Software-Defined Networking (SDN) Architecture for 6G Networks: A Comprehensive Review

Akshat Mehta[1], Kavisha Yadav[2]

[1]Student, Department of Artificial Intelligence and Data Science, Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India.
[2]Assistant Professor, Department of Artificial Intelligence and Data Science, Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India

---

Abstract - *Sixth-generation (6G) systems are being designed around very high data rates, strict latency and reliability targets, massive connectivity, built-in artificial intelligence, sensing, and the joining of terrestrial and non-terrestrial infrastructure. Running such a network with device-centric, manually configured control would be impractical, which has renewed interest in Software-Defined Networking (SDN) as a way to make network control programmable. This literature review is a systematic analysis of research articles published on SDN architecture for 6G. We take a narrative approach with systematic-style reporting, built around five core studies and extended with peer-reviewed work and standards published mainly between 2020 and 2026, plus foundational SDN research. The review covers SDN fundamentals, the evolution from 5G to 6G, and centralized, hierarchical, distributed, federated, edge-assisted and AI-assisted control architectures. It then examines how SDN interacts with network function virtualization, slicing, edge computing, Open RAN, reconfigurable intelligent surfaces, terahertz communication, sensing and non-terrestrial networks, and it reviews network management, routing and interference management, security, industrial IoT and AI-enabled control. The studies agree on the benefits of logically centralized, programmable control, and they increasingly favour hierarchical, multi-domain structures, but most of the evidence comes from surveys, conceptual architectures and small simulations. Controller scalability, state consistency, control-plane security, interoperability and the lack of common benchmarks and large testbeds come up again and again. We close with research gaps and future directions, among them distributed and secure multi-controller design, trustworthy AI-native control, RIS-aware and non-terrestrial control, and reproducible evaluation. The review reports no experiments, and the architecture it presents is a conceptual synthesis of existing literature.*

Keywords - 6G networks, software-defined networking, Open RAN, network slicing, AI-native networking, network function virtualization, network security, network architecture.

1. INTRODUCTION

1.1 From 4G to 6G

Each mobile generation has brought a new radio technology and a change in network architecture. 4G consolidated an all-IP packet core. 5G moved to a service-based core that splits control-plane from user-plane functions, runs network functions as virtualized software and supports slicing [1], aimed at mobile broadband at very high rates, ultra-reliable low-latency links and massive machine-type connectivity (eMBB, URLLC and mMTC) [2]. 6G research widens the scope once more. The ITU-R IMT-2030 framework defines six usage scenarios [3]. Three of them grow out of the 5G classes: immersive, massive, and hyper-reliable low-latency communication (HRLLC). The other three are new: integrated sensing and communication, AI and communication, and ubiquitous connectivity. Vision and survey papers add terahertz operation, intelligent radio environments, pervasive edge intelligence and space-air-ground integration [4]–[10]. 6G is still at the pre-standardization stage: 3GPP describes Release 20 as a study-phase release, with normative work expected in Release 21 [11].

1.2 Complexity and the need for programmable control

The capabilities planned for 6G make the network much harder to operate. It will mix radio access technologies, spread functions over far-edge, edge and cloud sites, include programmable radio elements, and serve a very large number of devices whose services have very different requirements [5], [12], [13]. Conventional networks keep control logic inside each device, configure devices largely one by one, and tie new services to new equipment or long integration cycles. That limits how quickly resources can be moved and how consistently policy can be applied end to end.

1.3 SDN and its relationship to NFV, cloud-native networking and AI

The intelligence used for traffic processing in SDN technology is decoupled from the forwarding equipment and centralized logically using software in which the forwarding plane is programmed through open interfaces [14]-[16]. ITU-T and the IETF have standardized the

framework and its terminology [17], [18]. SDN complements Network Function Virtualization (NFV), which runs network functions as software on general-purpose servers instead of dedicated appliances [19], [20]. NFV provides the virtualized functions, and SDN provides programmable connectivity between them. Cloud-native networking takes NFV further with containers and orchestration [21], and AI/ML adds the analytics and decision-making that can steer SDN controllers [6], [22], [23].

SDN is a networking paradigm that predates 6G and is not one of its new technologies. Its value for 6G lies in giving software-controlled, abstracted control over the technologies that 6G does introduce. The question for this review is therefore practical: which SDN architectures have been proposed for a network of 6G scale, variety and built-in intelligence, and what does each give up?

1.4 Motivation, scope and objectives

A survey of SDN-based 5G and 6G networks exists [12], as do focused studies of control-plane redesign [24], security [25], programmable radio environments [26] and interference-aware routing [27]. What we could not find was a cross-cutting comparison of SDN control architectures for 6G, read against the wider 6G technology ecosystem. This review aims to provide one. Its scope is SDN architecture, control and orchestration for 6G; radio and physical-layer techniques appear only where they affect control, as with RIS or terahertz beam management. The objectives are to: (i) summarize SDN fundamentals relevant to 6G; (ii) trace the evolution from SDN-enabled 5G to SDN-enabled 6G; (iii) compare architectural approaches objectively; (iv) review the interaction of SDN with major 6G technologies and with network management, routing, security, industrial IoT and AI; and (v) identify unresolved challenges, research gaps and future directions.

1.5 Contributions

1. A structured taxonomy and comparison of SDN architectural approaches relevant to 6G, with their documented trade-offs (Sections 5 and 12).
2. A synthesis of how SDN interacts with eleven 6G technology areas, distinguishing demonstrated from conceptual interaction (Section 6).
3. A cross-study analysis of network management, routing and interference management, security and AI-enabled control (Sections 7 to 11).
4. A critical analysis of challenges and research gaps that separates what is established from what is unresolved (Sections 13, 14 and 17).
5. A conceptual picture of an SDN-based 6G architecture assembled from the literature (Fig. 2), which has not been validated as a system.

This is a review: we ran no experiments and present no performance results as our own. The rest of the paper runs as follows. Section 2 sets out how the review was conducted and introduces the core literature. Section 3 reviews SDN fundamentals and Section 4 the evolution from 5G to 6G. Section 5 compares SDN architectures and Section 6 examines the technology ecosystem. Sections 7 to 11 treat network management, routing and interference, security, industrial IoT and AI-enabled SDN. Section 12 focuses on comparative analysis, sections 13-15 highlight issues, gaps and future direction, section 16 focuses on the Indian perspective, section 17 focuses on synthesized findings and section 18 on the conclusion.

2. REVIEW METHODOLOGY

2.1 Type of review

This is an example of a narrative review which outlines its methodology systematically. This is not a systematic review. There was no protocol registered before carrying out this review; there was no database search conducted systematically; there was no screening for duplicates; there was no risk of bias assessment; and there was no PRISMA flow diagram because all of these were not carried out. This review will rely mostly on peer reviewed and expert technical literature published between 2020 and 2026.

2.2 Sources and search strategy

The core set included five articles [12], [24]-[27]. Further research papers were selected through topic-specific search techniques as well as references from the core set and reviews. The references included in the bibliography come from IEEE, ACM, Springer, Elsevier and MDPI journals, arXiv, ITU-R, ITU-T, ETSI, IETF, 3GPP, NIST, and from the government of India. Searches paired SDN with 5G/6G architecture, controller design, hierarchical and distributed control, NFV, slicing, edge and fog computing, cloud-native networking, Open RAN, RIS, terahertz, ISAC, non-terrestrial networks, massive IoT, routing and interference, security, AI/ML and digital twins. Bibliographic data was mapped to the Crossref DOI metadata database whenever it had an associated DOI.

2.3 Inclusion and exclusion criteria

We included studies on SDN-based or SDN-relevant control, orchestration or architecture in 5G, beyond-5G or 6G settings, and studies that lay the technical foundation for them (SDN fundamentals, NFV, slicing, edge computing, Open RAN, RIS, security and AI). Peer-reviewed articles, standards and official documents took priority, and arXiv papers came in when no peer-reviewed source was available or a paper was especially relevant. We excluded work with no meaningful control or architecture link to SDN, purely physical-layer studies with no control implications, and sources whose bibliographic details we

could not verify. Comments about the important research papers have been made after going through their abstracts and reading parts of the articles; if it was not possible for us to verify some points, we have mentioned them in the table as "Not discussed" or "Not evaluated."

2.4 Classification and comparative analysis

The literature was classified based on six themes as follows: (i) basic understanding of SDN and controller architecture; (ii) needs and evolution to 6G; (iii) architectural approaches towards control placement; (iv) SDN interoperability with 6G technologies; (v) functional fields (control, routing, security, AI, industry usage), and (vi) open problems and gaps. The studies have also been categorized based on evidence maturity levels such as survey and position papers, conceptual architecture, simulations and emulations, prototypes and field trials, and operation implementation. These comparison criteria include aspects like architecture, scalability, latency, fault tolerance, security, applicability to AI and 6G. Broadly speaking, the process consisted of stages from the identification and relevance screening to classification, evidence maturity coding, comparative study and synthesis. This approach can suffer from three drawbacks: potential selection bias, rapid 6G developments, and dependence on abstracts to determine core papers' properties.

2.5 Core reference set

The five primary studies are presented in Table 1 below. Each study has something to do with a specific level/function, which will be discussed in section 12 below.

TABLE 1 CORE REFERENCE SET: SCOPE, SDN ROLE AND LIMITATIONS (AS STATED IN OR EVIDENT FROM THE SOURCES)

Ref.	Year	Type	Focus	SDN role	Limitation / gap
[12]	2022	Survey	SDN-based 5G/6G: architecture, resource, mobility and interference management; open issues	Organizes SDN-based system architectures and key issues	No new evaluated architecture; RIS, Open RAN and AI-native control not its focus (per abstract)
[24]	2023	Architecture proposal, simulation	5G control-plane limits; control-plane redesign for 6G	Moves end-user signalling out of the control plane, treating it as a user service	Process-algebra simulation versus 5G; RAN, RIS, edge and NTN not the focus
[25]	2024	Review-style	6G security through SDN and NFV	Centralized control and virtualized functions as security basis	Quantitative assessment not mentioned in the abstract; Scalability is not the key concern
[26]	2026	Architecture, optimization, simulation	SDN-oriented 6G IIoT architecture; RIS placement and selection	RIS abstracted as OpenFlow-style switches; four-plane architecture	Simulations Only; Single RIS Prototype; Lighter Protocols and Hardware Needed for Testing
[27]	2023	Survey	Using routing to mitigate interference in SDN-enabled beyond-5G networks	Centralized view used for interference-aware routing	Routing/interference focus; end-to-end architecture and security not its scope

3. FUNDAMENTALS OF SDN

3.1 SDN concept

SDN separates two jobs: deciding how traffic should be handled (control) and moving it (data). The deciding moves into software that sees the whole network. SDN grew from earlier programmable-network research and took off with OpenFlow, which opened the flow tables of commodity switches to external control [14]. Surveys describe the paradigm through four characteristics: decoupled planes, flow-based forwarding abstractions, a logically centralized network operating system, and applications that program the network through it [15], [16]. ITU-T Y.3300 and IETF RFC 7426 provide standardized frameworks and terminology [17], [18].

3.2 Traditional networking versus SDN

In traditional networks, both control and switching capabilities exist in all nodes, individual device configurations are carried out, and distributed algorithms are used to get the behavior of the whole network. SDN distinguishes itself on decision-making places and representations as shown in Table 2. The management capabilities of SDN include having an overall view, consistency, and automation; however, the downside of SDN is that the controller is critical now [28], [29].

TABLE 2 TRADITIONAL NETWORKING COMPARED WITH SDN (CHARACTERISTICS REPORTED IN THE LITERATURE)

Aspect	Traditional networking	SDN
Control logic	Distributed in each device; vendor-specific	Logically centralized software; open interfaces [15]
Configuration	Per-device, often manual or scripted	Programmatic and network-wide [28]
Network view	Local; inferred from protocols	Global topology and state at the controller [15]
Innovation cycle	Tied to device and protocol releases	Software-based; applications can be added to the control layer [16]
Principal concerns	Complexity, slow change, inconsistent policy	Controller scalability, resilience, security and interoperability [29], [30]

3.3 SDN control plane

It is responsible for generating forwarding commands and delivering the output to the data plane. It comprises a controller that keeps track of the topology of the network and interfaces with the applications using abstractions. Controller implementations differ in architecture and intended scale; model-driven and distributed platforms such as OpenDaylight and ONOS emphasize modularity, replication and high availability [31], [32]. The known concerns for this layer are performance, scalability, reliability and security [15], [29].

3.4 SDN data plane

Devices in the data plane forward packets by following the rules the controller has installed. OpenFlow modelled these rules as entries in flow tables [14]; programmable-pipeline approaches such as P4 allow the packet-processing behaviour itself to be specified [33]. In mobile networks the notion of “data plane” extends to radio elements, as in SoftRAN and FlexRAN, which expose radio-access control to a (logically) centralized controller [34], [35], and, in 6G research, to RIS [26].

3.5 SDN application plane

Network applications (routing, traffic engineering, load balancing, access control, monitoring) run above the controller and consume its abstractions. IETF terminology keeps the application plane separate from both the control plane and the management plane [18]. Large operators have reported centralized traffic-engineering applications in their inter-data-center wide-area networks [36], [37]. These show what the application plane can do, but they run in a bounded domain owned by one operator, which is much simpler than a heterogeneous mobile network.

3.6 Northbound and southbound interfaces

Southbound interfaces connect controllers to devices (OpenFlow, NETCONF, P4Runtime and, in the RAN, the O-RAN E2 interface [14], [33], [38]); northbound interfaces expose network services to applications, typically as REST-style APIs; east-west interfaces connect peer controllers [15]. Several authors note that no northbound standard has been universally adopted, which makes applications hard to port [15], [29]. 6G makes this worse, since each of its many domains brings its own control interface.

3.7 SDN controllers

Controllers range from single instances to clusters spread over several sites. Distributed platforms copy network state across instances to scale out and survive failures [31], [32], and elastic designs move switches between controllers as load changes [39]. Heller et al. showed that the number of controllers and where they sit shape both latency and resilience [40].

3.8 Centralized versus distributed SDN control

It is not necessary for logically centralized systems to be physically centralized. Logically centralized controllers have full view of the network and are easier to analyze; however, they limit scalability and are prone to failure. Distributed and hierarchical control systems have higher scalability and robustness, but the downside is that they maintain consistency of state and coordination of the instances of the system [32], [40]–[42]. The effect of inconsistency of distributed state on application that use the inconsistent state was shown by Levin et al. [41].

3.9 SDN programmability and relevance to 6G

Programmability is the most crucial attribute of the SDN paradigm in relation to 6G technology. Programmable networks mean that such networks can be configured through software not hardware, automation is possible, and heterogenous networks can be abstracted through a common interface [15], [16]. In 6G technology, programmability should cover radio networks components and RAN services [26], [34], [35], [38], virtualized components [20] and multi-domain resources through orchestration [43].

4. EVOLUTION FROM 5G TO 6G

The milestones within SDN in relation to the 5G-6G period are shown in Figure 1 below, where three phases have been distinguished. SDN began as a way to program forwarding devices [14], [15] and was soon applied to the cellular core and RAN [34], [44]–[46]. During 5G it was paired with NFV and network slicing, letting one physical network carry many programmable services [43], [47]–[49]. The third phase is still mostly on paper: multi-domain, intent-driven and AI-assisted control over radio, edge, RIS and non-terrestrial resources [6], [12], [24], [26].

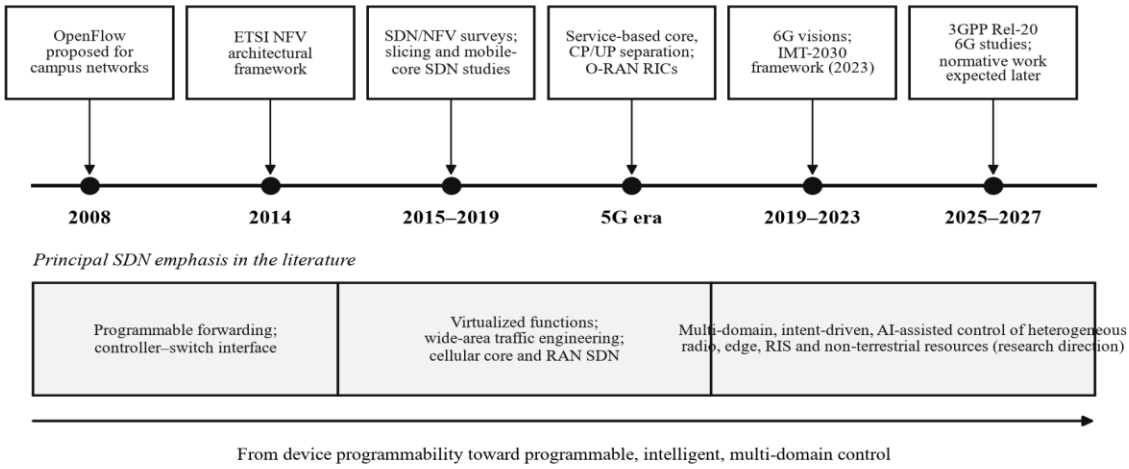


Fig. 1. How SDN has evolved from the 5G era toward 6G, compiled from the cited literature and standards [1], [3], [11], [14], [19]. The timeline is a schematic, and its last phase shows research directions, not deployed systems.

Table 3 compares 5G and 6G characteristics. We give numbers only where an authoritative source does, and the 6G figures are indicative ITU-R M.2160 study targets, not specified or delivered performance [3]. For SDN, the table implies four changes. Tighter latency targets leave less room for logic in a distant controller, and far higher device density makes reacting to every new flow too costly. Because the network spans RAN, RIS, edge and non-terrestrial segments, controllers must work across technologies and administrative boundaries. AI-native operation, finally, means building telemetry, model management and safety checks into the control plane [3], [6], [50].

TABLE 3 EVOLUTION OF NETWORK CHARACTERISTICS FROM 5G TO 6G AND IMPLICATIONS FOR SDN

Characteristic	5G	6G (research expectation)	Implication for SDN
Architecture	Service-based core; CP/UP separation; NFV and slicing [1]	AI-native, multi-domain, including non-terrestrial and programmable radio environment [3], [5], [6]	Hierarchical, multi-domain control and orchestration
Latency	1 ms user-plane target for URLLC [2]	Indicative 0.1–1 ms for study [3]	Fast loops need local control

Characteristic	5G	6G (research expectation)	Implication for SDN
Reliability	URLLC service class [2]	HRLLC usage scenario [3]	Resilient controller design; verified failure behaviour
Connectivity	Massive machine-type; 10^6 devices/km^2 [2]	Massive and ubiquitous connectivity; indicative 10^6–10^8 devices/km^2 [3]	Aggregate, proactive control; scalable state
Intelligence	AI mainly as add-on analytics [22], [23]	AI-native operation [6], [50], [51]	Intelligence layer integrated with control
Spectrum	Sub-6 GHz and millimetre-wave [12]	Exploration of sub-THz/THz bands [52], [53]	Beam and topology state in control decisions
Network automation	NFV MANO-based orchestration [19], [20]	Intent-driven, closed-loop automation [50], [54]	Intent interfaces; assurance loops
Sensing	Not a core network service	Integrated sensing and communication scenario [3], [55]	Sensing data as control input; open question
Edge integration	Multi-access edge computing [56]	Pervasive edge intelligence [5], [56]	Joint network–compute control
AI integration	Selective [23]	Pervasive, including in RAN and core [6], [51]	ML lifecycle management and safeguards
Security requirements	Slice isolation and service-based interface security [57]	Programmable, AI-driven, multi-tenant attack surface; trust and post-quantum considerations [25], [58], [59]	Zero-trust control plane; secure orchestration

5. SDN ARCHITECTURES FOR 6G

Work on mobile and future networks has organized SDN control in several ways, and the categories overlap in practice; a hierarchical design, for instance, is also a multi-controller design. For each approach we describe how it is built, its strengths and weaknesses, and its scalability, control latency, fault tolerance, security and fit with 6G. We do not rank them, since the right choice depends on the domain and the service. Fig. 2 combines these ideas into a generic SDN-based 6G architecture drawn from the literature.

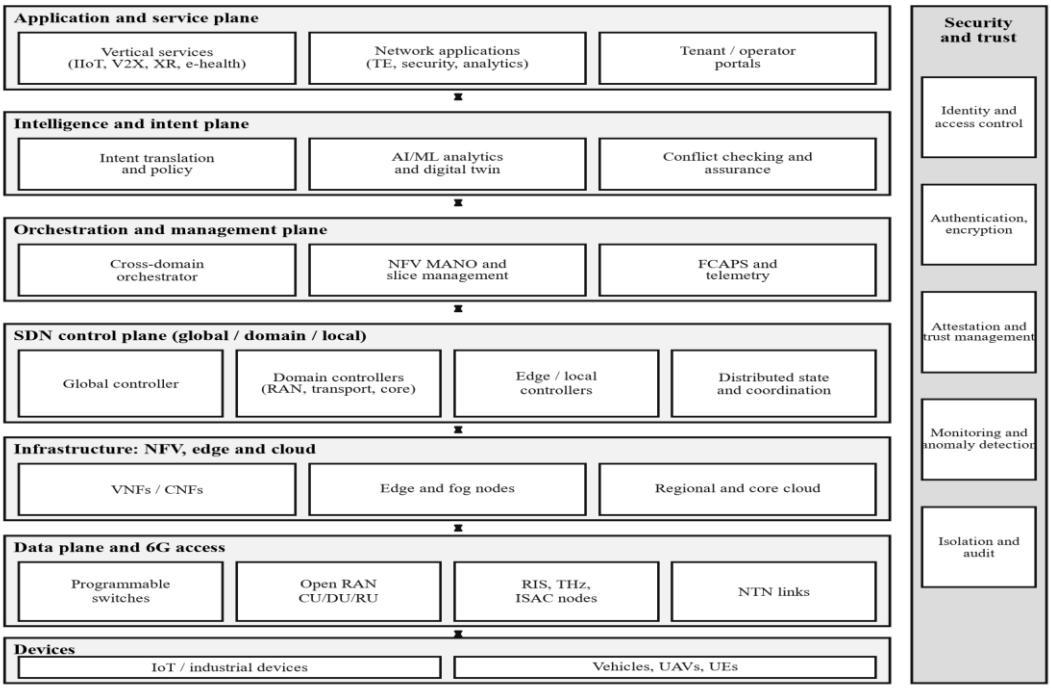


Fig. 2. A generic SDN-based 6G network architecture assembled from the surveyed work. It is conceptual and has not been validated experimentally. The layers draw on [12], [24], [26], [38], [43], [50], [58].

5.1 Centralized SDN

In the centralized model, one logical controller, possibly replicated for availability, holds the global view and programs every device [15]. Because it sees everything, policy is simple to reason about and optimization is straightforward. Operators have run centralized traffic engineering on their own WANs, as Microsoft's SWAN [36] and Google's B4 [37] show. However, scalability and reaction time of controllers is constrained by the size of the controller and round-trip time from the switch to the controller [29], [40]. The 5G/6G surveys therefore see centralization as suited to bounded domains and slow decisions, not to a whole heterogeneous, latency-critical 6G network [12], [24]. In our view, it is easiest to defend for policy and optimization and hardest for per-packet or per-frame control.

5.2 Hierarchical SDN

Hierarchical designs split control into tiers. In Kandoo, local controllers handle events within their scope and a root controller takes network-wide decisions [42]. Frequent local events never reach the root, which lightens its load, keeps fast loops near the data plane and improves scalability, although decisions that need the root remain slow [42]. The price is that tiers hide information from each other, which can make decisions sub-optimal, and each added tier brings more coordination and new failure modes. A failed tier can be contained only if degraded behaviour is defined in advance, and there are more components to secure. This suits 6G, whose control already runs on real-time, near-real-time and non-real-time timescales, as in O-RAN's controllers [38].

5.3 Distributed SDN

For distributed architectures, there exist several controllers operating in parallel, and each of them keeps its own version of the network state. ONOS and the elastic controller proposed by Dixit et al. represent such architectures [32,39]. Such architecture scales horizontally and provides high availability, but the state of the network must be consistent enough for proper application operation. The influence of inconsistent state on the performance of the system has been examined in detail by Levin et al. [41]. Proximity to devices makes the control path shorter [40], while replication makes the system resistant to failures. But high consistency conflicts with low latency; besides, security is at risk because of the possible attack channel via synchronization. Dependability of the control platform has always been a design problem.

5.4 Multi-controller SDN

In this case, the network is partitioned into domains, such that there is a controller for each domain, and the controllers have communication among each other using east-west interfaces. This is done to ensure that the controller is not overloaded and can be partitioned using organizational or technological boundaries, and that there is lesser damage in case of failure of a controller because then only the respective domain will fail unless other domains depend on it. The problem arises with coordination as optimization needs coordination among the controllers, inter-domain communication leads to increased latency, and boundaries lead to inefficient routing and bad handover decisions. This type of architecture scales well as the number of domains increases, and all the inter-controller connections need to be authenticated. All the survey papers related to SDN-based 5G/6G networks assume this scenario when separating RAN, Transport, Core, and Edge into different control domains [12], [49].

5.5 Federated SDN

The federation model goes even further with the idea that the controllers belong to different administrations and exchange information only by agreement on how they should do that. One of these models is DISCO, where the controllers coordinate their actions in the domains through the light-weight messaging interface [61]. The operators control the information privately but have a smaller view of the network, must negotiate the trust and do not exchange any information model between the domains. As for the controllers working independently, the isolated failures will not affect other parts of the system, but it is also harder to provide the end-to-end guarantees, and the trust can become the goal of the attacks.

5.6 Edge-assisted SDN

Edge SDN involves the placement of controllers, or parts of them, at edge/fog locations near the end-users and devices, in addition to computation offloading [56], [64], [65]. In this way, low latencies become possible, providing autonomy and joint network and computational control. The constraints arise from the edge itself, since there are few resources, different platforms and the need to synchronize with the upper layers. Replication in multiple locations makes possible fast decision-making, but the multiple locations have less physical security than the centralized one, thus expanding the attack surface. Since the 6G era is expected to involve intelligent edge, the solution seems appropriate even though the edge designs for SDN in 6G are mostly hypothetical [5], [56].

5.7 Cloud-native SDN

Cloud native SDN designs its control plane through containerized microservices that are scaled using an orchestrator using technologies like cluster management tools (Borg and Kubernetes) [21] and NFV [20]. The control software becomes elastic, quick to deploy and able to restart itself after a failure, though this depends on how state is managed. Its weak points are predictable performance for latency-critical control, awkward state

handling in stateless microservices, and the complexity of orchestration itself. Containers and the software supply chain also widen the attack surface [58]. The approach matches the cloud-native direction of the 5G core and O-RAN [1], [38], but we found no evidence on how such controllers behave under 6G latency targets.

5.8 AI-assisted SDN

In AI-assisted SDN, an analytics and decision layer reads telemetry and advises the controller or acts for it [22], [23]. ITU-T Y.3172 defines an ML framework for IMT-2020 networks, with pipelines and a sandbox [50]. The layer can predict, adapt to changing conditions and automate, but only as well as its data allows. Models drift, are hard to explain and can be manipulated by adversarial inputs [66], [67]. Where inference runs decides its latency, and training is usually off-line or central. A faulty or poisoned model can pass errors straight into control actions, so safeguards and fallback are essential. AI-native operation is a stated 6G goal [6], [51], but evidence at 6G scale so far comes only from simulations and component studies (Section 11).

5.9 Cross-domain SDN

Cross-domain SDN puts an orchestrator or root controller above the RAN, transport, core, edge and non-terrestrial controllers and coordinates them through abstractions (Fig. 3). In the slicing literature, orchestrating services end to end over several domains is singled out as a central problem [43], [47], [48]. Cross-domain control makes end-to-end service composition possible, but missing common information models and interfaces, and domains with conflicting goals, hold it back. It works on slow timescales, leaving fast loops to each domain, and couples the domains' failures and trust. It is essential for integrating space, air and ground segments [62], [63], but published designs are largely conceptual.

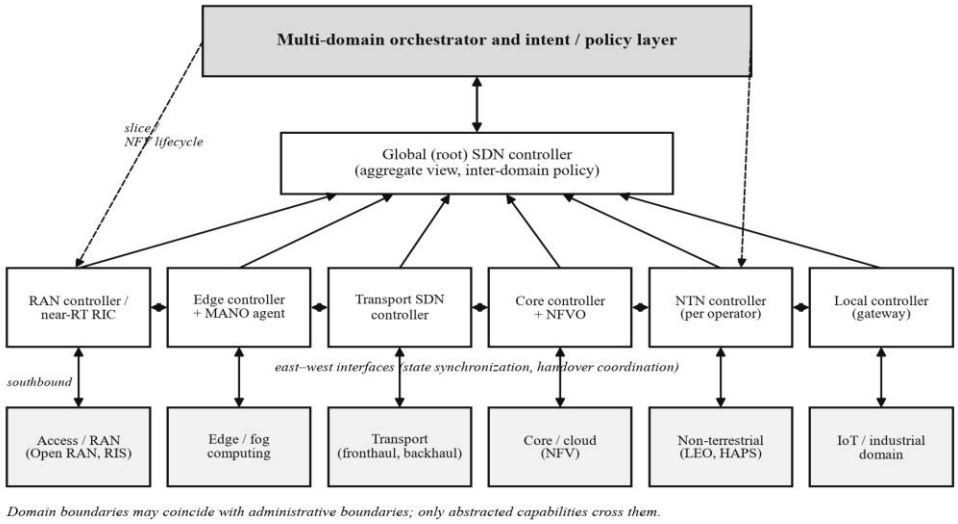


Fig. 3. SDN control and orchestration across 6G domains (conceptual, drawn from the cited work). Domain controllers talk to peers over east-west interfaces and pass aggregate state to a multi-domain orchestrator that manages the slice and NFV lifecycle [38], [43], [48], [61].

5.10 SDN for heterogeneous networks

One proposed use of SDN is to coordinate heterogeneous access technologies through a common control abstraction, letting a controller manage resources, mobility and interference across technologies [12]. Frameworks that apply SDN to cellular networks have been put forward as well [45]. Interoperability and standardization come up again and again as obstacles [12], [29]. In our view, the gain from unified control must be weighed against lost technology-specific optimization.

5.11 SDN-enabled RAN

SoftRAN proposed managing the base stations of an area as one logical unit. A central controller takes the radio-resource decisions that benefit from a global view, such as interference management and load balancing, while time-critical decisions stay distributed [34]. FlexRAN offered a programmable RAN platform with a real-time controller [35]. O-RAN generalizes the idea: its RAN Intelligent Controllers work at near-real-time and non-real-time timescales and connect through open interfaces such as E2, A1 and O1 [38], [49]. All three designs split RAN control between central and distributed parts, which bears directly on the hierarchy debate. How RAN controllers should coordinate with transport and core SDN controllers is still open [38].

5.12 SDN-enabled core networks

Surveys of mobile packet cores built on SDN and NFV return to the same themes: splitting the control and user planes, running core functions as virtual network functions, and flexible service chaining [46]. For instance, SoftCell had once done so on a grand scale in the cellular core [44]. The 5G core network architecture with services and CP/UP split [1], however, does some of that without using OpenFlow. For 6G, Yadav et al. would remove end-user signalling, such as registration and authentication, from the mobile control plane and carry it like user data [24], redrawing the boundary between the two planes. For the 6G core, then, deciding which functions sit in the control plane matters as much as deciding where controllers go.

Table 4 lists representative literature and the principal trade-off of each approach.

TABLE 4 SDN ARCHITECTURAL APPROACHES: REPRESENTATIVE LITERATURE AND PRINCIPAL TRADE-OFFS

Approach	Representative literature	Principal advantage	Principal limitation
Centralized	[15], [36], [37]	Global view; simple optimization	Scalability; single point of failure; control latency
Hierarchical	[38], [42]	Local loops; reduced root load	Information hiding; coordination across tiers
Distributed	[32], [39], [41]	Scale-out; availability	State consistency; synchronization overhead
Multi-controller	[12], [49]	Domain partitioning; bounded failure impact	Inter-domain coordination; sub-optimal global decisions
Federated	[61]	Administrative autonomy	Limited visibility; trust and policy negotiation
Edge-assisted	[56], [64], [65]	Low control latency; local autonomy	Constrained and numerous sites; wider attack surface
Cloud-native	[20], [21]	Elasticity; automated resilience	Latency predictability; state handling
AI-assisted	[6], [23], [50]	Prediction and automation	Explainability; robustness; data quality
Cross-domain	[43], [48], [63]	End-to-end service composition	No common information model; trust coupling
Heterogeneous-network SDN	[12], [45]	Unified abstraction across access types	Interoperability; loss of technology-specific optimization
SDN-enabled RAN	[34], [35], [38]	Radio-resource control with global information	Coordination with transport and core controllers
SDN-enabled core	[24], [44], [46]	CP/UP separation; flexible service chaining	Alignment with 3GPP interfaces; function allocation open

6. SDN AND THE 6G TECHNOLOGY ECOSYSTEM

We include only those 6G technologies whose interaction with SDN control is documented. How mature that interaction is varies widely: NFV, slicing and edge computing have extensive SDN literature, Open RAN and RIS have emerging SDN-style control concepts, and terahertz, ISAC and non-terrestrial networking have mainly indirect or conceptual links. See figure 4 for a quick sketch and table 5 for results.

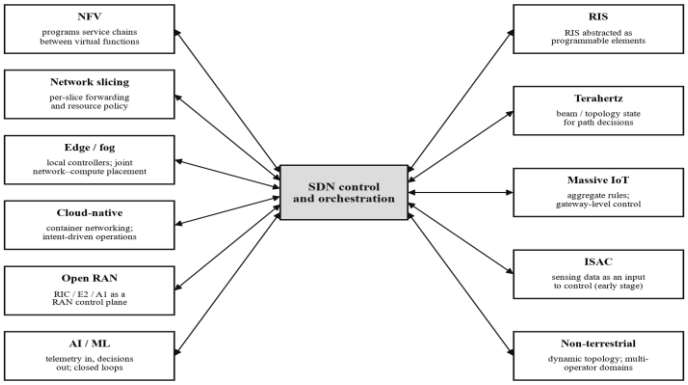


Fig. 4. Interaction between SDN control and orchestration and major 6G technologies, drawn from the cited work (conceptual). Annotations summarize the principal interaction reported or implied; interaction maturity varies and is summarized in Table 5.

6.1 Network function virtualization

NFV and SDN do different jobs that fit together. NFV runs virtualized functions on commodity infrastructure under MANO, and SDN connects them programmably, most visibly in service function chaining [19], [20]. The NFV literature identifies performance, portability and orchestration challenges [20]. For 6G security, Jaadouni et al. argue that SDN and NFV together provide flexibility and scalability for deploying security functions [25].

6.2 Network slicing

Several surveys single out SDN and NFV as what makes slicing possible in 5G [43], [47], [48]. SDN programs per-slice connectivity and, through virtualization hypervisors, can partition network resources [68]; NFV provides slice-specific functions. Persistent challenges are isolation, end-to-end orchestration and dynamic resource sharing [43], [48], together with slice-related security threats [57]. Whether 5G slicing mechanisms scale to the more dynamic, multi-domain 6G setting is not established.

6.3 Edge and fog computing

Moving computation close to users cuts latency, but it also turns resource allocation into a joint communication-computation problem [56], [65]; fog computing brings cloud services out to the network edge, near IoT devices [64]. In SDN terms, the edge both consumes services and hosts local controllers and inference, which supports hierarchical control (Section 5). We found few detailed treatments of SDN-based network-compute co-optimization for 6G.

6.4 Cloud-native networking

Cloud-native operation builds on container orchestration lineages [21] and on the cloud-native design of the 5G core and O-RAN [1], [38]. For SDN, this turns controllers and network functions into elastic software workloads. Automation gets easier, while latency becomes less predictable and the software supply chain becomes a security risk [58].

6.5 Open RAN

Open RAN breaks the RAN into separate, interoperable components and adds RICs that run at near-real-time and non-real-time scales and reach the RAN over open interfaces. Software applications can then program the RAN much as SDN applications program a network [38], [49]. The relationship between RICs and transport/core SDN controllers, and the security of the open interfaces, are identified as open research questions [38].

6.6 Artificial intelligence and machine learning

Section 11 covers AI/ML in depth. In ecosystem terms, SDN supplies the global telemetry and programmable actuation that AI-driven control requires, while AI supplies prediction and automation [22], [23], [50].

6.7 Reconfigurable intelligent surfaces

With the help of control over signal reflections, RIS will enable the network to customize its own wireless environment [69] - [71]. They are relevant to SDN due to coordination requirements in the implementation and configuration of RIS in the context of network topology and channel states. Based on core studies on RIS, the SDN model is described by Chiti et al. by wrapping of RIS devices into OpenFlow switches along with the use of beam mapping with virtual ports and set-covering and minimum spanning tree models for placement and selection [26]. This is the proof of the validity of the abstraction but we could not find any hardware results.

6.8 Terahertz communications

Therahertz waves have high bandwidth; however, they suffer from high spread loss, blockage loss, and narrow beam width [52], [53]. Little work has been done towards incorporating SDN into the terahertz-based communication network. This is an indirect relationship, as the controller can take decisions based on the network topology and status of the beam. This relationship is discussed in the SDN-5G/6G survey paper where mm-waves are considered [12].

6.9 Massive IoT

There are also some surveys that address the application of SDN in relation to the IoT, and have suggested the use of SDN to control the different types of devices and gateways as well as the implementation of the policies [72], [73]. It will not be feasible to control every single device at 6G density; hence, it makes sense to control the devices at the gateway/aggregate level.

6.10 Integrated sensing and communication

ISAC lets the same infrastructure both sense its surroundings and communicate [55], [74]. The ISAC surveys focus on signal processing, waveforms and resource sharing, and say little about the control plane, such as how sensing data could reach an SDN controller as network state. The SDN literature has not taken this up either, so the interaction remains conceptual.

6.11 Non-terrestrial networks

Satellites, high-altitude platforms and UAVs bring wide coverage, but their topology changes constantly [62], [75]. SDN-based designs for integrated space-terrestrial networks have been proposed to give a unified control view and to cope with dynamic topologies [63]. The open challenges are control latency over long links, mobility and coordination among operators [62], [63].

TABLE 5 INTERACTION BETWEEN SDN AND 6G TECHNOLOGIES: REPORTED ROLE AND EVIDENCE MATURITY

Technology	Reported or implied SDN interaction	Evidence in reviewed literature	Principal open issue
NFV	Service function chaining; connectivity for VNFs [19], [20]	Extensive; surveys and standards	Performance predictability; orchestration
Network slicing	Per-slice connectivity and resource partitioning [43], [47], [68]	Extensive; surveys, prototypes	Isolation; cross-domain orchestration; security [57]
Edge / fog	Local controllers; network–compute co-allocation [56], [64]	Substantial; conceptual for 6G	SDN-specific co-optimization for 6G
Cloud-native	Controllers as elastic workloads [21]	Indirect for SDN	Latency predictability
Open RAN	RIC as RAN control plane; open interfaces [38], [49]	Substantial survey and prototype literature	RIC–SDN coordination; interface security
AI/ML	Telemetry-driven prediction and control [23], [50]	Substantial for components; limited at 6G scale	Explainability; robustness
RIS	RIS as OpenFlow-style elements [26]	Emerging; simulation	Hardware validation; lighter protocols
Terahertz	Beam/topology state for path decisions (implied) [12], [52]	Sparse for SDN	Direct SDN studies lacking
Massive IoT	Gateway/aggregate control [72], [73]	Substantial for IoT; limited at 6G scale	Scalable per-device policy
ISAC	Sensing as control input (conceptual) [55], [74]	Not discussed in SDN literature reviewed	Control-plane integration of sensing
Non-terrestrial	Unified control of space–terrestrial networks [62], [63]	Conceptual	Dynamic topology; multi-operator control

7. SDN FOR 6G NETWORK MANAGEMENT

Few 6G-specific studies address how SDN would support network management. Most of the evidence below comes from SDN in data-center, wide-area, 5G and IoT settings, and how well it carries over to 6G is a matter of interpretation.

7.1 Resource allocation

SDN surveys present resource allocation as a main use of the global view [15], [28], and it is a principal topic of the SDN-based 5G/6G survey by Long et al. [12]. SoftRAN kept local the RAN decisions that had to be local and centralized those that gain from global information [34]. This pattern recurs: decisions are split by timescale and by how much information they need. The studies disagree on where the split should fall, which in our view depends on the latency budget and the cost of collecting global state.

7.2 Traffic engineering

Traffic engineering is where centralized SDN is most mature: operators have reported much better use of inter-data-center links once allocation was computed centrally [36], [37]. These are bounded, single-operator WANs, though, and say little directly about mobile networks. For the literature on 6G, multi-domain traffic engineering is necessary due to factors relating to both the transport domain and radio domain; however, few validated solutions have been proposed [12], [27].

7.3 Routing

Routing depends on the global view and, in 6G, on interference, so Section 8 covers both together.

7.4 QoS and QoE management

SDN supports QoS through flow classification, queue management and path selection; a survey of QoS in SDN covers both the mechanisms and their unsolved problems [76], and the SDN-5G/6G survey counts low latency and QoE among its open issues [12]. QoE, which depends on application perception, has received less attention than QoS, and closed-loop QoE control through intent and analytics is largely a proposal [50], [54].

7.5 Mobility management

Mobility is one of the four principal topics of [12]. SDN-based cellular frameworks centralize aspects of mobility and policy [44], [45], and Yadav et al. would simplify the mobile control plane by taking end-user signalling out of it [24]. Remaining concerns for 6G are mobility in highly dynamic terahertz and non-terrestrial topologies and the coordination of handovers across domains [12], [62]; for these cases, the solutions on offer are conceptual rather than validated.

7.6 Network slicing

Slice management combines orchestration, NFV and SDN programming, as discussed in Section 6.2 [43], [47], [48]. Slice assurance requires continuous monitoring and corrective actions, which is a natural application for AI-assisted control but has not been demonstrated at 6G scale.

7.7 Service function chaining

SDN steers traffic through ordered sets of virtualized functions, in the mobile core as in SoftCell, and in NFV architectures [19], [20], [44]. The literature identifies the joint optimization of placement and chaining as a challenge [20].

7.8 Load balancing

Load balancing appears at three levels: traffic across paths, load across radio cells (a motivating use case of SoftRAN [34]), and load across controllers, for which elastic assignment of switches to controllers has been proposed [39].

7.9 Energy optimization

Energy efficiency is listed among the open issues for SDN-based 5G/6G [12]. None of the sources we reviewed weighs the energy that SDN control, telemetry and AI infrastructure consume against the savings they enable, so we list this as a gap (Section 14).

7.10 Fault management

SDN can detect faults from global telemetry and reconfigure paths, but also introduces control-plane failure modes. Proposals include replication and diversity for dependable controllers [60], distributed controller platforms [32], and operating systems that isolate faulty applications [77]. Semantics for 6G recovery have yet to be established within multiple-tier controllers.

7.11 Network orchestration

Virtual function and slice orchestration for NFV has been standardized through MANO [19]; on the other hand, in slice studies, there is emphasis on the requirement of end-to-end and multi-domain orchestration which is the unresolved issue [43], [48]. Intent-based architecture will require an extra layer of translation.

8. ROUTING AND INTERFERENCE MANAGEMENT

8.1 Network-wide visibility and programmable control

Kazmi et al. survey how routing can reduce interference in SDN-enabled beyond-5G networks and ask how far a central network view can help [27]. In a dense wireless network, the path chosen for one flow changes the interference that other links see, so a controller that observes topology, link quality and load could in principle avoid path combinations prone to interference. SoftRAN argued much the same for the RAN, where base stations acting alone handle interference and load poorly compared with a controller that sees them all [34]. Table 6 lists the

routing and interference-management approaches we found.

TABLE 6 APPROACHES TO ROUTING AND INTERFERENCE MANAGEMENT IN SDN-ENABLED NETWORKS

Approach	Principle	SDN role	Evidence and limitation
SDN-based routing	Controller computes paths from a global view and installs rules [15]	Central path computation	Mature in wired WANs [36], [37]; wireless dynamics add overhead
Dynamic routing	Paths adapt to changing load and link state	Telemetry and rule update	Update latency and overhead bound responsiveness; evidence for 6G dynamics limited
Interference-aware routing	Path choice limits interference to other links [27]	Global view of links and interference	Survey-level evidence; centralized decisions may lag fast channel changes
Multi-path routing	Traffic split across several paths (comparative interpretation)	Flow-rule programming	Not specifically evaluated in the core set
QoS-aware routing	Constraints per service class [76]	Classification, queueing, path constraints	Mature for wired; 6G slice constraints not validated
Spectrum-aware routing	Routing combined with spectrum/radio-resource state	Cross-layer information at controller	Not found as a distinct SDN topic in the reviewed sources; related RAN control in [34], [38]
Resource-aware routing	Routing aware of compute and link resources	Joint network–compute view	Edge-focused studies are conceptual [56]
AI-assisted routing	Learning-based path selection [23], [78]	Telemetry and actuation	Reinforcement-learning routing evaluated by simulation [78]; robustness and stability open
RIS-assisted optimization	RIS placement/selection modifies the propagation graph [26], [70]	RIS as controllable resource	Simulation in small industrial scenario [26]
Cross-layer optimization	Joint decisions across routing, radio and compute	Orchestration and controller coordination	Largely conceptual; no common benchmark

8.2 Dynamic, QoS-aware and multi-path routing

Since SDN programs flow rules directly, dynamic and multi-path forwarding are easy to implement, and QoS-aware routing in SDN is widely surveyed [76]. Authors agree that all three benefit from the global view. Their common weakness is control-loop delay, from measurement to decision to rule installation, which limits how fast routing can follow rapidly changing wireless links [27], [40].

8.3 AI-assisted routing

Deep reinforcement learning has been used to optimize SDN routing, with evaluation in simulation [78], and [23] surveys ML for routing in SDN. These studies concern generic or wired topologies; the transfer to wireless 6G topologies with interference and mobility has not been demonstrated.

8.4 RIS-assisted optimization

In the core study of Chiti et al., RIS placement and selection are formulated using set covering (to select a minimal subset of RIS covering the users) and a minimum-spanning-tree approach (for connectivity), evaluated in a simulated factory scenario; the authors report coverage gains from RIS deployment, with the SDN controller using the RIS abstraction to manage the surfaces [26]. In our reading, the study shows that RIS can be treated as an SDN-managed resource and planned with graph-based methods, but not how it performs in operation, since hardware validation is future work.

8.5 Centralized versus distributed routing decisions

Centralized routing optimizes globally but is held back by controller capacity, control latency and failure exposure [29], [40]. Hierarchical and distributed approaches provide more scalability and response time but do not possess

global optimality and consistency [41], [42]. In such dynamic 6G environment where THz communication channels are easily blocked and there is presence of mobile nodes operating over non-terrestrial network, it is suggested from literature that the controller should quickly adapt locally to define constraints and policies. No study we reviewed shows this split working in 6G.

9. SECURITY IN SDN-ENABLED 6G

SDN centralizes control and opens new interfaces, which cuts both ways for security: the global view and programmable defences help, but the controller and interfaces become targets. SDN security surveys list the ways the controller, its interfaces and the data plane can be attacked, along with defences for each [30], [79]. For 6G, Jaadouni et al. argue that SDN and NFV together can underpin security architectures, citing centralized management, flexibility, scalability and agility, while noting open challenges [25].

9.1 Architecture, controller and interface security

Security recommendations for SDN are fairly settled: authenticate and authorize every interface, replicate and diversify controllers, isolate applications, and secure the software and its updates [30], [60], [79]. The controller needs special care, since whoever compromises it can reprogram the network. Replication, hardening, and isolation of applications are common practices, however, Rosemary is such a design where the controller infrastructure is robust despite the failure of applications [77]. Links from devices need to be authenticated, provide integrity and confidentiality for southbound interfaces, while northbound APIs should be properly authorized and rate limited so that any malicious or faulty application could not impose evil policies [30], [79]. O-RAN surveys have analysed the attack surface of Open RAN's open interfaces [38].

9.2 DDoS, slicing and virtual network function security

SDN and DDoS have a two-sided relationship: the global view helps detect and mitigate attacks, yet flow tables and the controller can themselves be saturated [80]. Slicing brings isolation attacks and threats peculiar to slices [57], and NFV exposes the virtualized functions, along with their management and orchestration, to attack [19], [20].

9.3 AI/ML security

Control models can be poisoned or misled by adversarial inputs [67], and their decisions are hard to explain [66]. Deep-learning intrusion detection for SDN works on standard datasets [81], but whether it holds up against an adaptive attacker has been studied far less.

9.4 Authentication, authorization, trust and zero trust

Zero-trust architecture stops trusting a request just because of where it comes from in the network. Every request is authenticated and authorized, and the decision is re-evaluated continuously [58]. Extending it to a multi-domain 6G control plane, between controllers or from orchestrator to controller, seems natural, but we found no validated design or overhead measurement. Trust management across operators, and for virtualized functions and models, remains open. NIST's lattice-based key-encapsulation standard and other post-quantum schemes matter for the long-term confidentiality of control channels [59].

9.5 Intrusion detection and secure orchestration

Detection draws on SDN telemetry and machine learning [30], [81]. Orchestration is secure only if lifecycle operations are authenticated, function images verified and policies checked before they take effect [19], [58]. Table 7 maps threats to affected components, impact, mitigations and remaining gaps. None of the listed mitigations is claimed to remove its threat entirely.

TABLE 7 SECURITY THREATS IN SDN-ENABLED 6G: AFFECTED COMPONENTS, IMPACT, MITIGATIONS AND REMAINING GAPS

Threat	Affected component	Potential impact	Existing mitigation	Remaining gap
Controller compromise	SDN controller	Network-wide reprogramming; loss of control	Hardening; replication and diversity [60]; application isolation [77]	Compromise of a root tier retains wide impact; verified designs for 6G absent
Southbound interface attack	Controller–device channel (OpenFlow, E2)	Rule tampering; eavesdropping	Authentication and encryption [30], [79]	Key management at scale; constrained devices
Northbound API abuse	Application–controller API	Harmful or conflicting policies	Authentication, authorization, policy checks [54], [79]	Semantic abuse by authorized apps; standardization

Threat	Affected component	Potential impact	Existing mitigation	Remaining gap
DDoS	Data plane, controller, flow tables	Service degradation; controller saturation	SDN-based detection and mitigation [80]	Adaptive and volumetric attacks; detection errors
Slice isolation attack	Shared radio, transport and compute resources	Cross-slice interference or leakage	Isolation mechanisms; monitoring [57]	Isolation guarantees on shared radio/compute unresolved
Rogue or vulnerable VNF	NFV infrastructure and MANO	Traffic interception; resource abuse	Image verification; MANO controls [19], [20]	Supply-chain trust
False telemetry	Monitoring and AI pipelines	Misleading decisions	Authenticated telemetry; consistency checks (conceptual)	Little 6G-specific evaluation in reviewed sources
AI/ML attack	Models and training data	Mis-optimization; evasion	Adversarial testing; fallback [67]	Robustness guarantees limited; explainability [66]
Identity/access failure	Management and orchestration	Unauthorized control actions	Zero trust; strong authentication [58]	Multi-domain identity federation
Distributed-controller attack	East–west state synchronization	State inconsistency; poisoned view	Replication and secure platform design [32], [60]	Byzantine-resilient designs at 6G scale not established

10. SDN FOR INDUSTRIAL IOT AND 6G

The IoT literature presents SDN as a way to manage heterogeneous devices and gateways with policy-driven control [72], [73]. For 6G industrial settings, the most specific source in the core set is Chiti et al. They propose an SDN-oriented architecture for industrial IoT with host, data, control and application planes, and they bring RIS under SDN control through an OpenFlow-style abstraction [26]. They argue that automated industrial systems such as remote robotic operation are expected to exceed what 5G can deliver, and they evaluate their design in a simulated factory with several RIS units and tens of devices [26].

In smart factories and mission-critical communication, the requirements are deterministic latency, high reliability and coverage in cluttered indoor spaces [5], [26]. SDN helps through local control, slicing and RIS-based coverage management, though the evidence comes from simulation. Remote operation and coordinated robots depend on bounded latency, and SDN work on autonomous systems handles this mostly through edge and local control concepts, without demonstrated systems [5], [56]. For intelligent transportation, mobility, availability and edge services make predictive handover and edge placement relevant, but we found no validated study specific to SDN in 6G. Smart cities, with massive IoT and multi-tenant services, point toward hierarchical, aggregate control [12], [72]. Across all these domains, SDN-based 6G is at the conceptual or simulation stage.

For RIS, the interaction supported by evidence is the abstraction of RIS as programmable forwarding elements, with placement and selection driven by the controller [26]; RIS fundamentals and potential benefits are reviewed in [69]–[71]. The authors of the core study suggest that production systems may need lighter protocols than OpenFlow and that hardware validation is still to come, so the SDN-RIS interface is not yet settled [26].

11. AI-ENABLED SDN FOR 6G

11.1 AI-assisted SDN demonstrated in the literature

ML has been applied to traffic classification and prediction, routing, resource management and security, both in networking generally [22] and in SDN specifically [23]. Examples include deep reinforcement learning for SDN routing, evaluated in simulation [78], and deep-learning intrusion detection for SDN, evaluated on intrusion datasets [81]. Most of these demonstrations work at component level, use simulated or dataset-based evaluation, and target wired or generic topologies. Reviews of AI-enabled 6G describe where AI may be applied in the network, but none reports a validated SDN-integrated 6G deployment [6], [51].

11.2 Application areas

Traffic and congestion prediction and resource allocation have the strongest basis, as the surveys in [22],

[23] show. Intelligent routing and anomaly detection have component demonstrations [78], [81]. Mobility prediction appears in general ML-for-networking surveys [22], while energy optimization gets little attention in the core set. Autonomous orchestration is what the ITU-T ML architecture framework aims at, with its ML pipelines, sandbox and orchestration of ML functions [50], and the IETF defines intent-based networking as turning desired outcomes into configuration with continuous assurance [54]. Digital twin networks have been surveyed as a way to test decisions before they are enforced [82].

11.3 Proposed future concepts

Several concepts remain proposals rather than demonstrated capabilities: closed-loop, intent-driven autonomous operation of multi-domain 6G networks [6], [54]; digital-twin-validated control actions [82]; and federated learning across domains to avoid sharing raw data [83]. Their feasibility within control-latency and trust constraints has yet to be shown.

11.4 Limitations of AI-enabled control

Recurring limitations include dependence on telemetry quality, concept drift, limited explainability [66], vulnerability to adversarial inputs and poisoning [67], and the lack of standard benchmarks. Most AI-for-SDN studies are also evaluated in isolation, so little is known about how AI decisions interact with hierarchical controllers and security mechanisms.

12. COMPARATIVE LITERATURE ANALYSIS

12.1 Comparison of studies

Table 8 compares the core studies with a set of representative others, and its entries are limited to what the sources state. “Not discussed” means the topic is absent from the source as we examined it; “Not assessed” means we did not verify that cell and left it open rather than infer a value. The table shows a pattern: each study is strong on one dimension (architecture, security, AI or scalability) and rarely covers several, and the studies closest to 6G are mostly surveys or conceptual designs.

TABLE 8 COMPARATIVE ANALYSIS OF CORE AND REPRESENTATIVE STUDIES

Study	Year	Primary focus	SDN role	6G technology	Security	AI/ML	Scalability	Major limitation
Long et al. [12]	2022	Survey: SDN-based 5G/6G	System architecture; management functions	mm-wave; massive MIMO	Open issue	Not discussed in abstract	Open issue	No new validated architecture
Yadav et al. [24]	2023	Control-plane redesign	Signalling treated as user service	Mobile core	Claimed benefit	Not discussed	Claimed; simulation	RAN, RIS, NTN not the focus
Jaadouni et al. [25]	2024	6G security via SDN and NFV	Centralized control	NFV	Core theme	Not discussed	Benefit stated	No quantitative evaluation reported
Chiti et al. [26]	2026	IIoT; RIS placement	RIS as OpenFlow-style switches	RIS; IIoT	Not discussed	Not discussed (optimization)	Small scenario	Simulation only
Kazmi et al. [27]	2023	Interference-aware routing	Centralized view for routing	Beyond-5G interference	Not discussed	Not assessed	Not assessed	Narrow scope
Kreutz et al. [15]	2015	SDN survey	Layered review of SDN	None (general SDN)	Open issue	Not discussed	Open issue	Pre-6G
Gudipati et al. [34]	2013	SoftRAN design	Centralized/distributed RAN control split	RAN	Not discussed	Not discussed	Not assessed	Pre-5G design

Study	Year	Primary focus	SDN role	6G technology	Security	AI/ML	Scalability	Major limitation
Foukas et al. [35]	2016	FlexRAN platform	Programmable RAN controller	RAN	Not assessed	Not assessed	Not assessed	Pre-6G; platform
Polese et al. [38]	2023	O-RAN survey	RIC as RAN controller	Open RAN	Discussed	ML in O-RAN discussed	Not assessed	Not an SDN-specific study
Afolabi et al. [43]	2018	Slicing and softwarization	SDN/NFV enabling slicing	Slicing	Not assessed	Not assessed	Challenges discussed	Pre-6G
Bi et al. [63]	2019	Space–terrestrial SDN	Unified control of integrated network	NTN	Not assessed	Not assessed	Not assessed	Conceptual
Scott-Hayward et al. [30]	2016	SDN security survey	Security of SDN	None (general SDN)	Core theme	Not discussed	Not assessed	Pre-6G
Xie et al. [23]	2019	ML for SDN survey	ML-driven control	None (general SDN)	Not assessed	Core theme	Not assessed	No 6G-specific evaluation
Levin et al. [41]	2012	State distribution	Distributed control state	None	Not discussed	Not discussed	State-consistency effects	Pre-6G; specific applications
Hassas Yeganeh and Ganjali [42]	2012	Kandoo hierarchy	Hierarchical control	None	Not discussed	Not discussed	Core theme	Pre-6G
Berde et al. [32]	2014	ONOS platform	Distributed controller	None	Not assessed	Not discussed	Core theme	Pre-6G

12.2 Comparison of architectural approaches

Table 9 sets the Section 5 approaches side by side on the same dimensions. It records their characteristics and trade-offs as the sources report them, in qualitative terms drawn from those sources.

TABLE 9 COMPARISON OF SDN ARCHITECTURAL APPROACHES (DOCUMENTED CHARACTERISTICS AND TRADE-OFFS; NOT A RANKING)

Architecture	Control model	Scalability	Latency	Fault tolerance	Complexity	6G suitability considerations
Centralized	Single logical controller	Bounded by controller capacity [40]	Round trip to controller	Needs replication	Lowest conceptual	Policy and optimization in bounded domains
Hierarchical	Local plus root controllers [42]	Improved through offloading	Low locally; higher globally	Tier-level containment	Moderate	Matches multi-timescale 6G control
Distributed	Peer instances with shared state [32]	Scale-out	Instances nearer to devices	Replication; consistency issues [41]	High (state sync)	Large domains; consistency needs unstudied

Architecture	Control model	Scalability	Latency	Fault tolerance	Complexity	6G suitability considerations
Multi-controller	Domain controllers with east–west links	Scales with domains	Inter-domain coordination cost	Domain-level containment	Moderate to high	Natural for RAN/transport/core split
Federated	Autonomous controllers, limited sharing [61]	Independent per owner	Negotiation overhead	Local failures isolated	High (trust, policy)	Multi-operator and NTN settings
Edge-assisted	Controllers at edge sites [56]	Replication across sites	Low for local decisions	Many sites; local autonomy	Moderate to high	Pervasive edge intelligence
Cloud-native	Elastic microservice controllers [21]	Horizontal scaling	Predictability concern	Automatic restart	High (orchestration)	Aligned with cloud-native core/O-RAN
AI-assisted	Analytics-driven decisions [50]	Depends on inference placement	Inference placement dependent	Model failure risk; fallback needed	High (ML lifecycle)	AI-native direction; robustness open
Cross-domain	Orchestrator over domain controllers [48]	Slow-timescale scope	Slow timescales	Cross-domain coupling	High (information models)	Space–air–ground integration

13. CURRENT CHALLENGES

Each challenge below pairs what earlier work has shown with what is still open.

Controller capacity and placement put a ceiling on how far SDN scales, and hierarchical and distributed designs raise that ceiling [32], [39], [40], [42]. Whether they cope with 6G device densities and event rates has not been shown.

As far as distributed control is concerned, old state negatively impacts application performance [41], whereas replication is a typical approach to obtaining availability [32]. But it is still unclear what level of consistency should be provided by 6G control state in multiple-tier architectures and which synchronization protocols can provide this.

Every trip to the remote controller adds control-plane latency [29], [40], and nobody has figured out how to separate local control from global control on the scale of sub-milliseconds [3].

Diversity in networks impedes cooperation between domains. Slicing and multi-domain orchestration are recognized open problems [43], [48], and concepts for multi-domain controllers exist [61], but domains and operators still lack shared information models and settled trust.

Mobility is central to SDN-based 5G/6G work [12], yet handover and control in fast-changing terahertz and non-terrestrial topologies remain unsolved [62].

On security and privacy, the threats to SDN are well documented [30], [79], [80], and slicing adds threats of its own [57]. Securing tiered controllers, VNFs, interfaces and ML pipelines as one system remains unsolved, and so does keeping telemetry private (Section 16 notes the Indian legal context).

For AI-driven control, methods exist for explaining black-box models [66], and the weakness of models against adversarial examples is well known [67]. What is missing is a way to give assurance for actions that AI takes inside closed control loops.

Energy efficiency is already listed as an open issue [12], but nobody has measured the net energy effect of the control, telemetry and AI infrastructure itself.

Standards and interoperability lag behind: there is still no common northbound standard [15], [29], 6G specification is in its study phase [11], and the relationship among SDN controllers, O-RAN RICs and orchestrators is unsettled [38].

When it comes to hardware, the use of programmable pipelines P4 is considered [33], and the implementation issues for SDN were examined [29]; however, there is no hardware solution for RIS and terahertz equipment as well as the OpenFlow replacement [26].

Finally, emulators and simulators cover parts of the stack [84]–[87], but there are no shared, reproducible benchmarks or large-scale testbeds for SDN-based 6G, and most of the evidence we reviewed comes from simulation [24], [26].

14. RESEARCH GAPS

Each gap below reflects limitations that recur across the studies we reviewed. Relevant work may exist outside that material.

1. There are no common architectural standards: the architectures we reviewed differ in layers, interfaces and terminology, and 6G standardization is incomplete [11], [12], [38].
2. Real-world validation is limited, since the core 6G-specific SDN studies are surveys or rely on simulation [24], [26].
3. Without reproducible benchmarks and standard metrics, studies use different scenarios and measures, so architectures cannot be compared numerically.
4. Distributed and hierarchical controllers have been evaluated in generic networks [32], [41], [42], not under 6G conditions.
5. Cross-domain orchestration is under-studied, and slicing across domains is repeatedly described as unsolved [43], [48].
6. Security evaluation is incomplete: surveys catalogue threats [25], [30], [79], but we found no integrated, quantified evaluation of 6G SDN security.
7. AI and SDN are integrated only at the component level in current studies [23], [78], [81].
8. RIS control under SDN lacks experimental validation, because the main SDN-RIS study relies on simulation [26].
9. SDN work on terahertz, ISAC and non-terrestrial control is sparse, and the interactions remain indirect or conceptual (Section 6).
10. No large-scale testbed or benchmark infrastructure for SDN-based 6G exists in the work we reviewed.

15. FUTURE RESEARCH DIRECTIONS

Table 10 links each gap to a proposed direction and a candidate approach. These are proposals drawn from the gaps above and from the cited studies, and none has been validated.

TABLE 10 RESEARCH GAPS AND PROPOSED FUTURE DIRECTIONS (PROPOSALS, NOT ESTABLISHED RESULTS)

Research gap	Proposed direction	Candidate approach
Distributed-controller evaluation	Distributed and hierarchical controllers for 6G; consistency models by state class	Comparative emulation and simulation using common topologies [32], [41]
AI-native control	AI-native SDN with guardrails and fallback	Closed-loop pilots following ML frameworks [50]
Intent-based networking	Intent-based 6G with verifiable translation and assurance	Formal intent models [54]
Autonomous orchestration	Autonomous multi-domain orchestration	Orchestrator–controller co-design [43]
Security evaluation	Secure multi-controller architectures; zero-trust SDN	Threat-model-driven testing [30], [58]
Cross-domain SDN	Inter-domain information models and trust frameworks	Federated controller designs [61]
Edge control	Edge-native SDN with joint network–compute control	Joint optimization [56]
RIS validation	RIS-aware SDN with lightweight protocols and hardware validation	Extend [26] to testbeds
ISAC integration	Control-plane exposure of sensing data	Conceptual models then prototypes [55]
Digital twins	Twin-validated control actions	Twin fidelity studies [82]
Data plane	Programmable data planes for radio and transport elements	P4-based and RAN-programmable platforms [33], [35]
Energy	Energy-aware control with accounting of control overhead	Measurement within benchmarks
Explainability	Explainable AI for network control	Explanation methods [66]
Privacy-preserving learning	Federated intelligence across domains	Federated learning prototypes [83]
Post-quantum security	Quantum-safe control channels	Protocol benchmarking with standardized primitives [59]

Research gap	Proposed direction	Candidate approach
Benchmarking	Reproducible benchmarks and large-scale testbeds	Open scenarios and metrics on existing tools [84], [85], [87]

The literature also mentions self-healing networks that detect and repair faults on their own, and integrated terrestrial and non-terrestrial control [62], [63]. Semantic and intent-driven communication has been proposed too, but its SDN implications remain unexplored in the work we reviewed.

16. INDIA-SPECIFIC PERSPECTIVE

Official sources state that India released its Bharat 6G Vision document in March 2023. It sets 2030 as the year by which India should be a leading contributor to how 6G is designed, developed and deployed, on three principles: affordability, sustainability and ubiquity. The Technology Innovation Group on 6G prepared it. The government has since backed a Bharat 6G Alliance that brings together companies, universities, research institutes and standards bodies, and is funding testbeds, including terahertz and advanced optical-communication facilities [88]. These initiatives give SDN-based 6G architectures somewhere to be studied and validated, and they respond to the testbed shortage noted in Section 14.

The statutory context includes the Telecommunications Act, 2023 [89] and the Digital Personal Data Protection Act, 2023 [90]. The second matters for SDN-based networks because telemetry and AI pipelines may carry personal data. A legal analysis is beyond this review, and we make no claim about compliance. The SDN literature we reviewed does not discuss the technical conditions for deployment in India. We offer, as a hypothesis for future study, that varied environments, a mix of equipment generations and uneven backhaul would favour hierarchical control with clearly defined degraded modes. Testbed evaluation of SDN-RIS and terahertz control, and interoperability studies of open interfaces within the Bharat 6G ecosystem, are clear opportunities. We leave policy and spectrum questions, and regulatory material beyond the cited source, to other work.

17. REVIEW FINDINGS

1. The studies agree on the value of separating control from forwarding, of a global view and of programmability in complex networks, and on the need to combine SDN with NFV, orchestration and, increasingly, AI [12], [15], [25], [50].
2. They differ mainly on where control is placed (centralized, hierarchical, distributed or federated), where the control/user-plane boundary lies [24], and whether radio elements are abstracted as Open RAN RICs or as OpenFlow-style elements [26], [38].
3. The capabilities that matter most for 6G appear to be multi-domain orchestration, hierarchical control with fast local loops, programmable abstraction of diverse resources and telemetry-fed automation.
4. The same limitations keep coming back: scalability, state consistency, control-plane latency and security, interoperability, and the lack of validation at scale [12], [29], [30], [41].
5. Terahertz, ISAC and non-terrestrial control have had little direct SDN attention, while RIS and Open RAN are further along but still lack settled SDN interfaces [26], [38], [63].
6. None of the following have yet been implemented on a real device: SDN architecture for 6G, AI control mechanism, control technique for RIS, or cross-domain orchestrator.
7. Questions to be answered: What level of control does the state demand? Consistency, protection of hierarchical controllers and AI algorithms, integration of RICs with SDN controllers, benchmarking, and the energy cost of intelligence-based control.

Therefore, SDN-based 6G network management may prove to be a viable option to consider. Nonetheless, the evidential basis is somewhat shaky – solid at its fundamentals but weak at systems level.

18. CONCLUSION

This review organized and compared the literature on SDN architecture for 6G networks. SDN began as a way to program forwarding devices, was applied to mobile cores and RANs together with NFV and slicing, and is now being extended in research toward multi-domain, intent-driven and AI-assisted control. The main architectures depend on compromise between global visibility, scalability, latency, fault tolerance, security and complexity, where there is no single architecture shown to be applicable to all 6G components. The connection between SDN and 6G technologies is rather developed for NFV and slicing, emerging for Open RAN, RIS and edge computing, and conceptual for terahertz, ISAC and non-terrestrial network. Network management, routing and interference management, and security, as well as AI control, are rather grounded, but need proof of concept for the scope of 6G.

It is marked by survey-oriented research, designs, and simulation studies on a small scale. It lacks any benchmarks and testbeds of considerable size, and cannot address issues of consistency of states, security of control planes and AI solutions, interoperability and standardization. Such features define the scope of the research: distributed and secure multi-controller architecture, AI-native control that can be trusted, RIS-aware and non-terrestrial control, as well as reproducible

testing. No experiments are included in the literature review, while the architecture is only conceptualized.

REFERENCES

[1] 3GPP, "System architecture for the 5G System (5GS)," 3rd Generation Partnership Project, Tech. Spec. TS 23.501.

[2] ITU-R, "Minimum requirements related to technical performance for IMT-2020 radio interface(s)," Report ITU-R M.2410-0, Nov. 2017.

[3] ITU-R, "Framework and overall objectives of the future development of IMT for 2030 and beyond," Recommendation ITU-R M.2160-0, Nov. 2023.

[4] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?," Nature Electron., vol. 3, no. 1, pp. 20–29, Jan. 2020, doi: 10.1038/s41928-019-0355-6.

[5] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Netw., vol. 34, no. 3, pp. 134–142, May/Jun. 2020, doi: 10.1109/MNET.001.1900287.

[6] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," IEEE Commun. Mag., vol. 57, no. 8, pp. 84–90, Aug. 2019, doi: 10.1109/MCOM.2019.1900271.

[7] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland, and F. Tufvesson, "6G wireless systems: Vision, requirements, challenges, insights, and opportunities," Proc. IEEE, vol. 109, no. 7, pp. 1166–1199, Jul. 2021, doi: 10.1109/JPROC.2021.3061701.

[8] C.-X. Wang et al., "On the road to 6G: Visions, requirements, key technologies, and testbeds," IEEE Commun. Surveys Tuts., vol. 25, no. 2, pp. 905–974, 2nd Quart. 2023, doi: 10.1109/COMST.2023.3249835.

[9] Z. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," IEEE Veh. Technol. Mag., vol. 14, no. 3, pp. 28–41, Sep. 2019, doi: 10.1109/MVT.2019.2921208.

[10] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," IEEE Access, vol. 8, pp. 133995–134030, 2020, doi: 10.1109/ACCESS.2020.3010896.

[11] 3GPP, "Rel-20 planning and progress in TSG SA," 3GPP news item. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/sa-rel20 (accessed Oct. 2026).

[12] Q. Long, Y. Chen, H. Zhang, and X. Lei, "Software defined 5G and 6G networks: A survey," Mobile Netw. Appl., vol. 27, no. 5, pp. 1792–1812, 2022, doi: 10.1007/s11036-019-01397-2.

[13] J. R. Bhat and S. A. Alqahtani, "6G ecosystem: Current status and future perspective," IEEE Access, vol. 9, pp. 43134–43167, 2021, doi: 10.1109/ACCESS.2021.3054833.

[14] N. McKeown et al., "OpenFlow: Enabling innovation in campus networks," ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, Apr. 2008, doi: 10.1145/1355734.1355746.

[15] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[16] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1617–1634, 3rd Quart. 2014, doi: 10.1109/SURV.2014.012214.00180.

[17] ITU-T, "Framework of software-defined networking," Recommendation ITU-T Y.3300, Jun. 2014.

[18] E. Haleplidis, Ed., K. Pentikousis, Ed., S. Denazis, J. Hadi Salim, D. Meyer, and O. Koufopavlou, "Software-defined networking (SDN): Layers and architecture terminology," IETF, RFC 7426, Jan. 2015, doi: 10.17487/RFC7426.

[19] ETSI, "Network functions virtualisation (NFV); Architectural framework," ETSI GS NFV 002, V1.2.1, Dec. 2014.

[20] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 236–262, 1st Quart. 2016, doi: 10.1109/COMST.2015.2477041.

[21] B. Burns, B. Grant, D. Oppenheimer, E. Brewer, and J. Wilkes, "Borg, Omega, and Kubernetes," Commun. ACM, vol. 59, no. 5, pp. 50–57, May 2016, doi: 10.1145/2890784.

[22] R. Boutaba et al., "A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities," J. Internet Serv. Appl., vol. 9, Art. no. 16, 2018, doi: 10.1186/s13174-018-0087-2.

[23] J. Xie et al., "A survey of machine learning techniques applied to software defined

networking (SDN): Research issues and challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 393–430, 1st Quart. 2019, doi: 10.1109/COMST.2018.2866942.

[24] R. Yadav, R. Kamran, P. Jha, and A. Karandikar, "Applying SDN to mobile networks: A new perspective for 6G architecture," arXiv:2307.05924, 2023.

[25] H. Jaadouni, H. Chaoui, and C. Saadi, "Evolving security for 6G: Integrating software-defined networking and network function virtualization into next-generation architectures," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 6, pp. 909–914, 2024, doi: 10.14569/IJACSA.2024.0150692.

[26] F. Chiti, M. Lotti, S. Picchioni, and L. Pierucci, "SDN-oriented 6G industrial IoT architecture design and application to optimal RIS placement and selection," Sensors, vol. 26, no. 2, Art. no. 411, 2026, doi: 10.3390/s26020411.

[27] S. H. A. Kazmi, F. Qamar, R. Hassan, and K. Nisar, "Routing-based interference mitigation in SDN enabled beyond 5G communication networks: A comprehensive survey," IEEE Access, vol. 11, pp. 4023–4041, 2023, doi: 10.1109/ACCESS.2023.3235366.

[28] 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.

[29] S. Sezer et al., "Are we ready for SDN? Implementation challenges for software-defined networks," IEEE Commun. Mag., vol. 51, no. 7, pp. 36–43, Jul. 2013, doi: 10.1109/MCOM.2013.6553676.

[30] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 623–654, 1st Quart. 2016, doi: 10.1109/COMST.2015.2453114.

[31] J. Medved, R. Varga, A. Tkacik, and K. Gray, "OpenDaylight: Towards a model-driven SDN controller architecture," in Proc. IEEE Int. Symp. World of Wireless, Mobile and Multimedia Netw. (WoWMoM), 2014, pp. 1–6, doi: 10.1109/WoWMoM.2014.6918985.

[32] P. Berde et al., "ONOS: Towards an open, distributed SDN OS," in Proc. 3rd Workshop Hot Topics Softw. Defined Netw. (HotSDN), 2014, pp. 1–6, doi: 10.1145/2620728.2620744.

[33] P. Bosshart et al., "P4: Programming protocol-independent packet processors," ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 3, pp. 87–95, Jul. 2014, doi: 10.1145/2656877.2656890.

[34] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "SoftRAN: Software defined radio access network," in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN), 2013, pp. 25–30, doi: 10.1145/2491185.2491207.

[35] X. Foukas, N. Nikaein, M. M. Kassem, M. K. Marina, and K. Kontovasilis, "FlexRAN: A flexible and programmable platform for software-defined radio access networks," in Proc. 12th Int. Conf. Emerg. Netw. Exp. Technol. (CoNEXT), 2016, pp. 427–441, doi: 10.1145/2999572.2999599.

[36] C.-Y. Hong et al., "Achieving high utilization with software-driven WAN," in Proc. ACM SIGCOMM, 2013, pp. 15–26, doi: 10.1145/2486001.2486012.

[37] S. Jain et al., "B4: Experience with a globally-deployed software defined WAN," in Proc. ACM SIGCOMM, 2013, pp. 3–14, doi: 10.1145/2486001.2486019.

[38] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," IEEE Commun. Surveys Tuts., vol. 25, no. 2, pp. 1376–1411, 2nd Quart. 2023, doi: 10.1109/COMST.2023.3239220.

[39] A. Dixit, F. Hao, S. Mukherjee, T. V. Lakshman, and R. Kompella, "Towards an elastic distributed SDN controller," ACM SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, pp. 7–12, Oct. 2013, doi: 10.1145/2534169.2491193.

[40] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," in Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN), 2012, pp. 7–12, doi: 10.1145/2342441.2342444.

[41] D. Levin, A. Wundsam, B. Heller, N. Handigol, and A. Feldmann, "Logically centralized? State distribution trade-offs in software defined networks," in Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN), 2012, pp. 1–6, doi: 10.1145/2342441.2342443.

[42] S. Hassas Yeganeh and Y. Ganjali, "Kandoo: A framework for efficient and scalable offloading of control applications," in Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN), 2012, pp. 19–24, doi: 10.1145/2342441.2342446.

[43] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," IEEE Commun. Surveys Tuts., vol. 20,

no. 3, pp. 2429–2453, 3rd Quart. 2018, doi: 10.1109/COMST.2018.2815638.

[44] X. Jin, L. E. Li, L. Vanbever, and J. Rexford, "SoftCell: Scalable and flexible cellular core network architecture," in Proc. 9th ACM Conf. Emerg. Netw. Exp. Technol. (CoNEXT), 2013, pp. 163–174, doi: 10.1145/2535372.2535377.

[45] A. Bradai, K. Singh, T. Ahmed, and T. Rasheed, "Cellular software defined networking: A framework," IEEE Commun. Mag., vol. 53, no. 6, pp. 36–43, Jun. 2015, doi: 10.1109/MCOM.2015.7120043.

[46] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, "SDN/NFV-based mobile packet core network architectures: A survey," IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1567–1602, 3rd Quart. 2017, doi: 10.1109/COMST.2017.2690823.

[47] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," IEEE Commun. Mag., vol. 55, no. 5, pp. 80–87, May 2017, doi: 10.1109/MCOM.2017.1600935.

[48] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," IEEE Commun. Mag., vol. 55, no. 5, pp. 94–100, May 2017, doi: 10.1109/MCOM.2017.1600951.

[49] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "Open, programmable, and virtualized 5G networks: State-of-the-art and the road ahead," Comput. Netw., vol. 182, Art. no. 107516, 2020, doi: 10.1016/j.comnet.2020.107516.

[50] ITU-T, "Architectural framework for machine learning in future networks including IMT-2020," Recommendation ITU-T Y.3172, Jun. 2019.

[51] H. Yang et al., "Artificial-intelligence-enabled intelligent 6G networks," IEEE Netw., vol. 34, no. 6, pp. 272–280, Nov./Dec. 2020, doi: 10.1109/MNET.011.2000195.

[52] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," IEEE Access, vol. 7, pp. 78729–78757, 2019, doi: 10.1109/ACCESS.2019.2921522.

[53] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," Phys. Commun., vol. 12, pp. 16–32, Sep. 2014, doi: 10.1016/j.phycom.2014.01.006.

[54] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, "Intent-based networking – Concepts and definitions," IETF, RFC 9315, Oct. 2022, doi: 10.17487/RFC9315.

[55] F. Liu et al., "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," IEEE J. Sel. Areas Commun., vol. 40, no. 6, pp. 1728–1767, Jun. 2022, doi: 10.1109/JSAC.2022.3156632.

[56] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, 4th Quart. 2017, doi: 10.1109/COMST.2017.2745201.

[57] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, and M. Liyanage, "A survey on network slicing security: Attacks, challenges, solutions and research directions," IEEE Commun. Surveys Tuts., vol. 26, no. 1, pp. 534–570, 1st Quart. 2024, doi: 10.1109/COMST.2023.3312349.

[58] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST, Gaithersburg, MD, USA, Special Publication 800-207, Aug. 2020, doi: 10.6028/NIST.SP.800-207.

[59] National Institute of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard," Federal Information Processing Standards Publication (FIPS) 203, Aug. 2024, doi: 10.6028/NIST.FIPS.203.

[60] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN), 2013, pp. 55–60, doi: 10.1145/2491185.2491199.

[61] K. Phemius, M. Bouet, and J. Leguay, "DISCO: Distributed multi-domain SDN controllers," in Proc. IEEE Netw. Oper. Manage. Symp. (NOMS), 2014, pp. 1–4, doi: 10.1109/NOMS.2014.6838330.

[62] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," IEEE Netw., vol. 35, no. 2, pp. 244–251, Mar./Apr. 2021, doi: 10.1109/MNET.011.2000493.

[63] Y. Bi et al., "Software defined space-terrestrial integrated networks: Architecture, challenges, and solutions," IEEE Netw., vol. 33, no. 1, pp. 22–28, Jan./Feb. 2019, doi: 10.1109/MNET.2018.1800193.

[64] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st Ed. MCC Workshop Mobile Cloud Comput., 2012, pp. 13–16, doi: 10.1145/2342509.2342513.

[65] M. Satyanarayanan, "The emergence of edge computing," Computer, vol. 50, no. 1, pp. 30–39, Jan. 2017, doi: 10.1109/MC.2017.9.

[66] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, "A survey of methods for explaining black box models," ACM Comput. Surv., vol. 51, no. 5, Art. no. 93, 2018, doi: 10.1145/3236009.

[67] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in Proc. Int. Conf. Learn. Represent. (ICLR), 2015.

[68] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on network virtualization hypervisors for software defined networking," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 655–685, 1st Quart. 2016, doi: 10.1109/COMST.2015.2489183.

[69] E. Basar, M. Di Renzo, J. de Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," IEEE Access, vol. 7, pp. 116753–116773, 2019, doi: 10.1109/ACCESS.2019.2935192.

[70] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," IEEE J. Sel. Areas Commun., vol. 38, no. 11, pp. 2450–2525, Nov. 2020, doi: 10.1109/JSAC.2020.3007211.

[71] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," IEEE Commun. Mag., vol. 58, no. 1, pp. 106–112, Jan. 2020, doi: 10.1109/MCOM.001.1900107.

[72] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for Internet of Things: A survey," IEEE Internet Things J., vol. 4, no. 6, pp. 1994–2008, Dec. 2017, doi: 10.1109/JIOT.2017.2746186.

[73] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the Internet-of-Things," in Proc. IEEE Netw. Oper. Manage. Symp. (NOMS), 2014, pp. 1–9, doi: 10.1109/NOMS.2014.6838365.

[74] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," IEEE Netw., vol. 35, no. 5, pp. 158–167, Sep./Oct. 2021, doi: 10.1109/MNET.010.2100152.

[75] O. Kodheli et al., "Satellite communications in the new space era: A survey and future challenges," IEEE Commun. Surveys Tuts., vol. 23, no. 1, pp. 70–109, 1st Quart. 2021, doi: 10.1109/COMST.2020.3028247.

[76] M. Karakus and A. Durresi, "Quality of service (QoS) in software defined networking (SDN): A survey," J. Netw. Comput. Appl., vol. 80, pp. 200–218, Feb. 2017, doi: 10.1016/j.jnca.2016.12.019.

[77] S. Shin et al., "Rosemary: A robust, secure, and high-performance network operating system," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2014, pp. 78–89, doi: 10.1145/2660267.2660353.

[78] G. Stampa, M. Arias, D. Sanchez-Charles, V. Muntes-Mulero, and A. Cabellos, "A deep-reinforcement learning approach for software-defined networking routing optimization," arXiv:1709.07080, Sep. 2017.

[79] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2317–2346, 4th Quart. 2015, doi: 10.1109/COMST.2015.2474118.

[80] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 602–622, 1st Quart. 2016, doi: 10.1109/COMST.2015.2487361.

[81] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), 2016, pp. 258–263, doi: 10.1109/WINCOM.2016.7777224.

[82] Y. Wu, K. Zhang, and Y. Zhang, "Digital twin networks: A survey," IEEE Internet Things J., vol. 8, no. 18, pp. 13789–13804, Sep. 2021, doi: 10.1109/JIOT.2021.3079510.

[83] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS), PMLR vol. 54, 2017, pp. 1273–1282.

[84] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid prototyping for software-defined networks," in Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw. (HotNets), 2010, pp. 1–6, doi: 10.1145/1868447.1868466.

[85] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in Modeling and Tools for Network Simulation. Berlin, Germany: Springer, 2010, pp. 15–34, doi: 10.1007/978-3-642-12331-3_2.

[86] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in Proc. 1st Int. Conf. Simulation Tools Techn. Commun., Netw. Syst. (SIMUTools), 2008, doi: 10.4108/ICST.SIMUTOOLS2008.3027.

[87] N. Nikaein et al., "OpenAirInterface: A flexible platform for 5G research," ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 5, pp. 33–38, Oct. 2014, doi: 10.1145/2677046.2677053.

[88] Press Information Bureau, Government of India, "India's 6G vision 'Bharat 6G Vision' document envisages India to be a frontline contributor in design, development and deployment of 6G technology by 2030," press release. [Online]. Available: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2083233 (accessed Oct. 2026).

[89] Government of India, "The Telecommunications Act, 2023," Act No. 44 of 2023.

[90] Government of India, "The Digital Personal Data Protection Act, 2023," Act No. 22 of 2023.