International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, Delaware, USA
Volume 13– No. 3, June 2026 – www.ijais.org

Advances in SDN: A Survey on Network Virtualization, Traffic Management, and Resource Allocation

Vetrivelan Tamilmani
Principal Service Architect
SAP America

Aniruddha Arjun Singh
ADP
Sr. Implementation Project Manager

Vaibhav Maniar
Oklahoma City University
MBA / Product Management

Rami Reddy Kothamaram
MS in Computer Information Systems
California University of management and science

Dinesh Rajendran
MSC. Software Engineering
Coimbatore Institute of Technology

Venkata Deepak Namburi
Department of Computer Science
University of Central Missouri

ABSTRACT

A new paradigm in network architecture, software-defined networking (SDN) allows for programmable, centralized, and flexible control of network resources. Data centers, clouds, and next-gen networks benefit from SDN's increased agility, scalability, and automation thanks to the separation of control and data planes. This paper provides a detailed overview of the SDN fundamentals, SDN architecture, northbound and southbound interfaces, advantages compared to traditional networking, and the SDN issues with implementation. It is coupled with Network Function Virtualization (NFV) and Virtual Data Centers (VDCs) that are explored with an aim of highlighting the dynamic resource allocation, traffic management, and network virtualization. The traffic and resource optimization based on SDN with the use of traffic engineering, Quality of Service (QoS)-aware routing, and machine learning is discussed as well. The discussion of the newly appearing paradigms such as edge-fog computing, 5G / 6G network environments is also offered to demonstrate the utmost importance of efficient, energy-aware and flexible resource planning in the modern IoT and high-speed network. Finally, the article also identifies the significance of efficient security the role, interoperability standardization and AI-driven optimization as the key to the prospect of SDN in a complex heterogeneous network infrastructure. The given insights are expected to facilitate the SDN-based networks studies and practice in the future.

Keywords

Traffic Management, Software-Defined Networking (SDN), Resource Allocation, Network Function Virtualization (NFV), Edge Computing, 5G/6G Networks.

1. INTRODUCTION

A new paradigm has emerged with the advent of cloud computing (CC), which allows users to tap into a shared pool of configurable computing resources such as networks, servers, storage, applications, and services whenever they need them [1]. Online service providers like Google Cloud, Amazon Web Services, and Microsoft Azure charge customers on an as-needed basis and supply these together. CC allows users to install the applications and deploy the servers within hours and this reduces the cost of running and increases the scalability [2]. CC is a flexible and cost-effective option to the existing IT requirements because the external provider rents physical infrastructure and charges the clients when they use it.

Simultaneously, improvements in Software-Defined Networking (SDN) have shifted the paradigm for network management by separating the data plane and control plane, allowing for centralized control and an overlay view of the network [3]. SDN extends programmable, dynamic architecture that is often defined using OpenFlow protocols that allow network applications to execute on a Network Operating System (NOS). This is the methodology that generalizes the complexity of hardware, offers flexibility and efficient resource allocation like bandwidth, memory, and sharing hardware. SDN not only improves the performance of the network but also reduces the operation cost and develops scalable multi-tenant environments.

The network virtualization is also the complement to SDN which provides the network platforms with scalability, elasticity as well as logical separation. Network virtualization together with SDN also ensures that there is the efficient utilization of resources, the improved control of traffic and an easy way of supporting the new network services [4]. It is possible to say that virtualized networks need an efficient traffic management strategy so that they can meet different network traffic needs, Quality of Service (QoS), and optimize system output in general. These procedures enable the flexible expansion and resource adjustment to the growing user demands.

Traditional mobile networks have constraints that are intrinsic to their design, such as high cost, tightly coupled control and data plane, manual configuration of devices, inefficient use of resources, and others despite these improvements. Combining SDN with network virtualization paradigms improves traffic management, efficient allocation of resources, and cost-effective, flexible, and programmable network architectures; these are the concerns that these approaches must address.

1.1 Organization of the Paper

The paper is organized in the following way: Section 2 Fundamentals of Software-Defined Networking; Section 3, Network Virtualization in SDN; Section 4, Traffic Management in SDN; Section 5, Resource Allocation in SDN. A literature review is provided in Section 6 and Section 7 contains final key findings and future directions.

2. FUNDAMENTALS OF SOFTWARE-DEFINED NETWORKING

In today's data centres, SDN is used to build and implement a network architecture that is both nimble and flexible. It is a special approach to computer programming that enables service and digital resource administrators to manage network services with a higher abstract and reliable functionality. This process is done using system separation, which determines where data traffic is to be sent via the control plane.

2.1 SDN architecture (Application, Control, and Data Plane)

Traditional SDN designs often have three levels. The complete network infrastructure, as shown in Fig. 1, is part of the SDN design.

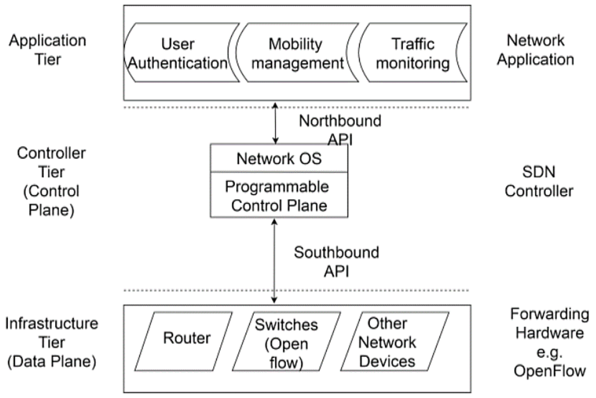

Fig 1: SDN Architecture

2.1.1 Infrastructure layer (Data Plane)

Ethernet switches and routers are examples of hardware components used in both virtual and physical networking. It is also known as a data plane. The data plane is usually in charge of data forwarding. They talk to a controller at the control layer over an interface called a southbound API. The OpenFlow Protocol is the most widely used Southbound API protocol.

2.1.2 SDN Controller Control Plane

The SDN controller is the node of the SDN architecture. It's also an important and intelligent architectural layer of SDN. All data plane systems are managed through the SDN controller. It also regulates the layers of the implementation. Through interfaces, the SDN controller communicates and regulates these top and bottom layers with the API [5]. The architecture further separates the APIs into northbound APIs and southbound APIs. These APIs are named simply because of their interaction with the control plane’s north and south directions. The APIs provide an interface in the architecture between distinct layers.

2.1.3 Application Plane

Network application and maintenance authentication, energy-efficient networking, and privacy tracking are examples of high-level functional applications that show how the data plane is divided into user control and maintenance. SDN is an approach to application development that divides the network into a control plane and a forwarding plane [6]. The control logic is physically separated from the packet forwarding devices by this. The concept is to further extend this control strategy by introducing a centralized management entity called Controller.

2.2 Southbound and Northbound APIs (e.g., OpenFlow, REST APIs)

Programmable interfaces (APIs) are vital in software-defined networking (SDN) since they allow for communication between various architectural layers [7]. Two primary categories of APIs are used: Southbound APIs and Northbound APIs.

Types of Northbound API:

Current SDN controllers support a range of Northbound APIs, which can be broadly categorized into three groups:

- **RESTful APIs:** The most common, lightweight APIs based on HTTP methods, widely used for integration with orchestration platforms.
- **Specialized Ad-hoc APIs:** Custom-built APIs specific to certain SDN controllers, often optimized for vendor-specific functions.
- **Programming Language-based Interfaces:** Domain-specific languages such as Frenetic, Pyretic, and NetKAT that allow developers to define complex network policies programmatically.

Southbound API the SDN controller and forwarding devices, including switches and routers, communicate with each other over the Southbound API [8]. Its primary function is to communicate controller-to-device policies, flow entries, and forwarding rules.

Types of Southbound APIs

The SDN controller and the network forwarding devices (firewalls, switches, routers, and the like) are linked using southbound APIs. The controller can use them to manage devices, create forwarding rules, and monitor traffic. While OpenFlow has been the most dominant standard, several other protocols and approaches have been developed to extend functionality. The main types include:

- **OpenFlow Protocol:** The most widely adopted Southbound API, enabling standardized communication between controllers and switches using flow table entries. Provides fine-grained forwarding control but limited flexibility for new protocols.
- **NETCONF:** An IETF standard focused on device configuration and monitoring. Often used with YANG models for structured management of network devices, suitable for configuration rather than real-time flow control.
- **P4 Runtime:** A protocol-independent interface for programmable data planes, allowing controllers to define dynamic packet-processing rules using the P4 language. Offers greater flexibility for modern use cases like 5G, IoT, and edge computing.

The most widely adopted Southbound API is the OpenFlow protocol, which provides a standardized method for controllers to program and manage forwarding tables in switches. Other protocols are coming up including NETCONF and P4 Runtime which are potential alternatives/complements, with more programmability and flexibility.

2.3 Advantages of SDN Over Traditional Networking.

The use of access control lists (ACLs), less maintenance, and easier administration are just a few of the many benefits of SDN over more conventional approaches to network design. Since the entire network can be managed from a single location, it simplifies controls and management. Numerous benefits distinguish SDN from conventional networking. Following are a few examples:

- **SDN Centralized Management and Control:** One-way SDN makes it easy because the control and management of the networking devices is centralized.
- **On-Demand Quality of Service:** The system exploits the SDN centralized control intelligence to consolidate services provided by LTE and WAN with the aim of satisfying the increase computational needs of mobile users.
- **Traffic and Resource Categorization in Edge Network:** The ability to uniquely handle each tagged and clustered packet in the edge network is a result of a virtualized network architecture that integrates service function chaining, VNFs, and NFV. As a result, home networks can have their QoS tailored to their specific needs [9]. Videos and audio are both part of streaming media. Through its support of decoupled operation of hardware network resources, SDN makes it easier to put these resources into action.
- **Mobility Support for Internet of Vehicles (IOV):** Rapid vehicles can offload computations to smart distant clouds using software-defined networking, which are then passed to the roadside unit (RSU). The controller backs the RSU while it sets up the communication channel with the fog node, ensuring that the route has enough resources. As a result, fog nodes normally optimize their computation of IOV operations according to the controller's log of fog node capabilities.
- **Load Balancing Support in Future Networking:** The objective of this study is to reduce the duration of VNF state migration through the use of service function chaining and the enablement of SDN architecture among many NFV nodes [10]. Restricting the capabilities of OpenFlow-enabled devices in 5G core networks, making due with the restricted resources of NFV nodes, and achieving the necessary quality of service through infrastructure are the specific objectives. The goal is to minimize the end-to-end time for computational state movement.
- **Topology Discovery:** One important feature of software-defined networking is event-based topology discovery. When it comes to reducing unnecessary packets for topology discovery, TEDP is superior to OpenFlow and standard LLDP [11]. Topological graph mapping is utilized by the TEDP through the usage of probe packets. The SDN controller is notified of one forwarding device by these packets. Therefore, LLDP's discovery technique, which led to a rise in IP network traffic, is inferior to SDN's.
- **Fault Localization:** Centralized administration and reconfiguration aid in the localization of defects in SDN. Based on projections of service unavailability, it tackles faults proactively.

2.4 Challenges in SDN Deployment

There are a number of obstacles to widespread use of SDN, notwithstanding its many advantages. Performance, scalability, security, and interoperability are some of the main difficulties, as seen in Fig. 2:

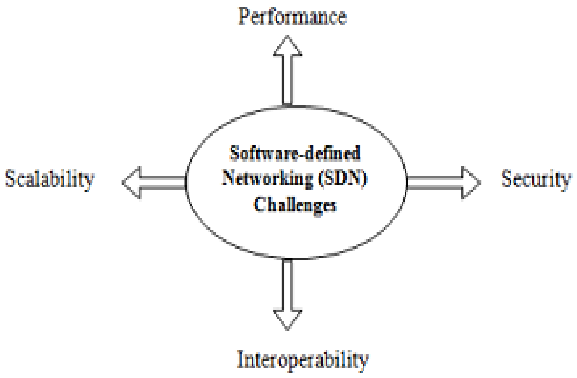

Fig 2: Challenges in SDN

2.4.1 *Performance*

Managing high-performance and secure packet transmission flows is a major challenge in software-defined networking deployment. Performance and programmability/flexibility are two key considerations [12]. Two metrics used to measure the performance of SDN, a flow-based technique, are the maximum number of flows that the controller can process per second and the setup time for a flow.

2.4.2 *Scalability*

Scalability in software-defined networking mostly refers to the controller's capacity to handle increasing network demands. Here, two enormous problems emerge: inter-controller communication (the east-west interaction between several controllers) and throughput, which represents the transmission of network information between nodes and a controller.

2.4.3 *Security*

Sharing network traffic across multiple users and devices is just the beginning of what software-defined networking (SDN) has to offer. Security must be prioritized for wider deployment due to the increased attack surface [13]. To address this, a working group on security has been established within the Open Networking Foundation (ONF) [14]. While SDN offers flexibility and programmability, it lacks standardised mechanisms for handling topology awareness, delay, packet loss, loop detection, and error resolution.

2.4.4 *Interoperability*

Interoperability is essential for a smooth transition from traditional networks to SDN. While deploying entirely new services based on SDN would be straightforward in theory, it requires all network devices to be SDN-enabled. In practice, large existing networks support critical infrastructure and cannot be completely replaced, making a full swap impractical.

2.5 Integration of Network Virtualization, Traffic Management, and Resource Allocation

Modern SDNs are able to support operations that are flexible, efficient, and scalable because of the combination of virtualization of networks, traffic control, and resource allocation. Network virtualization, through technologies such as VNFs and NFV, decouples network services from physical hardware, allowing dynamic provisioning and multi-tenant support [15]. Traffic management leverages the centralized intelligence of SDN controllers to optimize routing, balance loads, and enforce QoS, ensuring that network performance meets the varying demands of applications. Improved utilisation and reduced bottlenecks are the results of resource allocation strategies, which dynamically assign compute, storage, and bandwidth resources according to application requirements and network conditions [16]. Network efficiency, scalability, and dependability are all improved by combining virtualized resources, intelligent traffic handling, and adaptive allocation. This is especially true in complex contexts like 5G networks, the IoT, and cloud computing.

3. NETWORK VIRTUALISATION IN SDN

Virtualizing a network involves isolating and abstracting the underlying physical network before splitting it into smaller virtual networks. A considerable amount of research on cloud computing platforms, virtualized service functions, and the security issues surrounding them. Nevertheless, networks may also be sliced using several networking techniques. As an example, physical (photonic) layer slices are formed by WDM, link layer slices by virtual local area networks (VLANS), and forwarding table slices by multiple protocol label switching (MPLS) [17]. Network virtualization, in its turn, is aimed at introducing slices to the entire network, including all protocol layers. The resources of each slice of the virtual network are slice-specific and consist of a view of network topology, connection bandwidths, and resources of CPU and forwarding table of the switches.

3.1 Virtual Network Functions (VNF) and Network Function Virtualization (NFV)

The European Telecommunications Standards Institute (ETSI) defined both the architecture and the requirements for VNFs, as well as NFV. The three main components of the NFV platform are VNF, NFVI, and NFV MANO, which stand for Network Function Virtualization Management and Orchestration. Conventional network approaches are inadequate to manage the exponential expansion of digital devices, including smartphones and IoT sensors, which use a wide variety of applications and rely on extremely fast transmission technology [18]. This calls for investigating potential applications outside of VMs.

E-NFV, a key component of Cisco DNA, is one of the NFV-based methodologies proposed. With the help of E-NFV, network security and complexity challenges can be better managed by IT departments in network organizations. As a whole, NFV eliminates the need for specialized hardware like firewalls, gateways, and transcoders, allowing for rapid deployment of new network capabilities and elastic scale [19]. VNFaaS, virtualization of mobile base stations, and virtualization of CDNs are a few examples of NFV use cases identified by ETSI. These examples all contribute to the development of more streamlined, adaptable, and programmable networks that can accommodate new technologies.

3.2 SDN-NFV Integration

The integration of the two technologies is a complex endeavor due to the fact that the data and control planes must be segregated in SDN and the network functions and physical infrastructure must be decoupled in NFV. SDNV is a proposed solution that provides a comprehensive framework for demonstrating the correlation and integrating SDN with NFV. The first architecture allows for VNFs to communicate with the controller (NFV-C), whereas the second allows for VNFs to communicate with the switch (NFV-AC). The absence of a quantitative analytical model makes the selection of architecture all the more crucial. According to the SDN-NFV software switch performance evaluation, SR-IOV and DPDK are two examples of high-speed frameworks that can significantly accelerate packet forwarding [20]. Improved understanding of design trade-offs and identification of potential performance bottlenecks in SDN-NFV deployments are two outcomes of this study. The general trends in SDN-NFV integration include research on integration processes and performance and research on the aspect of operational convenience where practical and technical benefits of integrating these two technologies are put in the limelight.

3.3 Virtual Data Centers (VDC) and Resource Allocation Techniques

A Virtual Data Centre (VDC) refers to a collection of cloud-based infrastructural resources including compute, memory, storage and bandwidth that is tailored to satisfy the enterprise business requirements. According to the IaaS model, VDC allows organizations to establish their own IT infrastructure of any level of complexity and virtual structures that mimic the functionality of physical equipment [21]. A VDC is sold as a managed, on-demand service, which offers scaling and flexibility in computing to an enterprise in a shared cloud model, which is a virtualized equivalent of a conventional data center. Its main strength is in the dynamically allocated resources which enables businesses to maximize their use, minimize expenses and attain the true cloud computing at enterprise level.

4. TRAFFIC MANAGEMENT IN SDN

Network traffic management plays a vital role in ensuring that quality assurance of data transmission reliability and safety are done optimally by reducing bandwidth wastage, decreasing congestions, and high QoS. Load balancing, traffic shaping, coding and segmentation are effective means that ease user experience, resource optimization and low operation costs. The QoS management enables the allocation of priority to traffic that is of importance and ensures that there is enough bandwidth, low latency and reliability. The SDN control centrality and programmability emphasize the benefit of traffic control and unveil an optimal platform to implement advanced methods in traffic control. Having a global perspective on the network, SDN controllers are able to be more efficient in the analysis of link status, traffic patterns, and routing decision-making than traditional distributed systems. The centralized approach facilitates optimized performance, enhanced resource utilization and service delivery of certain Service Level Agreements (SLAs).

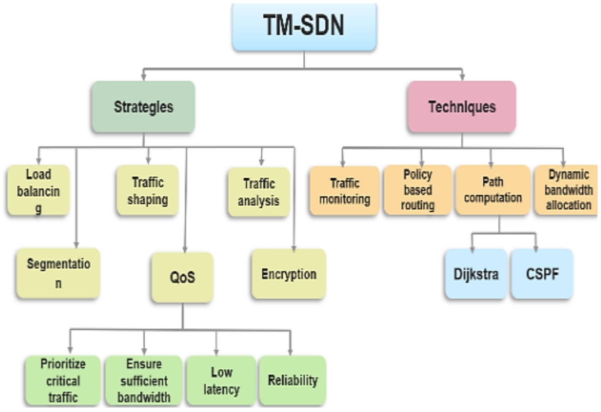

Fig 3: TM-SDN

Fig. 3 introduces a summary of Traffic Management in SDN (TM-SDN), and it is important to note that there are two dimensions: strategies and techniques. It has strategies such as load balancing, traffic shaping, traffic analysis, segmentation, QoS and encryption, and QoS also provides prioritization of critical traffic, adequate bandwidth, low latency, and reliability. Techniques focus on traffic monitoring, policy-based routing, path computation using algorithms such as Dijkstra and CSPF, and dynamic bandwidth allocation.

4.1 Traffic Engineering Approaches (Load Balancing, Congestion Control)

Data centers and cloud computing rely on traffic engineering to optimize resource utilization and ensure QOS while handling enormous data volumes. For cellular core networks, there are QueuePusher, QNox, Cloud-MAC, and ProCel; for WLAN VPN virtualization, Plug-n-Serve, ALTO, OpenQoS, Pronto, QoS for SDN in future networks, and FlowQoS are among the proposed frameworks. These mechanisms collectively aim to improve efficiency, scalability, and service quality across diverse networking environments.

4.1.1 Load Balancing

High availability, scalability, and performance are guaranteed by load balancing (LB), an essential component of modern computer networks. In order to avoid bottlenecks caused by a rise in data and access traffic, server processing capabilities should boost in tandem. Hardware updates or replacements, though, can be time-consuming, costly, and disruptive. In this context, LB technology comes into play, distributing a high amount of concurrent traffic across numerous computing machines, which improves server processing capacity and decreases response time to user requests. Websites, File Transfer Protocol (FTP) servers, and business critical application servers are the most common users of this technology.

4.1.2 Congestion Control

In IoT, the massive interconnection of devices and sensors often leads to congestion when traffic demand exceeds transmission capacity, particularly in wireless networks. Congestion may occur at the link level (buffer overflow due to higher packet arrival rates than service rates) or at the node level (multiple sensor nodes contending for the same channel). Similar issues exist in SDN-based networks, where congestion can appear at the controller (excessive flow requests), the switch flow table (overflow of flow rules), or the controller–switch communication link (bandwidth constraints). Addressing these challenges requires congestion-aware routing and load-balancing strategies that enhance packet delivery ratios while maintaining efficient resource utilization in both IoT and SDN environments.

4.2 QoS-Aware Routing Mechanisms

QoS-sensitive routing protocols are mechanisms that are used to choose paths in the network rather than paths that are optimal in terms of bandwidth or path length, but instead paths that meet desired QoS criteria, including latency, jitter, bandwidth, and packet delivery ratio. Unlike the traditional ways of routing where the minimal route is usually used, QoS-aware routing considers other performance parameters to attain the performance requirements that the route taken meets [22]. Such an approach is particularly necessary in the fields of 6G and IoT where different applications, including the real-time health status of a patient up to the self-driving car, require highly stable and low-latency networks. QoS sensitive routing in the SDN-based architecture can be dynamically run through centralized controllers that observe the network state and deploy flow rules depending on that state. These mechanisms enhance the utilization of resources by allocating the bandwidth intelligently, prioritizing traffic that is delay-sensitive, and redistributing traffic when there is a congestion or failure [23]. QoS policies when applied into routing decisions give a trade-off between performance, reliability as well as efficiency and in the process enable heterogeneous services to co-exist in the same network infrastructure.

4.3 Role of Machine Learning and AI in SDN Traffic Management

ML and AI are a significant aspect of improving traffic management in SDN as they allow traffic classification and prediction, as well as dynamic decision-making. SDN controllers have the benefit of accessing inherent flow data in OpenFlow switches, where forwarding rules (flow entries) are a match to packets at varying granularities, providing flexibility in the collection of data. The SVMs, NN and DT are supervised learning methods that have been popular in traffic classification but they depend on well labeled training data, which can be difficult to find out because of the dynamic nature of the network applications. SDN can maximize traffic inspection and resource allocation by configuring flow granularities and examining a limited number of packets at the controller and deploying the flow rules. ML-based traffic management may be implemented as centralized (non-distributed) or distributed mode whereby the nodes collaborate towards a similar objective. ML-driven strategies offer a more efficient way to handle traffic, offer adaptive strategies, proactive strategies, and are more efficient due to making traffic adjustment decisions in response to the current state of the network, as opposed to conventional approaches, which have a rigid timetable that is not responsive to network state.

5. RESOURCE ALLOCATION IN SDN

SDN can be used to optimize bandwidth, processing, and storage by using the centralized controller to manage the resources dynamically and efficiently. SDN provides fairness and QoS and allows adapting to the changes in the traffic by means of such techniques as flow scheduling, dynamic bandwidth assignment, and priority queuing. Although mobility and heterogeneous demand is a challenge, SDN can be effective in the next-generation network because of enhanced optimization and machine learning strategies.

5.1 Centralized vs. Distributed Resource Allocation

The centralized computing systems are centered in the central computing server or server cluster that is normally remote data center where all data processing processes are carried out. These architectures would have the capacity to generate high scale data and provide robust computing capabilities [24]. However, their reliance on remote infrastructure causes additional latency, and this can be a significant issue with applications of IoT that are time-sensitive and need real-time or near-real-time processing. This is one of the weaknesses that make a centralized solution not as adjusted to new 6G IoT environments where ultra-low latency and responsiveness are the key issues.

Alternatively, the data processing functions are distributed across various nodes that may be edge devices or intermediate fog nodes that may be placed even closer to the sources of data. This decentralization, in the edge nodal cloud paradigm, reduces the latency by processing the data at the place of generation in order to make the data more responsive to real time applications [25]. Also, it is useful in reducing the congestion generated by the network by reducing the necessity to transfer all the data to a remote data center. Consequently, distributed resources allocation provides features of scalability, efficiency, and flexibility necessary to meet the heterogeneity and dynamic demands of the next-generation IoT networks.

5.2 Energy Efficiency in SDN-based Network

Energy efficiency is an important issue in the field of IoT because the resources of devices are limited, and sensing, transmission, and reception are quite power-intensive. Aggregation of data is one of the techniques used to decrease transmissions, although there are problems with the heterogeneity of devices, dynamic topology, and the variety of QoS requirements [26]. SDN-based networks, in this regard, are a potential remedy, as they can be used to centrally monitor residual energy, dynamically reroute, and perform load balancing to give preference to energy efficient paths [27]. Nevertheless, the fact that the topology can be changed often, and routes can also be updated, might add more overhead to the system, and it is thus necessary to develop adaptive mechanisms to balance the energy consumption with the QoS needs.

5.3 Resource Allocation in 5G/6G and Edge Computing Environments

Integration Distributing processing power in Internet of Things (IoT) networks, which are expected to handle massive amounts of data is the goal of edge-fog computing. It becomes even stronger with the entry of 6G, which promises to provide unparalleled network capabilities, such as high-speed data delivery and a very low latency. Edge computing is a process of operating data at the network edge, that is, it is located near the data source, making it faster and saving bandwidth. Fog computing, on the other hand, moves cloud processing closer to the devices, so data can be processed locally or at adjacent nodes. By distributing data management tasks in this way, latency is reduced even further. Still, worries about managing resources have prevented these connected devices from reaching their full potential. For 6G IoT-centric edge fog computing to run well, resources need to be distributed wisely. The task at hand is to oversee the administration of both physical and network resources. Additionally, resource management needs to be flexible enough to accommodate the ever-changing IoT environment, which includes things like network conditions and device capabilities.

6. LITERATURE OF REVIEW

This review of SDN, covering virtualization, traffic, and resource management, highlights key trends, findings, and technologies to inform future research and practice.

Papavassiliou (2020) special issue presents notable contributions from various parts of the ecosystem mentioned earlier. Topics covered include architectures and implementations of SDN and NFV, as well as approaches to SDN-NFV integration and orchestration. The articles also address optimization, network management, and security-related issues. The following stands out: nine high-quality articles one review and eight original research pieces—that tackled all of the issues listed above and more have been accepted after a thorough review process. The shift from black boxes to white boxes, and the subsequent facilitation of 5G network topologies, have been made possible by the contributions of SDN and NFV [28].

Yi et al. (2020) framework for efficient and flexible resource allocation is designed to address the VDC mapping problem, which involves a logically centralized and physically distributed approach. By using technology like SDN and NFV, the architecture separates the management of server resources from those of network resources. Achieving high resource utilization can be achieved by a more flexible and targeted management of the entire resource allocation process. The label propagation algorithm, which groups virtual nodes in a VDC request into clusters based on the communication frequency between any two of them, is used to implement a location-aware VDC partitioning procedure before VDC mapping. This algorithm makes use of VDC requests as the mapping out of various topologies [29].

Zarca et al. (2019) demonstrates and tests a new security architecture for SDN/NFV-enabled Internet of Things (IoT) networks that operates the virtual security of Authentication, Authorization, Accounting (AAA) and Channel Protection. It incorporates cyber-situational awareness and includes a framework based on policies. Continuous and dynamic performance of these management functions is possible. As a VNF installed dynamically at the edge, the virtual AAA handles access control for IoT devices to the network and enables scalable device bootstrapping. It consists of network authenticators. In addition, the system enables the application of virtual channel-protection proxies as VNFs and the dynamic distribution of crypto-keys for IoT M2M communications; the ultimate objective is to create secure tunnels between IoT devices and services by utilizing contextual decisions learnt by the cognitive framework [30].

Rego et al. (2018) Integrating SDN with the IoT in a smart city setting is the basis of the proposed new control system. This control system adjusts the routing of everyday and emergency urban traffic on the fly whenever an emergency happens to reduce the time, it would require, to get the emergency resources to the scene of an accident. The design is based on a program and a set of IoT networks comprising of traffic lights and cameras. So that emergency response units may travel more easily, the algorithm regulates resource requests and route modifications. A Smart City model running on an SDN Mininet is then used to evaluate the idea. In addition, the method may be expanded to accommodate more Internet of Things (IoT) nodes since it accounts for their energy consumption, which grows proportionally as the number of nodes increases [31].

Singh and Jha (2017) delivers an exhaustive synopsis of SDN's advancements relative to conventional networks. This research looks at the history of SDN, its architecture and related technologies, including OpenFlow's protocols and standards. Furthermore, the fundamental idea of combining OpenFlow with NEs, like optical switches, is also addressed. carried out an architectural survey without bias. New technologies that can handle massive amounts of internet traffic and enable infrastructure and service providers to dynamically adjust their resources according to user demands are being introduced by software-defined heterogeneous network architecture [32].

Nguyen, Do and Kim (2016) provide an overview of SDN, NV, and NFV, then describe the current design of LTE mobile networks and the challenges they encounter. It accomplishes this by analyzing and categorizing numerous recent studies on SDN and virtualization in LTE mobile networks; by proposing a taxonomy based on the different levels of the carrier network; and by providing a thorough examination of the modifications to protocol operation and architecture that result from implementing SDN and virtualization in mobile networks. The name of the suggested design is SDVMN. also give a list of specific applications and use cases that can utilize SDVMN. Finally, revisited SDVMN open issues and the future research [33].

Table 1 provides a synopsis of the recent research on SDN, including methodology, main discoveries, obstacles, and future prospects of developing virtualization, traffic, and resource management.

Table 1. Literature Summary on Advances in SDN: Virtualization, Traffic, and Resource Management

Reference	Study on	Approaches	Findings/Insights	Challenges	Future Work
Papavassiliou (2020)	A 5G Network Architecture's Role for SDN and NFV	An analysis of the designs, integration methods, and orchestration strategies for SDN and NFV	A more adaptable rollout of 5G is made possible by SDN and NFV, which pave the way from black-box to white-box networking.	Optimization, network management, and security remain complex	Further research on integration and orchestration methods to improve network performance
Yi et al. (2020)	Efficient Virtual Data Center (VDC) mapping and resource allocation	SDN/NFV-based logically centralized but physically distributed resource allocation; label propagation algorithm for VDC clustering; location-aware partitioning	Decoupled server and network control allows flexible, high-utilization rescue allocation	Complexity in mapping and partitioning VDCs efficiently	Explore more dynamic and adaptive VDC mapping algorithms; improve scalability
Molina Zarca et al. (2019)	Security framework for IoT networks using SDN/NFV	Policy-based, cyber-situational awareness framework; virtual AAA and channel protection VNFs deployed at edge	Dynamic and scalable IoT device authentication and secure M2M communication achieved	Efficient management of dynamic crypto-key distribution; handling contextual decisions in real-time	Expand cognitive framework capabilities; support larger IoT deployments; integration with AI-driven security policies
Rego et al. (2018)	SDN-IoT integration for smart city emergency traffic control	SDN-based control system; IoT networks (traffic lights, cameras); dynamic route adjustment; Mininet emulation	Reduced emergency response times; scalable energy consumption with node count	Real-time computation and coordination among large IoT networks	Incorporate predictive analytics for traffic; optimize energy efficiency further; test in real urban scenarios
Singh & Jha (2017)	SDN evolution and architectures	Comprehensive survey; OpenFlow standards; software-defined heterogeneous network architectures	SDN enables dynamic resource management and supports high internet traffic; promotes network flexibility	Interfacing with diverse network elements; managing heterogeneous environments	Explore new SDN-enabled technologies; study integration with emerging network paradigms (e.g., optical switching)
Nguyen, Do & Kim (2016)	SDN/virtualization in LTE mobile networks	Overview of SDN, NFV; SDVMN architecture; hierarchical taxonomy; protocol and architecture analysis	SDN/virtualization provide flexible, efficient LTE network architecture; specific use cases identified	Protocol adaptation and operational challenges in LTE networks; scalability	Investigate SDN/NFV impact on future LTE/5G networks; propose optimized hierarchical architectures

7. CONCLUSION AND FUTURE WORK

SDN is another novel idea that overcomes the drawbacks of conventional networks by creating a physical separation between the data plane and the control plane, which allows for more centralized management, dynamic resource allocation, and programmability. When compiling this overview, the importance of SDN, NV, TES, and RMS in improving network performance and facilitating next-generation infrastructures was considered. SDN in combination with NFV and VDCs enhances scalability, multi-tenancy and QoS-sensitive and application-specific control. The implementation of SDN in the environment of IoT, smart city and 5G/6G implementations, which could be used to implement energy-aware, adaptive, and context-aware decision-making, were also discussed. SDN is associated with the problems of scalability, interoperability, security, and complexity of orchestration, which should be considered to implement it at large scales. Altogether, SDN is a key facilitator of flexible, automated and smart networking.

The next step in AI-based traffic prediction, real-time anomaly detection, and energy-efficient scheduling should be conducted to provide resilient, secure, and sustainable SDN ecosystems. Standardization, inter-domain coordination, and large-scale testbeds and other work are needed to speed up the adoption of SDN in heterogeneous and mission-critical networks.

8. REFERENCES

[1] O. Narmanlioglu and E. Zeydan, “Software-defined networking based network virtualization for mobile operators,” *Comput. Electr. Eng.*, vol. 57, pp. 134–146, Jan. 2017, doi: 10.1016/j.compeleceng.2016.09.011.

[2] S. Gupta, N. Agrawal, and S. Gupta, “A Review on Search Engine Optimization: Basics,” *Int. J. Hybrid Inf. Technol.*, vol. 9, no. 5, pp. 381–390, May 2016, doi: 10.14257/ijhit.2016.9.5.32.

[3] J. H. Cox *et al.*, “Advancing Software-Defined Networks: A Survey,” *IEEE Access*, vol. 5, pp. 25487–25526, 2017, doi: 10.1109/ACCESS.2017.2762291.

[4] N. R. and E. Sonia S.V., “A Survey and Comparison of SDN Based Traffic Management Techniques,” *Asian J. Appl. Sci. Technol.*, vol. 04, no. 03, pp. 10–18, 2020, doi: 10.38177/ajast.2020.4302.

[5] P. Vijay Tijare and D. Vasudevan, “The Northbound APIS of Software Defined Networks,” *Int. J. Eng. Sci. Res. Technol.*, vol. 5, no. 10, 2016, doi: 10.5281/zenodo.160891.

[6] A. Gelberger, N. Yemini, and R. Giladi, “Performance Analysis of Software-Defined Networking (SDN),” in *2013 IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, IEEE, Aug. 2013, pp. 389–393. doi: 10.1109/MASCOTS.2013.58.

[7] T. E. Ali, M. A. Abdala, and A. H. Morad, “SDN Implementation in Data Center Network,” *J. Commun.*, vol. 14, no. 3, pp. 223–228, 2019, doi: 10.12720/jcm.14.3.223-228.

[8] H. Kim and N. Feamster, “Improving network management with software defined networking,” *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 114–119, Feb. 2013, doi: 10.1109/MCOM.2013.6461195.

[9] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, “Software-defined networking (SDN): a survey,” *Secur. Commun. Networks*, vol. 9, no. 18, pp. 5803–5833, Dec. 2016, doi: 10.1002/sec.1737.

[10] A. Kushwaha, P. Pathak, and S. Gupta, “Review of optimize load balancing algorithms in cloud,” *Int. J. Distrib. Cloud Comput.*, vol. 4, no. 2, pp. 1–9, 2016.

[11] P. Manso, J. Moura, and C. Serrão, “SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks,” *Information*, vol. 10, no. 3, p. 106, Mar. 2019, doi: 10.3390/info10030106.

[12] M. J. . Alenazi, “Distributed SDN Deployment in Backbone Networks for Low-Delay and High-Reliability Applications,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, 2019, doi: 10.14569/IJACSA.2019.0101274.

[13] P. Pathak, A. Shrivastava, and S. Gupta, “A survey on various security issues in delay tolerant networks,” *J Adv Shell Program.*, vol. 2, no. 2, pp. 12–18, 2015.

[14] D. K. Hong, Y. Ma, S. Banerjee, and Z. M. Mao, “Incremental Deployment of SDN in Hybrid Enterprise and ISP Networks,” in *Proceedings of the Symposium on SDN Research*, New York, NY, USA: ACM, Mar. 2016, pp. 1–7. doi: 10.1145/2890955.2890959.

[15] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, and F. Ahmad, “Security issues in software defined networking (SDN): Risks, challenges and potential solutions,” *Int. J. Adv. Comput. Sci. Appl.*, 2019, doi: 10.14569/ijacsa.2019.0101042.

[16] A. Balasubramanian, “AI-Driven Optimization of Urban Mobility: Integrating Autonomous Vehicles with Real-Time Traffic and Infrastructure Analytics,” *Int. J. Innov. Res. Creat. Technol.*, vol. 5, no. 5, pp. 1–13, 2019.

[17] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, “Survey on network virtualization hypervisors for software defined networking,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 655–685, Oct. 2016, doi: 10.1109/COMST.2015.2489183.

[18] S. Pahune, “Sensor Data Collection and Performance Evaluation using A TK1 Board,” University of Memphis, 2019.

[19] A. Laghrissi and T. Taleb, “A Survey on the Placement of Virtual Resources and Virtual Network Functions,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1409–1434, 2019, doi: 10.1109/COMST.2018.2884835.

[20] M. S. Kumar and P. J, “Analysis of Network Function Virtualization and Software Defined Virtualization,” *JOIV Int. J. Informatics Vis.*, vol. 1, no. 4, pp. 122–126, Nov. 2017, doi: 10.30630/joiv.1.4.40.

[21] N. T. Patel and G. Khilari, “Deploying Virtual Data Center on Cloud,” *J. Emerg. Technol. Innov. Res. (JETIR*, vol. 4, no. 4, 2017.

[22] M. A. Razzaque, C. S. Hong, and S. Lee, “Data-Centric Multiobjective QoS-Aware Routing Protocol for Body Sensor Networks,” *Sensors*, vol. 11, no. 1, pp. 917–937, Jan. 2011, doi: 10.3390/s110100917.

[23] G. S. A. Talukder and A.-M. K. Pathan, “QoSIP: a QoS aware IP routing protocol for multimedia data,” in *2006*

8th International Conference Advanced Communication Technology, IEEE, 2006, pp. 6 pp. – 623. doi: 10.1109/ICACT.2006.206045.

[24] D. D. Rao, "Multimedia Based Intelligent Content Networking for Future Internet," in *2009 Third UKSim European Symposium on Computer Modeling and Simulation*, IEEE, 2009, pp. 55–59. doi: 10.1109/EMS.2009.108.

[25] S. K. Tayyaba and M. A. Shah, "Resource allocation in SDN based 5G cellular networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 2, pp. 514–538, Mar. 2019, doi: 10.1007/s12083-018-0651-3.

[26] A. Balasubramanian, "AI-Enabled Demand Response: A Framework for Smarter Energy Management," *Int. J. Core Eng. Manag.*, vol. 5, no. 6, pp. 96–110, 2018, doi: 10.5281/zenodo.14741022.

[27] O. Ahmed, F. Ren, A. Hawbani, and Y. Al-Sharabi, "Energy Optimized Congestion Control-Based Temperature Aware Routing Algorithm for Software Defined Wireless Body Area Networks," *IEEE Access*, vol. 8, pp. 41085–41099, 2020, doi: 10.1109/ACCESS.2020.2976819.

[28] S. Papavassiliou, "Software Defined Networking (SDN) and Network Function Virtualization (NFV)," *Futur. Internet*, vol. 12, no. 1, p. 7, Jan. 2020, doi: 10.3390/fi12010007.

[29] B. Yi, X. Wang, M. Huang, and Y. Zhao, "Novel resource allocation mechanism for SDN-based data center networks," *J. Netw. Comput. Appl.*, vol. 155, p. 102554, Apr. 2020, doi: 10.1016/j.jnca.2020.102554.

[30] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Enabling Virtual AAA Management in SDN-Based IoT Networks †," *Sensors*, vol. 19, no. 2, p. 295, Jan. 2019, doi: 10.3390/s19020295.

[31] A. Rego, L. Garcia, S. Sendra, and J. Lloret, "Software Defined Network-based control system for an efficient traffic management for emergency situations in smart cities," *Futur. Gener. Comput. Syst.*, vol. 88, pp. 243–253, Nov. 2018, doi: 10.1016/j.future.2018.05.054.

[32] S. Singh and R. K. Jha, "A Survey on Software Defined Networking: Architecture for Next Generation Network," *J. Netw. Syst. Manag.*, vol. 25, no. 2, pp. 321–374, Apr. 2017, doi: 10.1007/s10922-016-9393-9.

[33] V.-G. Nguyen, T.-X. Do, and Y. Kim, "SDN and Virtualization-Based LTE Mobile Network Architectures: A Comprehensive Survey," *Wirel. Pers. Commun.*, vol. 86, no. 3, pp. 1401–1438, Feb. 2016, doi: 10.1007/s11277-015-2997-7.

[34] Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., & Vattikonda, N. (2024). Leveraging Deep Learning Models for Intrusion Detection Systems for Secure Networks. Journal of Computer Science and Technology Studies, 6(2), 199-208.

[35] Narra, B., Buddula, D. V. K. R., Patchipulusu, H., Vattikonda, N., Gupta, A., & Polu, A. R. (2024). The Integration of Artificial Intelligence in Software Development: Trends, Tools, and Future Prospects. Available at SSRN 5596472.

[36] Achuthananda, R. P., Bhumeka, N., Dheeraj Varun Kumar, R. B., Hari Hara, S. P., & Navya, V. (2024). Evaluating Machine Learning Approaches for Personalized Movie Recommendations: A Comprehensive Analysis. J Contemp Edu Theo Artific Intel: JCETAI-115.

[37] Polu, A. R., Narra, B., Buddula, D. V. K. R., Hara, H., Patchipulusu, S., Vattikonda, N., & Gupta, A. K. Analyzing The Role of Analytics in Insurance Risk Management: A Systematic Review of Process Improvement and Business Agility.

[38] Gangineni, V. N., Tyagadurgam, M. S. V., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. (2024). AI-Powered Cybersecurity Risk Scoring for Financial Institutions Using Machine Learning Techniques (Approved by ICITET 2024). Journal of Artificial Intelligence & Cloud Computing.

[39] Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., & Chundru, S. K. (2024). A Machine Learning-Based Framework for Predicting and Improving Student Outcomes Using Big Educational Data (Approved by ICITET 2024). Available at SSRN 5515379.

[40] Gangineni, V. N., Pabbineedi, S., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Tyagadurgam, M. S. V. (2023). AI-Enabled Big Data Analytics for Climate Change Prediction and Environmental Monitoring. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 71-79.

[41] Pabbineedi, S., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., & Gangineni, V. N. (2023). Scalable Deep Learning Algorithms with Big Data for Predictive Maintenance in Industrial IoT. International Journal of AI, BigData, Computational and Management Studies, 4(1), 88-97.

[42] Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., & Penmetsa, M. (2023). Predictive models for early detection of chronic diseases in elderly populations: A machine learning perspective. Int J Comput Artif Intell, 4(1), 71-79.

[43] Polam, R. M. (2023). Predictive Machine Learning Strategies and Clinical Diagnosis for Prognosis in Healthcare: Insights from MIMIC-III Dataset. Available at SSRN 5495028.

[44] Bhumireddy, J. R. (2023). A Hybrid Approach for Melanoma Classification using Ensemble Machine Learning Techniques with Deep Transfer Learning Article in Computer Methods and Programs in Biomedicine Update. Available at SSRN 5667650.

[45] Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., & Tyagadurgam, M. S. V. (2022). Efficient Framework for Forecasting Auto Insurance Claims Utilizing Machine Learning Based Data-Driven Methodologies. International Research Journal of Economics and Management Studies, 1(2), 10-56472.

[46] Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. (2022).

Designing an Intelligent Cybersecurity Intrusion Identify Framework Using Advanced Machine Learning Models in Cloud Computing. Universal Library of Engineering Technology, (Issue).

[47] Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., & Bhumireddy, J. R. (2022). Leveraging Big Datasets for Machine Learning-Based Anomaly Detection in Cybersecurity Network Traffic. Available at SSRN 5538121.

[48] Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., & Penmetsa, M. (2022). Big Data-Driven Time Series Forecasting for Financial Market Prediction: Deep Learning Models. Journal of Artificial Intelligence and Big Data, 2(1), 153-164.

[49] Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., & Chundru, S. K. (2022). Leveraging Artificial Intelligence Algorithms for Risk Prediction in Life Insurance Service Industry. Available at SSRN 5459694.

[50] Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., & Nandiraju, S. K. K. (2022). Efficient Machine Learning Approaches for Intrusion Identification of DDoS Attacks in Cloud Networks. Available at SSRN 5515262.

[51] Polu, A. R., Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., Vattikonda, N., & Gupta, A. K. BLOCKCHAIN TECHNOLOGY AS A TOOL FOR CYBERSECURITY: STRENGTHS. WEAKNESSES, AND POTENTIAL APPLICATIONS.

[52] Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., & Kakani, A. B. (2022). Advance of AI-Based Predictive Models for Diagnosis of Alzheimer's Disease (AD) in Healthcare. Journal of Artificial Intelligence and Big Data, 2(1), 141–152.DOI: 10.31586/jaibd.2022.1340.