Reliability Improvement Using SDN: Issues and Challenges Ahead

Muhammad Usman Younus[1,2], Kalsoom Safdar[3,4], Hassan Moatasam Awan[5]
[1]Department of Computer Science & IT, Baba Guru Nanak University, Nankana Sahib, Pakistan.
[2]Ecole Doctorale Matheematiques, Informatique, Telecommunication de Toulouse, University of Toulouse (III) Paul Sabatier, Toulouse, France.
[3] Department of Computer Science & IT, University of Jhang, Jhang, Pakistan.
[4]Faculty of Electronic Engineering and Technology, University Malaysia Perlis, 02600 Arau, Perlis, Malaysia.
[5]Department of Informatics and Systems, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan.
*__Correspondence__: usman1644@gmail.com, kalsoomsafdar11@gmail.com
Citation | Younus. M. U, Safdar. K, Awan. H. M, "Reliability Improvement Using SDN: Issues and Challenges Ahead", IJIST, Vol. 8 Issue. 1 pp 102-114, January 2026
Received| December 05, 2025 Revised| January 01, 2026 Accepted| January 06, 2026 Published| January 10, 2026.

Significant improvements in network reliability are being observed across various types of networks due to their wide applicability. Novel architectures for various applications of emerging technologies have been introduced to address problems related to network reliability. Consequently, a novel networking approach, referred to as Software Defined Networking (SDN), is being implemented to improve reliability in conventional networks via revised architectures. This paper primarily aims to provide a broad overview of research associated with enabling technologies and reliability for the next generation of networks. Existing research on emerging technologies highlights strategies to improve reliability. Detailed SDN-based reliability techniques are discussed that make the system more reliable. It also provides guidelines to address reliability-related challenges across systems and applications, highlighting key research directions.

Keywords: Software Defined Networking, Reliability, WSN, SDN Controller, Network Failure

Introduction:

Recently, a novel paradigm, Software Defined Networking (SDN), has emerged to address the challenges and issues associated with different types of networks [1][2][3]. An SDN controller typically communicates through the Southbound Interface (SBI) [4] (e.g., OpenFlow Protocol) with network devices and exposes several characteristics and APIs [5] through the Northbound Interface (NBI) to the network. The centralized controller approach ensures controllable networks but also introduces potential reliability issues.

Currently, reliability [6] appears to be the most critical concern and has been considered a serious challenge due to the connectivity of everything. User experience and revenue may be adversely affected by network outages. Novel networking concepts have been introduced to provide simplification and innovation for network reliability. Such innovations include the adaptation of SDN paradigm concepts to simplify infrastructure management and maintenance. SDN provides real-time failure notifications, thereby ensuring network reliability [7]. Incorporating SDN to improve connectivity has been a significant step in the evolution of modern network infrastructure. Consequently, it has garnered considerable attention from both industry and academia.

This paper focuses on reliability, which can be significantly improved by incorporating SDN [8] into various systems and applications. As mentioned above, the incorporation of SDN for reliable connectivity within networks is being implemented in 5G networks, video streaming, and many other applications (e.g., wireless sensor networks (WSNs), power grid (PG) networks, computer networks, etc.). To fulfill the myriad applications within business and user requirements, a broad vision must be implemented to construct novel architectures by network operators. The 5G network [9] prioritizes reliable connectivity as a key design requirement, and SDN proves to be an effective option for providing reliable user connectivity. Reliability refers to a network's ability to recover smoothly from failures or overloads while remaining functional from the user's perspective. Nowadays, the widespread use of video applications necessitates reconsidering how networks provide end-to-end quality of service (QoS). Recent QoS network architectures consider jitter, delay, and bandwidth [10]. While these factors are vital for real-time video applications, they are insufficient to address network reliability. Therefore, reliability in video applications [11] requires consideration of the path selection process rather than relying on a single path, even if that path has previously met reliability requirements before a failure.

This paper provides a comprehensive overview of ongoing research on SDN-based technologies for reliability within different network schemes and applications. It encompasses several sections dedicated to specific topics as follows: Section II provides a brief discussion on SDN architecture, elucidating how it has emerged as a potential solution to offer benefits related to reliability; Section III reviews the literature on SDN-based reliability and presents a table summarizing the reliability of different types of networks and their applications; Section IV explains the various challenges associated with the reliability of SDN-based networks and highlights the techniques related to enhancing reliability; finally, Section V provides concluding remarks and future perspectives.

Background Reliability:

This section presents the fundamental characteristics of the SDN paradigm and highlights the issues that need to be addressed to improve the reliability of different SDN-based networks and applications.

Background:

SDN is a network paradigm that provides enhanced accessibility in central management, programmability, and the interaction between control and data planes, as defined by slightly different perspectives in the literature [12]. This separation of planes is a

fundamental principle across network disciplines. Hardware reconfiguration provides core functionality, as it constitutes a basic requirement for successful networking.

SDN enables programmable and centralized control of the network [12], and this novel paradigm has significantly influenced network development and management. The fundamental concept is similar to storage and computing resources, representing a logically centralized control plane, while the devices in the data plane include the packet-forwarding elements. Figure 1 illustrates a basic SDN architecture, which is divided into three planes as follows.

Data Plane:

The data plane is responsible for the implementation of various processing functions, such as packet buffering and retransmission of queued packets, on every packet.

Control Plane:

The control plane manages all possible situations and procedures, including the configuration and management of forwarding tables in the data plane. It also facilitates the exchange of local routing information with global routing information. High-level programming languages are typically used to implement control plane functionality, while more complex control programs run without extensive manual optimization.

Application Plane:

The application plane encompasses applications where high-level management policies, such as security, monitoring, and routing, are specified.

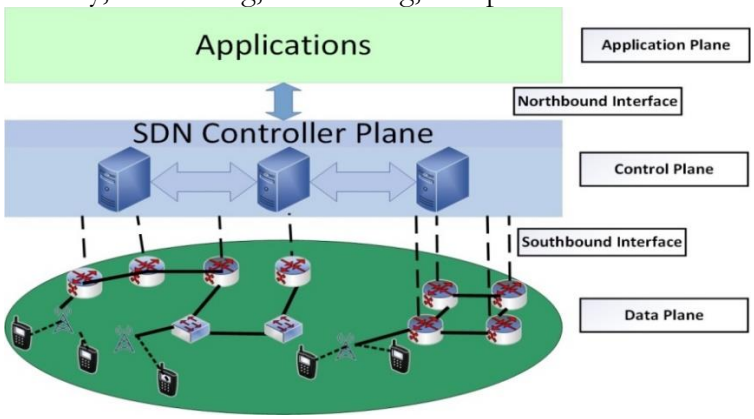

Figure 1. Software Defined Networks enabled networking architecture.

Reliability Issues:

Reliability has been a key concern, and implementing SDN architecture enhances both network reliability and flexibility. It automates the processes that previously required human intervention. Retrospective analyses over the past few decades have identified the first decade of data networking as predominantly decentralized and distributed. During the second period, the Internet and LANs were dominated by TCP/IP. Figure 2 shows why there is a need to maintain reliability during the transformation to SDN. The third era of data networking is characterized by a split between distributed protocols and centralized approaches, covering both private and local networks. This split is primarily due to two factors: the distributed nature of control and the emergence of data centers. The distributed nature of networking intelligence has been highly effective, whereas an Internet with a single central control point cannot scale in today's environment. Therefore, the reliability of the Internet is crucial due to the lack of a central point of control. The notion of completely centralizing the Internet is widely considered impractical. Meanwhile, data centers are facilities used to integrate components (e.g., telecommunication and storage systems) as they host virtual servers. Their commercial success has achieved remarkable levels of responsiveness and reliability.

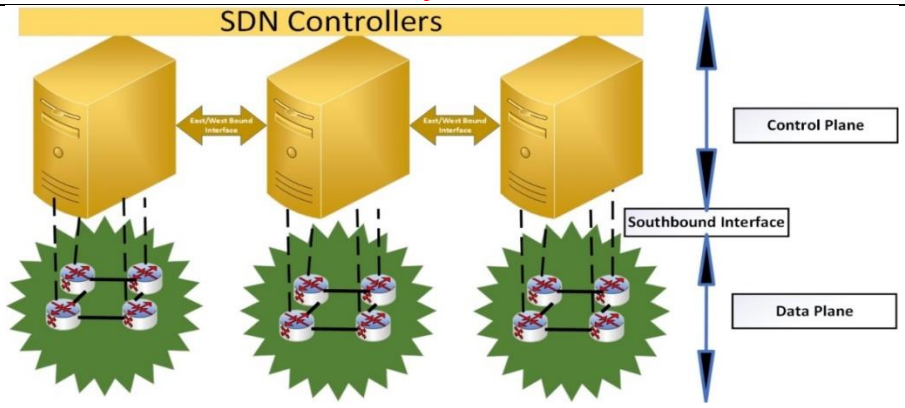

Figure 2. Data usage and virtualization goals.

Implementing SDN requires fundamental changes in the underlying technology to improve its performance, and achieving reliability can be challenging Although SDN is a promising solution for IT, its challenges vary depending on whether a centralized or distributed controller architecture is implemented (Figure 3). The effectiveness of the controller may be impaired by propagation delays, although a centralized approach has certain inherent reliability advantages in a centralized architecture, a single controller manages the entire network, which may collapse if that controller fails. To address this issue, organizations should optimize controller functions to enhance network reliability efficiently. The SDN controller should support multipath routing to improve fault tolerance. A feature comparison of both centralized and distributed controller architectures is given in Table 2.

Central controller-based SDN architecture.

Distributed controller-based SDN architecture.

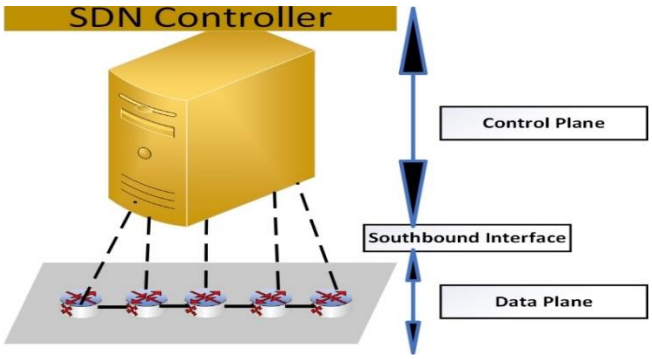

Figure 3: Central and distributed controller-based SDN architecture.

Table 1. Comparative view of centralized and distributed Controller Architecture.

Feature	Centralized Controller	Distributed Controller Architecture
Reliability	It has low reliability due to a single point of failure	It has High fault tolerance & redundancy due to a distributed architecture.
Scalability	Limited	Highly scalable
Failover Time	High	Low
Complexity	Deployment is simple	Synchronization is a little bit complex
Suitability	Small-scale networks	Industrial Internet of Things, B5G, Large-scale data center.

Everyone aims to use the network more efficiently based on load and demand by directing traffic dynamically. The challenge in achieving this lies in ensuring high network reliability. Hence, a distributed controller is preferable to a centralized controller when reliability is a critical concern. SDN does not inherently enhance the physical reliability of network equipment; its effectiveness depends on stable communication between the

controller and nodes. Its effectiveness largely depends on stable communication between the controller and network nodes, which provides an ideal means to achieve reliable OpenFlow communication.

SDN-Based Network Reliability:

Reliability is a key aspect of SDN, encompassing the system's ability to handle failures and notify relevant components or users. This term is defined as a combination of physical reliability, software reliability, and the effectiveness of protocols for network equipment, switches, controllers, and broken links, respectively. Service providers deploy reliable applications that notify end-users of delivery failures. [13]. SDN specifications primarily ensure data delivery to intended recipients through reliable protocols and architecture. Improving reliability is of vital importance because disconnections between the forwarding and control planes can easily occur due to network failures. A reliable SDN must have sufficient workload capacity to handle messages from the control and data planes without loss. The control plane, being the brain of the production network, is crucial for SDN-based network reliability. The hierarchical scheme for SDN-based reliability is shown in Figure 4.

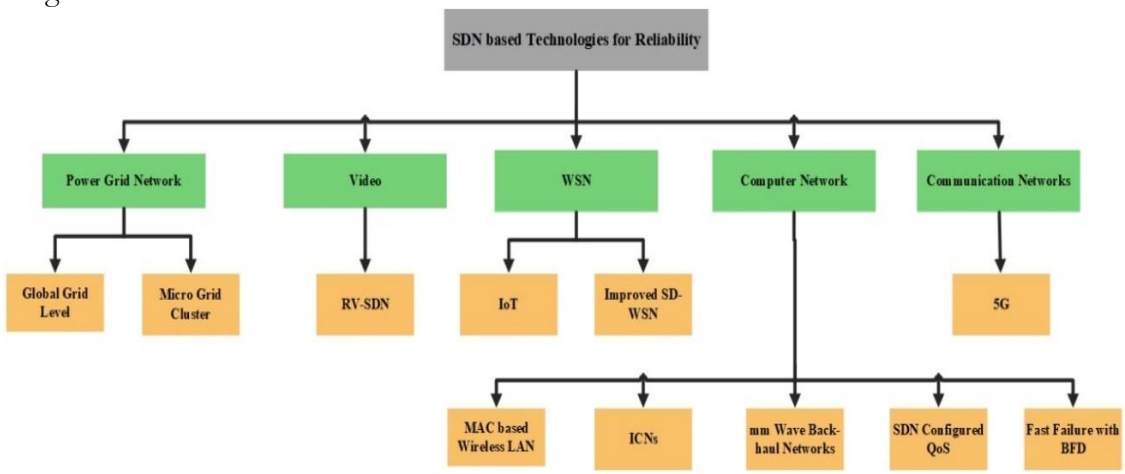

Figure 4. SDN-based technologies for reliability.

Reliability is a key design feature of network architectures, as discussed in the Background and Reliability section. For example, some researchers [14] proposed an improved gateway failure restoration mechanism to enhance resiliency in Universal Mobile Telecommunication System (UMTS) networks. Moreover, another study provided analytical models [15] for evaluating the reliability of UMTS networks at various stages. This work demonstrated that incorporating fault tolerance mechanisms into such networks can achieve substantial gains in network reliability. Another research effort based on LTE/EPC networks [16][17] highlights the critical concern of base station (BS) resiliency. Problems in conventional networks can, to some extent, be addressed through SDN technology. These advancements can be extended to wireless sensor networks (WSNs), vehicles, video streaming, 5G networks, power grid (PG) networks, and computer networks. Such developments improve network reliability and optimize network topology within industrial environments. Connectivity refers to networks' ability to guarantee proper data packet delivery, supported by mechanisms such as mobile tunnels and header compression. Mobile operators may experience considerable strain due to any network equipment failure within the Long-Term Evolution (LTE) packet core, potentially leading to temporary service outages [17]. Furthermore, these outages may result in significant penalties, affecting user experience and revenue. Therefore, reliability in the data plane [18] can be effectively improved when the SDN concept is applied in combination with LTE networks.

Fig. 5 shows an inverted pyramid representing technologies that are expected to play a predominant role in future Internet of Things (IoT) computing, as they have garnered significant attention from both industry and academia. The technologies below the IoT perimeter are considered the building blocks, while the technologies above are regarded as carriers of IoT. The SDN model should ideally be implemented using a top-down approach across these technologies. Recently, SDN has attracted considerable attention due to its many applications, though its adoption in IoT remains limited and under active development. Research and industrial communities are actively working on various projects [19] related to advancements in wireless sensor networks (WSNs). WSNs offer numerous benefits with broad applicability, including environmental monitoring, which is a vital aspect of IoT. However, hardware malfunctions can lead to node failures, which may affect WSN reliability.

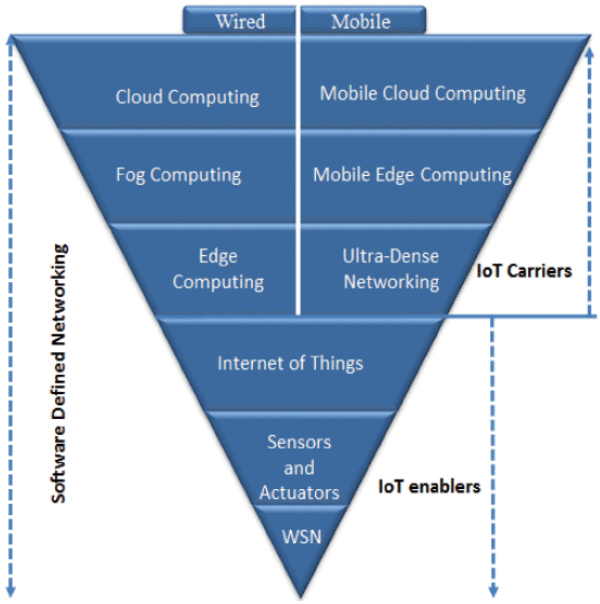

Figure 5. SDN enabled Network computing technologies [20]

WSN has been a great platform for personal wireless networks with a short range of communication. The SDN approach to WSN, called SD-WSN [21], alleviates most of the challenges in WSN and also plays a role in advancing the IoT paradigm. However, wireless channel conditions can still impact network reliability, even when data and control planes are tightly coupled in conventional networks. This can significantly impact network management, increasing both complexity and cost. Some authors in [22][23] proposed a framework that employs an edge computing layer to achieve high reliability for IoT applications. Therefore, SDN has been introduced to enhance WSNs, and a framework called the Improved Software-Defined Wireless Sensor Network (Improved SD-WSN) has been proposed to address challenges such as large-scale heterogeneous networks. It also targets the network coverage problem [24] and resolves it by improving network reliability. Lastly, this framework addresses node failures occurring due to energy consumption-related issues. Hence, optimizing WSN reliability requires developing schemes to reduce energy consumption and delay of network nodes in IIoT environments. Applications designed for IoT have to face many challenges, such as security, high availability, and high reliability.

Limited research has investigated frameworks for communication networks from a global perspective to design reliable and open networks. Currently, much attention has been paid to SDN. Thus, an effective and reliable network framework [25][26] has been proposed. This framework is capable of abstracting the control plane from the data plane using an external software controller. To attain the targeted goal, researchers have designed and

constructed the smart energy Internet with a microgrid cluster and a global-grid-level SDN framework in a hierarchical manner. This scheme provides efficiency, flexibility, and reliability to the power grid network. Another work has been proposed using SDN-enabled technologies (SDN-configured QoS [27] and fast failover combined with BFD [28]). These technologies improve the reliability of packet transmission for many kinds of computer networks.

Table 2. SDN-Based Schemes on Reliability.

Scheme	Description	Application	Reliability	Reference
DL-SDN	It offers the management and reliability of WSN. Also, it solves the network coverage problem.	WSN, Adaptive Industrial Environment IIoT	✓	[1]
5G-VANET	It incorporates fault tolerance to enhance the reliability and survivability of the UMTS network for network connectivity guarantee.	All-IP UMTS network, CDMA 2000	✓	[7]
SDN-enabled communication network	It provides latency, security, and reliability of communication networks.	Power Grids and Energy Operators	✓	[8]
RVSDN	It builds on previous work (e.g., VSDN) to provide QoS for video applications that need delay, jitter, and bandwidth.	Video applications	✓	[11]
CTMS with exponential distribution	It reveals the network recovery time by improving its reliability.	Cellular networks	✓	[17]
Resiliency Measurement Method	It measures the resiliency of BS deployment for network operators.	BSs, network operators, and planners	X	[18]
SD-WSN	It alleviates most of the challenges and ultimately fosters efficiency in WSN.	IoT	✓	[20]
Fog computing with SDN	It offers a framework for IoT applications to improve reliability.	Latency-sensitive IoT applications	✓	[23]
Improved GGSN Failure Restoration Mechanism	It reduces the network delay and signalling cost for the restoration of corrupted PDP context.	(UMTS)	X	[29]
VSDN	It makes an optimum path selection through a global network view, but has Linear-Message complexity.	Video applications.	X	[30]
RDSDN	The coordinator selects the controller with the highest reliability rate to assign the switches based on a global network view.	Video applications		[31]
SDN-based controller placement algorithm	It maximizes the network average reliability by addressing the problem of controller placement.	WSNs	✓	[32]

SDN-Enabled Traffic Control Algorithm	It facilitates the reliability in ICNs and mm Wave backhaul networks.	Computer Networks	✓	[33]

Best QoS is only possible if the paths are reliable to meet application requirements. Ensuring end-to-end QoS demands the network to select the feasible path in terms of delay, jitter, and bandwidth for video applications. Hence, determining the most reliable path (MRP) is a well-known issue between two nodes in a network. For this, Video over Software Defined Networking (VSDN) [30] ensures the optimum path selection by using a global network view but has a complexity of linear messages. The authors in [34] ensure the material delivery after a natural disaster by using MRP. They select the reliable path of higher reliability by providing the three shortest path algorithms (e.g., depth-first search) to compute the reliability. But the disadvantage is that it is limited in execution time

In contrast, Reliable Video over SDN (RVSDN) does not assume a natural disaster. This scheme is built upon previous video research (i.e., VSDN) merged with SDN for addressing and finding the issues related to the most reliable paths in a network. As the role of the centralized controller in SDN is very important, some researchers in [31] proposed a novel method called "Reliable Distributed SDN (RDSDN)" to find the reliability rate of each subnetwork, which depends on load, degree of nodes, and loss rate of links. The East/West-bound interface is used to share the reliability rates among the controllers. Thus, the controller's failure may trigger a fast recovery scheme to replace it. RDSDN is more reliable because it selects the controller with the highest reliability rate. It also considers metrics such as load, topology, distance, and link probability when computing reliability, thereby improving the switch-to-controller latency during recovery. The main objective of this proposed RDSDN is to manage the reliability based on SDN.

Some authors in [32] discuss the controller placement problem to maximize the network average reliability under the assumption of the shortest path between controllers and switches. Another research has been carried out on SDN-enabled resiliency in computer networks [33]. Such a scheme is enabled for proactive failure recovery, providing the reliability needed by ICNs and mm Wave backhaul networks. It also looks at split MAC-based wireless LANs and how to improve traffic control algorithms for SDN to optimize connection reliability. An extensive work has been targeted on reliability for various applications, as illustrated in Table 3.

Challenges:

A number of promising research areas should be explored to address the limitations in existing SDN-based reliability networks and to extend them further. This paper concludes with a discussion of directions for existing reliability challenges.

The network topologies should be validated and configured intelligently by the SDN controller to enhance network availability [35]. This intelligence makes the SDN controller susceptible to a single point of failure [36][37] due to the brain-split issue. Network traffic routes through alternative devices in case of the failure of one or more network devices to maintain flow continuity in legacy networks. The entire network may fail because the central controller is solely responsible for the SDN architecture, and in the absence of a standby controller. Thus, clustering of two or more SDN controllers can be enabled in an active-standby mode to maintain memory synchronization. The study in [38] reveals that, in the event of a controller failure, network traffic will be interrupted by a centralized controller, mitigated through a distributed architecture called "SiBF" that involves an army of rack managers (RMs). As a result, another standby controller (RM) handles flow requests when the master controller fails, whereas new backup flow entries are installed by SiBF in case of switch failures to route packets to their destinations. SDN controllers should support technologies (e.g., Multi-Chassis Link Aggregation Group (MC-LAG), Virtual Router

Redundancy Protocol (VRRP)) to increase network availability in case of path failures. A distributed algorithm operates through a load-balancing, multi-pathing technique that integrates central congestion and free multipathing in the event of controller failure. Reliability issues in a centralized architecture are also discussed in [39]. IT organizations should address this challenge by leveraging the main controller functions that enhance network reliability.

Different types of algorithms (such as intelligent optimization algorithms, artificial intelligence, the firefly algorithm, and machine learning algorithms) are of primary concern in key technologies and SDN-based WSN reliability. These algorithms can be applied gradually for dynamic network deployment, coverage optimization techniques, and node scheduling, making it more convenient for users to improve the reliability of SDN-based WSNs.

Current research indicates that the reliability of network hardware (such as nodes, routers, and switches) is considered an important factor, while reliability issues related to data collection, data transmission, and routing fault tolerance are also critical components in heterogeneous networks. Single-sink node mobility is considered when multiple sink nodes move simultaneously in heterogeneous WSN-based SDNs. Another important issue is prolonging the life cycle of a network to increase reliability. Establishing a joint optimization technique to enhance the performance of SDN-based networks is a challenging task and should be explored in future research to improve network reliability.

One of the major challenges in SDN is securing the SDN controller that ensures network reliability. The SDN controller acts as the brain of the network, making it a high-value target for cyberattacks such as Distributed Denial of Service (DDoS). If the controller is compromised or overwhelmed, the entire network may experience service disruption.

Additionally, the communication between the controller and switches is commonly implemented through the OpenFlow protocol, which can be vulnerable to interception, spoofing, or man-in-the-middle attacks if not properly secured.

SDN introduces another set of reliability challenges due to the trade-off between power efficiency and fault tolerance. Network components, such as switches, routers, and links, can be put into a sleeping state when there is no traffic to reduce power consumption. However, this also lowers redundancy and removes backup routes, making the system more vulnerable to failure. If any node or link fails when other routes are also inactive, the recovery time can be increased. The unpredictability of traffic patterns and their dynamics makes it more difficult to make energy management decisions without affecting reliability. Also, the energy-optimization algorithms add overhead processing to the controller, which can impact its performance and responsiveness. Optimization has also become complicated due to the lack of standardized measures for comparison between the energy saving and reliability. In hybrid SDN environments that integrate legacy infrastructure, coordinated energy management becomes even more challenging, increasing the risk of instability and reduced network resilience.

Conclusion:

This paper summarizes the state-of-the-art developments in networks and evaluates the need for reliability. Currently, networks demand the implementation of the most feasible reliability concepts. Therefore, novel SDN-based techniques have been a major concern for academia and industry over the last decade. In this paper, we target the improvement of reliability through the incorporation of SDN-based techniques into various systems and applications (e.g., 5G, video streaming, WSNs, and more). SDN solutions should be proposed and implemented as a means to meet the reliability demands of different networks and beyond. Generally, this paper reviews existing reliability issues and challenges, providing insights into various networks. Specifically, this research summarizes several significant studies and informs scientists of the latest trends in the domain. This work opens avenues

for future research focused on investigating SDN-based methods and strategies to enhance reliability. Massive efforts will be required for the future realization of networks in companies, laboratories, and industries. Although a few research works have been identified in the literature, further research is needed on SDN-based reliability issues.

Acknowledgement: We extend our heartfelt gratitude to Dr. Nisar Ahmed, who played an important role in improving the research article. Also, the manuscript has not been published or submitted to other journals previously.

Author's Contribution: M.U. Younus: Conceptualization, critical review, proposed architecture, and manuscript writing.

K. Safdar: Critical review, proposed architecture, and manuscript proofreading.

H. M. Awan: Manuscript formatting and refinement.

Conflict of Interest: The authors declare no conflict of interest.

References:

[1] Rajasekhar Chaganti, Wael Suliman, "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks," *Information*, vol. 14, no. 1, p. 41, 2023, [Online]. Available: https://www.mdpi.com/2078-2489/14/1/41

[2] Sarvesh Tanwar, Sumit Badotra, Harish Garg, "Blockchain and Software Defined NetworkingOpportunities, Challenges, and Future Trends," *Routledge*, 2026, [Online]. Available: https://www.routledge.com/Blockchain-and-Software-Defined-Networking-Opportunities-Challenges-and-Future-Trends/Tanwar-Badotra-Garg/p/book/9781032824369

[3] Ali Sadiqui, Moulay Rachid Filali, "Fundamentals of Software-Defined Networking Towards Intelligent and Flexible Networks," *Routledge*, 2026, [Online]. Available: https://www.routledge.com/Fundamentals-of-Software-Defined-Networking-Towards-Intelligent-and-Flexible-Networks/Sadiqui-Filali/p/book/9781041154280

[4] Suheib Alhiyari, Siti Hafizah AB Hamid, Nur Nasuha Daud, "A Survey of Link Failure Detection and Recovery in Software-Defined Networks," *Comput. Mater. Contin.*, vol. 82, no. 1, pp. 103–137, 2025, [Online]. Available: https://www.sciencedirect.com/org/science/article/pii/S1546221825000256

[5] M. Gharbaoui, C. Contoli, G. Davoli, D. Borsatti, G. Cuffaro, F. Paganelli, W. Cerroni, P. Cappanera, B. Martini, "An experimental study on latency-aware and self-adaptive service chaining orchestration in distributed NFV and SDN infrastructures," *Comput. Networks*, vol. 208, p. 108880, 2022, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128622000822

[6] Shahnawaz Ahmad, Iman Shakeel, Shabana Mehfuz, Javed Ahmad, "Deep learning models for cloud, edge, fog, and IoT computing paradigms: Survey, recent advances, and future directions," *Comput. Sci. Rev.*, vol. 49, p. 100568, 2023, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1574013723000357

[7] Ankit Bisht, Vandana Khaitan Nee Gupta, "Reliability analysis of 5G-VANET using cloud-fog-edge based architecture," *RAIRO - Oper. Res.*, vol. 58, 2023, [Online]. Available:https://www.researchgate.net/publication/376644954_Reliability_analysis_of_5G-VANET_using_cloud-fog-edge_based_architecture

[8] Sandipan Rakeshkumar Mishra, Bharanidharan Shanmugam, "SDN-Enabled IoT Security Frameworks—A Review of Existing Challenges," *Technologies*, vol. 13, no. 3, p. 121, 2025, [Online]. Available: https://www.mdpi.com/2227-7080/13/3/121

[9] Q. Long, Y. Chen, H. Zhang, and X. Lei, "Software Defined 5G and 6G Networks: a Survey," *Mob. Networks Appl. 2019 275*, vol. 27, no. 5, pp. 1792–1812, Nov. 2019, doi: 10.1007/s11036-019-01397-2.

[10] P. Chavan and P. Chavan, "Automation of AD-OHC Dashbord and Monitoring of Cloud Resources using Genrative AI to Reduce Costing and Enhance Performance,"

2024 Int. Conf. Innov. Challenges Emerg. Technol. ICICET 2024, 2024, doi: 10.1109/ICICET59348.2024.10616299.

[11] S. Paramasivam and R. Leela Velusamy, "Quality of service aware routing in software defined video streaming: a survey," *Peer-to-Peer Netw. Appl. 2023 164*, vol. 16, no. 4, pp. 1739–1760, May 2023, doi: 10.1007/s12083-023-01484-y.

[12] B. K. Balasubramanian, K. P. Kumar, S. Sriramulu, and T. Chandrasekar, "Software-defined vehicular networks: adaptive QoS path selection for Per-OpenFlow data enhancement," *J. Supercomput. 2026 822*, vol. 82, no. 2, pp. 78-, Jan. 2026, doi: 10.1007/s11227-025-08203-9.

[13] V. P. Bijlwan and N. Kumar, "Deep Reinforcement Learning in Software Defined Networking: A Survey, Research Challenges, and Future Perspectives," *IEEE Commun. Surv. Tutorials*, 2026, doi: 10.1109/COMST.2026.3656733.

[14] André Souza, Marco Quagliotti, "A Generalized Cost Model for Techno-Economic Analysis in Optical Networks," *Photonics*, vol. 13, no. 2, p. 125, 2026, [Online]. Available: https://www.mdpi.com/2304-6732/13/2/125

[15] V. Scotti, D. Perez-Palacin, V. Brauzi, V. Grassi, and R. Mirandola, "Antifragility via Online Learning and Monitoring: An IoT Case Study," *Proc. - 2025 IEEE Int. Conf. Auton. Comput. Self-Organizing Syst. ACSOS 2025*, pp. 54–63, 2025, doi: 10.1109/ACSOS66086.2025.00022.

[16] "Exploring and Addressing the Vulnerabilities of Multimedia Services Over Mobile Networks : From Devices to Infrastructure." Accessed: Feb. 21, 2026. [Online]. Available: https://d.lib.msu.edu/etd/52469?__goaway_challenge=header-refresh&__goaway_id=6016e07b0087be3dff93b406a2c98e71&__goaway_referer=https%3A%2F%2Fd.lib.msu.edu%2F

[17] Vladimir Shakhov, Nikolai Shakhov, "Novel Continuous-Time Markov Chain-Based Model for Performance Analysis of Hybrid Free Space Optics and Radio Frequency Communications," *Appl. Sci*, vol. 15, no. 4, p. 1935, 2025, [Online]. Available: https://www.mdpi.com/2076-3417/15/4/1935

[18] S. Bi *et al.*, "Resilience and Failure Analysis in Next-Generation Communication Networks: A Contemporary Survey," *IEEE Trans. Netw. Sci. Eng.*, vol. 13, pp. 2793–2821, 2026, doi: 10.1109/TNSE.2025.3620950.

[19] David Olufemi, Ayodeji Olutosin Ejiade, Friday O. Ikwuogu, Phebe E Olufemi, "Securing Software-Defined Networks (SDN) Against Emerging Cyber Threats in 5G and Future Networks -A Comprehensive Review," *Int. J. Eng. Technol.*, vol. 14, no. 2, 2025, [Online]. Available: https://www.researchgate.net/publication/389946028_Securing_Software-Defined_Networks_SDN_Against_Emerging_Cyber_Threats_in_5G_and_Future_Networks_-A_Comprehensive_Review

[20] Pejman A. Karegar, Duaa Zuhair Al-Hamid, Peter Han Joo Chong, "UAV-enabled software defined data collection from an adaptive WSN," *Wirel. Networks*, vol. 31, pp. 69–90, 2025, [Online]. Available: https://link.springer.com/article/10.1007/s11276-024-03744-y

[21] N. B. Raut and S. Thangavelu, "Energy-Efficient Sleep Wake-Up Mechanism Based Routing Protocol Using Siamese Network and Optimized Fuzzy Interference System in Green IoT," *Int. J. Commun. Syst.*, vol. 38, no. 13, p. e70193, Sep. 2025, doi: 10.1002/dac.70193.

[22] B. Ramesh, C Mahesh, R. Sabitha, V.Priya, "Advances in Software-Defined Wireless Networks (SDWN): Solutions for Flexible and Scalable Communication," *Natl. J. Antennas Propagation,* vol. 7, no. 1, 2025, [Online]. Available: https://antennajournal.com/index.php/antenna/article/view/177

[23] A. Rahman *et al.*, "Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions," *Int. J. Commun. Syst.*, vol. 38, no. 1, p. e5429, Jan. 2025, doi: 10.1002/dac.5429.

[24] O. A. Razzaq, "Enhancing IoT-based wireless sensor network security with cryptographic techniques," *J. Discret. Math. Sci. Cryptogr.*, vol. 28, no. 4-A, pp. 1117–1130, Jun. 2025, doi: 10.47974/JDMSC-2102.

[25] Y. Bian, J. Cao, C. He, F. Liu, and Y. Guo, "Review of research on network reliability from the perspective of management science," *IET Conf. Proc.*, vol. 2025, no. 35, pp. 302–310, Dec. 2025, doi: 10.1049/icp.2025.3424.

[26] Radheshyam Singh, Line M.P. Larsen, "Enabling Green Cellular Networks: A Review and Proposal Leveraging Software-Defined Networking, Network Function Virtualization, and Cloud-Radio Access Network," *Futur. Internet*, vol. 17, no. 4, p. 161, 2025, [Online]. Available: https://www.mdpi.com/1999-5903/17/4/161

[27] Lakhal, H., Zegrari, M., Bahnasse, A, "Next-Generation Smart Grid Cybersecurity: A Systematic Review of OT Cyber Threats, AI-Driven Defense, Cyber Deception Techniques, and Emerging Security Strategies," *IEEE Access*, 2025, [Online]. Available: https://ieeexplore.ieee.org/document/11208597

[28] K. D. Umakant Kulkarni, "Maestro: QoE-Aware Dynamic Resource Allocation in Wi-Fi Networks," *Proc. ACM Netw.*, vol. 3, no. 1, pp. 1–24, 2025, [Online]. Available: https://dl.acm.org/doi/10.1145/3709371

[29] J. Poorvi, A. Kalita, and M. Gurusamy, "Reliable and Efficient Data Collection in UAV-Based IoT Networks," *IEEE Commun. Surv. Tutorials*, vol. 28, pp. 2531–2571, 2026, doi: 10.1109/COMST.2025.3550274.

[30] Harold Owens, Arjan Durresi, "Video over Software-Defined Networking (VSDN)," *Comput. Networks*, vol. 92, no. 2, pp. 341–356, 2015, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128615003199

[31] S. Moazzeni, M. R. Khayyambashi, and N. Movahhedinia, "Improving the Reliability of Software-Defined Networks with Distributed Controllers Through Leader Election Algorithm and Colored Petri-Net," *Wirel. Pers. Commun.*, vol. 109, no. 1, pp. 645–656, Nov. 2019, doi: 10.1007/S11277-019-06583-9.

[32] M. Farhan, L. Wang, N. Shah, H. Sidaq, B. Khan, and G. M. Muntean, "ReCAP: Reliability–Capacity Aware Joint Controller Placement and Routing Using a Hybrid AI Approach," *IEEE Trans. Reliab.*, vol. 74, no. 4, pp. 5686–5700, 2025, doi: 10.1109/TR.2025.3585239.

[33] Ahmad Jalili, "Enhancing Software-Defined Networking (SDN) Resilience against Cyberattacks: A Markov Model-Based Approach," *Int. J. Web Res.*, vol. 8, no. 2, 2025, [Online]. Available: https://ijwr.usc.ac.ir/article_221374.html

[34] C. H. Huang, K. H. Chang, C. H. Liu, T. Y. Chang, and Y. K. Lin, "Network reliability analysis on casualty rescue for natural disaster evaluation," *Ann. Oper. Res. 2023 3481*, vol. 348, no. 1, pp. 399–419, Feb. 2023, doi: 10.1007/s10479-023-05226-4.

[35] P. Ohri, A. Daniel, S. G. Neogi, and S. K. Muttoo, "Blockchain-based security framework for mitigating network attacks in multi-SDN controller environment," *Int. J. Inf. Technol. 2024 179*, vol. 17, no. 9, pp. 5591–5603, Jun. 2024, doi: 10.1007/s41870-024-01933-8.

[36] S. Troia, L. Borgianni, G. Sguotti, S. Giordano, and G. Maier, "A Comprehensive Survey on Software-Defined Wide Area Network," *IEEE Commun. Surv. Tutorials*, vol. 28, pp. 2805–2845, 2026, doi: 10.1109/COMST.2025.3594678.

[37] T. Darwish, T. A. Alhaj, and F. A. Elhaj, "Controller placement in software defined

emerging networks: a review and future directions," *Telecommun. Syst. 2025 881*, vol. 88, no. 1, pp. 18-, Jan. 2025, doi: 10.1007/s11235-024-01252-0.

[38] Q. M. Nguyen and E. Modiano, "Optimal Control for Distributed Wireless SDN: Theory and Architecture," *IEEE Trans. Netw.*, vol. 33, no. 5, pp. 2131–2147, 2025, doi: 10.1109/TON.2025.3560605.

[39] J. Li, F. De Marchi, Y. Lei, R. Joshi, B. Chandrasekaran, and Y. Xia, "Unlocking Diversity of Fast-Switched Optical Data Center Networks With Unified Routing," *IEEE Trans. Netw.*, vol. 34, pp. 33–48, 2026, doi: 10.1109/TON.2025.3590083.