Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems

Sunday Adeola Oladosu [1,*], Christian Chukwuemeka Ike [2], Peter Adeyemo Adepoju [3], Adeoye Idowu Afolabi [4], Adebimpe Bolatito Ige [5] and Olukunle Oladipupo Amoo [6]

[1] *Independent Researcher, Texas, USA.*
[2] *Globacom Nigeria Limited.*
[3] *Independent Researcher, Lagos, Nigeria.*
[4] *CISCO, Nigeria.*
[5] *Independent Researcher, Canada.*
[6] *Amstek Nigeria Limited.*

Magna Scientia Advanced Research and Reviews, 2021, 03(02), 095–107

Publication history: Received on 24 November 2021; revised on 26 December 2021; accepted on 29 December 2021

Article DOI: https://doi.org/10.30574/msarr.2021.3.2.0086

Abstract

Software-Defined Wide Area Networks (SD-WAN) have revolutionized the traditional approach to WAN by offering greater flexibility, cost-efficiency, and performance optimization. However, as network demands evolve, there is a growing need to take SD-WAN a step further. This review explores the conceptual evolution of SD-WAN from traditional WAN architectures to autonomous, self-healing network systems. The next phase of SD-WAN involves the integration of advanced automation, artificial intelligence (AI), and machine learning (ML) to enable networks that can dynamically adapt, self-manage, and resolve issues in real-time, thereby significantly reducing human intervention. Traditional SD-WAN primarily focuses on centralized management and static routing policies to improve network performance and reduce costs. While this has addressed many challenges in enterprise networks, it still lacks the ability to autonomously adjust to network failures, traffic shifts, or security breaches. The future of SD-WAN, however, envisions a more intelligent, self-healing infrastructure where networks can automatically detect, diagnose, and recover from faults without manual input. This model leverages AI and ML to analyze network data, predict potential disruptions, and take proactive measures to maintain optimal performance. In addition, the integration of edge computing, 5G technologies, and Internet of Things (IoT) devices will further enhance SD-WAN's ability to scale and meet the growing demands of modern enterprises. By shifting towards autonomous and self-healing systems, businesses can achieve more resilient, efficient, and secure networks that not only respond to issues but anticipate and prevent them. This review outlines the key technologies, benefits, and challenges associated with this evolution, offering a vision for a new era of SD-WAN that is both agile and intelligent, capable of delivering unprecedented levels of network reliability and performance.

Keywords: SD-WAN; Conceptual evolution; Traditional WAN; Self-healing network systems

1. Introduction

Software-Defined Wide Area Network (SD-WAN) is a transformative technology designed to enhance the management and optimization of wide area networks (WANs) by leveraging software-based solutions (Shukla and Stocker, 2019). SD-WAN enables enterprises to centrally manage and control their WAN architecture, which traditionally relied on costly and rigid hardware appliances for routing and traffic management. The core components of SD-WAN include the SD-WAN controller, which provides centralized policy management, the SD-WAN edge device, responsible for routing traffic, and the orchestration layer, which integrates the various elements of the network to ensure consistent and

* Corresponding author: Sunday Adeola Oladosu.

secure application delivery (Gooley et al., 2020; Rafique et al., 2020). The historical development of SD-WAN can be traced to the growing complexity and limitations of traditional WAN architectures. As businesses increasingly adopted cloud services, the reliance on legacy MPLS (Multiprotocol Label Switching) networks became unsustainable due to their high cost and rigidity. SD-WAN emerged as a solution to these challenges, offering enterprises a more flexible, scalable, and cost-efficient method to manage their WANs (Yang et al., 2019). Early adopters saw SD-WAN as an opportunity to modernize network management, reduce operational costs, and improve network performance.

Traditional WAN architectures were predominantly based on MPLS, a highly reliable but expensive network technology (Troia et al., 2020). In this setup, all traffic between branch offices and data centers was routed through a central hub, often resulting in inefficiencies and bottlenecks. Additionally, the complexity of managing these networks, along with the increasing demand for cloud services and mobile workforces, strained the capabilities of traditional WAN solutions. Security was another critical challenge, as enterprises had to deploy multiple disparate security solutions across their network. SD-WAN addresses these issues by providing centralized control over the entire network, allowing businesses to prioritize traffic based on application requirements and ensuring better performance through path selection algorithms. This dynamic traffic management enables cost reduction by leveraging less expensive internet connections, such as broadband or 4G/5G, in place of MPLS circuits. The flexibility introduced by SD-WAN further enhances network agility, allowing companies to scale their WAN infrastructures easily without heavy investments in new hardware (Gupta et al., 2018). Moreover, the technology improves application performance by directing traffic through the most optimal routes, reducing latency, and ensuring a better user experience.

This review aims to explore the next phase in the evolution of SD-WAN towards autonomous, self-healing networks. As SD-WAN technology matures, its capabilities are expanding beyond traditional traffic management and optimization. The introduction of artificial intelligence (AI) and machine learning (ML) into SD-WAN is expected to pave the way for autonomous systems that can self-configure, detect anomalies, and proactively correct issues without human intervention. These advancements are essential for handling the increasing complexity of modern enterprise networks, which demand more automation to meet real-time performance and security requirements (Qin et al., 2020). In addition, the review will discuss the future capabilities and implications of SD-WAN for network management. As organizations continue to embrace digital transformation and integrate diverse applications, SD-WAN will play a central role in ensuring seamless connectivity, security, and performance. The integration of self-healing and AI-driven capabilities into SD-WAN will redefine how enterprise networks are managed, shifting the focus from manual configurations to automated, adaptive systems that are more resilient and capable of self-optimization. This transition will likely have profound implications for network operations, security protocols, and the overall efficiency of business networks, necessitating a reevaluation of existing strategies and tools used in network management.

2. Current State of SD-WAN

Traditional Wide Area Networks (WANs) primarily rely on Multiprotocol Label Switching (MPLS) to connect enterprise locations across long distances (Liptak and Eren, 2018). In a traditional WAN, traffic is routed through a centralized hub, often creating network bottlenecks and inefficiencies. The control mechanisms are typically decentralized, with individual sites requiring separate configuration and management, which can result in complex and time-consuming operations. Additionally, MPLS circuits are costly, both in terms of installation and ongoing operational expenses, making them an impractical solution for many businesses looking to scale their network infrastructure. In contrast, SD-WAN provides a more flexible and cost-effective approach to managing wide area networks. One of the primary differences between traditional WAN and SD-WAN lies in the control structure: while traditional WAN architectures are centralized, SD-WAN offers centralized control through a software-based controller, which streamlines network management and allows for more dynamic control of traffic. SD-WAN leverages lower-cost broadband internet connections, such as DSL, fiber, or even 4G/5G, instead of relying on expensive MPLS circuits. This reduction in reliance on MPLS leads to significant cost savings, while also improving scalability, as businesses can easily add new locations without the need for complex hardware installations (Karakus and Durresi, 2019). Furthermore, SD-WAN allows businesses to dynamically allocate resources, optimizing bandwidth and reducing latency, making it more efficient and adaptable than traditional WAN solutions.

The key components of an SD-WAN solution include edge devices, controllers, and cloud-based management platforms (Wang et al., 2019). Edge devices, typically located at the branch offices or remote locations, serve as the gateways through which network traffic flows. These devices are responsible for enforcing policies set by the centralized SD-WAN controller, such as routing traffic, ensuring security, and managing traffic prioritization based on application needs. The SD-WAN controller, located in the data center or cloud, is the central point for managing the network configuration, applying policies, and making real-time decisions about traffic routing. A crucial aspect of SD-WAN is its ability to dynamically select paths for network traffic. This is facilitated through dynamic path selection, a functionality that

continuously evaluates the best available network routes based on factors such as network performance, reliability, and latency. This feature ensures that mission-critical applications are always routed through the most optimal path, improving overall performance. Application-aware routing is another key function, which enables SD-WAN to identify specific types of traffic (e.g., voice, video, or web traffic) and apply predefined policies to prioritize or shape traffic accordingly. This leads to enhanced user experiences, as high-priority applications receive the necessary bandwidth and latency for optimal performance. Traffic optimization is also a fundamental capability of SD-WAN, as it can compress and prioritize data to maximize the utilization of available bandwidth (Alwasel et al., 2020). Cloud-based management is another significant aspect of SD-WAN. It allows administrators to monitor and configure the network from a centralized, cloud-hosted platform. This cloud-based approach enables greater flexibility, allowing businesses to manage remote locations and branch offices with ease, regardless of geographic distance. Furthermore, it reduces the need for on-site management, contributing to lower operational costs and more agile network operations.

SD-WAN offers numerous benefits, primarily in the areas of bandwidth efficiency, flexibility, and centralized management (Majdoub et al., 2020). One of the key advantages of SD-WAN is its ability to maximize bandwidth utilization by intelligently routing traffic across multiple connections. With dynamic path selection and application-aware routing, SD-WAN ensures that bandwidth is allocated based on application requirements, leading to more efficient use of available network resources. This results in lower costs, as businesses can use more affordable internet connections without sacrificing performance. Flexibility is another notable benefit. SD-WAN can seamlessly integrate various types of network connections, including broadband, MPLS, and cellular networks, enabling businesses to choose the most cost-effective solution for each site. The centralized management provided by SD-WAN further enhances operational efficiency by allowing IT teams to configure, monitor, and manage the entire network from a single platform, simplifying network administration and reducing the risk of configuration errors.

However, despite its advantages, SD-WAN has some limitations. Security remains a critical concern, as businesses must ensure that the network traffic is adequately protected, particularly when using public internet connections. While SD-WAN solutions often include encryption and firewall capabilities, the decentralized nature of some SD-WAN implementations can create vulnerabilities if not managed properly (Kamaludeen et al., 2020). Scalability can also pose challenges, as large organizations may face difficulties in managing multiple remote locations with varying network demands. Furthermore, integrating SD-WAN with existing legacy infrastructure and systems may require additional resources and expertise, potentially delaying deployment and increasing costs. While SD-WAN offers significant enhancements in network performance, cost reduction, and flexibility compared to traditional WAN architectures, businesses must address ongoing challenges related to security, scalability, and integration as they adopt and expand their SD-WAN solutions.

2.1. Conceptual Evolution: From Traditional SD-WAN to Autonomous, Self-Healing Networks

Autonomous networks are an emerging concept that represents the next phase in the evolution of network management (Tanaka et al., 2020). These networks are designed to function independently with minimal human intervention, relying on advanced technologies like artificial intelligence (AI), machine learning (ML), and automation to make decisions, manage traffic, and optimize performance in real time. Unlike traditional networks, where human administrators must manually configure settings, troubleshoot issues, and adjust traffic, autonomous networks are capable of self-governing, meaning they can autonomously detect and resolve network problems, optimize resource usage, and adjust network configurations as needed. The key characteristic of an autonomous network is its ability to make decisions based on data collected from various network elements, user behavior, and external conditions, without human input. These networks leverage AI and ML algorithms to process vast amounts of data in real time, identifying trends, anomalies, and potential issues. AI enables the network to predict and adapt to changing conditions, ensuring optimal performance even in dynamic and unpredictable environments. ML algorithms continuously learn from historical data, improving network management by identifying patterns and proactively addressing issues before they impact performance. Automation within autonomous networks further streamlines processes, reducing the need for manual intervention and enabling faster response times to changing network demands (Gilbert, 2018).

Self-healing networks represent an essential component of autonomous networks, focusing specifically on resilience and fault tolerance (Dias et al., 2020). The concept of a self-healing network involves the ability to automatically detect, diagnose, and resolve network issues without human intervention. Traditional networks often require manual troubleshooting and configuration to address failures or performance degradation, which can lead to significant downtime and resource allocation challenges. Self-healing mechanisms, on the other hand, enhance network reliability by ensuring that any disruption whether due to hardware failure, congestion, or security breaches is automatically detected and resolved in real time. AI and ML play a pivotal role in the self-healing capabilities of modern networks. Through continuous monitoring and fault detection, these technologies can identify anomalies or failures in the network

infrastructure. Once an issue is detected, machine learning algorithms can determine the most appropriate action to resolve the problem, such as rerouting traffic, activating backup systems, or adjusting network configurations. Furthermore, predictive analytics, powered by AI, can forecast potential failures before they occur, allowing the network to take preemptive measures to avoid disruptions (Brundage et al., 2018). This proactive approach to network management significantly enhances the resilience of the network, reducing downtime and improving overall service continuity.

Automation and real-time adaptability are key drivers of innovation in autonomous networks. By leveraging data analytics, these networks can make proactive decisions based on the current state of the network, user demands, and external conditions. Real-time adaptability enables the network to adjust its behavior dynamically, ensuring that resources are allocated efficiently and that performance is optimized based on the immediate needs of applications and users (Lorenzo et al., 2018). For example, if network traffic spikes for a critical application, the network can automatically allocate additional resources to ensure that the application maintains optimal performance. Data analytics, integrated into autonomous networks, provides deep insights into network performance, user behavior, and application requirements. By continuously analyzing this data, AI and ML algorithms can identify emerging patterns and trends, enabling the network to make data-driven decisions that optimize traffic flow, bandwidth allocation, and load balancing. Continuous monitoring further enhances the network's ability to respond to issues in real time, while predictive analytics can foresee potential disruptions and adapt the network's behavior to mitigate their impact (Ivanov et al., 2019). This ability to make adaptive decisions allows autonomous networks to maintain high levels of performance and reliability, even under fluctuating and unpredictable conditions.

The convergence of SD-WAN with emerging technologies such as the Internet of Things (IoT), edge computing, and 5G networks is creating new opportunities for adaptive and resilient network management (Shirmarz and Ghaffari, 2020). The integration of SD-WAN with IoT enables networks to handle the massive influx of data generated by connected devices. IoT devices require low-latency communication and high bandwidth, which SD-WAN can manage effectively by dynamically adjusting network policies to ensure seamless communication between devices. SD-WAN's ability to prioritize traffic based on application requirements allows IoT networks to operate smoothly, even as the number of devices and data flows increases. Edge computing further enhances SD-WAN by enabling data processing closer to the source, at the edge of the network. This reduces latency, accelerates response times, and decreases the load on centralized cloud servers. By combining SD-WAN with edge computing, organizations can ensure that critical applications, especially those requiring real-time processing, receive the necessary resources without delays caused by distant data centers. The rollout of 5G networks is also poised to significantly impact SD-WAN's performance and reliability. 5G offers enhanced bandwidth, lower latency, and greater scalability compared to previous generations of mobile networks. This makes it particularly beneficial for applications that demand high-speed connections and minimal latency, such as augmented reality (AR), virtual reality (VR), and autonomous vehicles. SD-WAN, when integrated with 5G, can dynamically allocate resources and reroute traffic based on real-time data, ensuring that the network can handle the increased demand for bandwidth and the low-latency requirements of next-generation applications (Sanchez-Iborra et al., 2019). The combination of SD-WAN, IoT, edge computing, and 5G is set to create networks that are not only faster and more efficient but also more adaptable to the growing complexity and scale of modern enterprises.

The transition from traditional SD-WAN to autonomous, self-healing networks marks a significant evolution in the way we approach network management. Autonomous networks, powered by AI and ML, offer self-governing, resilient, and adaptable infrastructures capable of addressing the increasing demands of modern businesses. Self-healing mechanisms enhance network reliability by automatically detecting and resolving issues, while automation and real-time adaptability ensure that networks can optimize performance dynamically. As SD-WAN converges with IoT, edge computing, and 5G, the networks of the future will be more efficient, flexible, and capable of supporting the next generation of digital technologies. This evolution in network design will provide businesses with unprecedented levels of operational efficiency and performance, while also laying the groundwork for the fully autonomous networks of tomorrow (Clemm et al., 2020).

2.2. Key Technologies Enabling the Evolution of SD-WAN

Artificial Intelligence (AI) and Machine Learning (ML) play a pivotal role in the evolution of SD-WAN by driving automation, anomaly detection, and predictive maintenance (Vemula et al., 2020). AI enables SD-WAN systems to autonomously make decisions regarding traffic routing, bandwidth allocation, and network optimization. Through ML algorithms, these networks can analyze large volumes of network data in real time, detecting anomalies that could indicate network congestion, security threats, or hardware failures. This proactive approach allows for immediate adjustments to maintain optimal performance and reliability. The role of deep learning, a subset of ML, is particularly

significant in adapting network behavior to enhance user experience. Deep learning models are capable of processing vast amounts of data from various sources, including user applications and network traffic patterns, enabling SD-WAN to learn and evolve based on real-time conditions. These systems can identify patterns in traffic flows, predict future network demands, and adjust configurations to ensure minimal disruption. As a result, deep learning not only improves the overall network experience for users by optimizing routing and minimizing latency, but it also enables SD-WAN to operate with greater efficiency, adapting to the complex needs of modern enterprise networks. Network automation is crucial in reducing human intervention and improving the speed and accuracy of decision-making processes in SD-WAN. Automation empowers SD-WAN systems to autonomously detect network issues, adjust configurations, and optimize performance without manual intervention. This reduces the risk of human error and allows for more responsive network management, especially in dynamic environments with high traffic variability. Furthermore, automation ensures that routine tasks such as traffic management, network segmentation, and security policies are consistently applied, reducing the administrative burden and enhancing operational efficiency. Orchestration tools are central to managing the complexity of modern network infrastructures (Casellas et al., 2018). They integrate multiple network components, such as edge devices, controllers, and cloud-based systems, into a cohesive framework. Through orchestration, SD-WAN networks can maintain end-to-end visibility, enabling centralized control while simultaneously allowing for the dynamic and automated adjustment of network resources. This capability is essential for scaling SD-WAN to meet the demands of growing businesses and ensuring that resources are allocated optimally across the network.

SD-WAN and Software-Defined Networking (SDN) complement each other to create more flexible and adaptive networks. SDN provides centralized control over network resources, allowing for dynamic adjustments to network configurations based on real-time conditions. SD-WAN extends this flexibility by integrating SDN principles with wide-area network management, optimizing traffic routing, and ensuring efficient bandwidth use (Mine et al., 2020). The synergy between SD-WAN and SDN enables enterprises to adapt quickly to changing business needs and ensures that network resources are utilized efficiently, supporting everything from cloud-based applications to remote work setups. The role of SDN in enabling dynamic resource allocation is particularly important in autonomous networks. As SD-WAN solutions evolve toward self-healing and fully automated systems, SDN acts as the backbone that allows for the seamless allocation of resources across diverse network environments. Through SDN, SD-WAN can leverage centralized control to automatically adjust bandwidth, prioritize critical applications, and re-route traffic in response to changing network conditions, ensuring that the network remains resilient and responsive even in high-demand scenarios.

Edge computing is a key technology enabling the evolution of SD-WAN by processing data closer to the source, which improves both efficiency and reduces latency (Yassin and Yalcin, 2019). By processing data at the edge of the network, closer to users or devices, SD-WAN can respond more quickly to application demands and minimize delays caused by sending data to centralized cloud data centers. This is particularly important for applications that require low-latency communication, such as video conferencing, IoT devices, and real-time analytics. Edge computing ensures that network performance remains high, even as data volumes and user demands increase. The integration of edge computing with SD-WAN enhances scalability and responsiveness. As SD-WAN networks grow and become more distributed, edge computing allows for localized processing and decision-making, enabling networks to handle increased workloads without overburdening central data centers. By decentralizing data processing, edge computing also ensures that SD-WAN can efficiently handle diverse workloads, including those from IoT devices and smart applications, which require immediate responses and localized control (Bhatia et al., 2019). This distributed architecture supports the future needs of enterprises, enabling them to operate with high efficiency and responsiveness in a rapidly changing digital landscape.

The evolution of SD-WAN is being significantly driven by key technologies such as AI, ML, network automation, SDN, and edge computing (Krishnan et al., 2019). AI and ML provide the intelligence needed for automation, anomaly detection, and network adaptation, while network automation and orchestration streamline management and decision-making processes. The integration of SDN allows for flexible and dynamic resource allocation, while edge computing reduces latency and enhances scalability. Together, these technologies are transforming SD-WAN from a static, manually managed network solution to a highly adaptive, self-healing, and autonomous system capable of supporting the complex and dynamic needs of modern enterprises. The continuous advancement of these technologies will enable the next generation of SD-WAN, improving performance, reliability, and efficiency across diverse network environments.

2.3. Benefits of Autonomous, Self-Healing SD-WAN

One of the primary benefits of autonomous, self-healing SD-WAN is significantly improved network reliability and uptime. Traditional networks often experience downtime due to a variety of issues, such as equipment failures, network congestion, or human error (Asghar et al., 2018). Autonomous SD-WAN systems, however, have the capability to

automatically detect and resolve these issues in real time. When a network failure or performance degradation occurs, the system can identify the problem, reroute traffic, or apply the necessary fixes without manual intervention, minimizing service interruptions. This self-healing capability not only reduces downtime but also enables continuous monitoring and proactive problem resolution. For instance, if a particular network path fails or a device malfunctions, the SD-WAN can instantly switch to an alternative route or initiate backup systems, ensuring minimal disruption to users and applications (Gaikwad et al., 2018). This leads to increased uptime, more consistent network performance, and ultimately a more reliable network environment for businesses and their users.

Autonomous SD-WAN enhances network efficiency and performance through real-time traffic optimization, intelligent bandwidth management, and dynamic policy adjustments (Pérez et al., 2019). In a traditional WAN, network traffic is routed based on fixed, predefined paths, often leading to inefficiencies, such as overburdened routes or suboptimal bandwidth usage. SD-WAN, on the other hand, utilizes dynamic path selection to route traffic over the best available network path based on real-time conditions, such as latency, bandwidth availability, and application requirements. Furthermore, intelligent bandwidth management enables SD-WAN to allocate network resources more effectively, prioritizing mission-critical applications, ensuring that performance-sensitive tasks receive the required bandwidth, while less critical tasks are allocated minimal resources. This leads to optimized network performance, reduced latency, and an overall enhanced user experience. With the ability to analyze traffic patterns, SD-WAN can also predict future bandwidth needs, making adjustments in real time, thus preventing bottlenecks before they impact performance (Duliński et al., 2020).

Autonomous, self-healing SD-WAN can result in significant long-term cost savings for businesses by reducing operational complexity and improving resource utilization. Traditional WAN architectures often require expensive dedicated connections, such as MPLS (Multiprotocol Label Switching), to ensure high performance and reliability. These networks also rely heavily on manual management, which involves high operational costs and delays in response time. In contrast, SD-WAN leverages broadband internet connections, which are more cost-effective while still providing robust performance through dynamic path selection and automated traffic management. Moreover, the automation of routine network management tasks, such as fault detection, traffic rerouting, and bandwidth allocation, reduces the need for manual intervention and the associated labor costs (Ilk et al., 2020). The self-healing nature of SD-WAN also reduces the cost of downtime, as issues are detected and resolved automatically, minimizing disruption to business operations. Additionally, the scalability of SD-WAN allows businesses to adjust resources as needed, avoiding over-investment in unnecessary infrastructure. Over time, these cost reductions make SD-WAN an attractive solution for enterprises looking to optimize their network infrastructure while maintaining high levels of performance and reliability.

The scalability and flexibility of autonomous SD-WAN are critical benefits for businesses that need to adapt their network infrastructure to changing needs. Traditional networks often require significant investment in physical infrastructure and complex reconfigurations when scaling up or down (Gui and MacGill, 2018). SD-WAN, however, offers the ability to seamlessly scale network resources by simply adjusting the software-defined policies that govern traffic routing, bandwidth allocation, and security settings. This flexibility allows businesses to scale their networks in response to growth, without the need for substantial physical upgrades or complex reconfiguration processes. Furthermore, SD-WAN can easily adapt to a wide variety of enterprise environments, from small businesses with limited IT infrastructure to large, global enterprises with diverse networking needs. The ability to integrate with cloud services, branch offices, remote workers, and IoT devices enables SD-WAN to support modern business environments that are increasingly decentralized and reliant on cloud-based services. By providing this level of flexibility, SD-WAN can accommodate the changing needs of businesses, regardless of their size or geographical distribution, making it an ideal solution for enterprises seeking to future-proof their networks. The benefits of autonomous, self-healing SD-WAN are numerous and impactful (Adam and Ping, 2018). By improving network reliability and uptime, enhancing performance and efficiency, reducing costs, and offering scalability and flexibility, SD-WAN addresses many of the challenges posed by traditional WAN architectures. As businesses increasingly rely on digital services, cloud applications, and remote workforces, the ability to implement a self-healing, adaptive network becomes essential. The continued evolution of SD-WAN, driven by automation and intelligent technologies, ensures that businesses can maintain high levels of performance, reliability, and cost-effectiveness in an increasingly complex and dynamic network environment.

2.4. Security Considerations in Autonomous SD-WAN

As SD-WAN technology evolves, so too must its security models. One significant trend in autonomous SD-WAN is the shift toward a zero-trust security architecture. In traditional network security models, trust was often implicitly granted once a device or user was authenticated within the network perimeter (Balachandran et al., 2020). However, in a dynamic and decentralized SD-WAN environment, where devices and users may frequently change locations or access

points, traditional perimeter-based security becomes inadequate. The zero-trust model assumes no implicit trust for any user or device, regardless of its location within or outside the network perimeter. Every access request is treated as potentially untrusted, requiring continuous authentication and validation, even for internal users or devices. This shift to a zero-trust model in SD-WAN helps mitigate the security risks associated with the increasing complexity of modern networks. It establishes robust security protocols that ensure secure communications across both public and private network infrastructures. However, the highly dynamic and self-healing nature of SD-WAN introduces new challenges, such as maintaining consistent security policies across rapidly changing network paths and multiple points of entry (Ventre et al., 2020). This requires advanced tools and processes to continuously monitor and enforce security measures as the network evolves.

Artificial intelligence (AI) plays a pivotal role in enhancing the security capabilities of autonomous SD-WAN. AI and machine learning (ML) technologies enable real-time threat detection and automated responses, crucial for the self-healing nature of SD-WAN (Zitouna, 2020). Traditional security solutions often rely on predefined rules and signatures to detect threats, which can be slow and ineffective against new, evolving attack vectors. In contrast, AI-driven security systems can analyze vast amounts of network traffic in real-time, identifying patterns and anomalies that may indicate malicious activity. Machine learning algorithms continuously learn from network behavior, improving their ability to detect sophisticated threats, such as zero-day attacks, insider threats, and advanced persistent threats (APTs). Once a threat is detected, AI can trigger automated responses, such as isolating compromised devices, rerouting traffic, or adjusting security policies to mitigate the threat without manual intervention. This automation is crucial for maintaining network integrity in a self-healing environment, where the network is constantly adapting and evolving. Moreover, the integration of AI-driven threat detection with security policies and compliance frameworks ensures that autonomous SD-WAN networks can not only respond to threats in real-time but also adhere to industry-specific regulations and standards. This integration helps businesses maintain regulatory compliance, even in dynamic, distributed network environments.

In an autonomous SD-WAN, ensuring secure data transmission is of paramount importance (Ivanciu et al., 2021). Since SD-WANs often leverage the public internet or hybrid network environments, data can traverse multiple untrusted networks, increasing the potential for interception, eavesdropping, or data manipulation. End-to-end encryption is critical to securing data as it moves across these potentially insecure networks. Autonomous SD-WAN architectures typically employ strong encryption protocols, such as IPsec or SSL/TLS, to protect data in transit. These encryption methods ensure that even if data is intercepted during transmission, it remains unreadable to unauthorized parties. Additionally, SD-WAN solutions often include features such as application-aware traffic management, which can dynamically adjust encryption levels based on the sensitivity of the data being transmitted (Kumar and Thakur, 2020). For example, critical business applications or sensitive customer data may be routed over more secure paths or subjected to higher levels of encryption, ensuring robust protection throughout the network. The self-healing nature of SD-WAN adds complexity to secure data transmission, as the network paths constantly change in response to varying conditions. However, this dynamic behavior does not compromise security, as SD-WAN solutions can implement real-time encryption across all active paths, maintaining consistent protection despite network changes. Furthermore, the integration of security features such as identity-based access control and segmentation ensures that data is only accessible to authorized devices and users, safeguarding sensitive information across the network. Security considerations in autonomous SD-WAN are critical to ensuring the reliability and integrity of modern, dynamic network environments. As organizations adopt zero-trust security models and integrate AI-driven threat detection and automated responses, SD-WAN becomes increasingly resilient to emerging threats. The combination of real-time threat mitigation, end-to-end encryption, and continuous monitoring ensures that autonomous SD-WAN can deliver secure and reliable performance (Liu et al., 2019). However, businesses must remain vigilant to the evolving nature of cybersecurity threats and invest in comprehensive, adaptive security strategies to safeguard their SD-WAN environments in the face of an ever-changing threat landscape.

2.5. Challenges and Considerations

One of the primary challenges organizations face when adopting autonomous SD-WAN is integrating it with existing legacy systems. Many enterprises still rely on traditional WAN architectures, such as MPLS (Multiprotocol Label Switching), which are often deeply embedded in their IT infrastructures (Ridwan et al., 2020). Legacy networks are typically designed with centralized control models, rigid configurations, and limited flexibility, which can be at odds with the decentralized, dynamic nature of SD-WAN. The transition from a traditional WAN to a self-healing, automated SD-WAN requires careful planning and coordination to ensure compatibility. Integrating autonomous SD-WAN with legacy systems involves addressing technical gaps in network architecture, such as differences in protocol support, management tools, and network configurations. For example, traditional WAN solutions may not have the capabilities to support real-time traffic optimization, dynamic path selection, or the extensive automation features inherent in SD-

WAN. Moreover, the complexity of managing legacy hardware and software while integrating new SD-WAN components can lead to compatibility issues, requiring extensive customization or the replacement of outdated hardware. This process can result in increased implementation time and costs, making the integration of SD-WAN into legacy networks a significant challenge for enterprises seeking to modernize their network infrastructure.

While automation and self-healing mechanisms offer significant benefits in SD-WAN, they can also introduce a new layer of complexity and operational overhead. Autonomous SD-WAN relies heavily on AI, machine learning, and real-time analytics to enable adaptive network behavior, detect anomalies, and make decisions without human intervention. However, this level of sophistication requires a substantial amount of data processing and analysis, which can increase the overall complexity of network management. Managing this complexity can be challenging for IT teams, particularly in organizations with limited experience in advanced network technologies (Culot et al., 2019). The deployment of self-healing networks involves continuous monitoring, algorithm fine-tuning, and ensuring that automation systems operate correctly without causing disruptions. If misconfigured or poorly managed, these automated systems could create more problems than they solve, leading to unpredictable network behavior or performance degradation. Additionally, the reliance on machine learning and AI to make network decisions requires consistent input of accurate data and constant updates to the algorithms. These requirements can lead to increased operational overhead, especially for organizations without dedicated teams for managing and overseeing AI and automation processes. Furthermore, self-healing mechanisms, which aim to detect and resolve network issues automatically, may introduce challenges in ensuring that these fixes align with organizational policies or compliance frameworks. Misalignments between automated responses and predefined network policies could create inconsistencies in network performance or security (Luckie et al., 2019). Therefore, enterprises must carefully balance the benefits of automation with the need for human oversight and continuous system optimization.

Another significant consideration in the deployment of autonomous SD-WAN is the risk of vendor lock-in and the challenges surrounding interoperability in multi-cloud environments. Many SD-WAN solutions are provided by specific vendors, each with proprietary technologies, management platforms, and integration methods. This can create a situation where an enterprise becomes dependent on a single vendor's products and services, limiting its ability to switch providers or adopt new technologies in the future. Vendor lock-in may result in higher long-term costs and reduced flexibility, particularly as businesses seek to scale or expand their networks (Hetemi et al., 2020). Interoperability is another critical concern, especially as more enterprises move toward multi-cloud environments and hybrid network architectures. In such configurations, organizations often use services from multiple cloud providers, each with its own set of APIs, security protocols, and network management tools. Ensuring seamless integration between SD-WAN solutions and various cloud environments is essential for maintaining a cohesive and efficient network. If an SD-WAN solution cannot effectively interface with a variety of cloud platforms or other third-party systems, organizations may face challenges in optimizing their network performance and scalability. To address these challenges, enterprises must prioritize vendor-neutral solutions that support open standards and ensure compatibility across diverse environments. Additionally, it is essential to invest in SD-WAN solutions that are designed to work seamlessly with both on-premises hardware and cloud-based services. This approach allows organizations to retain flexibility, avoid vendor lock-in, and ensure that their network infrastructure can evolve with future technological advancements. The adoption of autonomous SD-WAN technology brings numerous benefits, but it also presents significant challenges. Integrating SD-WAN into legacy systems, managing the complexity of automation and self-healing mechanisms, and addressing vendor lock-in and interoperability concerns are all critical considerations for organizations seeking to adopt this next-generation networking technology. Overcoming these obstacles requires careful planning, investment in compatible technologies, and a balanced approach to automation and human oversight. As SD-WAN technology continues to evolve, addressing these challenges will be essential for ensuring that businesses can fully realize the potential of autonomous, self-healing networks while maintaining security, flexibility, and operational efficiency (Veichtlbauer et al., 2020).

2.6. Future Trends and Opportunities in SD-WAN

The convergence of 5G technology and edge computing is expected to play a pivotal role in the future evolution of SD-WAN architectures, providing enhanced capabilities, particularly in mobile and IoT environments (Ruffini and Slyne, 2019; Tran-Dang et al., 2020). With the deployment of 5G, network speeds, latency, and reliability are set to improve dramatically, enabling SD-WAN to leverage these advancements to optimize performance. 5G's low latency and high bandwidth are crucial for SD-WAN, as they allow real-time communication and faster data processing, which are essential for modern applications such as IoT and autonomous systems. This enhancement is especially significant for industries relying on real-time data, such as healthcare, manufacturing, and logistics. Edge computing, when integrated with SD-WAN, can further enhance network performance by processing data closer to the source rather than sending it to centralized data centers. This reduces latency and enhances responsiveness, a key requirement for applications like

video streaming, virtual reality, and remote operations. As edge computing enables data to be processed locally, SD-WAN can dynamically manage network traffic more efficiently, ensuring that resources are allocated optimally across the network. The combination of 5G and edge computing will therefore empower SD-WAN to support a broader range of use cases and industries, particularly in environments with heavy data traffic and time-sensitive requirements (Liguori and Winandy, 2018).

The evolution towards fully autonomous networks is one of the most exciting prospects for SD-WAN technology (Khalili et al., 2019). Currently, SD-WAN provides automation in traffic management, route optimization, and policy enforcement; however, its future lies in extending these capabilities to create networks that require minimal human intervention. Fully autonomous SD-WAN systems will be able to self-manage, detect, and resolve network issues in real-time without relying on human operators. This means that networks could adapt dynamically to changes in traffic patterns, application requirements, and even environmental conditions, without the need for manual configuration or intervention. Artificial intelligence (AI) and machine learning (ML) will be central to achieving this level of autonomy. These technologies will enable SD-WAN to analyze network data, predict potential failures, and automatically apply corrective actions before issues arise. Moreover, fully autonomous networks will be capable of continuously learning and improving from historical data, enhancing decision-making and adaptability (Khan et al., 2018). In the future, such networks could perform tasks such as load balancing, fault detection, and performance tuning in real-time, ensuring that the network operates at peak efficiency at all times. As businesses increasingly demand more agile and resilient networks, the shift toward autonomy will be critical in transforming network management and reducing operational overhead.

The impact of autonomous SD-WAN will be profound across various industries, offering significant benefits in terms of efficiency, security, and scalability (Derhab et al., 2019). In the finance sector, the ability to automatically optimize network traffic and ensure high levels of performance and reliability will be crucial, particularly for banks and financial institutions that rely on real-time transactions and sensitive data. Autonomous SD-WAN will also enable more effective cybersecurity measures, detecting and mitigating potential threats in real-time, which is essential in an industry where data privacy and security are paramount. The healthcare industry will greatly benefit from the enhanced capabilities of SD-WAN, especially with the increasing adoption of telemedicine, IoT-enabled medical devices, and electronic health records. Autonomous SD-WAN will provide healthcare providers with secure, reliable, and low-latency connectivity for these critical services, enabling faster diagnosis, remote monitoring, and more efficient patient care management (Siddiqi et al., 2019). Furthermore, the ability to adapt to varying bandwidth demands in real-time will be vital for healthcare environments that rely on high-definition video streaming, data analytics, and cloud-based applications. In retail, SD-WAN will transform how businesses manage their networks, particularly as more companies embrace e-commerce and digital transformations. Autonomous SD-WAN will enable seamless customer experiences, optimized for performance and reliability, regardless of whether customers are shopping online or in-store. Retailers will also benefit from real-time traffic optimization to ensure their supply chains, payment systems, and customer service platforms run smoothly, improving both operational efficiency and customer satisfaction (Dash et al., 2019; Omar ET AL., 2020). In addition, manufacturing and logistics industries will see improvements in the deployment of connected devices and automation systems. As factories and warehouses increasingly rely on IoT devices, SD-WAN will be integral to ensuring the connectivity and performance of these devices in real-time, supporting the automation of critical processes, inventory management, and data analytics (Singh, 2018; Basu et al., 2020).

The future of SD-WAN is promising, with key advancements in 5G, edge computing, and autonomous network capabilities driving its evolution. As networks become more autonomous, industries will see improvements in efficiency, performance, and security, enabling them to meet the demands of increasingly complex, data-driven environments (Jiang ET AL., 2018; McKee et al., 2018). The adoption of SD-WAN in sectors such as finance, healthcare, and retail will continue to grow, unlocking new opportunities for businesses to innovate and enhance their operations. As these technologies mature, SD-WAN will play a central role in transforming network management, offering a more dynamic, resilient, and scalable solution for the future of enterprise networks (Radcliffe ET AL., 2019).

3. Conclusion

This review has explored the potential transformation of SD-WAN from its traditional architecture to the emerging paradigm of autonomous, self-healing networks. Traditional SD-WAN has already revolutionized enterprise networks by offering centralized control, improved performance, and cost savings. However, as network demands continue to grow, the next phase of SD-WAN evolution involves the integration of autonomous capabilities, enabled by artificial intelligence (AI), machine learning (ML), and real-time data analytics. These technologies will empower SD-WAN to dynamically adapt to network conditions, predict potential issues, and autonomously resolve problems without human intervention. Self-healing networks will enhance network resilience by reducing downtime, improving uptime, and

enhancing the user experience through intelligent traffic management. Moreover, the future of SD-WAN will witness greater integration with cutting-edge technologies such as 5G and IoT. The low latency and high bandwidth capabilities of 5G, coupled with the proximity-based data processing power of edge computing, will allow SD-WAN to operate at unprecedented levels of performance. This convergence will drive more efficient and scalable networks, enabling real-time adaptability to business needs.

The future of SD-WAN is poised for continued growth, driven by the ongoing advancements in automation, machine learning, and the integration of new technologies like 5G and IoT. As these technologies mature, SD-WAN will transition towards fully autonomous, self-healing networks capable of managing complex infrastructures with minimal human oversight. This will not only optimize network performance but also significantly reduce operational costs and increase scalability, making SD-WAN an essential part of the next generation of enterprise networking solutions. The industries that adopt these advancements early will benefit from improved efficiency, agility, and resilience, paving the way for the broader transformation of the digital landscape. As such, the future of SD-WAN is bright, offering vast opportunities for innovation and growth across multiple sectors.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adam, I. and Ping, J., 2018, August. Framework for security event management in 5G. In *Proceedings of the 13th international conference on availability, reliability and security* (pp. 1-7).

[2] Alwasel, K., Jha, D.N., Hernandez, E., Puthal, D., Barika, M., Varghese, B., Garg, S.K., James, P., Zomaya, A., Morgan, G. and Ranjan, R., 2020. Iotsim-sdwan: A simulation framework for interconnecting distributed datacenters over software-defined wide area network (sd-wan). *Journal of Parallel and Distributed Computing*, *143*, pp.17-35.

[3] Asghar, A., Farooq, H. and Imran, A., 2018. Self-healing in emerging cellular networks: Review, challenges, and research directions. *IEEE Communications Surveys & Tutorials*, *20*(3), pp.1682-1709.

[4] Balachandran, C., Ramachandran, G. and Krishnamachari, B., 2020, November. EDISON: a blockchain-based secure and auditable orchestration framework for multi-domain software defined networks. In *2020 IEEE International Conference on Blockchain (Blockchain)* (pp. 144-153). IEEE.

[5] Basu, K., Hamdullah, A. and Ball, F., 2020, June. Architecture of a cloud-based fault-tolerant control platform for improving the qos of social multimedia applications on sd-wan. In *2020 13th International Conference on Communications (COMM)* (pp. 495-500). IEEE.

[6] Bhatia, J., Modi, Y., Tanwar, S. and Bhavsar, M., 2019. Software defined vehicular networks: A comprehensive review. *International Journal of Communication Systems*, *32*(12), p.e4005.

[7] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

[8] Casellas, R., Martínez, R., Vilalta, R. and Muñoz, R., 2018. Control, management, and orchestration of optical networks: evolution, trends, and challenges. *Journal of Lightwave Technology*, *36*(7), pp.1390-1402.

[9] Clemm, A., Zhani, M.F. and Boutaba, R., 2020. Network management 2030: Operations and control of network 2030 services. *Journal of Network and Systems Management*, *28*(4), pp.721-750.

[10] Culot, G., Fattori, F., Podrecca, M. and Sartor, M., 2019. Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, *47*(3), pp.79-86.

[11] Dash, R., McMurtrey, M., Rebman, C. and Kar, U.K., 2019. Application of artificial intelligence in automation of supply chain management. *Journal of Strategic Innovation and Sustainability*, *14*(3).

[12] Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M.A., Mukherjee, M. and Khan, F.A., 2019. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors*, *19*(14), p.3119.

[13] Dias, J.P., Lima, B., Faria, J.P., Restivo, A. and Ferreira, H.S., 2020, June. Visual self-healing modelling for reliable internet-of-things systems. In *International Conference on Computational Science* (pp. 357-370). Cham: Springer International Publishing.

[14] Duliński, Z., Stankiewicz, R., Rzym, G. and Wydrych, P., 2020. Dynamic traffic management for SD-WAN inter-cloud communication. *IEEE Journal on Selected Areas in Communications*, *38*(7), pp.1335-1351.

[15] Gaikwad, S., Tafleen, S., Gottumukkala, R. and Elgazzar, K., 2018, June. Fault tolerance of real-time video streaming protocols over sdn networks. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 101-107). IEEE.

[16] Gilbert, M., 2018. The role of artificial intelligence for network automation and security. In *Artificial Intelligence for Autonomous Networks* (pp. 1-23). Chapman and Hall/CRC.

[17] Gooley, J., Yanch, D., Schuemann, D. and Curran, J., 2020. *Cisco software-defined wide area networks: designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN*. Cisco Press.

[18] Gui, E.M. and MacGill, I., 2018. Typology of future clean energy communities: An exploratory structure, opportunities, and challenges. *Energy research & social science*, *35*, pp.94-107.

[19] Gupta, S., Meier-Hellstern, K. and Satterlee, M., 2018. Artificial intelligence for enterprise networks. In *Artificial Intelligence for Autonomous Networks* (pp. 263-284). Chapman and Hall/CRC.

[20] Hetemi, E., Jerbrant, A. and Mere, J.O., 2020. Exploring the emergence of lock-in in large-scale projects: A process view. *International Journal of Project Management*, *38*(1), pp.47-63.

[21] Ilk, N., Shang, G. and Goes, P., 2020. Improving customer routing in contact centers: An automated triage design based on text analytics. *Journal of Operations Management*, *66*(5), pp.553-577.

[22] Ivanciu, I.A., Botez, R., Iurian, C.M., Dumitrescu, A.V., Blaga, T.M. and Dobrota, V., 2021, November. An SD-WAN Approach for EUt+ Network. In *2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

[23] Ivanov, D., Dolgui, A., Das, A. and Sokolov, B., 2019. Digital supply chain twins: Managing the ripple effect, resilience, and disruption risks by data-driven optimization, simulation, and visibility. *Handbook of ripple effects in the supply chain*, pp.309-332.

[24] Jiang, Y., Yin, S. and Kaynak, O., 2018. Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond. *IEEE Access*, *6*, pp.47374-47384.

[25] Kamaludeen, M., Ismaeel, S. and Asiri, S., 2020, August. Next generation of network reference architecture in K-12 education sector. In *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1-6). IEEE.

[26] Karakus, M. and Durresi, A., 2019. An economic framework for analysis of network architectures: SDN and MPLS cases. *Journal of network and computer applications*, *136*, pp.132-146.

[27] Khalili, H., Khodashenas, P.S., Fernandez, C., Guija, D., Liolis, K., Politis, C., Atkinson, G., Cahill, J., King, R., Kavanagh, M. and Jou, B.T., 2019, January. Benefits and challenges of software defined satellite-5G communication. In *2019 15th annual conference on wireless on-demand network systems and services (wons)* (pp. 1-4). IEEE.

[28] Khan, M.A., Peters, S., Sahinel, D., Pozo-Pardo, F.D. and Dang, X.T., 2018. Understanding autonomic network management: A look into the past, a solution for the future. *Computer Communications*, *122*, pp.93-117.

[29] Krishnan, P., Duttagupta, S. and Achuthan, K., 2019. SDNFV based threat monitoring and security framework for multi-access edge computing infrastructure. *Mobile Networks and Applications*, *24*(6), pp.1896-1923.

[30] Kumar, D. and Thakur, J., 2020. Software-defined networks: Need of emerging networks and technologies. In *Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India* (pp. 411-443). Springer Singapore.

[31] Liguori, A. and Winandy, M., 2018. The diamond approach for SDN security. *IEEE Softwarization*.

[32] Liptak, B.G. and Eren, H., 2018. Computer Networks: LANs, MANs, WANs, and Wireless. In *Instrument Engineers' Handbook, Volume 3* (pp. 525-543). CRC Press.

[33] Liu, Y., Zhao, B., Zhao, P., Fan, P. and Liu, H., 2019. A survey: Typical security issues of software-defined networking. *China Communications*, *16*(7), pp.13-31.

[34] Lorenzo, B., Garcia-Rois, J., Li, X., Gonzalez-Castano, J. and Fang, Y., 2018. A robust dynamic edge network architecture for the internet of things. *IEEE network*, *32*(1), pp.8-15.

[35] Luckie, M., Beverly, R., Koga, R., Keys, K., Kroll, J.A. and Claffy, K., 2019, November. Network hygiene, incentives, and regulation: deployment of source address validation in the internet. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 465-480).

[36] Majdoub, M., El Kamel, A. and Youssef, H., 2020. DQR: an efficient deep Q-based routing approach in multi-controller software defined WAN (SD-WAN). *Journal of Interconnection Networks*, *20*(04), p.2150002.

[37] McKee, D.W., Clement, S.J., Almutairi, J. and Xu, J., 2018. Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. *CAAI Transactions on Intelligence Technology*, *3*(2), pp.75-82.

[38] Mine, G., Hai, J., Jin, L. and Huiying, Z., 2020, August. A design of SD-WAN-oriented wide area network access. In *2020 International Conference on Computer Communication and Network Security (CCNS)* (pp. 174-177). IEEE.

[39] Omar, I.A., Jayaraman, R., Salah, K., Debe, M. and Omar, M., 2020. Enhancing vendor managed inventory supply chain operations using blockchain smart contracts. *IEEE access*, *8*, pp.182704-182719.

[40] Pérez, M.Á.B., Losada, N.Y.S., Sánchez, E.R. and Gaona, G.M., 2019. State of the art in software defined networking (SDN). *Visión electrónica*, *13*(1), pp.178-194.

[41] Qin, W., Chen, S. and Peng, M., 2020. Recent advances in Industrial Internet: insights and challenges. *Digital Communications and Networks*, *6*(1), pp.1-13.

[42] Radcliffe, D., Furey, E. and Blue, J., 2019, December. An SD-WAN solution assuring business quality VoIP communication for home based employees. In *2019 international Conference on smart applications, Communications and networking (SmartNets)* (pp. 1-6). IEEE.

[43] Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R.U. and Dou, W., 2020. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *22*(3), pp.1761-1804.

[44] Ridwan, M.A., Radzi, N.A.M., Wan Ahmad, W.S.H.M., Abdullah, F., Jamaludin, M.Z. and Zakaria, M.N., 2020. Recent trends in MPLS networks: technologies, applications and challenges. *IET Communications*, *14*(2), pp.177-185.

[45] Ruffini, M. and Slyne, F., 2019. Moving the network to the cloud: The cloud central office revolution and its implications for the optical layer. *Journal of Lightwave Technology*, *37*(7), pp.1706-1716.

[46] Sanchez-Iborra, R., Santa, J., Gallego-Madrid, J., Covaci, S. and Skarmeta, A., 2019. Empowering the internet of vehicles with multi-RAT 5G network slicing. *Sensors*, *19*(14), p.3107.

[47] Shirmarz, A. and Ghaffari, A., 2020. Performance issues and solutions in SDN-based data center: a survey. *The Journal of Supercomputing*, *76*(10), pp.7545-7593.

[48] Shukla, A. and Stocker, V., 2019, July. Navigating the landscape of programmable networks: looking beyond the regulatory status quo. In *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*.

[49] Siddiqi, M.A., Yu, H. and Joung, J., 2019. 5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices. *Electronics*, *8*(9), p.981.

[50] Singh, S., 2018. SD-WAN service analysis, solution and its applications.

[51] Tanaka, T., Hirano, A., Kobayashi, S., Oda, T., Kuwabara, S., Lord, A., Gunning, P., Gonzalez de Dios, O., Lopez, V., Lopez de Lerma, A.M. and Manzalini, A., 2020. Autonomous network diagnosis from the carrier perspective. *Journal of Optical Communications and Networking*, *12*(1), pp.A9-A17.

[52] Tran-Dang, H., Krommenacker, N., Charpentier, P. and Kim, D.S., 2020. Toward the internet of things for physical internet: Perspectives and challenges. *IEEE internet of things journal*, *7*(6), pp.4711-4736.

[53] Troia, S., Zorello, L.M.M., Maralit, A.J. and Maier, G., 2020, July. SD-WAN: an open-source implementation for enterprise networking services. In *2020 22nd International Conference on Transparent Optical Networks (ICTON)* (pp. 1-4). IEEE.

[54] Veichtlbauer, A., Heinisch, A., Tüllenburg, F.V., Dorfinger, P., Langthaler, O. and Pache, U., 2020. Smart Grid Virtualisation for Grid-Based Routing. *Electronics*, *9*(11), p.1879.

[55] Vemula, S., Gooley, J. and Hasan, R., 2020. *Cisco Software-Defined Access*. Cisco Press.

[56] Ventre, P.L., Salsano, S., Polverini, M., Cianfrani, A., Abdelsalam, A., Filsfils, C., Camarillo, P. and Clad, F., 2020. Segment routing: A comprehensive survey of research activities, standardization efforts, and implementation results. *IEEE Communications Surveys & Tutorials*, *23*(1), pp.182-221.

[57] Wang, A., Zha, Z., Guo, Y. and Chen, S., 2019. Software-defined networking enhanced edge computing: A network-centric survey. *Proceedings of the IEEE*, *107*(8), pp.1500-1519.

[58] Yang, Z., Cui, Y., Li, B., Liu, Y. and Xu, Y., 2019, July. Software-defined wide area network (SD-WAN): Architecture, advances and opportunities. In *2019 28th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-9). IEEE.

[59] Yassin, A. and Yalcin, F., 2019. Enterprise transition to Software-defined networking in a Wide Area Network: Best practices for a smooth transition to SD-WAN.

[60] Zitouna, I.E., 2020. Learning-based Orchestrator for Intelligent Software-defined Networking Controllers. *International Journal of Software Engineering & Applications (IJSEA)*, *11*(6).