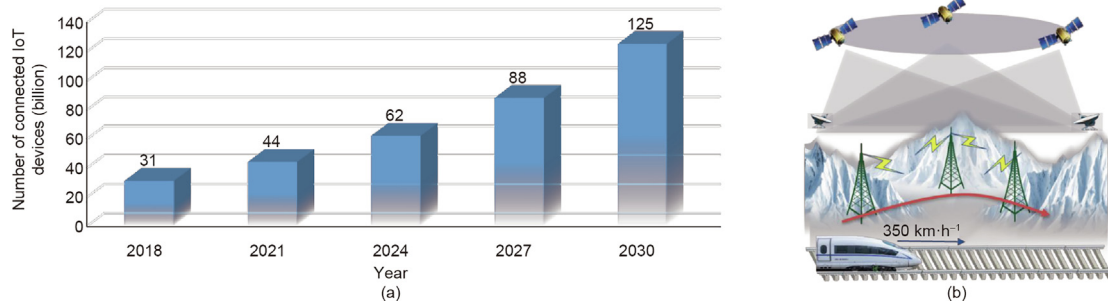


Fig. 1. (a) The rapidly increasing trend in the number of IoT devices; (b) emerging HSR network scenarios. HSR: high-speed railway.

Table 1  
Research on networking automation and intelligence.

Number	Research and project name	Organizations	Countries/regions	References
1	Knowledge plane for the Internet	MIT	United States	[3]
2	SINET	NGIT	China	[4,5]
3	PINet	NDSC	China	[6,7]
4	IBN	Cisco	United States	—
5	ADN	Huawei	China	—
6	Self-driving network	Juniper	United States	[8]
7	IDN	Huawei	China	—
8	ZTN	ETSI, Ericsson	European Union	[9]
9	SONIC	Microsoft	United States	—
10	KDN	Polytechnic University of Catalonia, Broadcom, Cisco, Intel, NTT, etc.	Spain, United States, Japan, etc.	[10,11]

SINET: smart identifier networking; SONIC: software for open networking in the cloud; NGIT: National Engineering Laboratory for Next Generation Internet Technologies.

automation and intelligence. However, integral network automation is a long-term process with continuous iterative functional evolutions. First and foremost, for the new era of network innovation, a novel network functional architecture is required to support networking automation and intelligence. There are several challenges involved in building a high-level intelligent network architecture. Below, we list three main technical challenges, which are also our proposed technical goals in the near future.

(1) **High-level network awareness:** The network intelligence should understand users' intentions and automatically translate them into network operations. It should constantly be able to automatically monitor the network statuses, health conditions, and service requirements.

(2) **High-level network automation:** The network automation should automatically configure corresponding hardware or software parameters to meet the predefined target states. It should also perform self-correction to address issues or to bring itself back to the desired state. In addition, it should automatically manage network users and update service functions.

(3) **High-level network diagnosis:** The network should constantly communicate with the environment, reporting and exchanging necessary diagnosis information. It should analyze and perform introspection, defend from external and internal threats, and self-heal with service motion feedback.

To achieve the aforementioned goals, we believe that the network functional architecture should be equipped with many core capabilities for networking automation. Here, we provide a brief summary of 12 core functional capabilities that are required. The network functional architecture must: ① self-recognize and understand user intentions; ② self-translate intentions into network operations; ③ self-monitor the network environment and statuses; ④ self-detect various service requirements; ⑤ self-configure required functions; ⑥ self-correct when a decision error is detected; ⑦ self-manage network users, such as malicious users; ⑧ self-update service functions to optimize delivery; ⑨ self-analyze introspection using machine learning; ⑩ self-

defend from external and internal threats; ⑪ self-heal with service motion feedback; and ⑫ self-report when an unexpected situation arises. The relationship between technical challenges and core required capabilities is shown in Table 2.

### 3. The smart identifier networking (SINET) paradigm

The future network should incorporate all types of superior advanced network technologies for smart collaboration [12]. With this perspective, SINET is proposed based on prior works [13,14]. Fig. 2 shows the functional architecture of SINET.

Table 2  
Technical challenges and core capabilities of networking automation.

Technical challenges	Core required capabilities and research issues
High-level network awareness	<ul style="list-style-type: none"> <li>• Self-recognize and understand user intentions</li> <li>• Self-translate intentions into network operations</li> <li>• Self-monitor the network environment and statuses</li> <li>• Self-detect various service requirements</li> </ul>
High-level network automation	<ul style="list-style-type: none"> <li>• Self-configure required functions</li> <li>• Self-correct when a decision error is detected</li> <li>• Self-manage network users, e.g., malicious users</li> <li>• Self-update service functions to optimize delivery</li> </ul>
High-level network diagnosis	<ul style="list-style-type: none"> <li>• Self-analyze introspection using machine learning</li> <li>• Self-defend from external and internal threats</li> <li>• Self-heal with service motion feedback</li> <li>• Self-report when an unexpected situation arises</li> </ul>

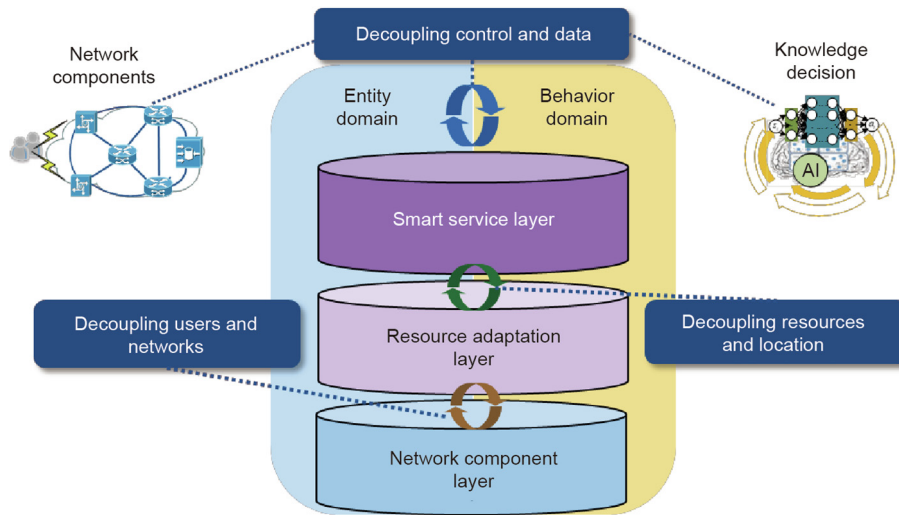


Fig. 2. SINET functional architecture. AI: artificial intelligence.

To promote network automation and intelligence, SINET is vertically divided into three layers and horizontally divided into two domains. The three layers include the smart service layer, the resource adaptation layer, and the network component layer, while the two domains are the behavior domain and the entity domain.

- The smart service layer is mainly in charge of translating users' intentions and managing the registered services. The resource adaptation layer dynamically schedules network resources and builds function-groups to satisfy the service demand from the smart service layer. The network component layer is mainly used to coordinate network components to carry out specific network operations.
- The behavior domain is a specific functional domain for network awareness and network diagnosis. It is composed of digital information (labeled by behavior descriptions) in three layers, and is in charge of analyzing network behaviors and service requirements. It is also the policy conveyancer that generates the decisions or the rules for specific actions. The entity domain is composed of actual network entities

(labeled by entity identifiers), and acts as the actual executor according to the decisions from the behavior domain.

Based on this novel network functional architecture, vertical autonomic mappings among the three layers are further introduced to enable the network to dynamically meet various service requirements and allow it to update its service functions in order to intelligently optimize delivery. In addition, horizontal autonomic mappings between the two domains promote network automation according to the network awareness and diagnosis. Fig. 3 illustrates an example of how SINET supports network intelligence.

- **From the top down, SINET accomplishes self-service awareness and self-function deployment.** The smart service layer converts the user's intentions into specific network requirements, such as bandwidth and delay, which are further passed on to the resource adaptation layer. When receiving the service demands, the resource adaptation layer orchestrates function-groups while the network controller generates optimal packet transmission schemes. At the network component layer, reasonable components are coordinated to form function-groups that can carry out the specific tasks.

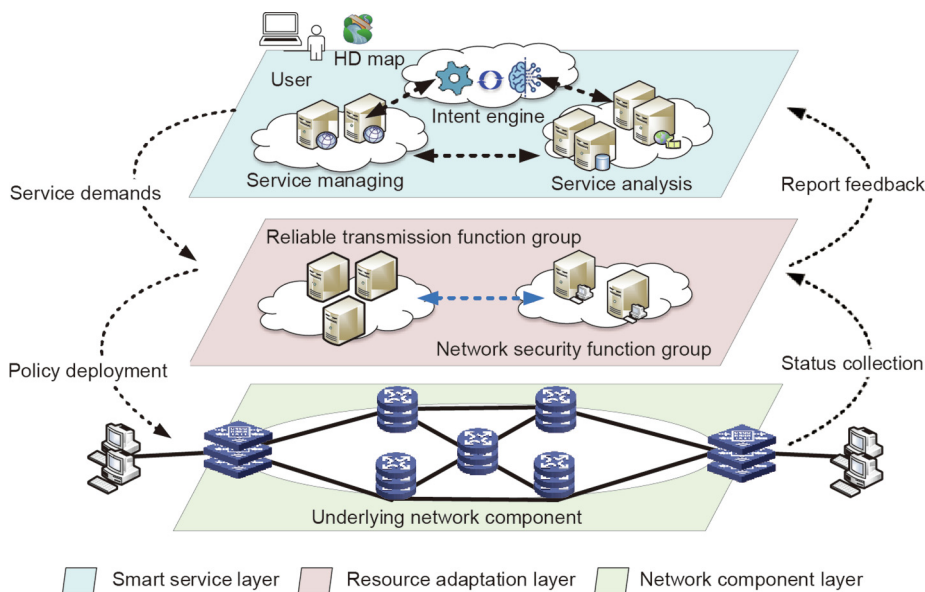


Fig. 3. An application illustration in SINET. HD: high definition.

- **From the bottom up, SINET accomplishes self-feedback, self-diagnosis, and optimization.** Network telemetry technologies, such as in-band network telemetry, are applied in the network component layer to monitor the network and resource statuses, such as bandwidth, latency, and queue occupancy. These telemetry metrics are further analyzed for updating function orchestration and optimizing packet transmission in the resource adaptation layer. In addition, service execution reports and notifications are sent to the smart service layer for self-healing with service motion feedback.

The above analysis simply explains how SINET enhances network automation and intelligence. Automatic perception and acquisition in the entity domain can provide information for self-analysis and other capabilities, which enhances the automation of SINET. Intelligent data analysis in the behavior domain can improve capabilities such as self-configuration, and realizes the intelligence of SINET. This decoupled design provides significant benefits in promoting network automation and intelligence, and hence has great potential for improving network performance in many aspects, such as security, mobility, energy consumption, and efficiency.

#### 4. Conclusions

Networking automation opens up a new era of network innovation, while providing new challenges to network researchers. The vision of networking automation is not just an idealistic one; the networking industry is already on the move toward this goal. It is worth mentioning that network intelligence is currently in the ascendant, requiring more peer researchers to participate, collaborate, and make contributions to innovate the network infrastructure, in order to achieve the most ambitious goal in the networking industry.

#### Acknowledgments

This work is supported by the National Key Research and Development Program (2018YFE0206800), the National Natural Science Foundation of Beijing (4212010), and the Major Key Project of Peng Cheng Laboratory (PCL2022Y04).

#### References

- [1] The Internet of Things: a movement, not a market. Report. London: IHS Markit.
- [2] Kerravala Z. Digital transformation requires an autonomous network. Report. San Jose: Extreme Networks; 2019 May.
- [3] Clark DD, Partridge C, Ramming JC, Wroclawski JT. A knowledge plane for the Internet. In: Proceedings of the SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication; 2003 Aug 25–29; Karlsruhe, Germany; 2003.
- [4] Zhang H, Su W. Fundamental research on the architecture of new network—universal network and pervasive services. *Chin J Electron* 2007;35(4):594–8. Chinese.
- [5] Zhang H, Luo H. Fundamental research on theories of smart and cooperative networks. *Chin J Electron* 2013;41(7):1249–54. Chinese.
- [6] Wu J. Thoughts on the development of novel network technology. *Sci China Inf Sci* 2018;61(10):101301.
- [7] Hu Y, Li D, Sun P, Yi P, Wu J. Polymorphic smart network: an open, flexible and universal architecture for future heterogeneous networks. *IEEE Trans Netw Sci Eng* 2020;7(4):2515–25.
- [8] Kalmbach P, Zerwas J, Babarczy P, Blenk A, Kellerer W, Schmid S. Empowering self-driving networks. In: Proceedings of ACM SIGCOMM 2018 Afternoon Workshop on Self-Driving Networks (SelfDN 2018); 2018 Aug 24; Budapest, Hungary; 2018.
- [9] Gallego-Madrada J, Sanchez-Iborrab R, Ruiz PM, Skarmeta AF. Machine learning-based zero-touch network and service management: a survey. *Digit Commun Netw* 2022;8(2):105–23.
- [10] Mestres A, Rodriguez-Natal A, Carner J, Barlet-Ros P, Alarcón E, Solé M, et al. Knowledge-defined networking. *ACM SIGCOMM. Comput Commun Rev* 2017;47(3):2–10.
- [11] Wu D, Li Z, Wang J, Zheng Y, Li M, Huang Q. Vision and challenges for knowledge centric networking. *IEEE Wirel Commun* 2019;26(4):117–23.
- [12] Zhang H, Quan W, Chao H, Qiao C. Smart identifier network: a collaborative architecture for the future internet. *IEEE Netw* 2016;30(3):46–51.
- [13] Zhang H, Feng B, Quan W. Fundamental research on smart integration identifier networking. *Chin J Electron* 2019;47(5):977–82. Chinese.
- [14] Quan W, Zhang H. Future Internet architecture: research status, hot topics, and development practice. *Sci China Sin Inf* 2017;47(6):804–10. Chinese.