论文推荐

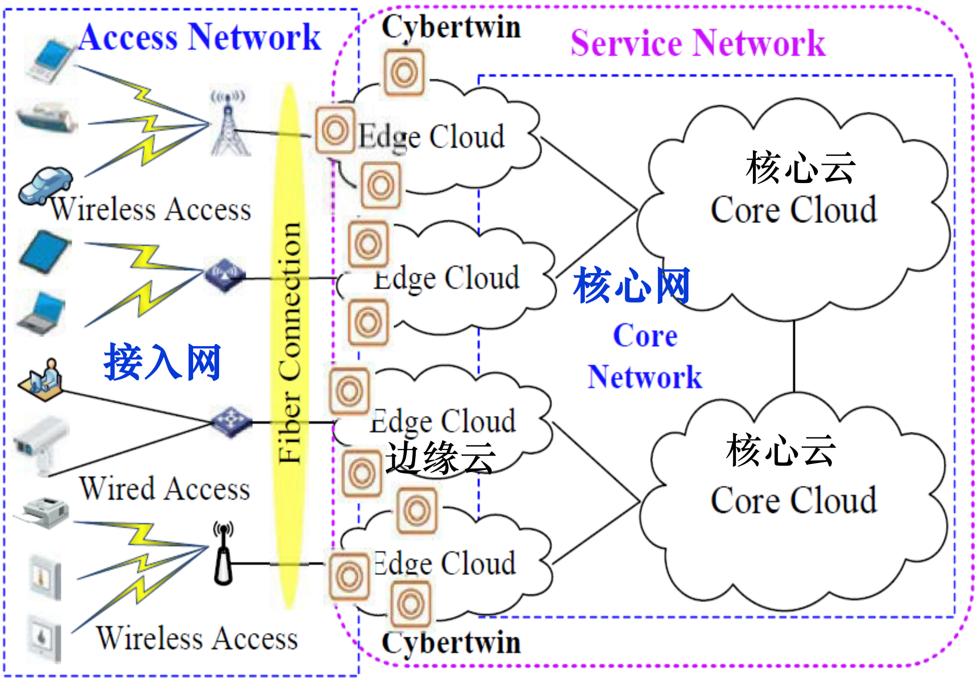
鹏城实验室于全院士团队：基于赛博孪生（Cybertwin）的下一代网络架构

临菲信息技术港

万物互联及其应用的快速发展，呼唤新的网络架构。鹏城实验室于全院士团队 2019 年 12 月在 IEEE Wireless Communications 发表论文“Cybertwin: An Origin of Next Generation Network Architectur”，提出了基于赛博孪生（cybertwin）的下一代网络架构。

基于 Cybertwin 的网络架构

该文提出的基于 cybertwin 的下一代网络体系结构，适应于未来网络从端到端（end-to-end）连接至云到端（cloud-to-end）连接的演进。



基于 cybertwin 的下一代网络架构

这种新架构，可用四个关键组件、三种网络和三种服务商来概括：

1、四个关键组件

- **核心云**

通过高速光链路全连接，构成核心网。与现有云网络不同，这些核心云作为网络基础设施服务，为终端提供计算、缓存和通信资源。

- **边缘云**

更快地响应终端请求，帮助核心云提供很高质量的网络服务。

- **赛博孪生（cybertwin）**

Cybertwin 是虚拟网络空间中"人"和"物"的数字表示，提供最核心的网络功能。

- **终端**

"终端"即网络中的人和物，通过对应的 cybertwin 直接从网络获取服务。

2、三个网络

- **接入网**

负责终端与边缘云的连接。有线和无线都可。

- **核心网**

负责边缘云和核心云之间、以及所有核心云之间的连接。

- **服务网**

用于应用服务的逻辑网络，部署在云网络的顶部，为终端提供服务。

3、三种运营商

- **电信运营商**

提供接入网终端和云之间、以及核心网不同云之间的高速通信管道。它可以将其网络资源出售或出租给云运营商。

- **云运营商**

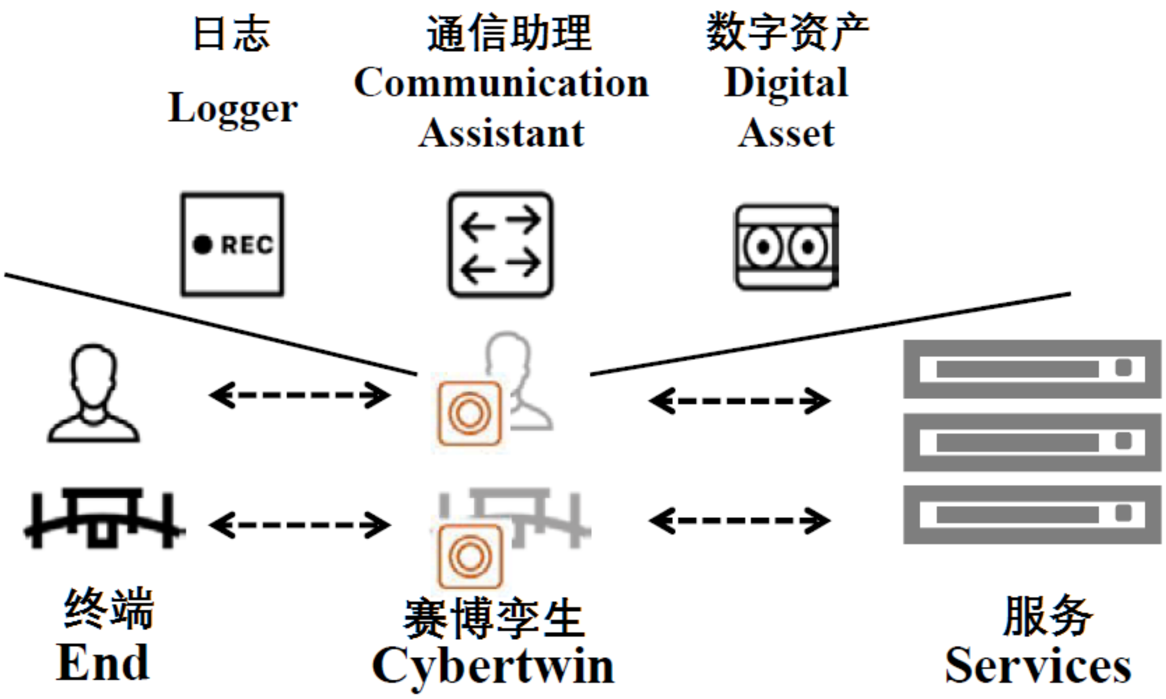
提供信息基础设施服务而非一般信息服务的一种新的运营商。

- **应用服务提供商**

将其应用和内容服务委托给云运营商，提高服务质量并降低成本。

Cybertwin 的主要功能

赛博孪生（Cybertwin）具有多种功能：通信助理、日志（网络行为记录）和数字资产等。



基于赛博孪生的通信

- **通信助手**

Cybertwin 是人或物在虚拟世界的表示，它作为物理世界中人或物的助手，能够更好地实现多种用户体验。基于 cybertwin 的通信模型要求终端首先连接到它的 cybertwin，cybertwin 代表该终端从云网络获取所需的服务。所需服务由边缘云和核心云通过分布式云网络操作系统共同提供，该操作系统汇集了各种计算、缓存和通信资源。

- 日志

通信通过 cybertwin 完成，这意味着 cybertwin 可以实时获取并记录有关终端行为的所有数据。与传统的数据获取和存储不同，这些数据属于终端“孪生”cybertwin，而不属于运营商。

- **数字资产**

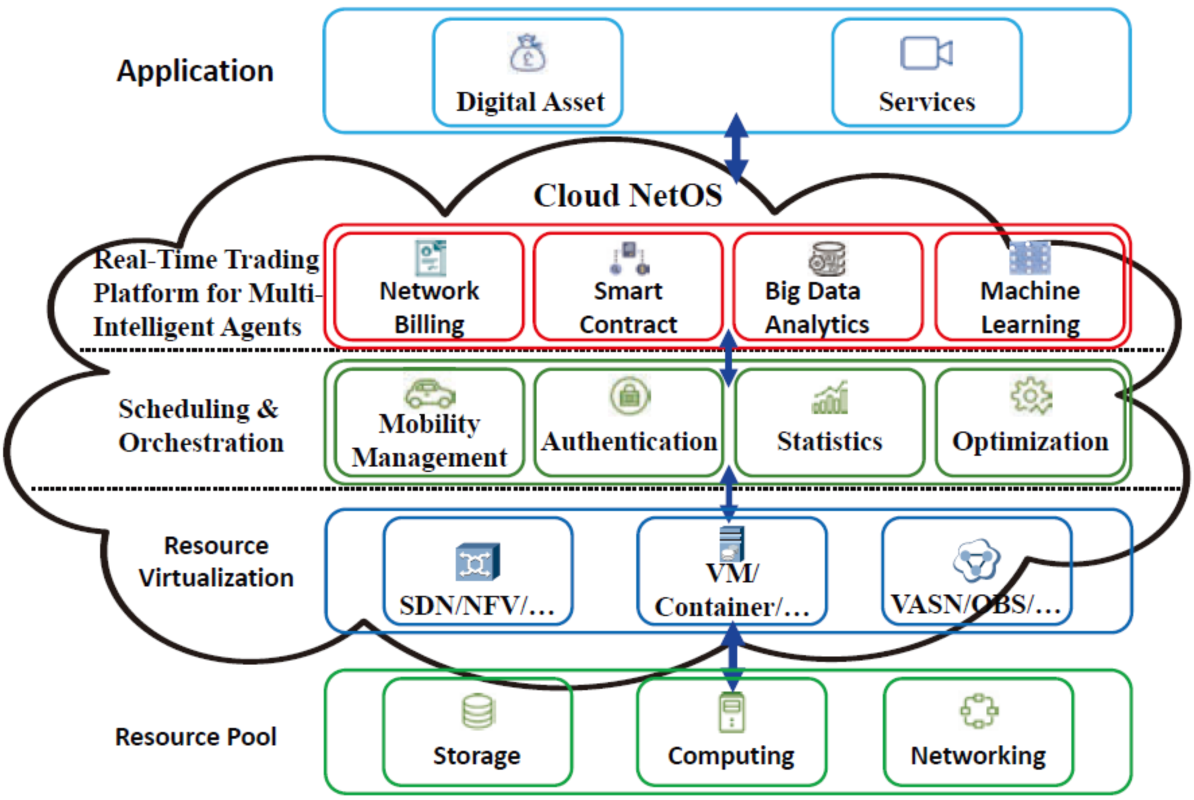
Cybertwin 可以将记录的行为数据转换为数字资产，为数据所有者带来经济价值，并可能催生一种新的商业模式 C2X（customer-to-everything）。

云网络操作系统

这种新的云网络操作系统，通过为终端、电信运营商、应用服务提供商和云运营商等多个代理建立一个实时的市场驱动交易平台，以分布式方式工作。

为了支持这个实时交易平台，可以使用 SDN 和 NFV 等资源虚拟化方法，并作为云网络操作系统的基础。

应用服务和数字资产数据服务可以在云网络操作系统之上执行。



云网络操作系统

网络架构设计特色

基于 cybertwin 的未来网络在以下方面具有许多新的强大功能，详见原文：

- 移动性
- 安全性
- 可用性(QoS 保证)
- 可扩展性

附：原文（见下页）

Cybertwin: An Origin of Next Generation Network Architecture

Quan Yu, Jing Ren, Yinjin Fu, Ying Li, and Wei Zhang

Abstract

With the fast development of IoE and its applications, the ever increasing mobile Internet traffic and services bring unprecedented challenges, including scalability, mobility, availability, and security, which cannot be addressed by the current clean-slate network architecture. In this article, a cybertwin based next generation network architecture is proposed to accommodate the evolution from end-to-end connection to cloud-to-end connection in the future network. As a digital representation of humans or things in the virtual cyberspace, cybertwin serves in multiple capacities, such as communications assistant, network behavior logger, and digital asset owner. The new and unique characteristics of the cybertwin make the proposed network flexible, scalable, reliable, and secure. Further, we advocate a new cloud network operating system which can work in a distributed way through a real-time multi-agent trading platform to allocate 3C (computing, caching, communication) resources. We also propose cloud operator, a new operator that can provide and manage the resources to the end users and offer location and authentication services for humans and things in cyberspace. Some promising and open research topics are discussed to envision the challenges and opportunities of the cybertwin in the future network architecture.

Introduction

Next generation networks will face the demand of billions of people and hundreds of billions of devices to be connected. Accordingly, the future network architecture is expected to accommodate the explosively increasing mobile Internet traffic and various services and applications through heterogeneous networks. Internet of Everything (IoE) has been considered as the future of the Internet and could achieve intelligent connections of humans, processes, data and things [1], with the help of next generation mobile communication and artificial intelligence (AI) technology to make networked connections more relevant and valuable than ever before. In comparison with the traditional end-to-end connection, a revolutionary feature of the network architecture in IoE is to support ubiquitous data collection, aggregation, fusion, processing, distribution and service [2]. The disruptive change raises many issues and challenges for the network architecture design of IoE, scalability, mobility, security and availability, and so on.

In the current Internet architecture, the IP protocol uses the IP address for both identity and locator of the device attached to the network, so it cannot address the dramatically increasing demands of mobile devices and services thereby leading to the scalability problem. In addition, the network trustworthiness depends on not only the security of the end-to-end physical connections, but also the trusted user who accesses the network. However, in the current Internet architecture, the anonymous access compromises the network trustworthiness which results in the security issue. Furthermore, in the current network architecture it is difficult to coordinate the network resources among multiple network service providers to offer the personalized quality of service (QoS) guarantee and availability during a single communication process, which leads to the availability issue. All these challenging issues in the current network architecture are critical and severely impeding the fast growing development of mobile traffic and services.

To address the challenges, information-centric networking (ICN) architectures were proposed, such as Named Data Networking [3], Content-Centric Networking [4], and DONA [5]. But these designs are incompatible with the existing IP network infrastructure. MobilityFirst [6] is motivated by accessing from mobile platforms, but it neglects the availability and security management. The eXpressive Internet Architecture (XIA) project [7] aims to improve both the evolvability and trustworthiness of the Internet by using a set of control and management protocols that deliver trustworthy network service to users, but it does not consider independent availability and cost-efficient scalable network management. ChoiceNet[8] introduces a new economy plane to support advertisement of choices to users, but it does not provide real-time trading for short-term contracts.

Recently, cloud-computing-centric network architectures were provided to achieve network resource sharing, to handle the big data explosion from IoE devices, and to simplify management tasks [9], such as Nebula [10], CloNet [11], and Cloud Integrated Network [12]. NEBULA [10] provides resilient networking services (including dependability, security, flexibility and extensi-

Quan Yu, Yinjin Fu, Ying Li, and Wei Zhang (corresponding author) are with Peng Cheng Laboratory; Jing Ren is with the University of Electronic Science and Technology of China; Wei Zhang is also with the University of New South Wales.

Digital Object Identifier: 10.1109/MWC.001.1900184

1536-1284/19/$25.00 © 2019 IEEE

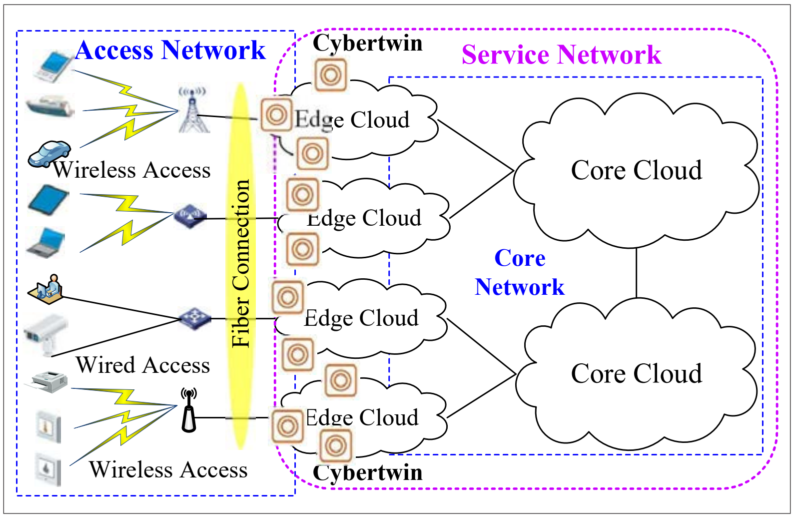


FIGURE 1. Cybertwin based cloud-centric network architecture.

bility) for the future Internet architecture using ultra-reliable routers, an extensible control plane and use of multiple paths upon which arbitrary policies may be enforced. However, its scalability and performance are still limited due to the ignorance of processing capability at the network edge. Further, it does not consider the issue of mobility support to accommodate the increasing demands of mobile devices and services. The CloNet architecture [11] introduces a cloud networking architecture in a multi-administrative domain scenario, where network and data centre domains interact to provide a dynamic elastic network connection service to cloud customers. Further, it deploys computing and storage resources distributed in the network to allow for a better end-user experience and to lower the dependency on network capacity. However, it does not address the mobility services in the cloud networking and its simple access control policy selection cannot satisfy high-level security goals. The cloud integrated network (CIN) architecture [12] embeds the edge clouds into the future network to provide the optimum performance and economics for both virtualized networking functions and other performance critical web services. It introduces a network operating system (OS) to abstract all network resources and manage the utilization to create exactly the needed capacity from the source to the destination. However, it does not solve the challenges on mobility and availability in cloud networking.

Clearly there are many challenges in providing scalability, security, mobility and network security for future network architecture designs. In this article, we propose a cybertwin based cloud-centric network architecture for future generation networks. By introducing cybertwin, which serves as a communications assistant, network behavior logger, and digital asset manager of humans and things in the IoE, we design a new network architecture to address scalability, security, mobility, and availability of future generation networks. In our cybertwin based future network design, the locator and identifier separation scheme makes the network address become an internal address, which is opaque to the external network for safety. Meanwhile, it also offers benefits on scalability to mitigate the address exhausted problem using two independent namespaces for naming and addressing. Then, we can build a cyber-physical-social systems (CPSS) indexing to exhibit the mobility of humans or things and the location of network services. Then, cybertwin can naturally and essentially provide security services in its design by exploiting behavior tracking and authentication service, and further defending against distributed denial of service (DDoS) attacks and IP address hijacking. Cybertwin can support always-online service when an end device accesses the edge cloud in the access network, and provide the collaboration service for application or data content among the core clouds and edge clouds with high availability and low latency. Moreover, in our cloud-centric design, a cloud network OS is provided to perform distributed collaboration decisions with the economy principles and big data mining to meet the demand on intelligent adaption and load balance between the end needs and cloud resources.

Cybertwin Based Network Architecture

Figure 1 shows our proposed cybertwin-based next generation network architecture. In this new architecture, there are four key components, that is, Core Cloud, Edge Cloud, cybertwin and the Ends. Their functions are summarized as follows.

Core Cloud: Fully-connected with each other to build the core networks through high-speed optical links. Unlike existing cloud networks, for example, Amazon AWS, which only provide cloud computing service as a particular application service, these core clouds in our proposed architecture provide computing, caching and communication resources for the ends as a network infrastructure service.

Edge Cloud: Resides between the core cloud and the ends. Although the resource it can provide is much less than the core cloud, it can respond faster to the ends' request due to its proximity to them. Thus, the edge clouds can help the core clouds in providing a very high quality of network services.

Cybertwin: The most critical network function provided by the proposed network architecture. It is a digital representation of humans or things in the virtual cyberspace and is located at the edge cloud. It serves in multiple capacities, that is, communication assistant, network data logger, and digital asset owner. It provides a new cybertwin based communication model to replace the end-to-end communication model. Details of cybertwin will be given in the next subsection.

The Ends: Refers to humans and things in the network. They are customers of the network services and are connected to the network via various access methods. In the proposed new network architecture, the ends no longer need to establish a connection with a specified server following the traditional end-to-end communication model. Instead, the ends acquire services directly from the network through the cybertwin.

To support the above four components, three kinds of networks, that is, access network, core network, and service network, are employed in the proposed network architecture design.

Access Network: Responsible for connecting the ends and edge clouds. Both wired and wireless access techniques can be used.

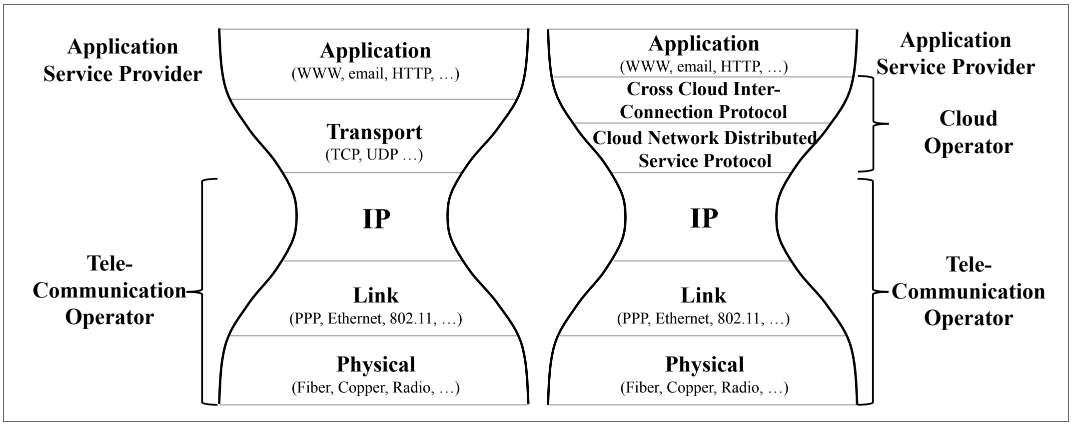


FIGURE 2. The main building blocks of sandglass model for new network architecture.

Core Network: In charge of establishing the connections between edge clouds and core clouds, as well as the connections among all core clouds.

Service Network: A logical network for application services which are deployed on top of the cloud network to provide services to the ends.

The three kinds of networks are operated by telecommunications operators, cloud operators and application service providers, respectively.

Telecommunications Operator: Offers high-speed communication pipes between the ends and clouds in access networks and among different clouds in core networks. It can sell or lend its networking resources to the cloud operators.

Cloud Operator: A new operator who provides information infrastructure services, not the general information services. Some of its key features are explained below:

- Provides computing, caching and communication resources to the ends by replacing or compressing the existing core networks, cloud computing service providers, cloud storage service providers (e.g., AWS, Azure, Baidu, Al, and so on), CDN service providers, and so on.
- Provides a brand new operating environment for cybertwin.
- Provides function of authentication for humans and things via biological features, online behavior, and so on.
- Provides various trust levels for humans and things.
- Provides the real-time location service to humans and things.

Application Service Provider: Delegates their application and content services to the cloud operator which deploys these services in the edge and core cloud. It can provide a high quality of service and reduce the cost because there is no need to implement a dedicated server.

Compared with the traditional Internet, we keep the IP layer as the "thin waist" of the stack but allow the evolutions of other layers (Fig. 2). This means we inherit the connectionless packet switch mechanism and allow the incremental updates of the legacy network infrastructure. The transport protocol is replaced by the cloud network distributed service protocol and the cross-cloud operator interconnection protocol. The cloud network distributed service protocol is designed to deal with the multi-dimensional resources including computing, caching, and communication resources of a cloud operator in a distributed way. Based on this protocol, a cloud network operating system can be built for each cloud operator. The cross-cloud interconnection protocol is used to provide network services through the cooperation of different cloud operators.

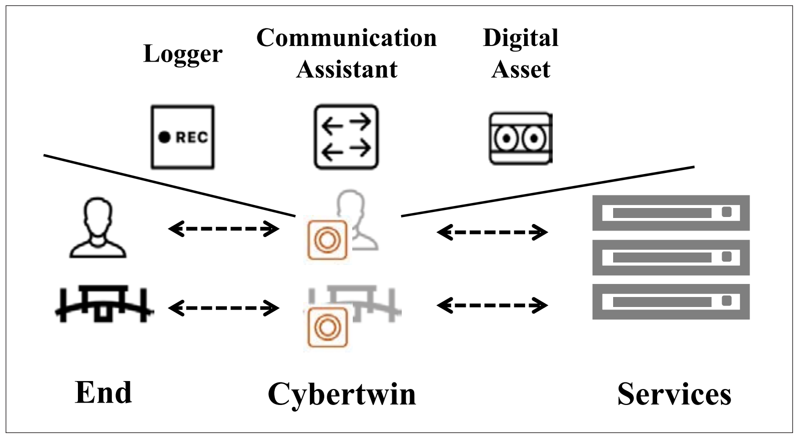


FIGURE 3. Cybertwin based communication.

Cybertwin

In the proposed network architecture design, cybertwin is the key component to replace the traditional end-to-end communication model. As shown in Fig. 3, it has three fundamental functions: communication assistant, logger and digital asset.

For the Communication Assistant Function: Cybertwin is the digital representation of humans or things in the virtual world and also acts as the virtual network ID of humans and things. As the assistant of humans or things in the physical world, cybertwin can better achieve various QoE because it knows well the users' QoS and will pay the cost to negotiate with telecommunications operators and cloud operators for the resource. Unlike establishing the end-to-end connections between the end and the server which provides the services, the cybertwin based communication model requires the ends to first connect to its cybertwin that will acquire the required service from the cloud network on behalf of the ends. The required service is provided by the edge cloud and core cloud jointly through the distributed cloud network operating system which pools various computing, caching, and communication resources. To provide a high quality of service, cybertwin may request the service from multiple locations simultaneously.

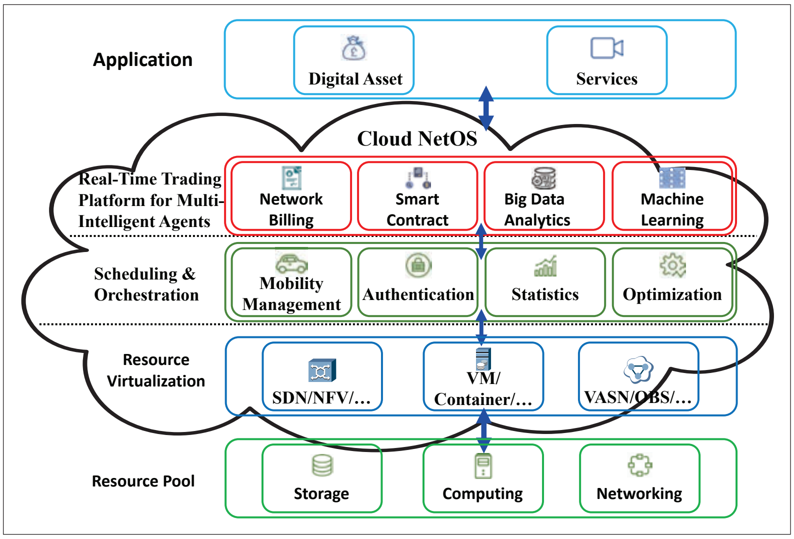


FIGURE 4. Cloud network operating system.

For the Logger Function: In the proposed network architecture design, communication should be completed through cybertwin. It means that the cybertwin can obtain and log all data about the end's behavior in a real-time fashion. Traditionally, these data are acquired and stored by a few companies and may be abused without the permission of the ends. However, cybertwin is the digital representation of the ends and does not belong to any particular company.

For the Digital Asset Function: Cybertwin can also convert these logged behavior data into a digital asset by processing these data as a service and publishing the service to other entities including the application service providers and cloud operators. This service can break the monopoly in which only a few big companies gather these valuable data. Further, it can also bring economic value to the owners of the data and may give birth to a new business model, C2X (customer-to-everything).

One of the benefits of using cybertwin is to support the locator/identifier split. In existing networks, the bottleneck problem to implement locator/identifier split is the lack of an identity authentication mechanism. Without the authentication mechanism, the networks cannot know whether a user is the one who declares. As a communication assistant, cybertwin has the ability to provide identity authentication.

More benefits of the cybertwin based communication model, including security, mobility, availability and scalability, will be discussed in detail in the next section.

Cloud Network Operating System

A massive number of users and large scale cloud-centric networks in future generation networks pose great challenges in the allocation of multi-dimensional resources, that is, computing, caching and communication resources. In the existing network architecture, the resources are scheduled and utilized independently with each other, resulting in the inefficiency and latency problems. Further, the centralized management and allocation of the multi-dimensional resources become infeasible because a large number of users, various cloud networks, and multi-operators hardly cooperate via a centralized mechanism.

We advocate a new cloud network operating system which can work in a distributed way via establishing a real-time market driven trading platform for multi-agents (i.e., the ends, telecommunications operators, applications service providers, and cloud operators.) On this platform, the multi-dimensional resources will be priced based on the scarcity of the resources dynamically based on some economic principles, for example, traffic demand, importance and popularity of the services, and so on. Other methods such as big data analytics, machine learning, network billing, and so on, are also employed to help price the resources. When the cloud operators and the ends make a deal, we propose to use the real-time blockchain based smart contract to record real-time transactions among multi-agents. This smart contract can overcome the bad real-time problem of the current blockchain mechanism. When some resources become scarce, the resource will be reallocated according to the smart contract.

To support this real-time trading platform, resource virtualization methods like SDN [13] and NFV can be employed in a limited scope and used as the basis for the cloud network operating system that runs in a broader range in a distributed way, as shown in Fig. 4. Some other technologies, including mobility management, authentication, statistics, and optimization, are applied for providing the capabilities of scheduling and orchestration, which use the virtualized resource to perform the contract signed through the real-time trading platform. As illustrated in Fig. 4, application services and digital assets data service can be performed on top of the cloud network operating system.

Features of Cybertwin Based Next Generation Network Architecture Design

Our cybertwin based future network design has a number of new and powerful features in terms of mobility, security, availability, scalability, and so on. We show these features in the following.

Mobility

It was recently predicted in [14] that global mobile data traffic would grow nearly twice the growing speed of fixed IP traffic. This fundamental shift from fixed to mobile traffic in Internet usage represents a unique and timely opportunity to take into account the special requirements of mobile devices and applications. Adding mobility to the current Internet architecture is challenging, because the current Internet naming system is based on the host address, typically the IP address. In our network architecture design, we use the object identifiers (IDs) to name humans, things and services, and use the network address to indicate their locations. We also propose to build a mapping between object IDs and the network address in cyberspace to support mobility. This mapping can be dynamically managed in the core clouds and edge clouds. The end devices get the mapping from an edge cloud, and the edge cloud further obtains the mapping information from a core cloud. Then, we can build a cyber-physical-social systems (CPSS) indexing to exhibit the mobility of humans or things and the location of network services.

The process of the primary communication and the mobility management with cybertwin is shown in Fig. 5 and described in the following steps.

- When an end requests a service, it first connects to its cybertwin hosting at the edge cloud.
- The cybertwin gets the collaborated service from the edge cloud and core cloud according to the scheduling of the cloud network operating system. Then, it passes on the required service data to the end.
- When an end moves to a new location, the movement only requires the end to connect to its cybertwin through a new access point. When the end disconnects from the original access point, the cybertwin can cache the service data and continue to provide these data to the end when it connects to the cybertwin again.
- If the end moves further to a new position, it can connect to the original cybertwin, which may lead to a longer delay.
- The cybertwin may also need to migrate to another edge cloud that is closer to the end, and establish a new connection to acquire the required service.
- After the migration, the end will connect to the new cybertwin. The end could still keep the connection with the original cybertwin so as to choose the best cybertwin.

The above procedure shows that cybertwin can perform quick backup and real-time migration to support high availability and low latency. It is an always-on connection to serve the ends continuously.

MobilityFirst [6] uses a massively scalable global name resolution service to support seamless mobility at scale, while each router employs in-network storage to cope with varying link quality and disconnections. XIA [7] can also support mobility with the locator and identifier separation scheme, and the mobile host keeps the stationary host informed of its new address. In our network architecture design, cybertwin builds a mapping between object IDs and network address in cyberspace to support mobility and employs edge clouds to address disconnections by storing the network states.

Security

Security includes both network security and privacy protection. Since anonymity is the core issue of Internet security, cybertwin can essentially provide security services in its design by exploiting behavior tracking and authentication service, further defending against DDoS attacks and IP address hijacking. In our design, the locator and identifier separation scheme makes the network address an internal address, which is opaque to the external network for safety. Furthermore, we combine the naming mechanism with an authentication mechanism to ensure there is no imposter. Different authentication methods can also be employed. For example, we can identify humans with the biological characteristics and apply a digital signature for things or service authentication. A unified object identification can also help improve network security with the cyberspace real-name system. With the help of cybertwin, the behavior of anyone or anything in cyberspace is auditable and traceable. Furthermore, cybertwin can obtain and log all data about the end's behavior realtime, thereby giving extra protection to personal privacy.

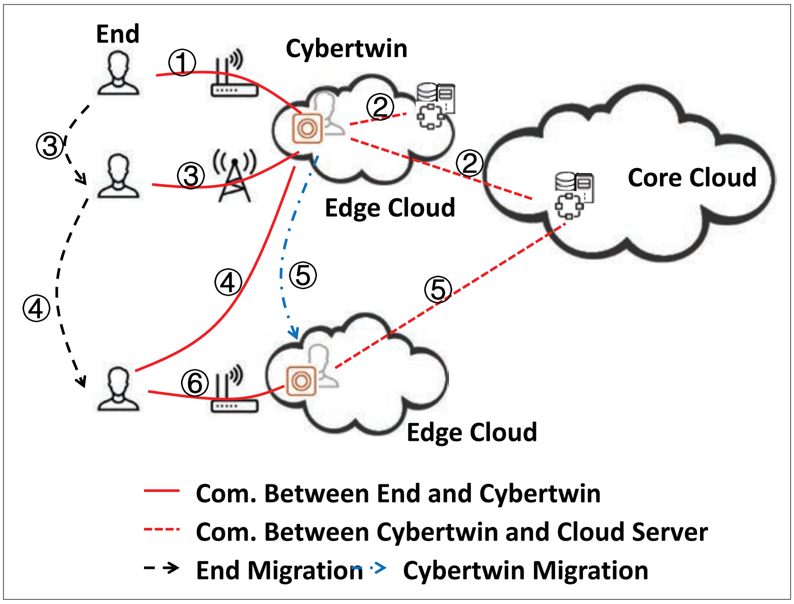


FIGURE 5. The process of mobility management with cybertwin.

Availability (QoS Guarantee)

Today's Internet supports many critical applications that underpin the foundations of our modern society. However, the current state of availability of the Internet is far from being commensurate with its importance. As more critical processes are conducted as part of the IoE, the need for availability in IP networks increases. Any interruption to the transmission of data over networks negatively impacts these processes. Mission critical applications such as augmented reality require ultra-high reliability and ultra-low latency, while others like process automation are less demanding. Because QoS requirements are indeed application-dependent and various, IoE presents different QoS requirements from conventional homogeneous networks.

In the proposed cloud centric design, cybertwin can support always-online service when an end device accesses the edge cloud in an access network. It can also provide the collaboration service for application or data content among the core clouds and edge clouds with high availability and low latency. A cloud network OS is provided to perform a distributed collaboration decision with the economic principles and big data mining to meet the demand on intelligent adaption and load balance between the end needs and cloud resources. We provide a series of dynamic price adjustment rules based on the occupancy rate of resource in computing, caching and communications, and define the corresponding price (e.g., traffic fee) for the network resources. With the help of cybertwin, we can provide the personalized QoS guarantee for various ends.

In addition, the cross-cloud cooperative service can also be implemented among multiple cloud operators. It becomes possible to make trade among ends, application service providers, cloud operators and telecommunications operators using smart contracts based on blockchain technology.

Our proposed cybertwin based cloud-centric network architecture can address the scalability problem. Different from the traditional cloud-network-end model, our network architecture provides a cloud-centric direct communication model to shorten the network access path.

Furthermore, in a multiple cloud operator scenario, a cross cloud operator interconnection protocol is needed with some principles in simplicity and openness, de-centralized autonomy and centralized cooperation to embody network territory and network sovereignty.

Scalability

The future Internet is expected to connect billions, and some day trillions, of objects and support information exchange among them. However, the scalability challenge of the Internet stems from the conflict between the unprecedentedly high traffic surge and the exhaustion of IP addresses and the explosion of corresponding route table. A content delivery network (CDN) can partially alleviate the network traffic jam by duplicating and caching data locally, but cannot thoroughly solve the problem due to its high cost and inflexibility. Network address translation (NAT) and IPv6 are the effective methods to mitigate the IPv4 address exhaustion, but these methods incur extra complexity.

Our proposed cybertwin based cloud-centric network architecture can address the scalability problem. Different from the traditional cloud-network-end model, our network architecture provides a cloud-centric direct communication model to shorten the network access path. Furthermore, our network design has low complexity by pushing the intelligence, processing power and communication capabilities down to edge clouds or devices near the end, such as a node in a local area network, or an edge gateway. It can avoid long-distance access to the cloud and reduce the network access latency by responding to user requests instantly. Hence, our cloud-centric network architecture can alleviate the route table expansion by improving the network access efficiency.

In the proposed cybertwin based cloud-centric network architecture, we leverage the locator/identifier split scheme to offer benefits on scalability using two independent namespaces for naming and addressing [15]. It uses an object ID with the 128 bits IPv6 format or 48 bits EUI-48 format to identify humans, devices, and services (data and apps) in the cyberspace. The network address, such as IPv4/ IPv6, becomes an internal address, which is opaque to the external network. We can build a mapping between object IDs and network address in cyberspace to link the ends with access point and save the IP addresses. Hence, the address exhausted problem can be alleviated by the mixed usage of object IDs and network address.

Conclusion and Future Work

In this article, we have proposed cybertwin based next generation network architecture design. We have introduced cloud operators and cybertwin in the proposed network architecture. We have demonstrated the critical concepts of the architecture and provided key features to demonstrate the value of the cybertwin. However, to achieve a safer and more scalable architecture, there are still some research issues to be addressed.

Incremental Deployment: As a new network architecture, it is vital to achieve incremental deployment. As shown in Fig. 2, we keep the IP layer as the "thin waist" of the stack but allow the evolutions of other layers, which provides a possibility for incrementally deploying. The cybertwin can be implemented as an application on top of the current Internet. Thus, users with cybertwin and traditional anonymous users can coexist, which need some cooperation protocols. By applying differential service for different kinds of users, users can be incented to use cybertwin. To upgrade the best-effort packet delivery to cloud-centric network, we can leverage many existing technologies, such as technologies of edge cloud and radio access network of 5G.

Identity Authentication: This is critical to network security as it makes the network behavior traceable. There are three types of objects including humans, things, and services needed to be authenticated. Some efficient and trusted authentication methods or frameworks should be developed, such as biological characteristics based identification for humans.

Digital Asset Management: There are a vast number of digital assets hosting in a large number of cybertwins. It is essential to develop a digital asset management framework to standardize the metadata model for the digital assets, to catalog the digital assets, and to perform permission of the digital assets' usage.

Cross-Cloud Operator Resource Scheduling: This is a vital issue for the future network design. A series of cooperation principles shall be determined to guide the cooperative resource scheduling among different cloud operators.

AI Power Based Cybertwin: Since cybertwin is the digital representation of the humans or things in cyberspace, AI techniques can be applied to the deployment and collaboration among multiple cybertwins for high efficiency and QoS guarantee.

Smart Contract Based Cloud Resource Coordination: Blockchain technology has emerged as a solution to consistency problems in peer to peer networks. Smart contract based coordination becomes an attractive mechanism for resource management in distributed systems of single-cloud or cross-cloud operator without the need for a trusted (physical) third party.

Data Privacy Protection and Security: Cybertwin can obtain all data about the end behaviors, and convert the data into a digital asset by wrapping the data as a service and publishing the service to other entities. Hence, it becomes a critical challenge for the data management, which may need relevant laws and techniques to guide and protect the data privacy and security.

References

[1] S. Abdelwahab *et al.*, "Enabling Smart Cloud Services Through Remote Sensing: An Internet of Everything Enabler," *IEEE Internet of Things J.*, vol. 1, no. 3, 2014, pp. 276–88.

[2] A. Mondal, S. Bhattacharjee, and S. Chakraborty, "Viscous: An End to End Protocol for Ubiquitous Communication over Internet of Everything," *Proc. IEEE 42nd Conf. Local Computer Networks (LCN)*, 2017, pp. 312–20.

[3] A. Afanasyev *et al.*, "A Brief Introduction to Named Data Networking," *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2018, pp. 1–6.

[4] C. Severance, "Van Jacobson: Content-Centric Networking," *Computer*, vol. 46, no. 1, 2013, pp. 11–13.

[5] T. Koponen *et al.*, "A Data-Oriented (And Beyond) Network Architecture," *ACM SIGCOMM Computer Commun. Review*, vol. 37, no. 4, 2007, pp. 181–92.

[6] A. Baid and D. Raychaudhuri, "Wireless Access Considerations for the Mobilityfirst Future Internet Architecture," *Proc. 35th IEEE Sarnoff Symposium*, 2012, pp. 1–5.

[7] D. Naylor *et al.*, "XIA: Architecting a More Trustworthy and Evolvable Internet," *ACM SIGCOMM Computer Commun. Review*, vol. 44, no. 3, 2014, pp. 50–57.
[8] G. N. Rouskas *et al.*, "Choicenet: Network Innovation through Choice," *Proc. 17th Int'l. Conf. Optical Networking Design and Modeling (ONDM)*, 2013, pp. 1–6.
[9] J. Pan, S. Paul, and R. Jain, "A Survey of the Research on Future Internet Architectures," *IEEE Commun. Mag.*, vol. 49, no. 7, 2011.
[10] T. Anderson *et al.*, "A Brief Overview of the Nebula Future Internet Architecture," *ACM SIGCOMM Computer Commun. Review*, vol. 44, no. 3, 2014, pp. 81–86.
[11] P. Murray *et al.*, "Cloud Networking: An Infrastructure Service Architecture for the Wide Area," *Proc. Future Network & Mobile Summit*, 2012, pp. 1–8.
[12] M. K. Weldon, *The Future X Network: A Bell Labs Perspective*, CRC Press, 2016.
[13] S. Jain *et al.*, "B4: Experience with a Globally-Deployed Software Defined WAN," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, 2013, pp. 3–14.
[14] V. Cisco, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022," White Paper, 2018.
[15] D. Farinacci *et al.*, "The Locator/Id Separation Protocol (LISP)," RFC 6830, 2013.

Biographies

Quan Yu received the B.S. degree in radio physics from Nanjing University, China, in 1986, the M.S. degree in radio wave propagation from Xidian University, China, in 1988, and the Ph.D. degree in fiber optics from the University of Limoges, France, in 1992. He is currently a research professor at the Peng Cheng Laboratory. His main areas of research interest are the architecture of wireless networks and cognitive radio. He is an Academician of the Chinese Academy of Engineering (CAE) and the founding Editor-in-Chief of the *Journal of Communications and Information Networks* (JCIN).

Jing Ren [S'12, M'17] received her B.E. and Ph.D. degrees in communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2007 and 2015, respectively. Currently, she is an instructor at UESTC and a research assistant at Peng Cheng Laboratory. Her research interests include network architecture and protocol design, information-centric networking, and software-defined networking.

Yinjin Fu [S'11, M'14] received his B.S. in mathematics from Nanjing University in 2006, and the M.S. and Ph.D. degrees in computer Science from the National University of Defense Technology of China in 2008 and 2013, respectively. Currently, he is an assistant researcher at the Peng Cheng Laboratory. His current research interests include computer network architecture, cloud computing and big data storage.

Ying Li received her B.E. and Ph.D. degrees in communication engineering from the National University of Defense Technology, Changsha, China, in 2001 and 2006, respectively. Currently, she is a researcher at the Peng Cheng Laboratory. Her research interests include network architecture design, MIMO, and cognitive radio.

Wei Zhang [S'01, M'06, SM'11, F'15] received his Ph.D. in electronic engineering from the Chinese University of Hong Kong in 2005. Currently, he is professor at the University of New South Wales, Sydney, Australia. His current research interests include 5G and UAV communications. He serves as Editor-in-Chief of *IEEE Wireless Communications Letters* and Editor-in-Chief of the *Journal of Communications and Information Networks*. He is Chair of the IEEE Wireless Communications Technical Committee. He is a member of the Board of Governors of the IEEE Communications Society.