

A Brief Review on Various Routing Algorithms and its Issues

Randhir Kumar¹, Dr. Harsh Lohiya², Mr. Manoj Kumar Yadav³

Research Scholar¹, Associate Professor², Assistant Professor³

Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India

Abstract: Routing algorithms are fundamental to the efficient and reliable transmission of data across computer networks, as they determine suitable paths for forwarding packets between source and destination nodes. This paper provides a comprehensive review of routing algorithms, emphasizing their underlying principles, classifications, challenges, recent developments, and practical applications in modern communication networks. It begins by examining the importance of routing and the historical evolution of routing techniques, highlighting the transition from conventional approaches to advanced and adaptive methods. Major categories, including distance-vector, link-state, and path-vector algorithms, are discussed in detail, along with hybrid techniques that combine the strengths of multiple routing paradigms. The paper further investigates key challenges such as routing loops, scalability, convergence, network dynamics, and resource constraints. Recent research trends and advancements aimed at improving routing efficiency, reliability, scalability, and adaptability are also explored. Overall, the study provides a consolidated understanding of routing algorithms and their continuing role in addressing the demands of increasingly complex and dynamic computer networks.

Keywords: A brief review on various routing algorithms and its issues

I. INTRODUCTION

The rapid expansion of computer networks has made efficient and reliable data transmission essential for effective communication and information sharing. A key component of this process is the use of routing algorithms, which determine appropriate paths for transferring data packets from their source to their intended destination. These algorithms play a fundamental role in network operation by managing packet forwarding and optimizing the utilization of available network resources. Therefore, a clear understanding of routing algorithms is essential for analyzing how modern networks achieve connectivity, efficiency, reliability, and effective data delivery.

The primary aim of this research paper is to present a comprehensive study of routing algorithms used in computer networks. The study examines their historical development, fundamental concepts, classifications, operational principles, limitations, recent technological advancements, practical applications, and potential future directions. By bringing these aspects together, the paper provides a structured overview of routing techniques and highlights their importance in the design and management of contemporary network infrastructures.

Routing algorithms have evolved significantly alongside the development of computer networking technologies. Early routing approaches relied on relatively simple mechanisms, whereas modern techniques employ sophisticated strategies to accommodate large-scale, dynamic, and heterogeneous networks. Traditional distance-vector protocols, such as Routing Information Protocol (RIP), established important foundations for distributed routing, while link-state protocols, including Open Shortest Path First (OSPF), introduced more advanced mechanisms for topology awareness and path selection. This progression demonstrates the continuous efforts to improve routing performance, scalability, adaptability, and reliability.

Despite substantial advances, routing algorithms continue to encounter several challenges that can affect network performance and stability. Problems such as routing loops, slow convergence, excessive control overhead, scalability limitations, and security threats remain important concerns in network environments. Furthermore, the increasing



complexity and dynamic nature of modern networks require routing mechanisms to respond efficiently to changing traffic conditions, failures, and resource availability. Addressing these issues remains an active area of research, encouraging the development of more robust and intelligent routing strategies.

Recent developments in networking have introduced new opportunities for improving routing performance. Emerging approaches based on machine learning and artificial intelligence can support adaptive routing decisions by analyzing network conditions and traffic patterns. Similarly, Software-Defined Networking (SDN) provides centralized and programmable network control, enabling flexible management of routing operations. Blockchain-based approaches have also attracted attention for enhancing trust, security, and transparency in distributed networking environments. The integration of these technologies with conventional routing mechanisms has the potential to improve network efficiency, resilience, security, and adaptability.

This research paper provides a comprehensive perspective on routing algorithms through theoretical analysis, comparative discussion, and examination of practical applications. It considers the evolution and classification of routing techniques while also investigating their underlying principles, limitations, and emerging developments. By evaluating both conventional and contemporary approaches, the study aims to provide a clearer understanding of the role of routing algorithms in modern computer networks and the opportunities for developing more efficient, secure, scalable, and intelligent routing solutions.

II. LITERATURE REVIEW

Routing algorithms constitute a fundamental element of computer networking, as they determine the paths through which data packets are transmitted between source and destination nodes. With the continuous growth and diversification of network infrastructures, researchers have extensively investigated methods for designing, evaluating, and improving routing algorithms to address changing performance, scalability, reliability, and security requirements. This section reviews the existing research on routing algorithms, with particular emphasis on their classification, performance assessment, major challenges, and emerging technological developments.

Algorithm Classification

Initial research in routing primarily concentrated on developing efficient methods for route calculation and packet forwarding. Algorithms such as Bellman-Ford, Dijkstra's algorithm, and distance-vector techniques established the theoretical foundation for modern routing protocols. As computer networks became larger and more complex, researchers introduced advanced routing mechanisms capable of maintaining network connectivity and selecting efficient paths under changing conditions. Link-state protocols, including OSPF and IS-IS, use information about network topology to calculate suitable routes, whereas path-vector protocols such as BGP employ path-related information to support routing between autonomous systems. These approaches differ in their route-selection mechanisms, information exchange procedures, computational requirements, and scalability, making them suitable for different network architectures and operational environments.

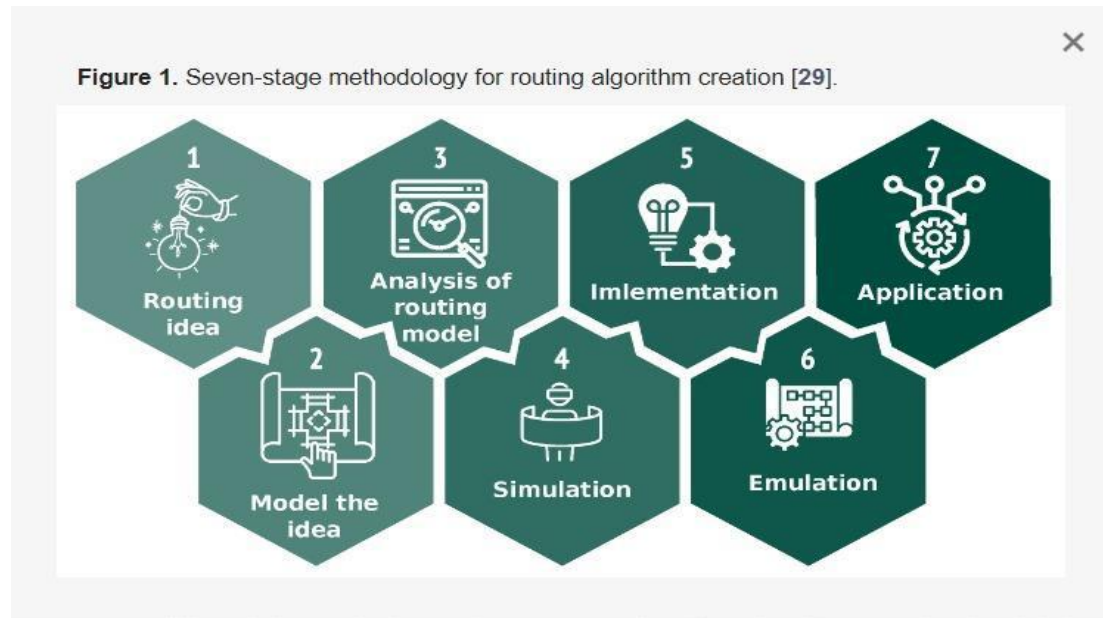
Performance Evaluation

Performance evaluation has received considerable attention in routing research because the effectiveness of a routing algorithm depends on its ability to deliver data efficiently under different network conditions. Common evaluation parameters include convergence time, routing overhead, routing table size, throughput, packet delivery ratio, latency, computational complexity, and resource consumption. Researchers frequently conduct comparative analyses to examine the strengths and limitations of different routing techniques with respect to scalability, reliability, adaptability, and network resource utilization. Network simulation platforms such as ns-3 and OPNET have also been widely used to model diverse network scenarios and evaluate routing behavior under controlled and realistic conditions. Such evaluations help researchers identify performance bottlenecks and determine the suitability of routing algorithms for specific network environments.



Challenges

Although routing technologies have advanced considerably, several challenges continue to affect their performance and reliability. Routing loops, packet black-holing, route oscillations, and excessive routing overhead can negatively influence network stability and data delivery. Changes in network topology, link failures, and frequent route updates may further create convergence problems and result in inconsistent routing information among network nodes. In addition, security threats such as route hijacking, malicious route advertisements, and denial-of-service attacks introduce significant risks to routing infrastructure. These challenges become more pronounced in large-scale and highly dynamic networks, where routing decisions must be made rapidly while maintaining accurate and secure network information. Consequently, developing adaptive, scalable, and secure routing mechanisms remains an important area of research..



Emerging Trends

Recent advances in artificial intelligence and networking technologies have created new opportunities for enhancing routing algorithms. Machine learning techniques, including reinforcement learning and neural-network-based models, are increasingly being investigated for intelligent route selection, traffic prediction, and adaptive network optimization. Software-Defined Networking (SDN) provides centralized and programmable network management, allowing routing policies and traffic flows to be dynamically configured according to current network conditions. In addition, blockchain-based approaches are being explored to improve the security, integrity, and trustworthiness of routing information, particularly in distributed and decentralized environments. The integration of these technologies with conventional routing mechanisms offers promising possibilities for developing routing systems that are more intelligent, adaptive, secure, scalable, and resilient. These developments provide several potential directions for future research in the field of computer network routing.

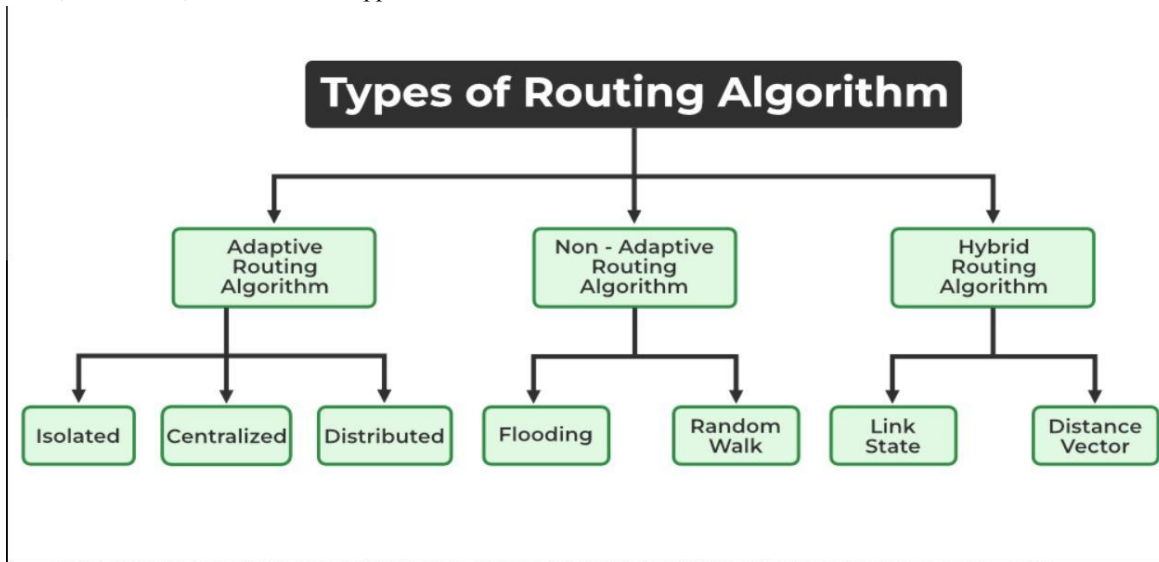
III. CLASSIFICATION OF ROUTING ALGORITHMS

Routing algorithms can be broadly categorized according to the way routing information is obtained, processed, and utilized for selecting paths. Based on their adaptability and decision-making mechanisms, routing algorithms can be classified into adaptive, non-adaptive, and hybrid approaches. Each category has distinct characteristics and is suitable for particular network conditions and requirements.



Adaptive Routing Algorithms

Adaptive routing algorithms dynamically modify routing decisions according to changes in network conditions. Factors such as link availability, congestion, delay, bandwidth, and network topology can influence the selection of forwarding paths. Based on the manner in which routing information is processed, adaptive routing can be further divided into isolated, centralized, and distributed approaches.



Isolated Adaptive Routing

In isolated adaptive routing, individual nodes independently select forwarding paths using information available locally. A node does not require a complete view of the network or continuous coordination with other nodes to make routing decisions. Instead, routing choices may be based on parameters such as hop count, link quality, delay, or the current status of neighboring links. Although this approach has relatively low communication overhead, its decisions may be less effective because each node has only limited knowledge of the overall network state.

Centralized Adaptive Routing

Centralized adaptive routing relies on a dedicated controller or central management entity to collect network-wide information and determine appropriate routing paths. The controller analyzes parameters such as topology, traffic conditions, link utilization, and network policies before generating routing decisions. These decisions are subsequently communicated to the participating network devices. Software-Defined Networking (SDN) is a prominent example of this approach, where a logically centralized controller can manage forwarding behavior according to global network objectives. Centralized routing can provide improved coordination and network-wide optimization, although controller availability, processing requirements, and communication overhead may become important considerations.

Distributed Adaptive Routing

Distributed adaptive routing allows multiple network nodes to participate in routing decisions without relying on a single centralized controller. Nodes exchange information with neighboring devices and independently update their routing knowledge based on the information received. Through repeated information exchange, the network gradually develops consistent routing information and determines suitable paths. Distance-vector and link-state routing protocols represent important examples of distributed routing. This approach provides greater resilience and avoids dependence on a single control point, although the exchange of routing information can introduce communication overhead and convergence-related challenges.



Non-Adaptive Routing Algorithms

Non-adaptive, or static, routing algorithms generally determine forwarding behavior without continuously responding to changes in network conditions. The routing decision remains relatively independent of current congestion, link utilization, or dynamic topology changes. These approaches are often simpler to implement and require fewer control resources, making them suitable for specific network environments.

Flooding

Flooding is a simple routing technique in which a received packet is forwarded through multiple available outgoing links, generally excluding the link from which the packet arrived. Consequently, several copies of the same packet may propagate through different portions of the network until the destination is reached. Flooding can provide high delivery reliability when network topology or destination paths are uncertain. However, unrestricted duplication can significantly increase network traffic, consume bandwidth, and cause congestion. Therefore, practical implementations often incorporate mechanisms such as hop limits, sequence numbers, or selective forwarding to control redundant transmissions.

Random Walk

Random walk routing forwards a packet by selecting the next-hop node randomly from the available neighboring nodes. The forwarding decision is not necessarily based on the destination, shortest path, or a comprehensive knowledge of network topology. Its decentralized nature makes it simple to implement and potentially useful in environments where routing information is limited. However, random path selection can result in unnecessarily long routes, increased transmission delay, and inefficient resource utilization, particularly in large or highly distributed networks.

Hybrid Routing Algorithms

Hybrid routing approaches integrate characteristics of different routing strategies to achieve a balance between computational efficiency, routing accuracy, scalability, and convergence. By combining complementary mechanisms, hybrid algorithms attempt to overcome some of the limitations associated with individual routing approaches.

Link-State Routing

Link-state routing protocols maintain information about the connectivity and status of links within a network. Routers exchange link-state information, allowing each participating router to construct a representation of the network topology. Once the topology information is available, a shortest-path algorithm, commonly Dijkstra's algorithm, can be applied to calculate appropriate routes to different destinations. Open Shortest Path First (OSPF) is a widely used example of a link-state routing protocol. Link-state techniques generally provide rapid adaptation to topology changes and accurate route computation, but maintaining and distributing topology information can generate considerable processing, memory, and communication overhead.

Distance-Vector Routing

Distance-vector routing determines routes by exchanging information about destination distances and next-hop directions among neighboring routers. Each router maintains a routing table containing information about reachable destinations and associated distance metrics. Periodic or triggered updates received from neighboring routers are used to revise these entries. Routing Information Protocol (RIP) is a well-known example that primarily uses hop count as its routing metric. Distance-vector methods are relatively simple and require less topology information than link-state techniques. However, they can experience slow convergence, routing loops, and the count-to-infinity problem, particularly in larger or rapidly changing networks.

Hybrid Routing Approach

Hybrid routing combines features of different routing paradigms to obtain improved performance across diverse network conditions. Such approaches may combine the local information exchange of distance-vector mechanisms with selected topology-awareness features associated with link-state routing. The objective is to achieve faster convergence, better scalability, reduced overhead, and improved route stability. Enhanced Interior Gateway Routing Protocol (EIGRP), for example, incorporates characteristics associated with both distance-vector and more topology-aware



routing mechanisms. Hybrid approaches can therefore provide a flexible alternative when neither purely distance-vector nor purely link-state routing adequately satisfies network requirements.

Issues in Routing Techniques

Routing techniques must address several challenges that can influence network efficiency, reliability, scalability, and security. These challenges become increasingly important as networks grow in size, experience frequent topology changes, and support diverse traffic requirements.

Routing Loops

A routing loop occurs when packets are repeatedly forwarded among two or more routers because of inconsistent, outdated, or incorrect routing information. Instead of progressing toward the intended destination, packets continue circulating within the network. Such behavior can consume bandwidth, increase transmission delays, and contribute to congestion. Persistent routing loops may also cause packet loss and significantly reduce the overall efficiency of the network.

Count-to-Infinity Problem

The count-to-infinity problem is primarily associated with distance-vector routing protocols. It occurs when routers incorrectly propagate information about an unreachable destination and gradually increase the metric associated with that destination. As neighboring routers repeatedly exchange incorrect information, the estimated distance may continue to rise until a predefined maximum metric is reached. This behavior can significantly delay convergence and temporarily destabilize routing decisions. Techniques such as split horizon, route poisoning, and hold-down mechanisms are commonly used to reduce the impact of this problem.

Routing Convergence

Routing convergence represents the process through which routers update their routing information and reach a consistent state after a change in network topology or link availability. Rapid convergence is important because inconsistent routing information during this period can cause packet loss, temporary loops, black-holing, or selection of inefficient paths. The convergence time of a routing protocol is therefore an important parameter when evaluating its responsiveness and reliability, particularly in dynamic networks.

Scalability

Scalability refers to the ability of a routing mechanism to operate effectively as the number of network nodes, links, and destinations increases. Routing protocols designed for small networks may generate excessive processing, memory, or communication overhead when applied to large-scale infrastructures. As the network expands, maintaining routing tables, exchanging updates, and calculating routes can become increasingly demanding. Scalable routing mechanisms must therefore minimize unnecessary overhead while maintaining accurate and timely routing information.

Security Vulnerabilities

Routing protocols can be exposed to a range of security threats that may compromise network operation and data transmission. Attacks such as route hijacking, spoofing, malicious route advertisements, and denial-of-service attacks can manipulate routing information or interfere with legitimate communication. An attacker may redirect traffic toward an unintended destination, disrupt connectivity, or create excessive routing overhead. Consequently, authentication, integrity protection, secure routing mechanisms, and effective detection techniques are essential for protecting routing infrastructure.

Routing Table Overflow

Routing table overflow can occur when the amount of routing information exceeds the available memory or processing capacity of a network device. This problem is particularly relevant in large-scale networks containing numerous destinations and frequently changing routes. Excessive routing entries can increase memory consumption and processing overhead, potentially resulting in packet drops, unstable route selection, or degraded forwarding performance. Effective route aggregation, hierarchical routing, filtering mechanisms, and appropriate resource management can help control routing-table growth and improve network stability.



IV. SUMMARY AND RESULTS

This research has presented a comprehensive examination of routing algorithms used in computer networks, with emphasis on their fundamental concepts, classification, operational characteristics, limitations, and emerging developments. Through an extensive review and analysis of existing research, the study has consolidated important findings related to the design, functionality, performance, and optimization of routing techniques.

- The analysis demonstrates that routing algorithms can be broadly categorized into adaptive, non-adaptive, and hybrid approaches. Adaptive routing techniques, including isolated, centralized, and distributed methods, modify routing decisions according to network conditions. Non-adaptive approaches, such as flooding and random walk, rely on relatively simple forwarding mechanisms without continuously responding to network-state changes. Hybrid approaches incorporate characteristics of multiple routing strategies to achieve improved performance, scalability, convergence, and resource utilization.
- The study also identifies several persistent challenges that influence the reliability and efficiency of routing mechanisms. Routing loops, slow convergence, scalability limitations, routing-table growth, and security threats can adversely affect network performance. These challenges become more significant in large, dynamic, and heterogeneous network environments. Consequently, routing protocols must incorporate mechanisms that can respond effectively to topology changes, reduce unnecessary overhead, maintain stable routes, and protect routing information from malicious activities.
- In addition, the review indicates that emerging technologies are creating new opportunities for improving conventional routing mechanisms. Machine learning and artificial intelligence can facilitate adaptive route selection and network-state prediction, while Software-Defined Networking (SDN) enables programmable and centralized control of routing operations. Blockchain-based mechanisms are also being investigated to strengthen trust, integrity, and security in routing information exchange. The integration of these technologies with established routing techniques could support the development of more intelligent, secure, scalable, and resilient network infrastructures.
- Overall, this research provides a consolidated perspective on routing algorithms by examining their principles, classifications, challenges, and technological developments. The findings emphasize that no single routing strategy is universally optimal; rather, the suitability of a routing algorithm depends on network topology, traffic characteristics, scalability requirements, resource availability, and security considerations. Future research should therefore focus on developing adaptive and intelligent routing frameworks capable of responding to increasingly dynamic network environments while maintaining high levels of efficiency, reliability, security, and scalability.

V. CONCLUSIONS

Routing algorithms are a fundamental component of modern computer networks, enabling reliable and efficient communication by selecting appropriate paths for the transmission of data packets. This research has provided a comprehensive review of routing algorithms, with particular emphasis on their fundamental concepts, classification, operational characteristics, challenges, and emerging developments. The study has consolidated findings from existing research to provide a structured understanding of the role and significance of routing mechanisms in contemporary networking environments.

The analysis demonstrates that routing algorithms can be broadly categorized into adaptive, non-adaptive, and hybrid approaches. Adaptive routing mechanisms dynamically modify routing decisions in response to changes in network conditions, such as topology, congestion, link availability, and traffic patterns. In contrast, non-adaptive techniques employ relatively simple and predetermined forwarding strategies, including flooding and random forwarding. Hybrid approaches integrate characteristics of multiple routing paradigms to achieve a suitable balance among routing efficiency, scalability, convergence, adaptability, and resource utilization. The selection of an appropriate routing approach depends largely on the characteristics, requirements, and constraints of the target network.



Despite significant developments in routing technologies, several challenges continue to affect network performance and reliability. Routing loops, slow convergence, scalability limitations, routing-table growth, and security vulnerabilities can lead to increased overhead, packet loss, latency, and network instability. These challenges become more prominent in large-scale, heterogeneous, and dynamic networks where routing information must be updated rapidly and accurately. Therefore, future routing mechanisms must be capable of adapting to changing network conditions while maintaining stable operation, efficient resource utilization, and strong security.

The study also identifies several emerging technologies that are influencing the development of next-generation routing solutions. Machine learning and artificial intelligence provide opportunities for intelligent route selection, traffic prediction, and adaptive network optimization. Software-Defined Networking (SDN) enables programmable and centralized management of network resources, allowing routing policies to be dynamically adjusted according to network requirements. Similarly, blockchain-based mechanisms offer potential benefits for improving the integrity, authentication, and trustworthiness of routing information, particularly in distributed environments. The integration of these technologies with conventional routing approaches may contribute to the development of more intelligent, secure, scalable, and resilient routing frameworks.

Overall, this research provides a consolidated perspective on routing algorithms and their continuing importance in computer networks. The findings indicate that there is no single routing algorithm capable of providing optimal performance under all network conditions. Instead, routing strategies must be selected and designed according to factors such as network topology, traffic characteristics, scalability, resource availability, reliability, and security requirements. Future research should focus on developing adaptive, intelligent, and secure routing frameworks that can efficiently respond to dynamic network environments. Such advancements can contribute significantly to improving the performance, reliability, scalability, and resilience of next-generation computer communication networks.

REFERENCES

1. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach Pearson.
2. Tanenbaum, A. S., & Wetherall, D. J. (2018). Computer Networks. Pearson Education.
3. Zhang, L., & Estrin, D. (2006). Route Science: Computational Challenges in the Routing Architecture of the Future Internet. IEEE Communications Magazine, 44(10), 134-141.
4. McQuillan, J. M., Richer, I., & Rosen, E. C. (1980). The New Routing Algorithm for the ARPANET. IEEE Transactions on Communications, 28(5), 711-719.
5. Moy, J. (1998). OSPF Version 2. RFC 2328.
5. Murphy, S., Badger, M., & Ooghe, S. (2008). The Border Gateway Protocol (BGP). RFC 4271.
6. Rosen, E. C., Viswanathan, A., & Callon, R. (2001). Multiprotocol Label Switching Architecture. RFC 3031.
7. Kong, J., Park, S. H., & Choi, H. J. (2018). A Survey on Software-Defined Networking. IEEE Communications Surveys & Tutorials, 20(2), 1091-1132.
8. Zhang, H., Hu, H., & Fan, J. (2019). Blockchain Technologies in Networking: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 21(4), 3798-3837.
9. Mao, Q., Zhang, J., & Letaief, K. B. (2021). Machine learning for intelligent end-to-end communication toward 6G: From network access, routing to traffic control and streaming adaptation. IEEE Journal on Selected Areas in Communications, 39(8), 2343-2360.
10. Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Ghribi, A., Goldschmidt, T., et al. (2018). A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities. Journal of Internet Services and Applications, 9, 16.
11. Mammeri, Z. (2019). Reinforcement learning based routing in networks: Review and classification of approaches. IEEE Access, 7, 55916-55950.



12. Ayoubi, S., Limam, N., Salahuddin, M. A., Shahriar, N., Boutaba, R., Estrada-Solano, F., & Caicedo, O. M. (2018). Machine learning for cognitive network management. *IEEE Communications Magazine*, 56(1), 158–165.
13. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1), 14–76.
14. Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, 16(3), 1617–1634.
15. Rana, A., & Dhaka, V. S. (2021). A review on software-defined networking and its applications in modern computer networks. *Computer Networks*, 199, 108404.
16. Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. *IEEE Communications Surveys & Tutorials*, 19(3), 1657–1681.
17. Zhang, S., Zhang, H., Di, B., & Song, L. (2019). Cellular UAV-to-X communications: Design and optimization for multi-UAV networks. *IEEE Transactions on Wireless Communications*, 18(12), 5899–5913.
18. Letaief, K. B., Shi, Y., Lu, J., & Lu, J. (2019). The roadmap to 6G: AI empowered wireless networks. *IEEE Communications Magazine*, 57(8), 84–90.
19. Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network*, 34(3), 134–142.
20. Strinati, E. C., Barbarossa, S., Gonzalez-Jimenez, J. L., Ktenas, D., Cassiau, N., Mazarico, D., & others. (2021). 6G: The next frontier: From holographic communications to artificial intelligence and quantum technologies. *IEEE Transactions on Vehicular Technology*, 70(6), 5201–5210.
21. Ferrag, M. A., Maglaras, L., Moschogiannis, S., & Janicke, H. (2018). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419.
22. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544–546.
23. Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016). A survey of security in software defined networks. *IEEE Communications Surveys & Tutorials*, 18(1), 623–654.
24. Alsmadi, I., Alazzam, I., & others. (2020). Security and privacy issues in software-defined networking: A survey. *Journal of Network and Computer Applications*.

