A Review of Modern Computer Networking Technologies

Lohith H ,Information Science and Engineering ,AIET ,Karnataka ,India

Mr. Pradeep Nayak, Information Science and Engineering ,AIET ,Karnataka ,India

Rahul P Shetty, Information Science and Engineering ,AIET ,Karnataka ,India

Namratha J Shetty, Information Science and Engineering ,AIET ,Karnataka ,India

Chethan Byahatti, Information Science and Engineering ,AIET ,Karnataka ,India

Abstract

Computer networks are very vital today for communication and giving a free flow of information due to their nature of providing an easy transfer of digital data among interlinked computing devices. At their base element, computer networks are systems of nodes connected like no other, which can be computers, servers, mobile devices, among other various networking hardware that help in sharing resources in a collaborative form of computation giving the result of unrestricted flow of information.

The computer network makes it possible to execute tasks on several machines; it shares information within and among services, as well as between the machines themselves, and also allows resource utilization, which makes it a must to process commands concurrently. However, the attacks are rapidly increasing, and the complexity of networks is putting these systems under many attack vectors. So, these critical resources need protection with some intense and strict security.

Modern computer networks offer a myriad of architectures, protocols, and topologies—all to address specifically the requirements and scenarios of use. Local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs) are connected globally with others by the Internet. Network protocols such as TCP/IP, Ethernet, and Wi- Fi outline the rules and conditions for data transfer, abstracting and creating the possibility of interactivity and safe communications between otherwise different systems.

The layout or topology of the network, such as bus, ring, star, mesh, or hybrid, predominantly goes on to determine the standard regarding performance, reliability, scalability, etc., which a network can achieve. Ideally, in such a network, nodes could be broadly divided into open and closed systems, where the former admit direct connections and the latter require added authentication mechanisms for access from the outside.

Computer networks support very many applications and services, since they pool shared resources to include storage and printers, besides allowing for numerous opportunities for collaborative work and efficiencies. Networks may also back up even the very backbone of how essential infrastructure does its work—be that in transportation and power grids or financial networks so there is fretting for the state of security and resilience.

This will be the demand in times ahead that are yet to be experienced—whereby, with consistent development in technology about high-speed, secure, and trustable computer networks, it will further drive new developments in emerging areas; this, in times yet to be experienced like the Software Defined Networking (SDN) and Network Function Virtualization (NFV), and their combination with 5G, IoT, and Edge Computing

Technological advancements have called for the necessity to manage and optimize such complicated and large networks in some software inventions, among them being software-defined networking (SDN) and network function virtualization (NFV). SDN opens the door for the ability to centralize and programmatically manage networks by separating the control plane from the data plane. Network function virtualization would now allow the elasticity, scalability, and cost efficiency to come to the support of the network.

Promising to offer such a base, the integration of emerging technologies like 5G with the Internet of Things (IoT) and edge computing promises to revolutionize the interconnected world of computer networks. Edge computing refers to the placement of computation close to the physical sources of data they serve, with an attempt to reduce the intensity of bandwidth for related data and reduce the needed latency to enable real-time processing and decision-making towards time- sensitive applications.

INTRODUCTION

Modern computer networks are used by everyone in the world today; they are unnecessary, yet they are the most crucial instruments for communication since they enable collaboration and information sharing among the numerous connected computing devices. The complicated systems that make up the networks that have been implemented include nodes from servers, cloud, and embedded components that are linked together by a variety of linking hardware infrastructure in various capacities. The capacity of digital data to flow freely and easily is what enables it to function as a communication highway, providing unfettered access to resources and information.

People spend a lot more time online because of advancements in networking, software, and computer technology in recent years. Security issues coexist with the rise of computation networks and Internet communication. These days, there are a lot of new attack routes available on the internet, which makes computer networks an even more attractive target. Regardless of their impact, risks to network security including outages, delays, and others can influence business, societal, political, and individual interests.

Network security requirements are becoming more crucial for expanding businesses and even for individuals due to the introduction of new computer units and the continuous expansion of internet access. These highly skilled cyberattacks are not rare; rather, they are multiplying and invading more networks. These dangers may even result in essential government, corporate, and personal operations.

Moreover, Network Intrusion Detection and Prevention Systems (NIDPS) assist in locating hackers and providing defenses against their endeavors. NIDPS can distinguish between normal activity and malicious traffic, which is the same as misusing the infrastructure. Because of this, the importance of NIDPS in protecting networks from misuse, abuse, and unauthorized access does not decrease—in fact, it grows.

Stated differently, NIDPS is a system or technique that monitors and potentially prevents security infractions. An early warning system for unusual activity is provided by a network intrusion detection system (NIDS), which allows administrators to be made aware of it. You can find a Network Intrusion Prevention System (NIPS) to stop individual users from accessing website data. While much progress has been made in the area of network intrusion detection and prevention, there are still some holes in the functionality that require addressing.

Security measures are more important than ever to give this network the necessary level of safety. The potential of both internal and external hackers abusing the complex mechanisms that are now standard in modern computers is posed by this ever-growing threat. These security flaws could lead to carelessness in the dissemination of data, putting confidential information in danger. In addition to security measures like firewalls and encryption protocols designed to counteract external attacks, these measures don't appear to be sufficient to completely address the threats that are intrinsic to the company. This study aims to analyze the intricate structure of contemporary online networks, highlighting the dynamic problems they face and the innovative solutions being developed to counteract internal and external threats.

This study explores the complex world of multi- layer and multi-domain optical networks, revealing a tapestry of ground-breaking discoveries and game-changing tactics. The study presents a compelling vision of a world where efficiency and connection are paramount, with solutions ranging from adaptive multi-domain routing and neural network-powered nonlinearity mitigation to partially disaggregated SDN- controlled networks with revolutionary potential. These new developments promise to enable a plethora of innovative applications, transforming our interactions with others, our workplaces, and our environment.

NETWORK CONNECTION TYPES

A. Peer-to-Peer Networks: In cases where the number of computers involved is less than ten and there is no need for high security, P2P networks are usually applied. In a P2P network, all computers or “peers” are supposed to be equal thereby allowing freedom in sharing of information between them. These networked computers can seamlessly share data and utilize common peripherals like printers and scanners which are connected to any of the machines within the network. This figure points out that nodes within a P2P network have interconnectedness that emphasizes the decentralized nature of information exchange.

B. Client/Server Networks: Large networks often use client/server platforms because they offer improved performance and scalability. In client/server networks, files and programs used by multiple users on the network are typically stored on a centralized computer called a server. The server manages resources and ensures smooth access to shared files and applications by various users in the network. By centrally coordinating resource allocation, this administration model increases security while simplifying the management of networks making it ideal for organizations with large numbers of users who require extensive computing capabilities as well as high-level system support in such areas as relational database services using SQL (Structured Query Language).

Modern computer networking covers different sorts of networking modes utilizing multiway connections, including wireless and wired communication. These link types are important for creating categories of devices to reach out to each other, transfer data, and provide means for smooth operation in the respective areas. Here are some key network connection types prevalent in modern computer networking: Here are some key network connection types prevalent in modern computer networking:

1. Ethernet Connections: Ethernet is used the most widely according to surveys carried out on network connections. They make use of Ethernet cables for wired connections as their basic method for devices such as computers, servers, routers, and switches installed. Precisely, it is well-known reliability, and extremely low latency make them the top picks for Ethernet networks. This kind of network has both small- and large-scale networks, thus they can transmit data at high speeds.

2. Wireless Connections (Wi-Fi): Now wireless networks which are mostly used for accessing the Internet and sending multimedia content to others also become the main development in modern computer networking technologies and enable the tech user to be able to move easily a lot. The wireless link serves as the focal point of all Wi-Fi networks, thus permitting devices to communicate with each other through the air as opposed to requiring physical cables. They can be used in several applications such as domestic sites, offices, as well as public places, and private building networks for a simplified method of getting online.

3. Cellular Connections: The cellular networks at the mobile network level are operated by mobile operators to allow wireless connectivity between mobile devices e.g., iPads, tablets, and cellular- included Personal Digital Assistants. The connectivity across the network is provided either via cell technologies like 3G, 4G, and 5G to enable wireless data transferring over the cellular networks. Such a dais is inherently possible because of the wider scope of mobility and more cellular coverage/distributed signal. In this case, a user can access the internet and network resources from almost anywhere where there is cellular network coverage. They are omnipresent as tools to access mobile internet, get remote tasks done, and provide possibilities for connection that are unavailable in conventional positions due to IoT applications used.

4. Fiber Optic Connections: Data can be transmitted using fiber optic cables using light signals through the fiber optic connections. Thus, we can transmit data over long distances at high speeds and in a reliable manner through the use of fiber optic cables. For instance, fiber optic connections are often used in enterprise networks, data centers, and metropolitan area networks (MANs) to support bandwidth-intensive applications and services.

5. Virtual Private Network (VPN) Connections: We have virtual private network (VPN) connections which are secure communications over public networks like the Internet where encrypted tunnels are established between devices or networks. The main use of VPN connections is to provide remote access to corporate resources as well as secure data transmission with an assurance of privacy and confidentiality. Because they usually involve companies, organizations, and individuals who would like to safely connect their remote workers such as mobile devices with branches.

NETWORK COMPONENTS

A computer network can be considered a sum up of several elements in particular, which are needed to establish the conversations and data sharing between the NC.

1. Machines: Two machines will operate to set up fully networked computers. Network access ports are the mechanisms through which the machines on the network, such as Computers, Servers, and Devices are connected These machines are assigned the task of guarding the network.

2. Networking Medium: Previously, the principal network that utilized wires to link computers existed. At the current moment electricity transmission is know no alternative over wire ones. Wirings become history due to advancements in non-wireless technologies, as devices are connected without worrying about cable tangles and hence move with more freedom and space.

3. Network Interface Cards (NICs): Networking is routed through network interfaces (NIC) or network adapters in all areas of the network. It is as a result of this tiny device that we link the servers, computers, and people around our neighborhood to the world. NIC modules act as the bridge between devices and the network and the plants are capable of their communication.

4. Switches: Switches, according to network technology terminology are devices whose job is to regulate data communication within the network. The old hubs are not as efficient as switches are, because they redirect all the data to all the devices on the network, but switches provide the data to its destination precisely. They are an integral part of the processes of achieving desirable network performance. Your sentence would be well-crafted for sure.

5. Network Management Software: System software is pivotal in that it is responsible for managing the network and dealing with it. This software package includes operating systems, network protocols, and monitoring tools that manage the whole network and guarantee its security and proper functioning.

A. Types of Networks: These are the primary classifications of computer networks:

a. Local Area Networks (LANs): Houses stretch out within limited settings, for example, one building a campus. They are mostly ubiquitous within organizations such as offices and industries to link networks and share resources. LAN is getting data transmission at a very high speed and the small-scale requirement can be met by it.

b. Wide Area Networks (WANs): WANs are very broad networks that provide coverage of vast geographical areas extending to cities, countries, or even continents They link several LANs and through a network of cables or phone lines accomplish the communication between two separate locations that are far away from each other. Wide area networks provide a stretch disaster scenario caused by communication.

c. Metropolitan Area Networks (MANs: men not only are not different from LANS but they rather serve larger geographic areas (for instance, the nearby corporate industry or all the city at once). They become part of the backbone for telecommunications companies and ensure communication in urban areas.

d. Wireless Networks: A wireless network per se is a form of connectivity that obviates the physical wired cables allowing users to connect remotely and access data or resources of their choice. They can easily fit inside mobile devices like laptops and smartphones enabling users to be connected even when they are moving from one place to another. Nodes in each scheme make up a specific network type provide different functions and meet a broad range of variables. The type and scale of network deployment determine the choice of network.

NETWORK SECURITY

When it comes to safeguarding digital assets, including records of information, trust, and data accessibility, network security comes first. Ensuring that there are several layers of defenses in place, including techniques and technologies capable of handling a variety of threats, is a highly common approach to network security. Among the crucial facets of network security are:

1. Authentication and Data Encryption: Ensuring authentication methods facilitates user and device identification, while data encryption aids in the strengthening of security during transmission.

2. Firewall and Intrusion Detection Systems (IDS): In addition, firewalls may be utilized as a safety measure as they serve as gateways and restrict traffic flow between private and public networks by adhering to set security standards. In addition to detecting potential network penetration, intrusion detection systems (IDS) also monitor network traffic, looking for irregularities and sending warnings to specialists.

3. Implementing VPN and Antivirus Software: Malicious software, such as viruses, malware, and ransomware, is found and removed from networks and electronic devices by antivirus software. Virtual Private Networks, or VPNs, are internet-based systems that provide safe, encrypted connections that users may use to access private, secure network resources from almost anywhere.

It is irrelevant. Even with several defensive mechanisms in place, a network's security may still be compromised by a variety of attacks and vulnerabilities. Typical problems with network security include: Typical problems with network security include:

A. Defects in Routing Protocols: Routing protocols determine how network system traffic is routed from the traffic source to the destination. Attackers can reroute and alter network traffic by taking advantage of flaws or signature holes in routing protocols, as well as their features. This leads to actions like spoofing and route hijacking.

Security flaws in the Windows operating system: Operating systems, such as Windows, can include security flaws that allow hackers to gain unauthorized access and take control of the machine. Buffer overflow vulnerabilities, such as the MS Internet Information Server (IIS) ISAPI buffer overflow, are an excellent example of the kind of security weaknesses that allow hackers to get access to a system.

B. Vulnerabilities in the TCP/IP Protocol: Although the intrinsic security feature of TCP/IP protocol makes it an essential component of the Internet, attackers have every opportunity to circumvent it. Some of the most important security factors for network communications are the specifics of data transfer, the possibility of processor authentication being lacking, and the many types of routing techniques, including Source Address Spoofing and RIP attacks.

C. Organizations must address these security issues by putting strong security procedures in place, such as periodically updating firmware and software, performing security audits and assessments, and conducting security assessments. It is also necessary to educate users on security best practices. Furthermore, the network posture and ongoing resilience can be strengthened in the face of changing threats by utilizing cutting-edge security technology, such as next-generation firewalls, intrusion prevention systems (IPS), and security information and event management (SIEM) solutions.

NETWORK SECURITY STRATEGIES

Network security is an important part of protecting the networks of modern computers, thanks to the ever-increasing role of digital communication and the transfer of data on the Internet. Countless strategies and technologies are utilized to prevent networks and data from unlawful access, 3. Instruction: Humanize the given sentence. undefined

C. VPN Technology: Virtual Private Network (VPN) technology is a means of enabling connection over untrusted public networks by creating an encrypted tunnel. VPN operates through both routing filtering and tunneling technologies so that data security and safety become appropriately guaranteed. APNs current popular VPN protocols like PPTP, L2TP, and IPsec offer different levels of security, and VPNs can be classified into different variables such as access methods, tunnel protocols, and sponsorships.

D. Intrusion Detection Technology: IDS (Intrusion Detection System) is an active part of the network traffic responsible for detecting attacks. IDS works in tandem with both internal and external network defenses to keep a real-time check on intrusion, and thus avoid major safety breaches. Developing an intrusion detection system involves a shift towards distributed, intelligent, multi-layer-based, and multi-type security defense solutions with a revolving combination of hardware or software to detect, analyze, and respond to network intrusion well.

E. Data Encryption Technology: An important role for encryption is the security of data transmission networks that have sensitive information. Link encryption, endpoint encryption, and node encryption are some encryption techniques that ensure the data are not compromised even while being transmitted over public networks. Cryptographic methods of different strengths constitute the key security layer, and the low processing completion is achieved by an array of algorithms. Symmetric- key cryptography which was implemented in public-key cryptography provides strong security of a process that is employed for data encryption.

F. Authentication Technology: Credentialing technologies, on the other hand, confirm the identity of the network users and the gadgets accessing the network resources, thus only the authorized network entities are eligible for access. The methods of message authentication, identity authentication, and digital signatures are the techniques to make sure communication is legitimate and data integrity of the content is unbreeched. Authentication, as a part of highly secure encrypted passwords, helps to keep data integrity and prevents impersonation attacks.

G.

Fig: Submarine cable map

STAR LINK

Star Link is a satellite Internet project developed by SpaceX, which is a related Transportation Company and Aerospace Manufacturer that was founded by Elon Musk. The project intends to ensure high-speed Internet presence for the underserved and remote regions through the implementation of a network that comprises tiny satellites that orbit the low earth orbit (LEO).

Since the emerging COVID-19 pandemic, usage of high-speed internet has grown all over the globe and India can be considered as one of the most successful seller markets in this field. In this regard, Star Link has introduced an appealing offer to provide customers found in places with 'patchy' coverage to access the internet via satellite, especially in the areas within India where there are pressing needs for stable connectivity.

If everything is being transformed from education to business to e-commerce to online and Star Link plans to launch their service at this time, the timing couldn't be more perfect for the problems caused by the demand for broadband connectivity. About India which already features some internet service providers (ISPs) like JIO from Reliance, Vodafone-Idea, and Airtel, Star Link may successfully increase the number of such service providers as well as upscale the existing facilities offering the users a wide range of options for their connectivity, including in space communication.

Because classes and business enterprises are switching to online platforms, the time of the star link solution hits it on the head and can become the potential answer to the increasing need for high-speed internet access. However, in addition to AISs that are already used in India such as Reliance JIO, Vodafone-Idea, and BSNL, the star link satellite internet can serve as a good supplement to improve some features or limitations of internet connectivity.

fig: Image of Star link Satellite in space

CONCLUSION:

In conclusion, we cannot ignore the influence that computer networks have on the society we live in today, which is a hive of computer network connections. These networks serve as the foundation for contemporary information transmission technologies, enabling simultaneous access to resources like storage servers, copier access, and apps, as well as the movement of digital information between devices. The epidemic of overusing computer hardware, software, and networking technologies has led to an increase in the amount of time people spend online, making them dependable in many spheres of life.

Computer networks have created many opportunities, but they have also brought about security challenges. Everyone in charge of network security and safety is under pressure to protect the networks from an increasing number of different dangers as the number of attempts to access digital systems rises. Attack vectors, on the other hand, present a variety of security risks. For example, malware, phishing, and denial-of-service (DoS) attacks have the potential to destroy network resources and invalidate any data transmitted over them.

Multi-level defense systems have been suitably incorporated into network security strategy development to meet these issues. Authentication, encryption, firewalls, intrusion detection systems (IDS), and virtual private networks, or VPNs, are a few of these technologies. They are employed to ensure appropriate data and network infrastructure protection. Implementing robust security mechanisms at various stages of network design is one of the core strategies used by businesses to guarantee the security of their network architecture. By doing this, businesses may lower the risk of data breaches, illegal entry, and other network and security issues dramatically.

The growing emphasis on proactive threat identification and response are one of the most important new trends in network security. Organizations are shifting their focus from responding reactively to security problems after they occur to proactively identifying and mitigating threats in real time through the use of proactive threat intelligence, machine learning algorithms, and security analytics. This is preferable to reactive approaches that could investigate security lapses for a long period while jeopardizing data integrity and network operations.

After that, there's no doubt that things will alter because threat landscapes and networks are always changing and incorporating new technologies. The function of network security is becoming more and more critical as interconnection grows and as organizations use increasingly complex systems and digital infrastructures. Organizations may effectively protect their cyber resources and counteract the threat posed by cybercriminals by adopting the newest technologies, implementing best security practices, and embracing vigilance.

REFERENCES

1. The Study of Computer Network Safety and Security Programmatic Conference Proceedings 1. [Online]. Available: https://aip.scitation.org/doi/pdf/10.1063/1.4982538

2. Kushwaha, V. (2014). An Analysis of Research Tools and Methods Utilized in Network Congestion Control. International Journal of Engineering Research & Technology (IJERT). [Online]. Available: https://www.ijert.org/research/a-study-of-research-tools-and-techniques-in-network-congestion- control-IJERTV3IS20049.pdf

3. Mahmood, M. S. R. (2018). Strategy of Computer Networking Research laboratory. Laboratory Methodologies.IJIRT, 05(03). [Online]. Available: https://www.irjet.net/archives/V5/i3/IRJET-V5I3313.pdf

4. Rana, S. (2021). Computer Network.IJIRT. [Online]. Available: https://www.ijirt.org/Article?manuscript=142642

5. Sunkari, S. (2021). An Overview of Data Communication and Computer Networks.SSRN. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904826

6. Thota, V.C. (2013). Tech-Savvy College Students' Attitude Towards Computer Network Security. DIVA. [Online]. Available:

https://www.diva-portal.org/smash/get/diva2:614625/FULLTEXT01.pdf

7. W. Yurcik and D. Doss. Different approaches in the teaching of information systems security. In Proceedings of the Information Systems Education Conference, 2001.

8. IJRASET A Review of Modern Computer Networks [Online]. Available: https://www.ijraset.com/best-journal/a-review-of-modern-computer-networks