Intra-Regional Vehicle Lightweight Network Deployment Scheme and Applications

Zenglong Yue, Jiangyi LV

Beijing Polytechnic, Beijing 100176, China

Abstract: With the rapid development of connected car technology, the network connectivity of smart connected cars and the number of smart devices connected to the Internet are increasing, resulting in large-scale data, which has caused problems such as bandwidth load, slow response speed, poor security, and poor privacy in traditional cloud computing models. Traditional cloud computing is no longer sufficient to support the diverse needs of today's intelligent society for data processing, so edge computing technologies have emerged. Multi-Access Edge Computing (MEC) emphasizes being closer to the user and the source of the data. At the edge of the network, it is lightweight for local, small-scale data storage and processing, which enables high-bandwidth and ultra-low latency access to edge-distributed applications, vehicles, and devices, as well as improved edge performance and cloud computing capabilities. This deployment approach utilizes full use of SD-WAN network architecture's flexible and consistent end-to-end control capabilities to implement edge terminal devices that provide fast, secure, and reliable network data services. It provides a guide for developing an extensive approach that combines vehicles, platforms, networks, and applications in the region.

Keywords: SD-WAN; 5G; CPE; MEC; Edge Computing

1. Introduction

The concept of software defined wide area network (SD-WAN) is a combination of SD and WAN, which means that the architecture and concepts of SDN are applied to WAN, and WAN is redefined through SDN, so that it can combine both network reliability and security for enterprise users, while delivering low cost for enterprise users. SD-WAN will provide enterprise customers with new options for cost-effective and flexible network changes [1].

SD-WAN will provide enterprise customers using four core values: first, it can efficiently realize multi-cloud and multi-network interconnection to meet the connectivity needs of different business scenarios; second, it can provide application identification and intelligent routing to ensure the experience of key enterprise applications; and third, it is an advanced.

2. The Architecture of SD-WAN: Logical Constructs and Functional Layers

Traditional Wide Area Networks (WANs) are fundamentally predicated on Multi-Protocol Label Switching (MPLS) and other dedicated lines for connection, which are renowned for their ability to deliver high-quality service guarantees. However, the deployment of WAN leased lines is characterized by substantial costs and extended timelines. Moreover, not all traffic necessitates transit via MPLS leased lines. The industry-proposed Software-Defined Wide Area Network (SD-WAN) [2] addresses these challenges by enabling traffic steering to either MPLS leased lines or alternative links, such as the Internet. When traffic is routed over the Internet, it can traverse through virtualized extended LAN tunnels, thereby optimizing the use of available network resources.

The SD-WAN network architecture, depicted in Figure 1, is logically stratified and functionally compartmentalized, comprising the network layer, management and control layer, and service presentation layer. Each stratum is delineated by clear functional boundaries and discrete operational responsibilities. The foundational layer encompasses the telecommunications network and the Customer Premises Equipment (CPE) of the users. In contrast, the uppermost layer is occupied by the SD-WAN controller. The controller assumes the pivotal role of remotely managing and configuring CPEs, issuing control directives via the NETCONF interface, and is also tasked with data aggregation and status monitoring. Furthermore, the controller interfaces with ancillary systems such as billing, service provisioning, and self-service applications through the use of RESTful APIs [2,3].

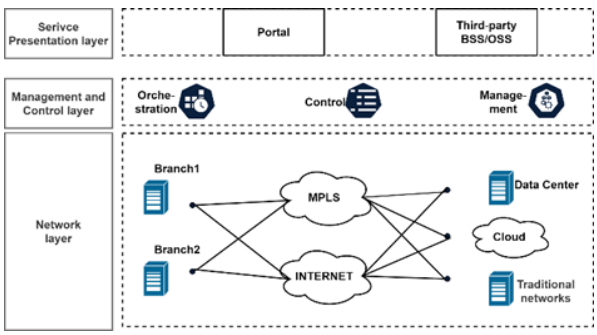

Figure 1. Types of SD-WAN Architectures.

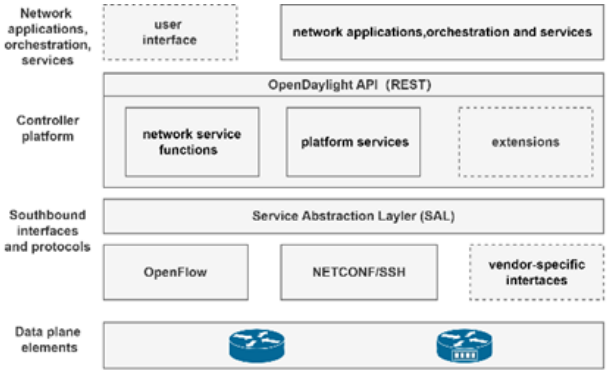

Figure 2. OpenDaylight controller architecture.

In the SD-WAN networking architecture, the management and control layer can be orchestrated by an OpenDaylight [4] controller, which is characterized by the following features:

(1) The southbound interface supports a suite of standard protocols, including OpenFlow, NETCONF, SNMP, PCEP, etc., and also accommodates proprietary interfaces.

(2) The Service Abstraction Layer (SAL) ensures that interactions between upper and lower layer modules are insulated from one another, thereby concealing the variances in southbound protocols and offering a uniform service interface for the functional modules of the upper layers.

(3) The adoption of the OSGi architecture addresses the issue of component isolation, fostering a more modular and dynamic system.

(4) YANG tools are utilized to directly generate the business management and streamlining the development process.

Open Daylight's software solutions are primarily employed for their multifaceted capabilities; the platform achieves not only data storage, retrieval, and event listening but also crucially supports the formation of controller clusters. As depicted in Figure 2, its architecture is compartmentalized into the southbound interface layer, control plane layer, northbound interface layer, and network application layer. The southbound interface layer encompasses various protocol implementations such as OpenFlow, NETCONF, and SNMP. The control plane layer constitutes the nucleus of Open Daylight, comprising the Model-Driven Service Abstraction Layer Interface (MD-SALI), foundational network function modules, network services, and network abstraction modules, with MD-SAL being the pivotal core module in the Open Daylight architecture. It functions as the controller's information management hub, tasked with data storage, request routing, and message subscription and distribution. The northbound interface layer includes the open RESTful API interface and AAA authentication components. The application layer comprises a suite of applications developed leveraging the interfaces of Open Daylight's northbound interface layer [3].

3. The G-SRv6 Technology Paradigm

With the advent of the 5G and cloud era, cloud-network convergence has emerged as a pivotal direction in the evolution of IP bearer networks, significantly influencing the trajectory of industry digital transformation. SRv6, as a cornerstone technology of the next-generation IP network, leverages its streamlined and programmable attributes, in tandem with SDN, to enable the flexible and intelligent connectivity of the IP network. This capability is essential for providing differentiated and assured services, facilitating the swift and comprehensive migration of enterprise applications to the cloud. SRv6 further enhances network functionality by supporting explicit packet forwarding path specifications in the header of each node, and it is also compatible with Virtual Private Network (VPN) services [4].

G-SRv6 represents an evolutionary advancement over SRv6, inheriting its core benefits such as source routing, native IPv6 support, programmability, and streamlined protocols. By implementing 32-bit compressed Segment Identifiers (SIDs), G-SRv6 markedly enhances network transmission efficiency and diminishes the overhead associated with the Segment List, thereby reducing transmission costs. Additionally, G-SRv6 enhances forwarding performance; with a shortened Segment List, the hardware's SID reading depth is reduced, preventing the need for secondary reads and thus increasing the forwarding rate [5].

As illustrated in the Figure2, China Mobile has constructed Smart WAN and cloud-based private networks, adopting a unified G-SRv6 protocol system to achieve end-to-end connectivity. This new technological framework, underpinned by a unified protocol, aims to integrate cloud, edge, endpoints, and networks. With end-to-end G-SRv6 connectivity, slicing, and visualization services, it addresses the stringent requirements for high quality, security, speed, and flexibility that are inherent to cloud-network convergence.

4. G-SRv6-Driven Integration of Cloud and Network Infrastructures

Traditional Software-Defined Wide Area Network (SD-WAN) architectures employ tunneling techniques to abstract the specific details of the underlying physical network, creating an end-to-end Overlay network by concatenating various tunnels. This approach results in an Overlay network that operates independently of the Underlay network, without awareness of each other. Consequently, it does not fully leverage the extensive access and backbone network resource advantages of carriers. The end-to-end connectivity is established through multiple tunnels, and the Customer Premises Equipment (CPE) at the network periphery lacks visibility into the overall end-to-end path. This limitation hampers the capability for comprehensive end-to-end quality assurance. To address these limitations, an integrated cloud-network program can be constructed by integrating the SDN (Software-Defined Networking) infrastructure with the fundamental protocol of G-SRv6 (Generalized Segment Routing for IPv6) [6] [7].

The end-to-end Overlay network system, as depicted in Figure 3, is implemented based on the China Mobile Smart Controller to ensure high-quality network communication for end devices. This system is instrumental in constructing a lightweight vehicle interconnection communication framework. The primary components of the system include the Smart WAN Controller, SD-WAN Customer Premises Equipment (CPE), network-connected vehicles, and edge devices [8]. Real-time transmission of vehicle information to the cloud platform is facilitated, enabling real-time data analysis and visualization.

(1) SW-WAN System Deployment Scheme

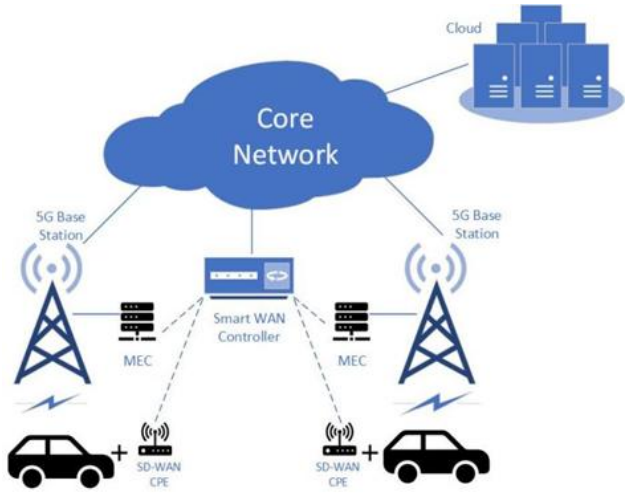

Figure 3. Smart SD-WAN network topology.

The intra-regional vehicle interconnection deployment plan is primarily contingent upon the deployment of MEC (Multi-Access Edge Computing) base stations at the front end and the installation of SD-WAN (Software-Defined Wide Area Network) supported CPE (Customer Premises Equipment) within the vehicles. This deployment facilitates a '5G wireless node + 5G edge computing' network architecture, which ensures data remains within the confines of the plant during low-latency communications. This architecture not only supports an expanded range of functionalities and more complex services but also possesses the capacity to integrate with plant-level private cloud platforms, as depicted in Figure 4.

In this network paradigm, field devices, encompassing general user devices, cameras, IoT (Internet of Things) devices, and others, forward the collected data to EdgeX [9]. EdgeX serves as the edge computing center's data processing and preliminary analysis hub, responsible for the function and transmission of data. The edge-side data processing reduces the physical distance and the number of communication layers, thereby inherently minimizing latency. Moreover, the system is endowed with a certain level of data computation capability and selectively exposes part of its interface. This selective exposure, coupled with the edge computing capabilities, also bolsters the data security of the overall system.

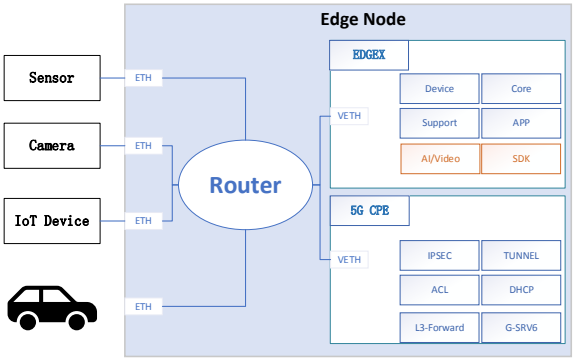

Figure 4. SD-WAN+EdgeX System Deployment Scheme.

(2) Implementing End-to-End Deployment Schemes

The network deployment process, as illustrated in the accompanying diagram, initially involves the deployment of Customer Premises Equipment (CPE) capable of supporting Software-Defined Wide Area Network (SD-WAN) technology, followed by the setup and verification of the Edge Node. The detailed implementation steps are outlined below:

To facilitate CPE plug-and-play functionality, an email containing a specially crafted URL from the network controller is necessary. This URL directs to the IP address of the CPE's management port and includes embedded CPE configuration parameters, such as Wide Area Network (WAN) interface settings, the network controller's IP address, and a site-specific token for secure authentication. Given that the IP address of the CPE's management port is typically factory-set and static, it serves as a reliable reference for establishing an initial connection and transmitting configuration data to the CPE.

Step 1: The network administrator performs a series of configurations on the network controller, including the establishment of a new site and the configuration of the WAN interface parameters for the CPE. The administrator has the option to either input the CPE's Equipment Serial Number (ESN) or omit it; omitting the ESN requires only specifying the CPE model for the site, without associating the CPE's ESN with it. Subsequently, the administrator dispatches an email with an encrypted URL to the site operator through the network controller, ensuring that the decryption key is communicated to the operator for URL access.

Step 2: The equipment administrator dispatches the designated CPE model to the respective site. If the CPE's ESN was not specified in Step 1, any unit of the specified model can be shipped to the site.

Step 3: The site operator, using a local terminal (personal computer or smart device), receives the operator email sent by the network administrator, follows the operational instructions to connect and power up the CPE, and initiates the operator process. The CPE establishes a connection with the network controller, which identifies the site based on the CPE's token, associates the ESN reported by the CPE with the site, and transmits the service configuration to the CPE.

The core services such as vehicle equipment data collection, control command execution, and equipment

services are deployed on the edge. Additionally, vehicle data analysis services and export services can be implemented within the enterprise cloud services. The deployment of microservices at the edge node enables real-time data acquisition, storage, and forward switching.

5. CONCLUSION

End-to-end deployment and implementation of Software-Defined Wide Area Network (SD-WAN) and Multi-Access Edge Computing (MEC) minimal systems demonstrate significant improvements in network reliability, flexibility, and operational efficiency. Safe remote control capabilities are made possible by SD-WAN technology, which also guarantees the stability and speed of vehicular data access. It offers an effective approach to achieving an integrated cloud-network convergence solution and enabling lightweight network deployment for regional networked vehicles.

Furthermore, the integration of SD-WAN with emerging technologies, such as edge computing, artificial intelligence (AI), and big data, enhances the functionality of applications including intelligent monitoring systems for Internet-connected vehicles, remote equipment control, and automated operations, maintenance, and upgrades. This integrated approach provides a comprehensive and feasible solution for the end-to-end integration of terminals, platforms, networks, and applications within the region.

Acknowledgment

This ITEM is supposed by Project: development of vocational skills training course for Automotive inspection and maintenance workers (2022H145), director: Lv Jiangyi.

References

[1] M. Gramaglia, V. Sciancalepore, F. J. Fernandez-Maestro, R. Perez, P. Serrano, and A. Banchs, “Experimenting with srv6: a tunneling protocol supporting network slicing in 5g and beyond,” in 2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2020, pp. 1–6.

[2] Vasileios Cheimaras, Spyridon Papagiakoumos, Nikolaos Peladarinos, et al. Low-Cost, Open-Source, Experimental Setup Communication Platform for Emergencies, Based on SD-WAN Technology. Telecom, 2024, 5(2):347-.

[3] Guo Guangming, Wang Jinshuai, Wang Rining, et al. A power communication scheme integrating 5G network and SD-WAN. Second International Conference on Informatics, Networking, and Computing (ICINC 2023). Vol. 13078. SPIE, 2024, 13078:130780G-130780G-5.

[4] Boudlal Hicham, Serrhini Mohammed, Tahiri Ahmed, et al. OpenDaylight SDN and NFV Integration in OpenStack Cloud: OpenSource Approach for Improving Network Services. International Conference on Innovative Computing and Communications, 2022:59-67.

[5] Cheng Weiqiang, Li Jinming, Zhang Shukun, et al. A comparative study of network processor chips for G-SRv6. International Conference on Computer Application and Information Security (ICCAIS 2023). Vol. 13090. SPIE, 2024, 13090:130903S-130903S-11.

[6] Zhang Zhenjiang, Li Chen, Peng ShengLung et al. A new task offloading algorithm in edge computing EURASIP Journal on Wireless Communications and Networking, 2021, 2021(1).2-3

[7] Zhenjie Yang, Yong Cui et al. “Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities.” International Conference on Computer Communications and Networks (2019). 1-9.

[8] Medved J, Varga R, Tkacik A, et al. OpenDaylight: Towards a Model-Driven SDN Controller architecture//2014 IEEE 15th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM).IEEE, 2014.DOI:10.1109/WoWMoM.2014.6918985.

[9] Aalwahab Dhulfiqar, Mohammed A. Abdala, Norbert Pataki, et al. Deploying a web service application on the EdgeX open edge server: An evaluation of its viability for IoT services. Procedia Computer Science, 2024, 235:852-862.