Advanced Journal of Engineering and Scientific Applications (AJESA)

Research Paper Open Access

Available online at www.ajesa.com.ng **Vol.2, No.1, January/February 2025.pp.9-20**

Technicality of Network Topologies: A Comprehensive Review

Oluharaotu, O.E.[1], Asogwa S.C.[2], Ugwoke, F.N.[3], Etuk E.A.[4]

[1,2,3,4] ***Department of Computer Science, Michael Okpara University of Agriculture Umudike Nigeria***

Corresponding author : [1]osmondo2008@gmail.com

Abstract

Network topology refers to the arrangement or layout of various elements (links, nodes, and devices) within a communication network. It plays a critical role in the performance, scalability, and management of network systems. Various topologies, such as bus, star, ring, mesh, tree, and hybrid, each offer unique advantages and challenges based on factors like data flow, fault tolerance, and resource allocation. This paper explores the technicalities of network topology, examining its impact on network design and operations. It delves into how topology influences data transmission efficiency, redundancy, and scalability, as well as the role of advanced technologies like software-defined networking (SDN) and virtualized network topologies. This paper also discusses the selection criteria for optimal topologies, considering factors such as cost, scalability, security, and ease of maintenance. This paper has provided insights into how modern networks evolve to meet the increasing demands of connectivity and data throughput.

Keywords: Network Architecture; LAN; MAN; WAN; Network Topology; BUS; MESH; RING; Tree; Hybrid; Emerging Trends; SDN; NFV; IoT; 5G; Quantum Networking

1. INTRODUCTION

Network topology refers to the physical and logical arrangement of nodes, devices, and the connections between them within a communication network. It is a crucial factor that influences network design, performance, and scalability. The technical aspects of network topology encompass a variety of considerations, including how data is routed through the network, how devices are interconnected, and how the topology impacts overall network efficiency and reliability.

At its core, network topology determines the structure of a network and directly impacts critical attributes such as data transmission speed, fault tolerance, and redundancy. Traditional topologies like bus, star, ring, and mesh, as well as more advanced and hybrid structures, each have distinct advantages and challenges (Kurose & Ross, 2017). For instance, a star topology centralizes communication through a central hub, simplifying management but introducing a single point of failure. In contrast, a mesh topology, characterized by interconnecting each device with multiple others, offers enhanced fault tolerance and redundancy, though at a higher cost and complexity (Forouzan, 2012).

With the rise of modern networking technologies, such as Software-Defined Networking (SDN) and Virtualized Network Functions (VNF), the traditional concepts of network topology have evolved. SDN allows for more flexible and dynamic network configurations through centralized control planes, enabling administrators to optimize traffic

Flows, increase resilience, and reduce overhead (Seetharaman et al., 2017). Similarly, network virtualization facilitates the abstraction of network components, allowing for the creation of virtual topologies that provide greater flexibility and scalability (Zhang et al., 2018).

In selecting the most appropriate network topology, factors such as cost, scalability, maintenance, and security play critical roles. The growth of data traffic and the demand for high-speed, low-latency connections in applications like cloud computing, IoT, and 5G networks further complicate the choice of topology, requiring a deeper understanding of how topology affects both current and future network performance (Sharma et al., 2020).

This paper explores the technical intricacies of network topology, highlighting the design principles, performance considerations, and the impact of emerging technologies on network structure. It aims to provide insights into how choosing the right topology can enhance the efficiency and resilience of modern communication networks.

2. NETWORK ARCHITECTURE

Network architecture refers to the overall design and structure of a network, which varies depending on its size, geographical coverage, and the number of devices involved. Common types of network architectures include:

Figure 1: Representing Network Architecture

Local Area Network (LAN): A LAN covers a small geographic area, such as a home, office, or campus. It typically connects computers and devices within a limited space and is characterized by high data transfer speeds and low latency. LANs are often built using star or bus topologies (Kurose & Ross, 2017).

Wide Area Network (WAN): A WAN spans a larger geographical area, such as cities, countries, or even continents. WANs connect multiple LANs and MANs (Metropolitan Area Networks) together. Due to the vast distances covered, WANs often rely on public or private leased lines and satellite links. The physical topology of a WAN can be complex, often incorporating mesh or hybrid structures (Forouzan, 2012).

Metropolitan Area Network (MAN): A MAN covers a larger area than a LAN but smaller than a WAN, typically covering a city or a large campus. MANs often connect several LANs within a metropolitan area and are designed to provide high-speed connections over moderate distances, making use of fiber optic or wireless technologies (Tanenbaum & Wetherall, 2011).

Each of these network types has its own architectural considerations regarding performance, scalability, and the necessary infrastructure for communication across varying distances.

3. FUNDAMENTALS OF NETWORK TOPOLOGY

Understanding the core principles of network topology is essential for designing and optimizing network infrastructures. Network topology can be analyzed from different perspectives, including its physical and logical configurations, as well as the various architectural scales in which they operate. Additionally, certain metrics play a significant role in assessing the effectiveness and efficiency of a network topology, guiding network designers in selecting the best structure for specific needs.

(a) Physical and Logical Topologies

Physical Topology refers to the actual layout of network devices and cables. It is the tangible arrangement of physical components such as computers, switches, routers, and cables. Examples of physical topologies include star, bus, ring, and mesh layouts, each representing how devices are physically connected in a network (Tanenbaum & Wetherall, 2011). The physical topology determines how the network components are arranged in space and affects factors such as cabling requirements, device placement, and the network's ability to expand.

Logical Topology, on the other hand, is concerned with the flow of data within the network. It defines the path data takes between devices, irrespective of the physical arrangement of components. Logical topology is crucial because it impacts data transmission and network protocols. For example, a network might have a physical star topology, but the logical topology could resemble a bus, where data travels in a single direction along the network (Forouzan, 2012). The logical topology influences factors such as network traffic flow, collision domains, and the behavior of data during transmission.

C. Network Topology Metrics

When evaluating network topologies, certain metrics are important in determining the suitability of a design for particular use cases. These metrics help assess the network's performance, scalability, and overall efficiency.

1. Distance: This refers to the physical length of the network and the distance over which data must travel. In LANs, distance is generally short, but in WANs, the distance can span hundreds or even thousands of kilometers. The topology chosen can impact the efficiency of data transmission across these distances. For instance, a star topology in a LAN reduces the distance each device needs to communicate with the central hub, while in a WAN, long-distance communication may involve more complex topologies like mesh or hybrid designs (Kurose & Ross, 2017).

2. Connectivity: Connectivity refers to how devices within the network are linked together and how data is transmitted between them. High connectivity generally means greater reliability and redundancy. For example, a mesh topology provides high connectivity because each node is connected to multiple other nodes, ensuring that if one path fails, an alternative path is available (Forouzan, 2012). In contrast, a bus topology may have limited connectivity, and a failure in the central bus could disrupt the entire network.

3. Scalability: Scalability is the network's ability to grow and handle increased loads or additional devices without a significant drop in performance. A topology that offers easy scalability allows for the addition of new nodes or links without requiring a major redesign. For example, star topologies are highly scalable since adding new devices usually involves only connecting them to the central hub (Tanenbaum & Wetherall, 2011). In contrast, bus topologies are less scalable because adding more devices can lead to data collisions and bandwidth limitations, impacting performance as the network grows.

D. Types of Network Topologies

Network topology refers to the physical or logical arrangement of devices in a network, and it can be classified into several different types. Each topology has its unique advantages and disadvantages, making it suitable for different types of network requirements. Below, we explore four common network topologies—bus, star, ring, and mesh—with a focus on their advantages, disadvantages, and typical applications.

1. Bus Topology

Description: In bus topology, all devices (nodes) are connected to a single central cable, called the "bus" or backbone. Data sent by any device travels along the bus and is received by all other devices, though only the intended recipient processes the data.

Published bimonthly by the Nigerian Institute of Electrical and Electronics Engineers (NIEEE) Awka Chapter, Nigeria..

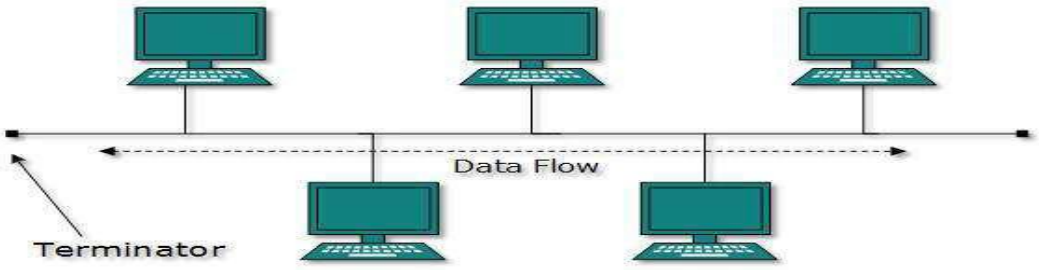

Figure 2: Represents of how devices are connected in bus topology and how data flows from one end to another.

Advantages:

Cost-Effective: Bus topology requires fewer cables than star topology and is thus more economical to set up, especially for small networks.

Easy to Implement and Extend: The simplicity of connecting new devices makes it easy to implement and extend.

Minimal Cabling: Since there is a single backbone, the amount of cable required is lower than in other topologies, reducing installation costs.

Disadvantages:

Single Point of Failure: If the central bus cable fails, the entire network is disrupted, making it less reliable.

Scalability Issues: Performance degrades as more devices are added, especially with increased network traffic.

Limited Performance: The shared bus can cause data collisions as only one device can transmit at a time, reducing network speed and efficiency in busy networks.

Applications:

Small networks: Suitable for small offices or local area networks (LANs) with few devices.

Temporary networks: Ideal for temporary setups or when the network size is not expected to grow substantially.

Legacy systems: Used in older network systems before more sophisticated technologies were developed.

2. Star Topology

Description: In star topology, all devices are connected to a central device, typically a hub or a switch. Data travels from the source device to the central hub, which then forwards it to the destination device.

Figure 3: Representation of how devices are connected in Star topology and how data flows in loop.

Advantages:

Reliability: If one device fails, the rest of the network continues to function, making it more fault-tolerant.

Ease of Management: The central hub simplifies network management, as issues can be isolated more easily.

Scalable: Adding new devices is simple—just connect them to the central hub without affecting the rest of the network.

Disadvantages:

Single Point of Failure: The central hub or switch is critical—if it fails, the entire network is down.

Higher Cost: Requires more cabling and network hardware (central hub/switch), making it more expensive than bus topology.

Dependence on Central Hub: The performance of the network is dependent on the capacity and efficiency of the central device.

Applications:

Home and office networks: Star topology is widely used in small and medium-sized networks due to its simplicity and scalability.

Enterprise networks: It is often the topology of choice in businesses, where central management and ease of expansion are necessary.

Wi-Fi networks: Wireless access points can serve as hubs in a star topology for wireless networks.

3. Ring Topology

Description: In a ring topology, each device is connected to two other devices, forming a continuous loop. Data travels in one direction (or sometimes two directions in a dual-ring setup) around the ring until it reaches the intended recipient.

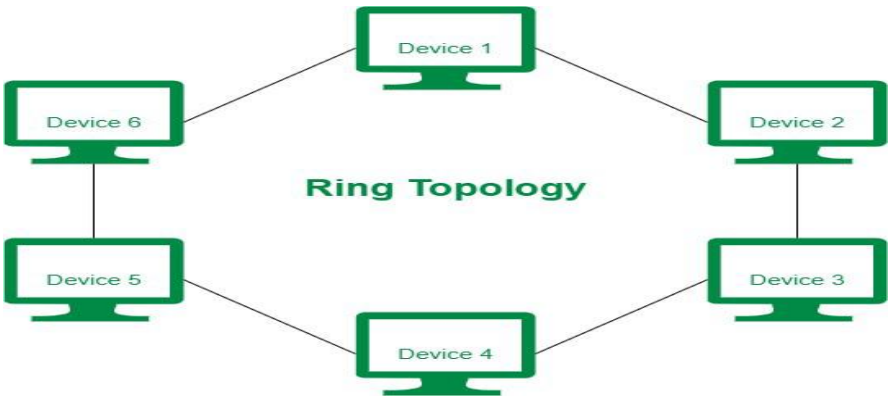

Figure 4: Representation of Ring topology and how data flows in loop

Advantages:

Data Integrity: Data travels in a consistent, circular manner, which can make the flow of data predictable and orderly.

No Data Collisions: Since each device can only transmit after receiving a signal from its predecessor, data collisions are minimized.

Simple to Install: The ring structure is easy to implement, especially in small-to-medium-sized networks.

Disadvantages:

Single Point of Failure: If one device or cable fails, the entire network can be disrupted unless a dual-ring or fault-tolerant mechanism is in place.

Data Transmission Delays: As the number of devices in the ring increases, data transmission speed can decrease due to longer travel times around the loop.

Difficult to Troubleshoot: Since data passes through all devices in the ring, pinpointing the cause of failure can be challenging.

Applications:

Token Ring Networks: Historically used in older office networks, such as IBM's Token Ring technology.

Fiber Optic Networks: Often used in long-distance communication networks, where high-speed transmission is critical, and fault tolerance can be implemented (e.g., dual-ring configurations).

Small-to-Medium Sized Networks: Suitable for networks where data integrity and predictable data flow are important.

4. Mesh Topology

Description: In mesh topology, every device in the network is connected to every other device, creating a fully interconnected system. This structure provides multiple paths for data to travel, increasing the redundancy and reliability of the network.

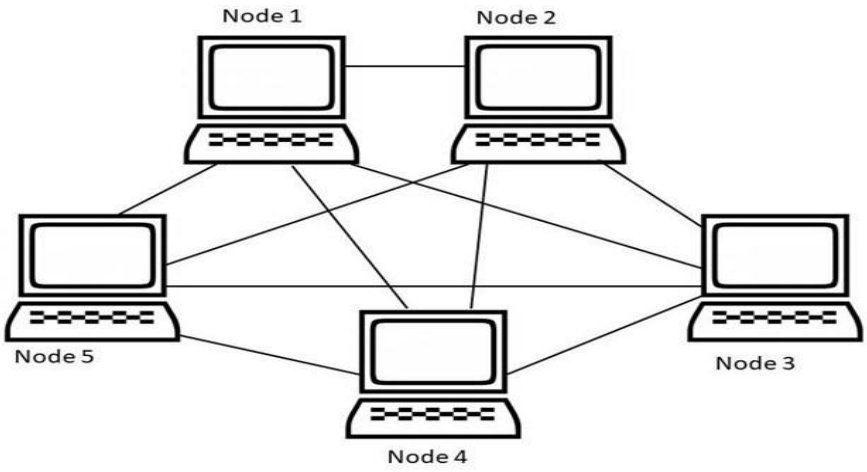

Figure 5: Represents of how devices are connected in Mesh topology and how data flows in devices.

Advantages:

Fault Tolerance: If one connection fails, data can still be transmitted through other paths, ensuring high availability and reliability.

Scalability: Mesh topology can handle large networks effectively by adding more devices and connections without significant performance degradation.

High Redundancy: Each device has multiple routes to communicate, which makes the network highly robust against failures.

Disadvantages:

Complexity: The wiring and configuration of mesh networks are more complex, requiring significant resources to implement and maintain.

High Cost: The need for multiple connections between devices increases both the cost of setup and maintenance.

Management Overhead: As the network grows, the complexity of managing and troubleshooting increases exponentially.

Applications:

Large-scale Networks: Used in large enterprise networks, where reliability and redundancy are critical.

Telecommunications Networks: Often used in backbone networks, where a high level of fault tolerance is necessary.

Military and Critical Systems: Essential in environments where network reliability and uptime are non-negotiable.

Tree Topology:

The network is divided into several levels/layers using this topology. A network is divided into 3 categories of network devices, mostly in LANs. The lowest layer is the access layer, which is where systems are linked. The distribution layer is the intermediate layer that acts as a link between the top and lower layer. The topmost layer, referred as core layer, is the network's nerve center. A point-to-point link exists between all nearby hosts. In a similar way as the bus, topology, in case if the root fails the whole network faces the problem. It is not, however, the only site of failure. Every connection acts as a single point of failure, separating the network in segments, which are inaccessible if it fails. Figure 6 represents of how devices are connected in tree topology and how data flows in devices.

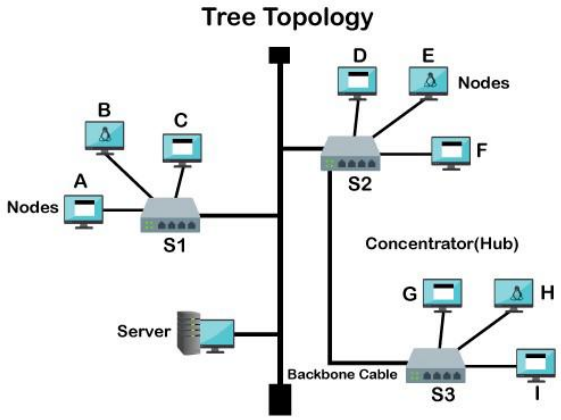

Figure 6: Representation of how devices are connected in tree topology and how data flows in devices.

Hybrid Topology:

It can be said as combination of several topologies. These are commonly used in big Multinational industries where there are personalized topologies for each department. These provide a great flexibility to the network system. Different topologies can be chosen and implement according to the needs and requirement of the user. Figure 7 represents how devices are linked in hybrid topology using an arrangement of star, ring and bus topology.

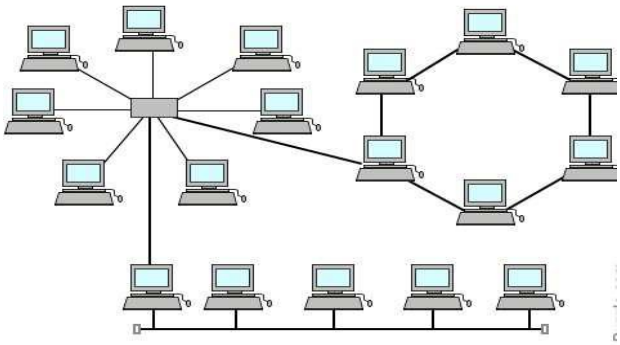

Figure 7: Representation of how devices are linked in hybrid topology using an arrangement of star, ring and bus topology.

4. IMPLICATIONS OF NETWORK TOPOLOGY ON NETWORK SECURITY

Network topology refers to the arrangement of various elements (links, nodes, devices) in a network. It plays a critical role in the network's overall performance, reliability, and, importantly, its security. The structure of a network can

either expose vulnerabilities or strengthen the system against potential security threats. Below, we explore how different topologies impact network security, the types of security threats, and the effectiveness of security measures like firewalls and intrusion detection systems.

1. Network Topology's Impact on Security Threats

a. Eavesdropping (Interception of Traffic)

Eavesdropping refers to the unauthorized interception of data as it traverses the network. Depending on the topology, certain network paths or segments may be more exposed to such threats.

Bus Topology: In this topology, data travels along a single shared medium (the bus), meaning any device connected to the bus can potentially intercept the data. This makes it vulnerable to eavesdropping, especially in unencrypted communication environments.

Star Topology: While star topology centralizes communication through a central switch or hub, it can be more secure compared to bus topology. However, the central device (like a switch or router) becomes a critical point of vulnerability. If an attacker compromises this device, they could intercept data from all connected devices.

Mesh Topology: This topology, with direct connections between multiple devices, can provide better security by creating redundant paths, making it harder for an attacker to intercept traffic. However, it may also introduce complexity in managing secure connections between numerous devices.

b. Spoofing (Impersonating a Device or User)

Spoofing occurs when an attacker impersonates another device or user on the network, potentially gaining unauthorized access to resources or launching further attacks.

Bus Topology: In bus topologies, devices connected to the same physical medium may be more susceptible to spoofing. Since the data is broadcasted, an attacker could easily inject malicious packets or spoof the MAC or IP address of legitimate devices.

Star Topology: Centralized devices like switches or routers can mitigate spoofing to some extent. However, an attacker could spoof the IP or MAC address of a legitimate device and gain unauthorized access if proper authentication mechanisms are not in place.

Mesh Topology: While mesh networks offer redundancy and resilience, spoofing can still occur if devices communicate through unsecured channels or without strong authentication. The complexity of the network also increases the potential for misconfigurations that attackers could exploit.

c. Denial of Service (DoS)

Denial of Service (DoS) attacks aim to disrupt network services by overwhelming the target with excessive traffic or exploiting network vulnerabilities.

Bus Topology: A DoS attack targeting the bus or shared medium can potentially disrupt the entire network. Since all devices share the same communication channel, a single point of failure can lead to widespread disruption.

Star Topology: A DoS attack targeting the central hub or switch can impact all connected devices, as the hub becomes the central point of failure. A well-placed attack on this device can render the entire network inaccessible.

Mesh Topology: Mesh topologies are more resilient to DoS attacks due to redundant paths. However, if an attacker targets key nodes or floods a central device, such as a router or gateway, the impact can still be significant.

2. Security Measures and Their Effectiveness

To mitigate the risks associated with different network topologies, several security measures can be implemented. These measures provide protection against common threats like eavesdropping, spoofing, and DoS attacks.

a. Firewalls

Firewalls act as a barrier between trusted internal networks and untrusted external networks (e.g., the internet). They monitor and filter incoming and outgoing traffic based on predefined security rules.

In Star Topology: Firewalls are typically placed at the entry or exit points of the central hub (usually at the router or gateway). This configuration can effectively protect the entire network from external threats.

In Mesh Topology: Firewalls can be distributed across different nodes, providing more granular control over traffic. However, the complexity of the network means that configuring and maintaining firewalls on each node can be resource-intensive.

b. Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

IDS/IPS are designed to detect or prevent suspicious activity and security breaches by monitoring network traffic for signs of malicious behavior.

In Star Topology: IDS/IPS systems can be deployed at the central switch or router. Since all traffic flows through the central hub, it becomes easier to monitor and detect threats at a single point.

In Mesh Topology: The distributed nature of mesh networks may require IDS/IPS systems at multiple points in the network, potentially increasing the complexity of detection. However, this also means that the system can provide more detailed insights into potential threats across different paths in the network.

c. Encryption and Authentication

Encryption ensures that data is unreadable to unauthorized users, while authentication ensures that only legitimate users or devices can access the network.

In Star Topology: End-to-end encryption can be implemented between devices and the central hub to prevent eavesdropping. Strong authentication mechanisms should be enforced at the central device to prevent unauthorized access.

In Bus and Mesh Topologies: Encryption can be implemented to secure the shared communication medium (in bus topology) or to protect communication across multiple devices (in mesh topology). Proper authentication protocols must also be established to mitigate spoofing risks.

3. Topology-Related Security Vulnerabilities

Certain network topologies have inherent vulnerabilities that could be exploited by attackers. Here, we explore some of the security risks tied to specific topologies:

a. Bus Topology Vulnerabilities

Single Point of Failure: The shared medium makes the entire network vulnerable if the bus or cable is compromised. If an attacker gains physical access to the medium, they could intercept or manipulate all data.

Lack of Segmentation: Without proper segmentation, an attacker who gains access to one device may be able to easily access other devices.

b. Star Topology Vulnerabilities

Centralized Vulnerability: The central hub (such as a switch or router) becomes a single point of failure. If the hub is compromised, the entire network is at risk.

Vulnerable to DoS Attacks: Since all communication passes through the central hub, any attack targeting this hub could disrupt the entire network.

c. Mesh Topology Vulnerabilities

Complex Management: With multiple redundant paths, mesh networks can become difficult to manage and configure. Misconfigurations or insecure devices could open multiple attack vectors.

Increased Surface Area: The large number of direct connections between nodes increases the number of potential points of entry for an attacker, making the network harder to secure comprehensively.

5. EMERGING TRENDS IN NETWORK TOPOLOGY AND ITS ROLE

The future of network topology is evolving rapidly with the advent of new technologies such as Software-Defined Networking (SDN), Network Functions Virtualization (NFV), and the increasing adoption of Internet of Things (IoT) devices and 5G networks. These emerging trends promise to transform the way networks are designed, managed, and secured. However, they also introduce a set of new challenges and open research questions that need to be addressed to ensure efficient, scalable, and reliable network infrastructures.

1. Software-Defined Networking (SDN)

(a) Overview: SDN separates the control plane from the data plane in networking, centralizing the network control in software-based controllers. This allows for more dynamic and programmable network management, where network policies can be applied centrally, making it easier to adjust routing, traffic flow, and security configurations.

(b) Impact on Topology: SDN enables more flexible and optimized network topologies that can adapt to changing conditions. Networks can be reconfigured on-demand, allowing for better management of resources and traffic patterns.

(c) Security in SDN: The centralized nature of SDN makes it an attractive target for attacks. Research into securing SDN controllers and data flows is critical.

(d) Research Directions: How to scale SDN architectures in large-scale, high-performance networks without sacrificing efficiency.

2. Network Functions Virtualization (NFV)

(a) Overview: NFV decouples network functions (e.g., firewalls, load balancing, routing) from proprietary hardware and runs them on standard servers. This allows for greater flexibility, cost savings, and scalability.

(b) Impact on Topology: NFV allows for dynamic network topologies where functions can be instantiated and decommissioned as needed. This increases the ability to adapt to traffic demands and fault tolerance.

(c) Research Directions: Designing and optimizing virtual topologies that can dynamically scale based on service demand and resource availability.

3. Internet of Things (IoT)

(a) Overview: Internet of Things (IoT) networking refers to the interconnection of physical devices, vehicles, buildings, and other items embedded with sensors, software, and network connectivity, enabling data exchange and automation. It improves efficiency, productivity and inform better decision making.

(b) Impact/Challenges: IoT networks are composed of various types of devices with different capabilities, which complicates network design. Data traffic and routing: Managing the massive data traffic generated by IoT devices in a scalable and efficient way.

(c) Research Directions: Designing network topologies that are optimized for IoT devices, such as low-power wide-area networks (LPWANs) or edge networks that process data closer to the source.

4. 5G Networks

(a) Overview: 5G represents the fifth generation of mobile networks, with promises of ultra-low latency, massive device connectivity, and high-speed data transmission. The network topologies for 5G will need to handle diverse use cases, including autonomous vehicles, smart cities, and augmented reality.

(b) Impact/Challenges: Ultra-reliable low-latency communication (URLLC): Ensuring high reliability and low latency for mission-critical applications like autonomous driving or remote surgery.

Massive device density: 5G will support a vast number of devices in a dense environment, raising questions about how to manage such a large number of simultaneous connections.

(c) Research Directions: Investigating how to partition a physical 5G network into multiple virtual networks (slices) optimized for different applications.

6. CONCLUSIONS

In conclusion, network topology is far more than just an organizational chart of how devices are connected; it directly impacts network performance, security, and scalability. As networks become increasingly complex with the rise of IoT, 5G, and cloud services, understanding and optimizing network topologies will be key to addressing current and future challenges in data management, security, and efficient service delivery.

Network topology plays a pivotal role in shaping the performance, scalability, and security of modern networks. The structure of a network—whether it's star, mesh, bus, or more dynamic configurations like Software-Defined Networks (SDN)—influences how data flows, how vulnerabilities are managed, and how easily a network can adapt to new demands.

Network Security is heavily influenced by topology. Centralized networks like those using star topology may have more straightforward security management, but they are also more vulnerable to attacks targeting the central hub. More complex networks, like those using mesh topology, offer redundancy and fault tolerance but are harder to secure.

The emergence of SDN and NFV is revolutionizing how networks are designed and managed. These technologies enable flexible, dynamic topologies that can scale with demand and adapt to changes on the fly, but they also present challenges in terms of scalability, reliability, and security.

Future applications such as IoT and 5G networks will require entirely new approaches to network topology. These applications demand ultra-low latency, high device density, and efficient management of massive amounts of data traffic, further emphasizing the need for innovative topologies.

References

1.Abdullah Khan (2023). Computer Networking Topologies. University Of Education, Lahore. https://www.researchgate.net/publication/369020366

2.Bangerter, S. Talwar, R. Arefi, and K. Stewart, (2014). "Networks and Devices for the 5G Era," IEEE Commun. Mag., 2014,

3.Deshpande, V., H. Badis, and L. George, (2018). "BTCmap: Mapping Bitcoin Peer-to-Peer Network Topology," in 2018 IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks, PEMWN 2018.

4.Diego, X., L. Marcon, P. Müller, and J. Sharpe, (2018). "Key Features of Turing Systems are Determined Purely by Network Topology," Phys. Rev. X,

5.Engels, G. (2018), "Clinical Pain and Functional Network Topology in Parkinson's Disease: A Resting-State fMRI Study," J. Neural Transm.,

6.Forouzan, B. A. (2012). Data Communications and Networking (5th Ed.). McGraw-Hill Edu.

7.Harrington D. L. (2015). "Network Topology and Functional Connectivity Disturbances Precede the Onset of Huntington's Disease," Brain,

8.Heasley, E., N. Clifford, and J. Millington, (2018). "Integrating Network Topology Metrics into Studies of Catchment-Level Effects on Habitat Diversity," Hydrol. Earth Syst. Sci. Discuss., 2018,

9.Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th Ed.). Pearson.

10.Ozkan-Canbolat, E. and A. Beraha, (2016). "Configuration and Innovation Related Network Topology," J. Innov. Knowl.,

11.Ozkan-Canbolat E. and A. Beraha, (2016). "A Configurational Approach to Network Topology Design for Product Innovation," J. Bus. Res.,

12.Rosell-Tarragó, E. Cozzo, and A. Díaz-Guilera, "A Complex Network Framework to Model Cognition: Unveiling Correlation Structures from Connectivity," Complexity,

13.Seetharaman, P., et al. (2017). "Software-Defined Networking: A Survey of Issues and Challenges." IEEE Communications Surveys & Tutorials, 19(3), 1992–2014.

14.Sharma, S., et al. (2020). "Design and Analysis of Network Topologies for Internet of Things." IEEE Access, 8, 43253–43262.

15.Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th Ed.). Prentice Hall.

16.Wierenga, L. M. et al., (2018). “A Multisampling Study of Longitudinal Changes in Brain Network Architecture in 4–13-year-old children,” Hum. Brain Map.,

17.Zhang, Y., et al. (2018). "Virtualized Network Topologies for SDN-Based Cloud Data Centers."