ISSN: 1692-8520 January 2026 IJABMTR | Volume 08 Issue 14

RELIABLE AND EFFECTIVE COMMUNICATION IN DATA AND NETWORKING

Mandiyam Riyaz Basha[1] Dr. G. Bhaskaran[2] Dr. M. Sakthivel[3]

1, Author Dept. of Computer Science., University of Madras - Chennai - 600005, India.
2, Co Author Prof., Dept. of Computer Science., University of Madras - Chennai - 600005, India.
3, Co Author Prof., Dept. of Computer Science., University of Madras - Chennai - 600005, India.

[1]mbasha1.c@edu.ksa.sa [2]drbhaskaranuonmsa@gmail.com [3]drsakthiveluonmsa@gmail.com

Abstract

Modern information systems rely heavily on data communication and networking to effectively transmit and exchange data across a variety of devices and networks. However, there are several issues in this area that limit network performance and the smooth flow of data. This review paper explores the key challenges encountered in data communication and networking and discusses potential solutions to address these issues. This report offers insights into the present status of research and shows the ongoing attempts to address these difficulties through an analysis of relevant articles and journals. The results of this review can help for better understanding the complicated world of data networking and communication, which will support the creation of reliable and effective communication systems.

Key Words: Networking, Data Transmission, NFV, SDN and QoS.

I . INTRODUCTION

Modern information systems rely heavily on data communication and networking to effectively transmit and share data across a variety of devices and networks. Our interconnected world is supported by these systems, which make communication, teamwork, and the smooth flow of information possible. The volume of data collected, transferred, and processed has significantly increased as a result of technological improvements, and there is a rising need for reliable and scalable data communication networks. Data transmission and networking do offer advantages and opportunities, but they also present a number of difficulties that prevent these systems from functioning properly and performing at their best. These difficulties cover a wide range of topics, including bandwidth restrictions, network security, and scalability. Taking care of these issues is

essential for maintaining secure data transfer, safeguarding private data, accommodating the developing network infrastructure, and promoting seamless communication across many platforms. As the demand for data-intensive applications and services rises, bandwidth restrictions present a serious problem. Network bandwidth is being strained by the exponential expansion in data volume caused by activities like video streaming, cloud computing, and IoT devices. Reduced data transmission speeds, network congestion, and delay can all be caused by insufficient bandwidth. To ease bandwidth constraints and improve network performance, researchers and professionals have suggested a variety of solutions, including traffic engineering, quality of service (QoS) mechanisms, and bandwidth optimisation algorithms. Networks for data communication must be always vigilant against security threats. The confidentiality, integrity, and accessibility of data are under danger from unauthorised access, data breaches, and denial of service (DoS) assaults. Implementing strong security measures to protect network infrastructure and sensitive data presents a challenge for network administrators and security professionals. In order to mitigate these security risks, encryption, firewalls, and secure protocols are crucial. Furthermore, the need for scalability becomes more urgent as connected devices and users continue to increase quickly. The

increasing needs for connectivity must be managed by network topologies and protocols without compromising performance. To improve network scalability and flexibility to the expanding network landscape, solutions including network virtualization, software-defined networking (SDN), and load balancing have been suggested. This review paper discusses the main problems with data networking and communication, analyses the research being done to solve these problems, and discusses possible solutions. This review study seeks to offer insights into the present status of research in the field and contribute to the comprehension of the complex environment of data communication and networking by examining appropriate studies. The results of this study can help create reliable and effective communication systems that meet obstacles and guarantee the uninterrupted flow of data in our linked world.

II. BANDWIDTH LIMITATIONS

The demand for data-intensive apps and services is always growing, which has had a big impact on network capacity. The amount of data being carried across networks has increased as more consumers take part in activities like video streaming, cloud computing, online gaming, and IoT devices. Network bandwidth, which refers to a network's maximum capacity to send data, is strained by this data flood. A lack of bandwidth can present several problems for networking and data communication. Network congestion, where the bandwidth is not enough to handle the volume of traffic, is one of the main problems. Data packets are delayed in their transmission during congestion, which increases latency. A data packet's latency is the amount of time it takes to go from its source to its destination. High latency can be detrimental to real-time applications like online gaming and video conferencing, where responsiveness is essential. Additionally, a lack of bandwidth can result in lower data transfer rates, which slows down download and upload speeds. Users that depend on quick and effective data transmission for their tasks may find this to be frustrating. Furthermore, bandwidth restrictions can make it difficult for network managers to give priority to important traffic, which can affect users' perceptions of the quality of service (QoS).

Researchers have suggested several methods to reduce bandwidth restrictions and improve network performance in order to address these issues. Traffic engineering approaches aim to optimize the utilization of available bandwidth by dynamically regulating network traffic. This includes routing algorithms that pick the most effective paths for data transmission and load balancing techniques that spread traffic over numerous network lines. Quality of Service (QoS) mechanisms are essential for efficient use of bandwidth resources. Network traffic is prioritized by QoS mechanisms according to predetermined criteria, ensuring that critical applications have access to enough bandwidth and latency. Techniques such as traffic shaping, admission control, and differentiated services (DiffServ) can be deployed to enforce QoS policies and boost the overall network performance. The effective compression and encoding of data, the reduction of redundant transmissions, and the optimisation of the transmission protocols are all features of bandwidth optimisation algorithms, which are created to make the most use of the available bandwidth. These algorithms are designed to keep the transmitted data's quality and integrity while consuming as little bandwidth as

II. BANDWIDTH LIMITATIONS

The demand for data-intensive apps and services is always growing, which has had a big impact on network capacity. The amount of data being carried across networks has increased as more consumers take part in activities like video streaming, cloud computing, online gaming, and IoT devices. Network bandwidth, which refers to a network's maximum capacity to send data, is strained by this data flood. A lack of bandwidth can present several problems for networking and data communication. Network congestion, where the bandwidth is not enough to handle the volume of traffic, is one of the main problems. Data packets are delayed in their transmission during congestion, which increases latency. A data packet's latency is the amount of time it takes to go from its source to its destination. High latency can be detrimental to real-time applications like online gaming and video conferencing, where responsiveness is essential. Additionally, a lack of bandwidth can result in lower data transfer rates, which slows down download and upload speeds. Users that depend on quick and effective data transmission for their tasks may find this to be frustrating. Furthermore, bandwidth restrictions can make it difficult for network managers to give priority to important traffic, which can affect users' perceptions of the quality of service (QoS).

Researchers have suggested several methods to reduce bandwidth restrictions and improve network performance in order to address these issues. Traffic engineering approaches aim to optimize the utilization of available bandwidth by dynamically regulating network traffic. This includes routing algorithms that pick the most effective paths for data transmission and load balancing techniques that spread traffic over numerous network lines. Quality of Service (QoS) mechanisms are essential for efficient use of bandwidth resources. Network traffic is prioritized by QoS mechanisms according to predetermined criteria, ensuring that critical applications have access to enough bandwidth and latency. Techniques such as traffic shaping, admission control, and differentiated services (DiffServ) can be deployed to enforce QoS policies and boost the overall network performance. The effective compression and encoding of data, the reduction of redundant transmissions, and the optimisation of the transmission protocols are all features of bandwidth optimisation algorithms, which are created to make the most use of the available bandwidth. These algorithms are designed to keep the transmitted data's quality and integrity while consuming as little bandwidth as

possible. Network administrators can lessen the effects of constrained bandwidth, relieve congestion, decrease latency, and increase data transfer rates by using these strategies. Research and development efforts are still being made in this area to find new ways to effectively use network bandwidth and meet the constantly increasing demand for data-intensive applications and services.

III. NETWORK SECURITY Fig. 1:

Networks for data communication are essential for conveying sensitive information, making them a target for many security risks. These networks are frequently threatened by unauthorised access, data breaches, and denial Unauthorised entry into a network, which could jeopardise its security and allow for the access of sensitive data, is referred to as unauthorised access. Unauthorised access to private data causes data breaches, which frequently expose sensitive information to bad parties. DoS attacks try to interfere with network services by utilising excessive amounts of network resources, making them unavailable to authorised users. Study in [1] shows an example of security threats. Active attack is the term used when unauthorised attackers watch, listen to, and alter the data stream in the communication channel. The attacks that come after are active in nature. A rogue node serves as a black hole for the sensor network, drawing all traffic there. In fact, this attack has the potential to impact even nodes that are located a great distance from base stations. The conceptual picture of a black hole/sinkhole attack is shown in Figure 1. According to figure 2, a catastrophic attack known as a "wormhole" occurs when an attacker captures packets (or bits) at one point in the network and tunnels them to another. Figure 2 (a and b) illustrates an instance of a wormhole assault. The attacker gets the routing request packet when it is broadcast by node B (such as the base station or another sensor) and replays it in the area. Each neighbouring node that receives this replayed packet will regard Node B as its parent and regard itself as being in its range. Therefore, even though the victim nodes are multiple hops away from B, the attacker in this example tricks them into thinking that B is nearby, creating a wormhole in the process. It is extremely difficult to guarantee the secrecy, integrity, and availability of data in data communication networks. Protecting data from unauthorised access and ensuring that only authorised people have access to sensitive information are two examples of maintaining confidentiality. Integrity is the maintenance of data accuracy and consistency, as well as the prevention of tampering with or modification during

transmission. The ability of the network to deliver data and services consistently and without interruption is referred to as availability. Different security techniques and technologies are used in data communication networks to overcome these security issues. The confidentiality of data is greatly protected by encryption. Data is encrypted using cryptographic techniques to prevent unauthorised people from reading it. Even if data is captured during transit, encryption ensures that it will remain incomprehensible without the decryption key. By monitoring and regulating incoming and outgoing network traffic in accordance with preset security policies, firewalls serve as a barrier between the internal network and external entities. Network security is improved by firewalls, which block unauthorised access and filter out potentially harmful traffic. To improve network security, user awareness and education are also essential. Security breaches can be considerably decreased by educating users about secure procedures such robust password management, spotting phishing efforts, and staying away from dubious websites or downloads. In conclusion, several security risks that could jeopardise data availability, confidentiality, and integrity exist for data communication networks. Protecting network infrastructure and data from unauthorised access, data breaches, and DoS attacks requires the deployment of security measures including encryption, firewalls, and user education. Maintaining the security of data communication networks requires constant attention to detail and remaining current with the most recent security procedures.

IV. SCALABILITY Securing scalability becomes a crucial concern as linked devices and users in data communication networks continue to increase dramatically. A network's capacity to accommodate the rising connectivity needs without performance degradation or bottlenecks is referred to as scalability. To handle the growing number of devices and users while maintaining effective performance, network architectures and protocols must change. Due to hardware resource constraints, rigid configurations, and the difficulty of managing a large number of devices, traditional network architectures frequently struggle to scale effectively. To address the scalability difficulty, numerous solutions have been proposed: • Network virtualizations: Multiple virtual networks can be built on a single physical infrastructure thanks to network virtualization. As a result of

separating network resources from the underlying technology, it offers a scalable and adaptable solution. Network virtualization enables effective resource allocation and traffic separation by allowing the creation and independent management of several virtual networks. By efficiently utilising the resources at hand and offering a more adaptable network infrastructure, this method improves scalability. • Software-Defined Networking (SDN): In network architectures, SDN separates the control plane from the data plane. By centralising network control and management tasks, administrators are now able to programmatically manage and set up networks using software tools. SDN makes it possible to manage network resources centrally and dynamically, which makes scaling easier and simplifies management of the network. SDN offers the adaptability to adjust to changing network demands and efficiently allocate resources based on the application requirements by detaching control from the underlying hardware. • Load balancing strategies: To maximise resource utilisation and prevent congestion, load

balancing solutions divide network traffic among several resources. Incoming requests are intelligently split between a number of servers or network devices by load balancers, preventing any one resource from becoming overloaded. By effectively handling more traffic and reducing performance deterioration, this increases network scalability. Different layers of load balancing can be used, such as network-level load balancing, DNS-based load balancing, or application-level load balancing. Through more effective resource utilisation, centralised management, and adaptable network topologies, these strategies improve network scalability. They enable network managers to respond to the rising expectations of users and linked devices without compromising performance or encountering bottlenecks. It's crucial to remember that scalability demands careful planning and considering variables like network topology, traffic patterns, and application needs. Network administrators must assess the unique requirements of their networks and select the most suitable scaling solutions in accordance.

V. SOFTWARE-DEFINED NETWORKING

Study in [3] proposed that network operators can handle flows in a more granular manner using SDN architecture and the OpenFlow protocol than they can with traditional networks using controllers. In a conventional network, flows (or packets) are often handled based on one or a few packet header attribute combinations, such as the longest

destination IP prefix, the destination MAC address, or a combination of IP addresses and TCP/UDP port numbers. SDN introduces centralised management and programmability of network resources by separating the control plane from the data plane. In an SDN design, the network is managed by a central controller who has a complete understanding of the network structure and traffic patterns. Because of this centralization, network managers are able to manage and configure network resources in a dynamic way by having a comprehensive and uniform view of the entire network. SDN's centralised management system has a number of benefits. It improves network flexibility in the first place. Administrators may quickly change and modify the network with SDN to meet evolving needs. Software allows for the definition and modification of network policies and configurations, offering a high level of flexibility and agility. As a result, new services and applications can be deployed more quickly, and network resources can be scaled up or down as necessary. Scalability is an additional advantage of SDN. The spread of network intelligence is made possible by the separation of the control plane from the data plane. SDN does away with the necessity of running complicated and resource-intensive protocols on individual networking devices by centralising control. Because they just need to concentrate on forwarding packets in accordance with the instructions they receive from the centralised controller, this simplifies the devices and increases their scalability. SDN enhances network security as well. Administrators can consistently apply security standards throughout the whole network thanks to a centralised controller that gives them a comprehensive view of the network. Real-time network traffic monitoring and analysis enables the identification and mitigation of security threats. A further line of defence against attacks is provided by SDN's programmability, which enables the deployment of security policies and controls at various network layers. SDN handles a number of networking and data transfer issues overall. It gives network infrastructure flexibility, scalability, and security. Network administrators are given additional power and flexibility to administer their networks thanks to SDN, which separates the control plane from the data plane, enables centralised management, and enables programmability. This architectural change creates room for creativity, streamlines network administration, and enables organisations to modify their networks to satisfy the constantly changing requirements of contemporary data communication.

7

VI. NETWORK FUNCTION VIRTUALIZATION

By operating network functions as virtualized software instances on common servers, storage, and networking resources instead of as dedicated hardware appliances, Network Function Virtualization (NFV) in [4], a method of detaching network hardware and software to enable network services to run on widely available cloud computing-style platforms is known as virtualization, and it has completely revolutionised the telecoms sector. Virtualization is expected to encourage innovation in the network infrastructure sector, much like it did for traditional IT, by facilitating quicker and less risky deployment of new services, enabling iterative service improvement, expanding the developer ecosystem to welcome new players, and lowering network cost structures through infrastructure sharing and automation. Study in [2] apply that one essential technology for the implementation of cloud computing is virtualization. Customers can often relocate their compute and data to a remote location using virtualization, with different effects on performance. Virtualization offers many advantages that would not be possible without it. Elasticity and scalability, cost efficiency, infrastructure independence, customizability, a streamlined access interface, etc. are a few advantages. Increased network infrastructure scalability becomes possible by virtualizing network functions. Traditional network services frequently call for specialised hardware appliances for every network function, which results in a large number of devices and increased complexity. Multiple network functions can be combined and executed as software instances on shared hardware resources thanks to NFV. By enabling the effective allocation and utilisation of resources based on demand, this consolidation enhances scalability. To meet shifting traffic patterns, virtualized network operations can be flexibly scaled up or down, ensuring optimal resource consumption and lowering the requirement for overprovisioning. Cost savings are yet another important benefit of NFV. Organisations can spend less on capital and operating expenses by detaching network services from specialised hardware. NFV makes use of common servers and commodity hardware, which is frequently less expensive, as opposed to spending money on expensive and specialised hardware appliances. By allowing for hardware consolidation, this method lowers the amount of energy used, the amount of space needed, and the cost of maintaining the hardware. The virtualization

component of NFV also makes it possible for more automation and orchestration, which lowers the need for human configuration and management and thus lowers operational expenses. By enabling quick network service deployment, NFV also improves network agility. Long procurement, implementation, and setup processes for specialised hardware are common with traditional network services. Faster service deployment and activation is possible with NFV because network services can be instantiated and provisioned as virtualized software instances. Organisations are able to develop new services, scale their networks effectively, and quickly adjust to shifting business requirements because to their increased agility. It also makes it easier to deploy technologies like network slicing, which enables the creation of several virtual networks on a same shared infrastructure to serve various use cases or clients. In conclusion, there are various benefits to divorcing network functions from specialised hardware and virtualizing network services. It boosts network agility through quick service deployment, lowers costs by leveraging standard servers and automation, increases scalability by optimising resource allocation, and makes resource allocation possible. In terms of network architecture, NFV represents a substantial shift that gives organisations more flexibility, financial savings, and operational efficiency when offering network services.

VII. CONCLUSION

Numerous issues affecting network performance, security, and scalability plague data communication and networking. In order to solve these problems, the review paper outlined the main difficulties and addressed alternative solutions, including SDN and NFV. To overcome the difficulties and progress the development of reliable and effective communication systems, it is crucial for researchers, network administrators, and policymakers to keep up with the most recent advancements in this sector.

REFERENCES [1]

Kumar, Vikash, Anshu Jain, and P. N. Barwal. "Wireless sensor networks: security issues, challenges and solutions." International Journal of Information and Computation Technology (IJICT) 4, no. 8 (2006): 859- 868.

[2] Basu, Srijita, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, and Pritika Sarkar. "Cloud computing security challenges & solutions-A survey." In 2007 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 347-356. IEEE, 2007.

[3] Karakus, M. and Durresi, A, "A survey: Control plane scalability issues and approaches in softwaredefined networking (SDN)," Computer Networks 112 (2017): 279-293. [4] Joshi, Kaustubh, and Theophilus Benson. "Network function virtualization." IEEE Internet Computing 20.6 (20