GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

A comprehensive survey of performance, security and privacy issues in the network interface layer of the TCP/IP

Emmanuel Asituha *

Department of computer science & software engineering, Jaramogi Oginga Odinga University of Science and Technology Bondo, Kenya.

GSC Advanced Research and Reviews, 2024, 18(03), 208–233

Publication history: Received on 04 February 2024; revised on 10 March 2024; accepted on 13 March 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.18.3.0112

Abstract

The network interface layer of the TCP/IP protocol suite, primarily comprised of the Internet Protocol (IP), serves as the backbone of modern internet communication. With its efficient data delivery, The network interface layer, presents key challenges in terms of performance, security, and privacy. This comprehensive survey delves into these three crucial aspects, analyzing the inherent vulnerabilities, limitations of the interface layer, and provide solutions of the related problems. The performance analysis explores throughput, latency, and bandwidth constraints, along with solutions such as bandwidth allocation and optimization techniques. Vulnerabilities within Network Interface Layer, including denial-of-service attacks and MAC address spoofing, are discussed, along with a review of existing security mechanisms. Privacy flaws are examined, covering MAC address tracking, profiling risks, and anonymization techniques, while also addressing privacy considerations on the Internet of Things. The survey analyzes several case studies providing comparative analysis of the network interface layer protocols, with support of the real world scenarios including performance analysis in high density environment, and security and privacy risks in smart homes networks. The findings provide a comprehensive understanding of the complexities surrounding performance, security, and privacy issues future directions and potential solutions.

Keywords: TCP/IP; NIL; Anonymity; Heterogeneous; Packet Fragmentation and Aggregation; Congestion Control Algorithm; MAC Address; Regulating Privacy

1. Introduction

Transmission Control protocol and Internet protocol (TCP/IP) was developed in the 1970s and adopted from ARPANET (the predecessor to the Internet) in 1983 [1]-[5]. As shown in Figure 1, the TCP/IP Protocol Suite is made up of a layered model, consisting of the application layer, transport layer, internet layer, and network interface layer, each having different functionalities in the suite. The TCP/IP protocol performs various functions in network communication, congestion, and error concealment in the application layer, end to end error recovery, transmission, and flow control in the transport layer, provision of logical addressing and routing of data packets using Internet protocol like, IPv4 in the internet layer, and the network interface layer, which is our main point of concern, it combines raw data into data frames, provides a physical interface for data transmission[6]-[9]. The theoretical frameworks of the network interface layer in TCP/IP includes understanding the network interface layer architecture, protocols, and standards that govern communication between devices at the physical and data link layers. This includes protocols such as Ethernet, Wi-Fi, and PPP (Point-to-Point Protocol), which define how data is transmitted and received over network interfaces [10]-12].

* Corresponding author: Emmanuel Asituha

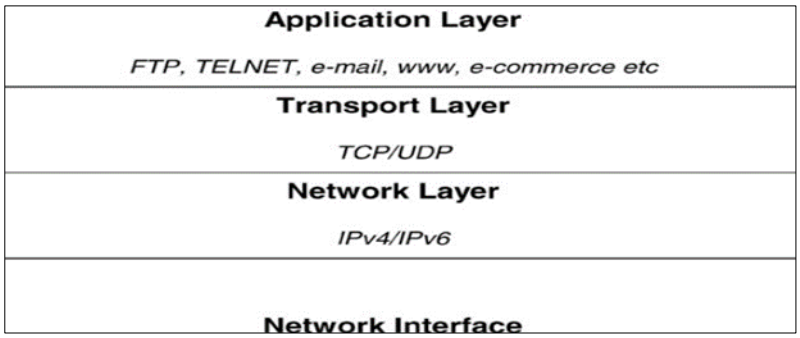

Figure 1 TCP/IP protocol suite

Extensive research has been done on network interface layer performance, security, and privacy issues [13]-[16]. Techniques like network traffic mapping, congestion control algorithms, and efficient routing protocols have been explored to improve network performance of the network interface layer. Researchers have identified and proposed mitigation mechanisms on various vulnerabilities in the network interface, such as Address Resolution Protocol (ARP) spoofing, Media Access Control (MAC) address spoofing, and Denial-of-Service (DoS) attacks [17]-[20]. Traffic sniffing, network intrusion detection, and user tracking in the network interface layer raise privacy concerns that researchers are actively addressing [21]-[24].

There is great significant advancements that have been made, despite this achievement, there are challenges in the network interface layer; trying to balance between performance and security can a times impact the network performance. New attack vectors and vulnerabilities emerge constantly, demanding ongoing research and development of robust security solutions [25], [26]. Balancing the need for network monitoring and security with individual privacy rights remains an ongoing debate.

The network interface layer plays a vital role in today's interconnected world, impacting various aspects of society and culture, e-commerce and online services needs, secure and reliable network interface layer for the smooth functioning of online activities [27]. Technological advancements are shaping the future of the NIL, Software-defined networking (SDN), provides greater flexibility and control over network traffic management, potentially improving performance and security in the network interface layer. Network function virtualization (NFV), allows for virtualization of network functions, potentially improving scalability and security in the NIL [28]-[30]. Emerging network technologies: New technologies like 5G and the Internet of Things (IoT) pose new challenges and opportunities regarding performance, security, and privacy in the NIL.TCP/IP is the foundation of modern networking. It's always changing and getting better to keep up with how much we use the internet [31], [32]. Because it's strong, can handle lots of traffic, and works well with different systems, it's the main way computers talk to each other worldwide. TCP/IP keeps improving, like with IPv6, which helps solve the problem of running out of internet addresses. It's a big part of how we stay connected, share information, and work together online [33]-[36].

1.1. Motivation of the Study

The network interface layer of the TCP/IP protocol suite is vital for internet communication, yet ongoing research and improvements are driven by several key issues. Performance motivations include accommodating the increasing demands on the internet, adapting to emerging technologies like IoT and 5G/6G, and addressing congestion and delay [37], [38]. Increased cyber threats, the lack of end-to-end encryption leaving data vulnerable, and privacy concerns arising from IP addresses and traffic analysis; the need to protect sensitive data, concerns about third-party access and data misuse, and identifying and mitigating privacy risks introduced by emerging technologies like SDN [39]. Overall, the study of performance, security, and privacy issues in the TCP/IP network interface layer aims to maintain and enhance internet efficiency, strengthen network security, and safeguard user privacy.

1.2. Research Contributions

This paper extensively provides an understanding of the performance, security, and privacy issues of the network interface layer of the TCP/IP. The research starts by providing a clear understanding of the architecture, and functionality of the network interface layer. The findings of the survey contribute to the existing body of knowledge; providing researchers, policymakers, and industries, a clear understanding and knowledge of the performance, security, and privacy issues at the network interface layer of the TCP/IP. The findings of this study offer valuable contributions

to the knowledge base on the network interface layer, aiding in the development of more secure, efficient, and privacy-preserving network communication systems:

- *Comprehensive Analysis:* It provides a comprehensive and in-depth analysis of various performance, security, and privacy issues impacting the network interface layer of the TCP/IP protocol suite.
- *Comparative Analysis:* It includes a comparative analysis of different network interface layer protocols, evaluating their performance, security strengths and weaknesses, and privacy considerations.
- *Real-world Scenarios:* It incorporates real-world scenarios like smart homes and open Wi-Fi networks, highlighting the challenges they pose and providing insights into potential solutions.
- *Mitigation Strategies:* It presents various mitigation strategies and best practices to address performance bottlenecks, security vulnerabilities, and privacy concerns in the NIL.
- *Ethical Considerations:* It emphasizes the importance of ethical considerations and regulatory frameworks in governing data privacy practices within the NIL
- *Future Research Directions*: It identifies future research directions by outlining areas like 6G, Software Defined Networking (SDN), and Network Function Virtualization (NFV) that require further exploration to enhance NIL performance, security, and privacy.

1.3. Structure

The paper is structures as follows: The first section provides an introduction of the survey; detailed background analysis, research motivation, contributions, and the methodology used in the research. Section 2 introduces an understanding of the architectural design of the network interface layer, protocols, and data flow within the layer. Section 3 delves into performance challenges; heterogeneous networks, congestion control algorithms, and ineffective network interface protocols. Section 4 discuses the security concerns; Denial of Service attacks, Zero day vulnerabilities, and Wiretapping and Eavesdropping. Section 5 analyzes the privacy concerns in the layer, providing an analysis of MAC address profiling and tracking, and mechanisms in regulating privacy. Section 6 provides a comprehensive analysis of the real world scenarios in performance, security, and privacy issues in network interface layer. Finally section 7 concludes the research, and providing future directions.

2. Methodology

In this study, the following methodologies to be used in order to fully do a comprehensive research:

- **Literature Review:** A review of existing research papers, literature/articles and technical documents on performance, security, and privacy in the TCP/IP network interface layer will be used. This will involve gaining information on current challenges, and best practices in mitigation.
- **Performance Evaluation:** Performance evaluation will involve analyzing factors such as throughput, latency, bandwidth constraints, and packet loss in the TCP/IP network interface layer. Optimization techniques, buffering and queuing mechanisms will be employed to improve the performance metrics.
- **Security Analysis:** Security analysis will focus on identifying vulnerabilities, threats, and attack vectors in the TCP/IP network interface layer. Common security mechanisms such as encryption, authentication, and access control will be evaluated for their effectiveness in mitigating these risks.
- **Privacy Assessment**: Privacy assessment will involve examining MAC address profiling and Tracking, and the privacy risks in IoT. Anonymity and pseudonymous techniques will be discussed as some remedies.
- **Recommendations and Future Directions:** Based on the findings of the survey, recommendations will be provided for improving performance, enhancing security, and protecting privacy in the TCP/IP network interface layer. Future research directions and areas for further investigation will also be identified.

2.1. The Architecture

The network interface layer, also known as the Link Layer or Network Access Layer, is the lowest layer in the TCP/IP networking model [40], as evident in Figure 2 below. It's primarily mandated with the transmission of data over the physical network medium. This layer defines the protocols and mechanisms necessary for devices to connect to and communicate on a local area network (LAN) or wide area network (WAN) [41].

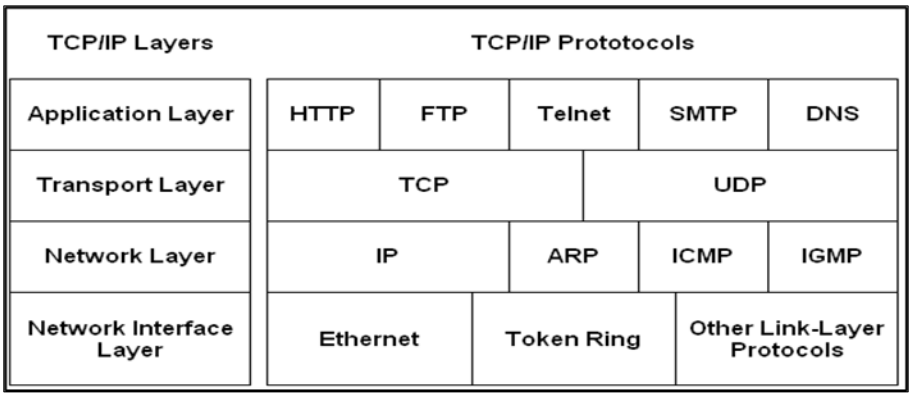

Figure 2 TCP/IP Layers

It consists of the following components:

- **The Network Interface Card** – it is the hardware devices that connect the host device to the network, it converts digital data into electrical signal so that it can be transferred over a physical media [42], [43].
- **Device drivers** – It is the software that allows the host computer's operating system to directly communicate with the network interface layer. it translates data formats [44] and provides instructions for the Network interface card to either receive or send data [45].
- **Media Access Control (MAC)** – adds network access segment on the local network segment, adding MAC address to each data packet for ease identification in the local network [46].
- **Physical Layer** – Deals with the transmission of data bit over the media, it also defines the electrical or optical signaling standard to be used [47].

2.2. Data Flow

A packet is the smallest unit of data that is transmitted over a network, it consists of the packet header, and payload [48]-[50]. As shown in Table 1 below, it demonstrates how such packets move in the network interface layer of the TCP/IP, using the top-down approach.

Table 1 Data Flow in Network Interface Layer

INCOMING PACKETS		
Network Media	***NIC Hardware***	***Device Drivers***
Electrical/Optical Signals	**Converts to Digital data**	**Translates frames format.**
MAC Layer	*Higher Layers*	
Verifies Integrity Checksum	Processes based on Destination and protocol information	
OUT-GOING PACKETS		
APPLICATION	HIGHER LAYERS	MAC LAYER
Generates data	Encapsulation	Adds Source and Destination MAC Address
Device Drivers	*NIC Hardware*	*Network Media*
Translates Frame Formats	Converts to electrical/optical Signals	

To fully ensure comprehensive data flow, set of rules called protocols are used to define how communications takes place in the Network interface layer [51] - [54]. Table 2 below summarizes the protocols and their basic functionalities. The Network Interface Layer, often referred to as the Link Layer in some models, is crucial in the realm of computer networking as it encapsulates the networking communication over physical hardware. At this layer, data flow is fundamentally about the transmission of packets between devices on the same network segment or link. It is responsible for the final encapsulation of higher-level frames into packets or bits that can be transmitted over network mediums like Ethernet, Wi-Fi, or other types of physical links. This involves not only the framing of data but also

addressing using MAC (Media Access Control) addresses, error detection and possibly correction through CRC (Cyclic Redundancy Check), and controlling access to the physical medium, ensuring that packet collisions are minimized in environments like Ethernet networks.

The process of data flow at the network interface layer is characterized by its close interaction with the hardware. Here, protocols such as ARP (Address Resolution Protocol) play a pivotal role in mapping IP addresses to the physical MAC addresses required for packet delivery on the same network. This layer is where the abstraction of data transmission over a physical medium becomes tangible; the digital data prepared by higher layers of the OSI model (or the Internet model) is converted into signals (electrical, optical, or radio, depending on the medium) that are transmitted over the connection. The layer's responsibility extends to the reception of incoming packets, their conversion from physical signals back into digital format, and their handoff to higher layers for further processing. This bi-directional flow of data ensures that the network interface layer is a critical junction point in the network stack, where the abstract world of network protocols meets the physical reality of network cables and signal transmissions.

Table 2 Network interface layer Protocols

Protocol	Functions
Ethernet (IEEE 802.3)	It defines the set of rules for grouping data into frames and transmitting them over a physical network medium.
Wi-Fi (IEEE 802.11)	It defines protocols for transmitting data over radio frequencies, handling network access and security, and managing communication between devices within the same network [55], [56].
Point-to-Point Protocol (PPP)	It establishes direct connection between two nodes across a sea, encapsulates IP packets for transmission over the serial link and provides features such as authentication, error detection, and dynamic addressing [57]-[62].
High-Level Data Link Control (HDLC)	HDLC is a bit-oriented protocol used for communication over synchronous serial links. It provides framing, error detection, and flow control mechanisms for reliable data transmission between devices [63], [64].
Frame Relay	Frame Relay is a packet-switching technology used in wide area networks (WANs). It defines the format of frames for transmitting data between network devices over a shared network infrastructure [65]. Frame Relay supports variable-length frames and provides mechanisms for congestion control and error detection.
Asynchronous Transfer Mode (ATM)	ATM is a cell-based switching technology used in both LAN and WAN environments. It breaks data into fixed-size cells and switches them through the network based on predefined routes [66], [67]. ATM provides high-speed, low-latency communication [68] and supports various types of traffic, including voice, video, and data.

3. Performance issues in Network Interface Layer

This section presents the performance of the network interface layer, digging deep into the performance challenges, and proposed solutions that can stabilize or increase performance.

3.1. Heterogeneous Networks

Heterogeneous Networks (HetNet) is a networking infrastructure that consist of different components, such as devices, protocols, and transmission mediums. The nature of heterogeneity comes in hardware, software, protocols, and network architecture [69]-[74]. Several challenges affect the performance of heterogeneous Networks in the network interface layer, discuss two main challenges will be discussed below.

3.1.1. Transmission Medium Difference

Transmission medium often differs from one architecture to another, transmission can be accomplished through fiber optics cables, copper cables, and the wireless radio frequency models etc. All the said mediums do have different characteristics ranging from bandwidth, error rate, and latency [75]-[79]. All of these characteristics of a transmission medium affect the performance of the network interface layer positively or negatively. In the Table 3 below, it provides a summary of different transmission mediums and how they impact performance [80] – [82].

Table 3 Transmission Mediums Performance

Transmission Medium	Bandwidth	Error Rate	Latency	Performance
Fiber Optics Cables	Extremely High	Very Low	Very Low	Optimal performance, low processing load, minimal transmission rates
Copper Cables	Moderate	Moderate	Moderate	Good performance
Wireless Radio Frequencies	Variable	Moderate	Variable	Performance depends on signal strength, congestion, prone to interference

3.1.2. Packet Fragmentation and aggregation

Packet fragmentation is the division of large chucks of data packets into smaller fragments to fit within a Maximum Transmission Unit (MTU) size of a network infrastructure [83], [84]. The MTU is the largest frame size which is 8 bit bytes that can be sent over to the packet. In a heterogeneous environment, different network architectures have different MTU frame sizes. For example, large sized packets are to be transferred, on a smaller MTU frame size, packet fragmentation is needed to ensure successful delivery. However, these fragmented packets will require that they are recollected together again at the receivers end which results to increase in latency [85], leading to low throughput, especially when the packets are not successfully delivered [86] – [89]. Figure 3 below demonstrates the packet fragmentation process [90].

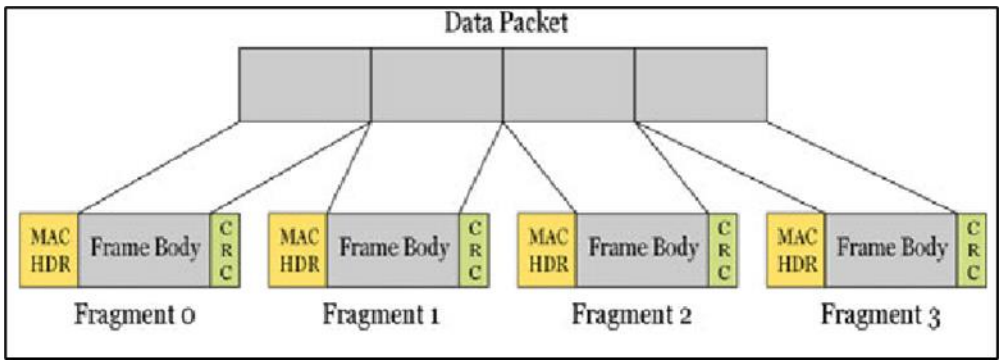

Figure 3 Packet Fragmentation

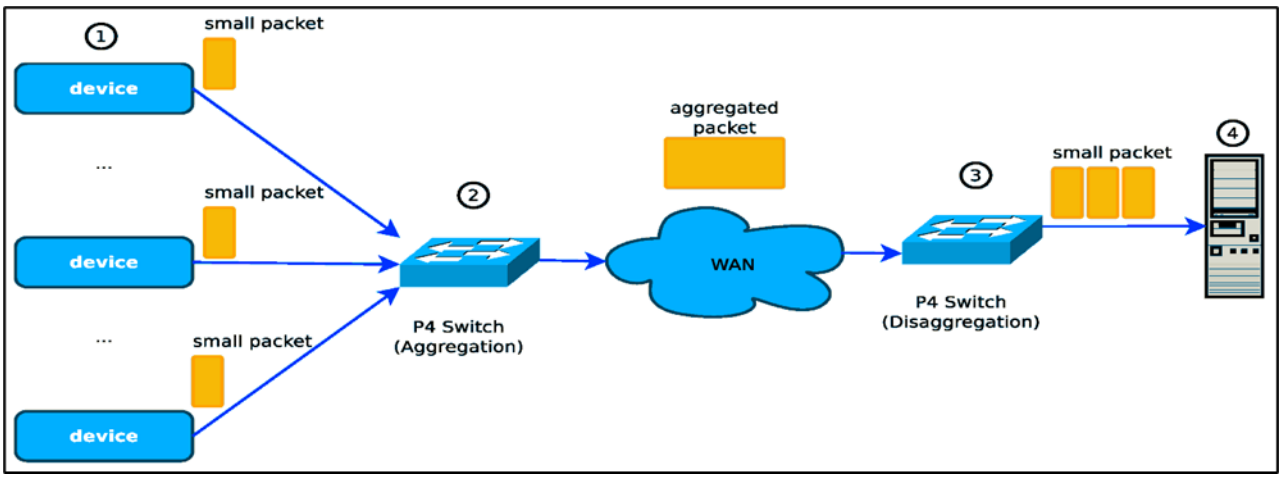

Figure 4 Packet Aggregation

In packet aggregation, it is the process of joining several small packets into a single large packet just before transmission as in Figure 4 below [91]. It is advantageous that this aggregation improves throughput, reducing on latency especially

where the network infrastructure supports voluminous data packets. However, the aggregation may also introduce challenges in managing packets, due the packets large number which in result may affect performance in some network architecture [92] – [95]. Consider a situation whereby large packet encounters errors or needs re-transmission, the entire packet needs to be resent, causing delays; some devices might not have enough buffer space to handle large packets, leading to congestion and delays.

3.2. Congestion Control Algorithms

Congestion control is a technique that controls the movement of data packets in a networking environment. TCP has implemented numerous models including congestion control algorithms to increase efficiency and increase performance of the network interface layer, this technique uses functionality like congestion avoidance, fast recovery, etc. [96]. However, such algorithm directly influences latency by altering with the sending rate, when the sending rate triggered by the algorithm is low, it impacts the throughput of packets leading to low performance [97]-[100]. The processing of this control algorithms adds up to the network interface layer workload. The complexity and sudden changes in the structure of the algorithm generally impacts the performance. Figure 5 below illustrates these congestion control algorithms.

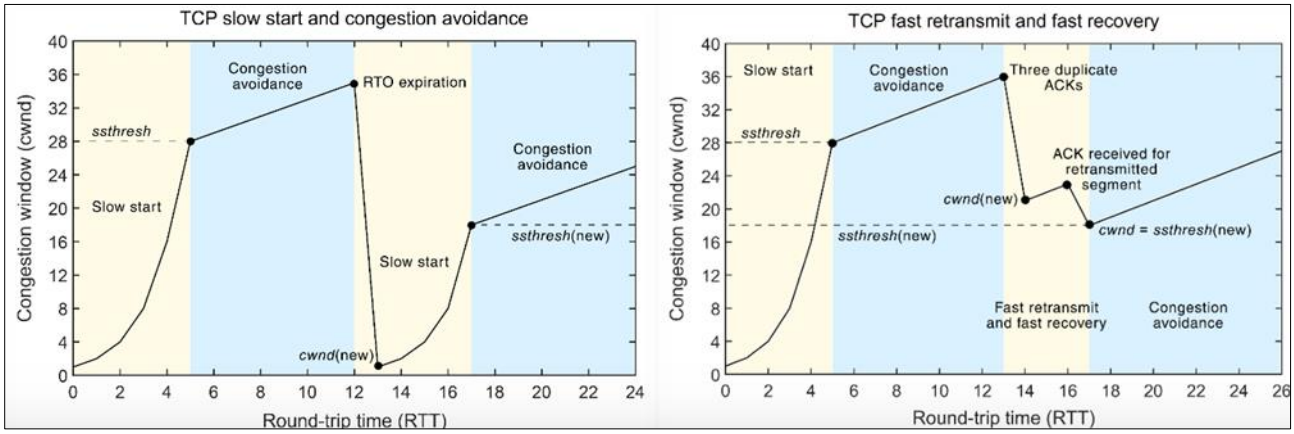

Figure 5 Congestion control algorithms

Transmission Control Protocol (TCP) has implemented utilizes various congestion control algorithms to manage congestion and optimize performance. Examples include Tahoe, Reno, New Reno, and TCP Vegas [101]-[103]. These algorithms use mechanisms like slow start, congestion avoidance, fast transmitted, and fast recovery to regulate the transmission rate based on network congestion signals such as packet loss and round-trip time [104]. In Table 4 below, it discusses some congestion control algorithms, their functionality and how they affect performance [105]-[109].

Table 4 Congestion Control Algorithms

Congestion Controls Algorithm	Function	Performance
TCP Reno	Acts as an alert for congestion due to packet loss.	Slows performance.
TCP Vegas	Congestion is detected before packet loss occurs.	Improves efficiency, but can lead to network connection delays/breakdown, slowing performance.
QUIC (Quick UDP Internet Connection)	Uses the network models predict packet size and sending rates.	Need for efficient calculation, increasing on workload, slowing performance

3.3. Ineffective Network Layer Interface protocols

The network interface layer has several protocols that ensure effective performance [110] of the layer as it is dependable the upper layers of the TCP/IP suite [111]. In a networking environment the TCP/IP suite is integrated into different infrastructure, this presents different performance metrics such protocols. For example, ethernet protocol, which its main role is to resolve the IP address of the Network Interface Card to their respective MAC addresses. The ethernet has some overheads that can impact the performance as shown in Figure 6 below [112], [113]. Ineffective

network layer interface protocols can create significant barriers to efficient and secure data communication within networks. Such protocols may exhibit poor performance in handling data packets, leading to increased latency, packet loss, and even total network failure under high traffic conditions. For example, protocols that are not designed to efficiently manage network congestion can result in excessive delays and dropped connections, severely impacting applications that rely on real-time data transmission, such as video conferencing or VoIP services. Additionally, these inefficiencies can escalate operational costs due to the need for more extensive network infrastructure to compensate for the shortcomings in data handling and transmission capabilities.

On the security front, ineffective network interface layer protocols are particularly concerning as they can leave networks susceptible to a variety of attacks, including interception, modification, and denial of service (DoS). Protocols lacking robust encryption and authentication mechanisms fail to protect data integrity and privacy, making it easier for attackers to exploit vulnerabilities. Furthermore, inadequate security features may not comply with regulatory standards, exposing organizations to legal and financial repercussions. The evolution of cyber threats necessitates continuous updates and improvements to these protocols to safeguard against emerging vulnerabilities and ensure compliance with current security standards. The efficiency and security of network interface layer protocols are therefore critical to the overall health and performance of computer networks, underscoring the importance of adopting and maintaining effective and up-to-date networking standards.

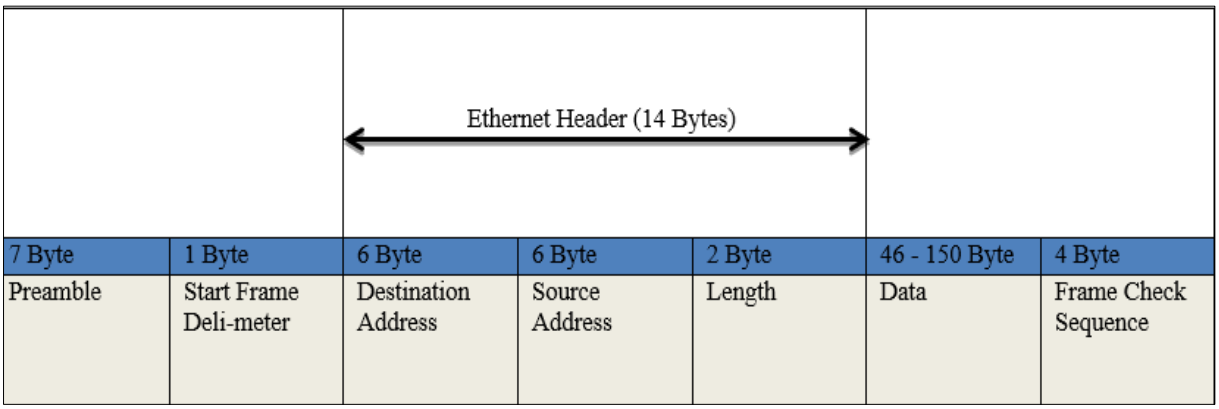

Figure 6 Ethernet Overhead

The Ethernet MTU is set to 1500 Bytes, only 1460 bytes is considered as a maximum data that a Ethernet frame can carry, therefore additional 20 bytes IP headers and 20 Bytes TCP header is needed to sum up to 1500 Bytes. If more than 1500 Bytes are to be sent over the network, it will be require that it is fragmented before it is sent, which can affect performance as discussed in packet fragmentation and aggregation [114], [115].

4. Security Concerns In the network Interface layer

The network interface layer is of importance to the TCP/IP Model as it is responsible for actual transmissions of data over the physical medium such as the Ethernet and WiFi, however despite its complexity in functionality, several security threats can target this layer, these includes of Denial of Service attacks, Zero Day vulnerabilities, and Wire tapping/eavesdropping [116]-[118].

4.1. Denial of Service attacks

Denial of Service attacks is designed to disrupt the normal functionality of the network interface layer by sending to many packets on the network that causes flooding, preventing normal operations like users accessing network resources [119]-[122]. This impacts the security of the network interface layer in several ways:

Excessive traffic and packets sent by the attacker to the network leads to consuming of the bandwidth, and exhausting computing resources such as the memory. This kind of attack involves sending fragmented packets with a malicious intent, in return the fragmented packets overwhelmed the target machine, which causes excessive processing power to reassemble the packets influencing the performance of the Network interface [123]. In Table 5 below, it discusses common types of DOS attacks in the Network Interface Layer, and proposed mitigation strategies [124] -[127].

Table 5 Types of DOS Attacks

DOS Attack	Explanation	Examples	Mitigation
Fragmentation Attacks	it exploits vulnerabilities to send fragmented packets that exhaust network resources [128] when reassembled.	Ping of Death	Packet Inspection
Flooding Attacks	It floods the network with a large volume of traffic, making the receiver become overwhelmed, and not able process legitimate traffic	SYN Floods, ICMP Ping Flood, and UDP floods	Traffic rate limiting and filtering
MAC Address Spoofing	DOS attack spoof MAC addresses to flood the network, leading to network congestion	Impersonation	Real-time traffic analysis.

In Figure 7 below, it depicts an attack take place, the attacker overwhelm the network infrastructure by flooding it with excessive traffic or exploiting vulnerabilities in network devices. This flood of traffic can consume bandwidth, exhaust resources like CPU or memory, or disrupt network connectivity, making legitimate network communication impossible [129]-[134].

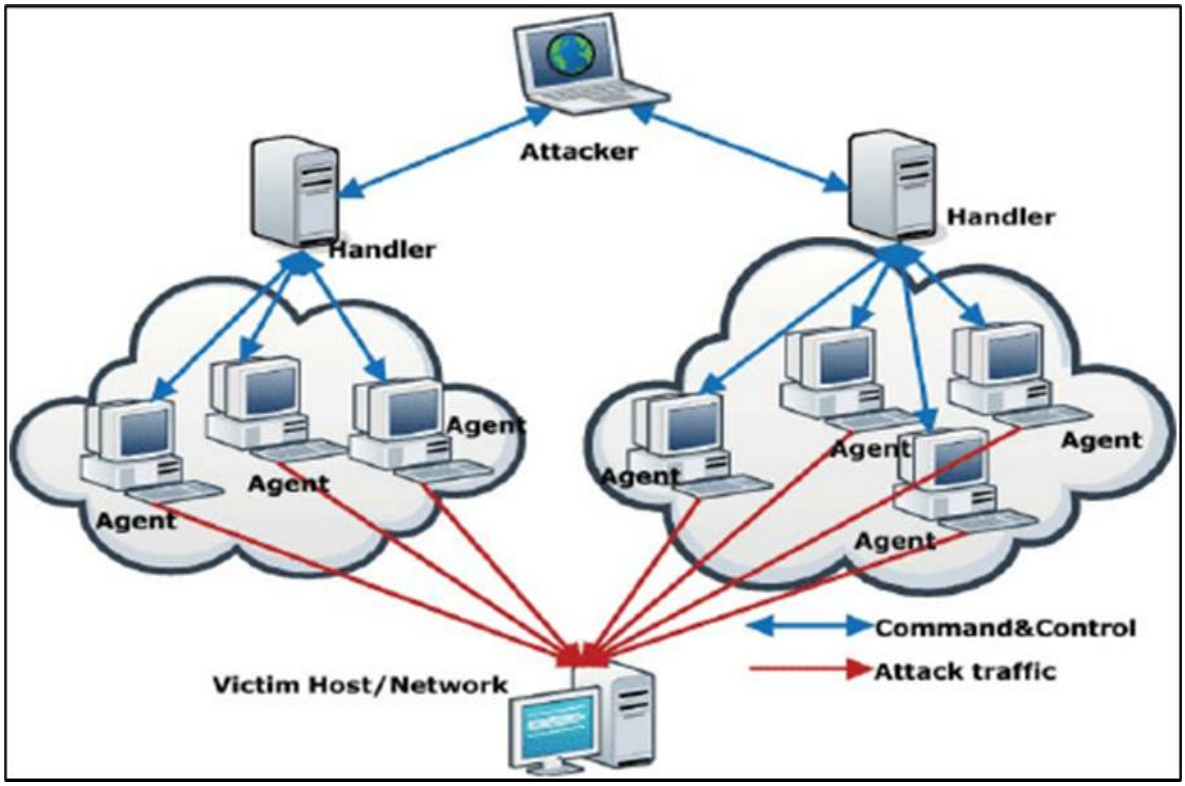

Figure 7 Typical DOS Attack

4.2. Zero-day Vulnerabilities

A zero-day vulnerabilities are kind of attacks that attackers exploit unknown vulnerabilities in the network infrastructure that has not yet being patched [135]. The zero-day vulnerabilities affect protocols in the network interface layer to execute unknown code, alter with normal communications and intercept traffic. For example in MAC protocol, attacker can exploit zero-day vulnerability in the MAC protocol altering with the MAC address leading to MAC address spoofing. Networking devices in the Network interface layer can be compromised to exploit unknown vulnerabilities leading to manipulation of traffic, access to unauthorized resources leading to disruption of services, impacting performance[136]. Figure 8 below explains how the zero day attack takes place, from its creation, release, exploitation, and patch release and deployment [137]-[139].

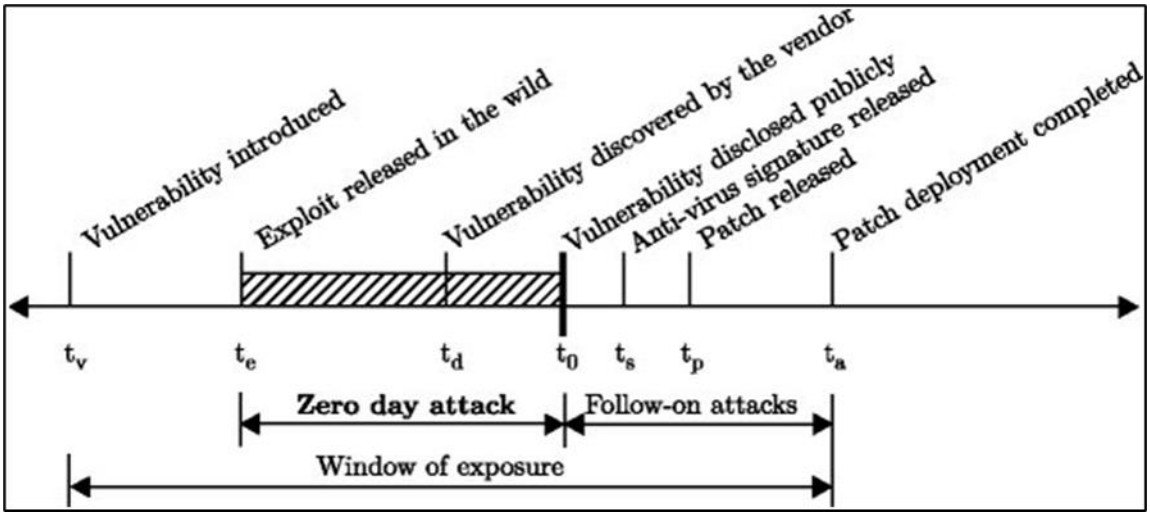

Figure 8 Zero day attack

Proposed mitigation strategies to compact zero-day attacks in the network interface layer of the TCP/IP: Separation of networking resources; subnetting and monitoring/restrict traffic flow in the subnets, this will help to limit the impact of the zero-day attack, which might have spread to the whole network if not segmented [140]-[142]. Implementation of quick and active patch management framework to patch network architecture flaws before they are exploited. This also include being updated with the newly discover vulnerabilities, how they can be exploited, and how they can be mitigated [143]. Creation of policy and work plan to counter zero-day attacks, that include of incident response plan, also coming out with a mechanism to detect any anomalies of the zero-day attacks [143]-[146].

4.3. Wiretapping and Eavesdropping techniques

Eavesdropping is the technique that an attacker passively or actively intercepts legitimate communication between two or more entities and listen or captures their communications [147]. On the other hand Wiretapping is the interception of active communication taking place in an electronic medium [148], both Wiretapping and eavesdropping have the same goal of unauthorized access to legitimate communications to listen or collect data with a malicious intent [149]-[152].

In Figure 9, below shows how eavesdropping attack takes place; the attacker is intercepting communication between the computer user and the requests and responses he is getting from the server/access point, hence the attacker is listening/capturing server client interactions [153], [154].

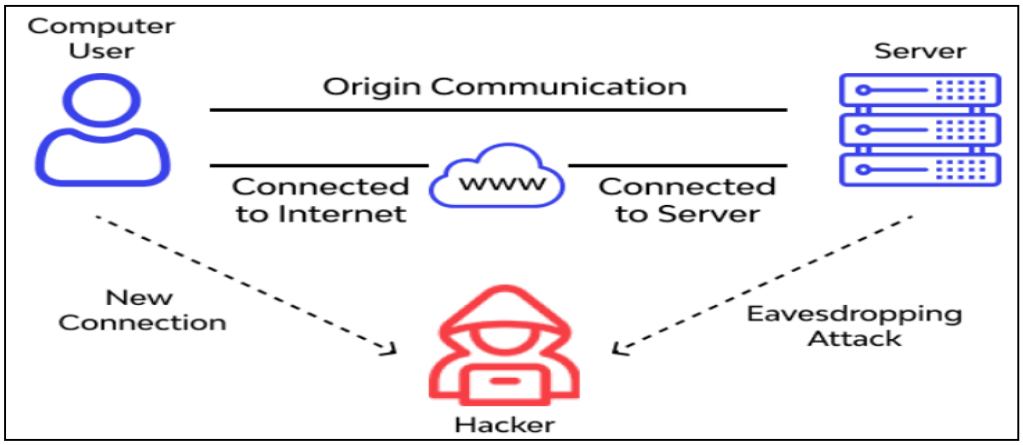

Figure 9 Eavesdropping Attack

Figure 10 below depicts how wiretapping takes place, the attacker scans the MAC address at the access point, and intercepts and listens/captures packets of the legitimate users [155].

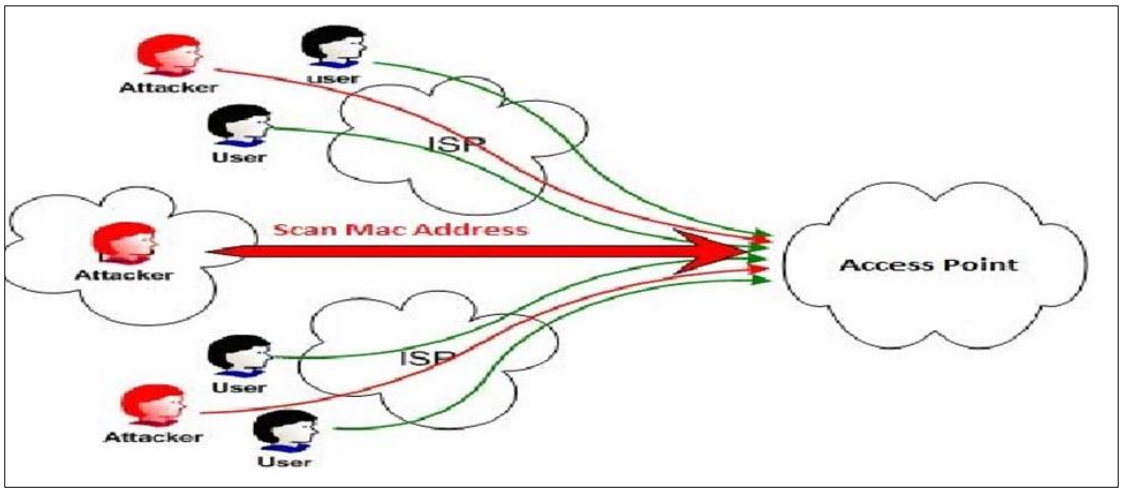

Figure 10 Wiretapping Attack

There are two mechanisms of eavesdropping which attacker use to accomplish their goal: Passive eavesdropping, from the word 'passive' involves inactively listening and interception of communication without triggering an alert [156]. Attacker captures communications that transverse across the network with an aim of collecting data. Active eavesdropping involves modification of network traffic, these include of alteration of data packets, injection of unknown payload, and fake packets to with an aim of redirecting traffic to hackers destination [157]. It Acts as a man in the middle attack, other mechanisms includes of session hijacking which takes over the entire communication/data transfer session and captures all communications, and evil twin access point which crates a fake Wi-Fi hot-spots , legitimate users connect to the network and their information is stolen during communication process [158]-[160]. Several mitigation strategies have been proposed to reduce the impact of wiretapping and eavesdropping attacks on network interface layer [161]-[162] as discussed in the Table 6 below.

Table 6 Eavesdropping Attacks Mitigation Strategies

Technique	Explanation
Network Segmentation	Separation of the network architecture will help reduce the impact and spread of the attack [163].
Packet Inspection and Traffic Analysis.	It will help identify forged/fake packets and unknown network connections, creates an alert and preventive measures taking i.e. blocking the forged packets.
Cryptography and Encryption	Encryption sent packets/received using several algorithms with a key only known to the sender and recipient [164].
Authentication and Verification	Authenticate and verify each network connections, involves regular scanning of connection profiles.

5. Privacy Concerns in the Network Interface layer

Privacy issues in the network interface layer of TCP/IP involve MAC address tracking and profiling, where devices' unique identifiers are exploited for monitoring and targeted advertising. Regulation efforts aim to safeguard user privacy, yet there are still gaps due to the decentralized nature of network management and the lack of standardized privacy protocols. Challenges include balancing privacy with network functionality, addressing jurisdictional laws in regulation, and mitigating vulnerabilities exploited by malicious actors [165]-[169]. Effective privacy measures demand collaboration among stakeholders to develop robust frameworks that uphold user rights while preserving network integrity.

5.1. MAC Address Tracking and Profiling

The Media Access Control (MAC) protocol in the network interface layer is associated with a unique identifier to the network interface card [170], which is licked up with the devices connected to the network. This kind of linkage affects the privacy of these connected devises. Numerous risks are associated with MAC Address Tracking and profiling. The

MAC addresses are unique identifiers each assigned network interface cards of networked devices, and they constantly remain the same over a period of time. This poses a risk in tracking the devices on the network for a long period of time leading to violation of privacy [171]. Secondly, MAC Address can reveal private information about device, and the user (movements, habits, and logs). Based on the collected information, attackers can use this information to launch an attack as in Figure 11 below. This address tracking and profiling have become prominent techniques in the realm of digital surveillance and targeted advertising, raising significant privacy concerns. Every device connected to a network has a unique MAC address, intended to control access and facilitate the delivery of data packets within local networks. However, this unique identifier can be exploited to track the device's movements across different networks. For example, retail environments, airports, and public spaces equipped with Wi-Fi networks can monitor the presence of devices by capturing their MAC addresses, even if the device does not connect to the network. Over time, the collected data can be used to profile individuals' habits, frequented locations, and even predict future movements. This level of tracking and profiling poses a substantial threat to personal privacy, as individuals may be unknowingly monitored and analyzed without their consent.

In response to these privacy concerns, some operating systems have introduced features to randomize MAC addresses during network scans, making it more difficult to track and profile devices consistently. However, this countermeasure is not universally adopted, and its effectiveness can vary, leaving gaps in privacy protection. Moreover, while MAC address randomization can provide a layer of anonymity, persistent tracking techniques and sophisticated data analysis can sometimes de-anonymize this information, linking the randomized MAC addresses back to individual devices and users.

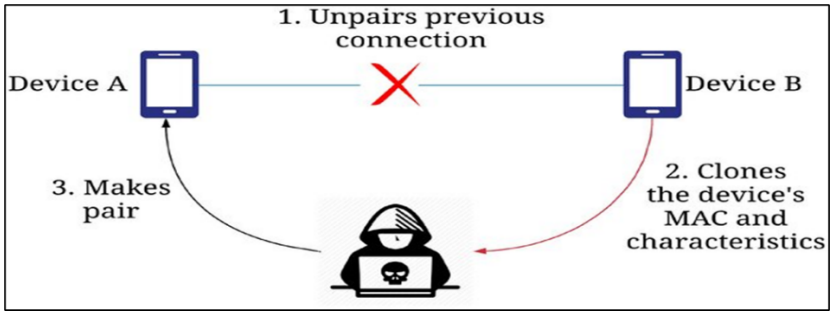

Figure 11 MAC Addresses Attack

The issue of MAC address tracking and profiling underscores a broader debate about privacy in the digital age, highlighting the need for stronger regulatory frameworks and technology solutions to protect individuals from invasive tracking practices and ensure their right to privacy in increasingly connected environments. MAC address anonymization techniques helps to mitigate the MAC Address tracking, and profiling [172] -[176] as in Table 7 below.

Table 7 MAC Address Anonymization Techniques

Technique	Description	Implementation
MAC Address Masking	This involves replacing part of the MAC address with a pseudonymous value to maintain privacy while maintaining compatibility with network protocols [177].	This technique obscures the original MA address while still allowing devices to communicate over the network.
MAC Address Encryption	Using Encryption mechanisms to prevent unauthorized tracking and profiling. (SSL/TLS, IPsec)	This helps to maintain the confidentiality and integrity of communication entities and channels
Random MAC Addressing Scheme	Frequently changing MAC addresses of devices over a time [178]	Reduce the rate and impact of MAC tracking and profiling
Virtual Private Networks	VPNs reroutes clients connections through a secure server [179].	It hides out to identify of clients on the network, masking their location

5.2. Regulating privacy, Gaps and Challenges

Nations across the world have come up with different enactments tries to cover the privacy of their data and communications in the internet [180]. However, there are still concerns about the privacy challenge in the network interface layer of the TCP/IP. General Data Protection Regulation (GDPR) [181] and California Consumer Privacy Act (CCPA) [103] have set policies and guidelines on how data can be processed, shared, and used but have not provided insights on the transmission of data in the Network Interface Layer.

Nations globally have telecommunication regulations that control surveillance, tracking and profiling of her citizens but due to jurisdiction differences it has become difficult to comply with such regulations due to lack of general uniform rules and regulations [182],[183]. Even as different nations advances in their technology, it is quit difficult to keep up with the technology advancements, making it had to balance between privacy [184] and technological advancements [185]. Ethical considerations and applicable legal and regulatory frameworks applicable are summarized in Table below [186], [187].

Table 8 Ethical Considerations

Ethical Considerations	**Description**	**Applicable Legal and Regulatory Frameworks**
Transparency and Consent	Individual and organizations need to practice transparency and consent with an aim of protecting user privacy Includes regulations in information disclosure, data collection and sharing practices.	Health Insurance Portability and Accountability Act (HIPAA) General Data Protection Regulation GDPR
Data Minimization	Practicing data minimization involves, collecting, processing of only required data that serves that specific purpose. This helps to reduce the impact of privacy breach.	Health Insurance Portability and Accountability Act (HIPAA)
User Training and Education	This is an approach to network privacy that aims at educating networking device users to exercise control over their data over the internet.	All applicable Frameworks
Fairness	Network privacy emphasize fairness and equity in data processing, ensuring equality in collecting, processing, and dissemination of network based data	All applicable Frameworks

6. Case Studies on Performance, Security, and privacy of the Network Interface Layer

Case studies exploring the performance, security, and privacy of network interface layers delve into the thin line balance between efficient data transmission, robust security measures, and user privacy. These studies analyze real-world scenarios to assess the impact of various protocols, hardware configurations, and network architectures on overall system functionality. They uncover vulnerabilities such as MAC address spoofing, protocol weaknesses, and data interception, while also highlighting strategies to enhance performance without compromising security or infringing upon user privacy. Through these investigations, insights are gained into optimizing network infrastructure to meet the evolving demands of a connected world while safeguarding sensitive information and maintaining operational efficiency.

6.1. Comparative analysis of the Network Interface protocol

The main aim of this comparative analysis was to perform a comparative analysis of the performance, security, and privacy of the network interface layer Protocols, evaluating their performance rating, security challenges and privacy concerns as in Table 9 below.

Table 9 Comparative Analysis of network interface layer Protocols

Network interface layer Protocol	Performance	Security	Privacy	References
Ethernet	High throughput, low latency.	Simple to use Prone to MAC address attacks.	Visible MAC addresses, lacking efficient privacy	[188] – [190]
Wi-Fi	Varies in speed depending on signal, might prone to signal blockage attacks	Prone to eavesdropping, unauthorized access [191], WPA2 Vulnerabilities	Prone to MAC address tracking. Random MAC addressing Scheme helps maintain privacy	[192] – [194]
Fiber Optics	High bandwidth, Low latency	MAC addresses vulnerable at end devices	Wired connection reduces the impact of attacks. Prone to MAC Address tracking and profiling	[195] – [199]
Cellular Networks	Differ in performance due to area coverage Prone to congestion	Secure in transmission [200] Prone to SS7 Vulnerabilities	Prone to tracking and profiling, location spoofing, MAC Address attacks	[201] – [203]

6.2. Real-world Scenarios and their challenges

Despite of massive innovations that have been done by the tech giant companies, the network infrastructure still faces performance, security, and privacy challenges in their quest to have 100% efficient systems [204] – [206]. Across the globe smart cities have been developed integrating diverse devices with specific functionality, for example the Internet of Things (IoT), and Sensor devices are AI powered [207] to even work smarter than humans. Maintaining such massive technology since they directly interact with people, collecting information about them, processing and even making decisions based on the data, protecting such information; ensuring that it is not prone to attacks or cannot be used for unintended purpose can be challenging [208] -[210].

Performing online services like banking, e-learning, tele-conferencing, and patient monitoring on a network infrastructure such as open Wi-Fi can be challenging in maintaining efficient online operations [211]-[213]. Potential performance challenges that one might face include network congestion, and low bandwidth which will affect the services provided. Protecting sensitive information like databases can be a changeling in an open connection, one is prone to attacks such as eavesdropping, low performance metrics, hacking, tracking, and data mining [214]-[216].

Rural areas and developing countries, face bandwidth challenges, where high-speed internet is often limited by inadequate infrastructure. In rural areas, the large population makes it economically illogical for internet service providers to provide such services, these leads to low internet connections; thus making access to internet related services limited [217]. Similarly, 3rd world countries face challenges in establishing robust network infrastructure to meet the growing demands of their populations. Bandwidth constraints hinder economic development by limiting access to online resources, hindering the growth of e-commerce, and limiting communication channels for businesses and individuals [218]. Without reliable internet access, businesses struggle to compete in the global market, and individuals are deprived of educational and job opportunities available through digital platforms. Addressing bandwidth limitations in rural and developing areas is crucial for bridging the digital divide and fostering inclusive economic growth and development.

Attackers can create fake Wi-Fi hotspots that look genuine to unsuspecting victims through spoofing MAC addresses. Once users connect to these malicious networks, attackers can intercept sensitive information, launch phishing attacks for stealing their credentials, distribute malware or eavesdrop on their network activities. Consequently, this puts the user's privacy and security on the line thus might result into identity thefts, financial losses or unauthorized access to personal data.

People may use MAC address spoofing as a means of avoiding device tracking or monitoring by network administrators [219], [220]. By using a MAC address that is not linked to their actual device identity, they can go unnoticed while accessing restricted or monitored networks. This could be used for gaining unauthorized entry to confidential information, circumventing network restrictions and engaging in illegal activities without any trace being left behind [221], [223].

A scenario where an online banking portal is under attack; attackers use a network of compromised computers (botnets) to undermine the bank's servers with a flood of requests. By overwhelming the available bandwidth capacity and computational resources, the traffic congestion overloads the network interface layer and either slows down or shuts down the service. Stuck trying to access their accounts, transfer funds or contact service agents, banking customers experience a disruption in service [224], [225]. Alongside the financial repercussions related to the interruption of service, the incident compromises the bank's reputation However, network security measures are undermined by this while making it possible for malicious acts to thrive under the cover of darkness.

The financial institution suffers financial losses and lasting damage to its image. In a Distributed Denial of Service attack, threat actors exploit vulnerabilities in network devices (such as routers or IoT devices) in order to amplify malicious traffic toward the victim's network [226] - [228]. This amplification of the attack puts additional strain on the capacity of the layer of the network (the network interface of the victim's network, in our example) to process legitimate traffic. It also complicates the mitigation efforts because, even if the source of the attack would be identified relatively quickly, the fact that the malicious traffic [229] appears to come from a number of legitimate sources makes it more difficult to effectively and completely mitigate an attack. The organization experiences increased downtime, more money has to be invested to get back to operations, and long-term financial and reputation risks might materialize due to legal and regulatory actions related to the failure to protect customer data or ensure availability.

Finally, The COVID-19 pandemic impacted the network interface layer of the TCP/IP stack, primarily due to the global transition to remote work and increased reliance on digital communication tools [230]. This shift resulted in a increase in internet bandwidth demand, causing strain on the Network interface layer and leading to potential slowdowns and latency issues. Network congestion exacerbated these challenges, especially in areas with limited broadband infrastructure. Security vulnerabilities were exploited by cybercriminals who took advantage pandemic to launch attacks targeting remote workers. Additionally, the rapid deployment of remote access solutions introduced new vulnerabilities, such as insecure protocols and mis-configured VPNs, making corporate networks susceptible to unauthorized access and data breaches. Supply chain disruptions further compounded security risks, as shortages of networking equipment led to the use of outdated or counterfeit devices containing vulnerabilities [231], [232].

Privacy concerns emerged as remote collaboration tools raised issues regarding data privacy and confidentiality. Instances of unauthorized access to virtual meetings highlighted the need for robust privacy safeguards at the Network Interface Layer. Moreover, government and employer surveillance measures aimed at curbing the spread of COVID-19 raised privacy concerns about the collection, storage, and sharing of personal data transmitted over networks [233] - [235]. During the COVID-19 pandemic, computer network privacy concerns escalated as remote work and online interactions surged, exposing individuals to heightened risks of data breaches, cyber-attacks, and surveillance. The rapid shift to remote work necessitated the use of virtual private networks (VPNs), often leading to increased vulnerabilities due to inadequate security measures or unfamiliarity with proper protocols. Additionally, the reliance on video conferencing platforms raised privacy issues regarding data collection, unauthorized access, and the potential for surveillance by both government entities and malicious actors. As individuals relied more on digital communication for work, education, and socializing, ensuring privacy protection became increasingly challenging, demanding robust security measures and heightened awareness of cyber threats to safeguard sensitive information and personal data.

7. Conclusion

In conclusion, this comprehensive survey has delved into performance, security, and privacy issues in the network interface layer of the TCP/IP protocol suite. Performance is impacted by factors such as heterogeneous networks, packet fragmentation, aggregation, and congestion control algorithms. These challenges impact throughput, latency, and bandwidth. Security vulnerabilities pose significant threats to the Network Interface Layer, including denial-of-service attacks, zero-day vulnerabilities, and wiretapping/eavesdropping attacks. These attacks disrupt normal network operations, compromise data integrity, and expose sensitive information. Mitigation strategies such as packet inspection, traffic analysis, encryption, and authentication are proposed. Privacy challenges included MAC address tracking, profiling risks, and data interception. MAC address anonymization techniques and encryption mechanisms help mitigate privacy risks and protect user anonymity. Moreover, regulatory frameworks and ethical considerations play a vital role in governing data privacy practices and ensuring transparency, consent, and fairness in data processing.

Despite technological advancements, there is still a need to look into performance, security, and privacy of the Network Interface Layer. Further research need to be done on emerging technologies like the 6G, Software Defined Networking (SDN), and Network Function Virtualization (NFV). Secondly there is a need to develop standardized, ethical considered, and interoperability mechanisms ensuring that new solutions are fully integrated across diverse network environments and protocols. By identifying key challenges and suggested mitigation strategies, this paper paves the way for future advancements in network communication technologies, ensuring the confidentiality, integrity, and availability of the network interface layer of the TCP/IP Suite.

Compliance with ethical approval

Disclosure of conflict of interest

The author declares that he has no conflict of interest.

References

[1] Buchanan W, Buchanan W. Transmission Control Protocol (TCP) and Internet Protocol (IP). Applied Data Communications and Networks. 1996:87-109.

[2] Kessler GC. An overview of TCP/IP protocols and the internet. InterNIC Document, Dec. 2004, 29:42.

[3] Kozierok CM. The TCP/IP guide: a comprehensive, illustrated Internet protocols reference. No Starch Press, 2005 Oct 1.

[4] Stewart R, Metz C. SCTP: new transport protocol for TCP/IP. IEEE Internet Computing. 2001 Nov, 5(6):64-9.

[5] Juledi AP, Simarmata J, Sihotang JI, Pakpahan AF, Sinlae AA, Siregar MN, Giap YC, Amin M, Parewe AM, Jamaludin J, Muttaqin M. Internetworking dan TCP/IP. Yayasan Kita Menulis, 2021 Dec 31.

[6] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[7] Kumar A, Karthikeyan S. Security Model for TCP/IP Protocol Suite. Journal of Advances in Information Technology. 2011 May 3, 2(2).

[8] Rhee MY. Wireless Mobile Internet Security. John Wiley & Sons, 2013 Mar 26.

[9] Kaur K, Kaur M, Kaur K, Madaan A. A comparative study of OSI and TCP/IP models. International Journal Of Engineering And Management Research. 2023, 13(2):127-35.

[10] Rahouma KH, Abdul-Karim MS, Nasr KS. TCP/IP Network Layers and Their Protocols (A Survey). InInternet of Things—Applications and Future: Proceedings of ITAF 2019 2020 (pp. 287-323). Springer Singapore.

[11] Mundra S, El Taeib T. TCP/IP protocol layering. International Journal of Computer Science and Information Technology Research. 2015 Jan, 3(1):415-7.

[12] Barak A, Gilderman I, Metrik I. Performance of the Communication Layers of TCP/IP with the Myrinet Gigabit LAN. Computer Communications. 1999 Jul 15, 22(11):989-97.

[13] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[14] Kaushik S. An overview of technical aspect for WiFi networks technology. International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956). 2012, 1(01):28-34.

[15] Yugha R, Chithra S. A survey on technologies and security protocols: Reference for future generation IoT. Journal of Network and Computer Applications. 2020 Nov 1, 169:102763.

[16] Mahaliyanaarachchi V. Security Issues and Mitigation Mechanisms in Distributed Systems. In2023 3rd International Conference on Advanced Research in Computing (ICARC) 2023 Feb 23 (pp. 172-177). IEEE.

[17] Farabi Fardin Khan, Nafis Mohaimin Hossain, Huda N, Sad Bin Anwar, Noor J. Mitigating DDoS Attacks Using a Resource Sharing Network. 2022 Dec 20.

[18] Gupta S, N. Lingareddy. Security Threats and Their Mitigations in IoT Devices. Springer eBooks. 2021 Jan 1, 411–24.

[19] Mannhart S, Rodrigues B, Scheid E, Kanhere SS, Stiller B. Toward Mitigation-as-a-Service in Cooperative Network Defenses. 2018 Aug 1.

[20] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[21] Oyekunle RA, Issa-Onilu GO. Impact of ubiquitous computing on users' teaching and learning experience. Nigerian Journal of Educational Technology. 2020, 1(2):27-39.

[22] Priyadarsini M, Bera P. Software defined networking architecture, traffic management, security, and placement: A survey. Computer Networks. 2021 Jun 19, 192:108047.

[23] Alam I, Sharif K, Li F, Latif Z, Karim MM, Biswas S, Nour B, Wang Y. A survey of network virtualization techniques for Internet of Things using SDN and NFV. ACM Computing Surveys (CSUR). 2020 Apr 16, 53(2):1-40.

[24] Moyano RF, Fernandez D, Merayo N, Lentisco CM, Cárdenas A. NFV and SDN-based differentiated traffic treatment for residential networks. IEEE Access. 2020 Feb 17, 8:34038-55.

[25] Neelam BS, Shimray BA. Improved network performance in CPS communication with distributed IPC mechanisms of recursive internetworking architecture (RINA). International Journal of Internet Protocol Technology. 2023, 16(1):68-74.

[26] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[27] Alnawayseh SE, Al-Sit WT, Ghazal TM. Smart congestion control in 5g/6g networks using hybrid deep learning techniques. Complexity. 2022 Oct 25, 2022.

[28] Han B, Gopalakrishnan V, Ji L, Lee S. Network function virtualization: Challenges and opportunities for innovations. IEEE communications magazine. 2015 Feb 19, 53(2):90-7.

[29] Mijumbi R, Serrat J, Gorricho JL, Bouten N, De Turck F, Boutaba R. Network function virtualization: State-of-the-art and research challenges. IEEE Communications surveys & tutorials. 2015 Sep 4, 18(1):236-62.

[30] Yi B, Wang X, Li K, Huang M. A comprehensive survey of network function virtualization. Computer Networks. 2018 Mar 14, 133:212-62.

[31] Abdelwahab S, Hamdaoui B, Guizani M, Znati T. Network function virtualization in 5G. IEEE Communications Magazine. 2016 Apr 19, 54(4):84-91.

[32] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[33] Wu M, Lu TJ, Ling FY, Sun J, Du HY. Research on the architecture of Internet of Things. In2010 3rd international conference on advanced computer theory and engineering (ICACTE) 2010 Aug 20 (Vol. 5, pp. V5-484). IEEE.

[34] Piraux M, Barbette T, Rybowski N, Navarre L, Alfroy T, Pelsser C, et al. The multiple roles that IPv6 addresses can play in today's internet. ACM SIGCOMM Computer Communication Review. 2022 Jul 30, 52(3):10–8.

[35] Ladid L. IPv6-the next big bail-out: will IPv6 save the internet?. InProceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing 2009 Jun 18 (pp. 1-7).

[36] Edelman B. Running out of numbers: Scarcity of IP addresses and what to do about it. InAuctions, Market Mechanisms and Their Applications: First International ICST Conference, AMMA 2009, Boston, MA, USA, May 8-9, 2009, Revised Selected Papers 1 2009 (pp. 95-106). Springer Berlin Heidelberg.

[37] Khan S, Hussain A, Nazir S, Khan F, Oad A, Alshehri MD. Efficient and reliable hybrid deep learning-enabled model for congestion control in 5G/6G networks. Computer Communications. 2022 Jan 15, 182:31-40.

[38] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021 2022 Nov 16 (pp. 91-111). Singapore: Springer Nature Singapore.

[39] Salameh AI, El Tarhuni M. From 5G to 6G—challenges, technologies, and applications. Future Internet. 2022 Apr 12, 14(4):117.

[40] Gopalan NP, Selvan BS. TCP/IP ILLUSTRATED. PHI Learning Pvt. Ltd., 2008 Feb 13.

[41] Davidson J. An introduction to TCP/IP. Springer Science & Business Media, 2012 Dec 6.

[42] Katsikas GP, Barbette T, Chiesa M, Kostić D, Maguire Jr GQ. What you need to know about (smart) network interface cards. InInternational Conference on Passive and Active Network Measurement 2021 Mar 29 (pp. 319-336). Cham: Springer International Publishing.

[43] Siracusano G, Galea S, Sanvito D, Malekzadeh M, Antichi G, Costa P, Haddadi H, Bifulco R. Re-architecting traffic analysis with neural network interface cards. In19th USENIX symposium on networked systems design and implementation (NSDI 22) 2022 (pp. 513-533).

[44] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec, 11(4):66.

[45] Wehrle K, Weingärtner E, vom Lehn H. Device driver-enabled wireless network emulation. In4th International ICST Conference on Simulation Tools and Techniques 2012 Apr 13.

[46] Stallings W. Local networks. ACM Computing Surveys. 1984 Mar 29, 16(1):3–41.

[47] Ibe OC. Fundamentals of data communication networks. John Wiley & Sons, 2017 Nov 29.

[48] Li R, Makhijani K, Dong L. New ip: A data packet framework to evolve the internet. In2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR) 2020 May 11 (pp. 1-8). IEEE.

[49] Hicks M, Kakkar P, Moore JT, Gunter CA, Nettles S. PLAN: A packet language for active networks. ACM SIGPLAN Notices. 1998 Sep 29, 34(1):86-93.

[50] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[51] Shah M, Soni V, Shah H, Desai M. TCP/IP network protocols—Security threats, flaws and defense methods. In2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) 2016 Mar 16 (pp. 2693-2699). IEEE.

[52] King A, Hunt R. Protocols and architecture for managing TCP/IP network infrastructures. Computer Communications. 2000 Sep 30, 23(16):1558-72.

[53] Sethi P, Sarangi SR. Internet of things: Architectures, protocols, and applications. Journal of Electrical & Computer Engineering. 2017 Jan 26.

[54] Waxvik E, Chun S. Networks and Telecommunications. InOfficial (ISC) 2 Guide to the SSCP CBK 2010 Dec 8 (pp. 219-278). Auerbach Publication

[55] Deng C, Fang X, Han X, Wang X, Yan L, He R, Long Y, Guo Y. IEEE 802.11 be Wi-Fi 7: New challenges and opportunities. IEEE Communications Surveys & Tutorials. 2020 Jul 29, 22(4):2136-66.

[56] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[57] GHALYAN A, Kait R, Ranga V. Review of Authentication Communication Protocols in Mobile (Vehicular) Network via FOG Computing. Authorea Preprints. 2024 Jan 30.

[58] Liu F, Xie T, Feng Y, Feng D. On the security of PPPoE network. Security and Communication Networks. 2012 Oct, 5(10):1159-68.

[59] Shirichian M, Sabbaghi-Nadooshan R, Houshmand M, Houshmand M. A QTCP/IP reference model for partially trusted-node-based quantum-key-distribution-secured optical networks. Quantum Information Processing. 2024 Mar 1, 23(3):87.

[60] Kizza JM. Computer network security protocols. InGuide to Computer Network Security 2024 Jan 20 (pp. 409-441). Cham: Springer International Publishing.

[61] Hercog D. Communication protocols: principles, methods and specifications. Springer Nature, 2020 Sep 28.

[62] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[63] Lv M, Huang H, Li X. An Ethernet Mapping High-Level Data Link Control Circuit Design. InThe International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery 2021 Jul 24 (pp. 1190-1197). Cham: Springer International Publishing.

[64] Jukic Z. Performance Analysis of the HDLC Protocol-NRM Mode. InNew Technologies, Development and Application II 5 2020 (pp. 317-331). Springer International Publishing.

[65] Cowley J. Communications and networking: an introduction. Springer Science & Business Media, 2012 Sep 14.

[66] Mascolo S, Gerla M. Asynchronous Transfer Mode (ATM) Congestion Control in Communication and Data Network Systems. InDatabase and Data Communication Network Systems 2002 Jan 1 (pp. 693-717). Academic Press.

[67] Lv Y, Su D. Blockchain Security Technology Based on the Asynchronous Transmission Mode of IoT Technology in Smart Cities. Wireless Personal Communications. 2022 Oct, 126(3):1965-80.

[68] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[69] Xu Y, Gui G, Gacanin H, Adachi F. A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges. IEEE Communications Surveys & Tutorials. 2021 Feb 17, 23(2):668-9

[70] Ghosh R, Lerman K. Structure of heterogeneous networks. In2009 International Conference on Computational Science and Engineering 2009 Aug 29 (Vol. 4, pp. 98-105). IEEE.

[71] Zhao Y, Li W, Liu F, Wang J, Luvembe AM. Integrating heterogeneous structures and community semantics for unsupervised community detection in heterogeneous networks. Expert Systems with Applications. 2024 Mar 15, 238:121821.

[72] Muhammad G, Akram M. Fuzzy fractional epidemiological model for Middle East respiratory syndrome coronavirus on complex heterogeneous network using Caputo derivative. Information Sciences. 2024 Feb 1, 659:120046.

[73] Zhang P, Che C, Jin B, Yuan J, Li R, Zhu Y. NCH-DDA: Neighborhood contrastive learning heterogeneous network for drug–disease association prediction. Expert Systems with Applications. 2024 Mar 15, 238:121855.

[74] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[75] Dao VA, Thuy TT, Bao VN, Dung TC, Quyen NX. Design of A Chaos-based Digital Radio over Fiber Transmission Link using ASK Modulation for Wireless Communication Systems. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems. 2024 Jan 16, 11(1):e3-.

[76] Yao CK, Lin HP, Cheng CL, Li YL, Du LY, Peng PC. Satellite Communication and Free Space Optics for Open Radio Access Network. Journal of Lightwave Technology. 2024 Feb 6.

[77] Ding J, Liu W, I CL, Zhang H, Mei H. Advanced progress of optical wireless technologies for power industry: an overview. Applied Sciences. 2020 Sep 16, 10(18):6463.

[78] Ghassemlooy Z, Uysal M, Khalighi MA, Ribeiro V, Moll F, Zvanovec S, Belmonte A. An overview of optical wireless communications. Optical Wireless Communications: An Emerging Technology. 2016:1-23.

[79] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[80] Sato KI, Okamoto S, Hadama H. Network performance and integrity enhancement with optical path layer technologies. IEEE Journal on selected areas in communications. 1994 Jan, 12(1):159-70.

[81] Deutsch A. Electrical characteristics of interconnections for high-performance systems. Proceedings of the IEEE. 1998 Feb, 86(2):315-57

[82] Vaigandla KK, Venu DN. A survey on future generation wireless communications-5G: multiple access techniques, physical layer security, beamforming approach. Journal of Information and Computational Science. 2021 Oct, 11(9):449-74.

[83] Fedorenko V, Samoylenko I, Samoylenko V. Fragmentation of data packets in wireless sensor network with variable temperature and channel conditions. Computer Communications. 2024 Jan 15, 214:201-14.

[84] Haggag A. Implementation and Evaluation of IPv6 with Compression and Fragmentation for Throughput Improvement of Internet of Things Networks over IEEE 802.15. 4. Wireless Personal Communications. 2023 May, 130(2):1449-77.

[85] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[86] Morais DH. Data communication systems protocol stacks. In5G NR, Wi-Fi 6, and Bluetooth LE 5: A Primer on Smartphone Wireless Technologies 2023 Jul 1 (pp. 9-15). Cham: Springer Nature Switzerland.

[87] Choi Y, Yoon J, Moon Y, Park K. Is Large MTU Beneficial to Cellular Core Networks?. InProceedings of the 7th Asia-Pacific Workshop on Networking 2023 Jun 29 (pp. 67-73)

[88] Han F, Li Q, Zhou J, Xu H, Jiang Y. APS: Adaptive Packet Sizing for Efficient End-to-End Network Transmission. In2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS) 2022 Jun 10 (pp. 1-10). IEEE.

[89] Kumar S, Andersen MP, Kim HS, Culler DE. Performant {TCP} for {Low-Power} wireless networks. In17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20) 2020 (pp. 911-932).

[90] Yazid M, Bouallouche-Medjkoune L, Aïssani D, Ziane-Khodja L. Analytical analysis of applying packet fragmentation mechanism on IEEE 802.11b DCF network in non ideal channel with infinite load conditions. Wireless Networks. 2013 Oct 27, 20(5):917–34.

[91] Kuaban GS, Atmaca T, Kamli A, Czachórski T, Czekalski P. Performance Analysis of Packet Aggregation Mechanisms and Their Applications in Access (e.g., IoT, 4G/5G), Core, and Data Centre Networks. Sensors. 2021 Jun 4, 21(11):3898.

[92] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[93] Kurose JF. Computer networking: A top-down approach featuring the internet, 3/E. Pearson Education India, 2005.

[94] Rodrigues S, Lv J. Synchronization in Time-Sensitive Networking: An Introduction to IEEE Std 802.1AS. IEEE Communications Standards Magazine. 2022 Dec, 6(4):14–20.

[95] Ibrahim AS, Youssef KY, Eldeeb AH, Abouelatta M, Kamel H. Adaptive aggregation based IoT traffic patterns for optimizing smart city network performance. Alexandria Engineering Journal. 2022 Dec 1, 61(12):9553-68.

[96] Hasan HH, Alisa ZT. Effective IoT congestion control algorithm. Future Internet. 2023 Mar 31, 15(4):136.

[97] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[98] Verma LP, Sharma VK, Kumar M, Kanellopoulos D. A novel delay-based adaptive congestion control TCP variant. Computers and Electrical Engineering. 2022 Jul 1, 101:108076.

[99] Donta PK, Srirama SN, Amgoth T, Annavarapu CS. iCoCoA: Intelligent congestion control algorithm for CoAP using deep reinforcement learning. Journal of Ambient Intelligence and Humanized Computing. 2023 Mar, 14(3):2951-66.

[100] Sun G, Li C, Ma Y, Li S, Qiu J. End-to-end tcp congestion control as a classification problem. IEEE Transactions on Reliability. 2022 May 20, 72(1):384-94.

[101] Mahawish AA, Hassan HJ. Improving RED algorithm congestion control by using the Markov decision process. Scientific Reports. 2022 Aug 3, 12(1):13363.

[102] Shi H, Wang J. Intelligent TCP Congestion Control Policy Optimization. Applied Sciences. 2023 May 30, 13(11):6644.

[103] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[104] Grazia CA. Future of TCP on Wi-Fi 6. IEEE Access. 2021 Aug 3, 9:107929-40.

[105] Zhang X, Zhang X, Zhang Y, Qiao W, Dong P. Design of Reliable Parallel Transmission System in Complex Heterogeneous Network. InInternational Conference on Emerging Networking Architecture and Technologies 2022 Oct 15 (pp. 198-208). Singapore: Springer Nature Singapore.

[106] Abadleh A, Tareef A, Btoush A, Mahadeen A, Al-Mjali MM, Alja'Afreh SS, Alkasasbeh AA. Comparative analysis of tcp congestion control methods. In2022 13th International Conference on Information and Communication Systems (ICICS) 2022 Jun 21 (pp. 474-478). IEEE.

[107] Bazi K, Nassereddine B. Comparative analysis of TCP congestion control mechanisms. InProceedings of the 3rd International Conference on Networking, Information Systems & Security 2020 Mar 31 (pp. 1-4).

[108] Dastagir J, Amir M, Rehman BU, Hameed S, Ashraf M. Optimized TCP congestion control over a wired network. Journal of Engineering and Applied Sciences. 2021, 40(1):8-14.

[109] Abdullah SM, Farag MS, Abdul-Kader H, Abo-Youssef SE. Improving the TCP Newreno Congestion Avoidance Algorithm on 5G Networks. Journal of Communications. 2023 Apr, 18(4).

[110] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[111] Rahouma KH, Abdul-Karim MS, Nasr KS. TCP/IP Network Layers and Their Protocols (A Survey). InInternet of Things—Applications and Future: Proceedings of ITAF 2019 2020 (pp. 287-323). Springer Singapore

[112] Antony J, Maity T. Analysis of Ethernet Control Network. IETE Journal of Research. 2023 Apr 3, 69(3):1588-96.

[113] Sentala B, Lubobya CS, Zulu A. Performance evaluation and compression of IP packets in a wireless local area network (WLAN). Journal of Wireless Networking and Communications. 2022, 11(1):1-0.

[114] Choi Y, Yoon J, Moon Y, Park K. Is Large MTU Beneficial to Cellular Core Networks?. InProceedings of the 7th Asia-Pacific Workshop on Networking 2023 Jun 29 (pp. 67-73).

[115] Lenders MS, Schmidt TC, Wählisch M. Fragment forwarding in lossy networks. IEEE access. 2021 Oct 19, 9:143969-87

[116] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[117] Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications. 2023 Jan 1, 209:103540.

[118] Taslimasa H, Dadkhah S, Neto EC, Xiong P, Ray S, Ghorbani AA. Security issues in Internet of Vehicles (IoV): A comprehensive survey. Internet of Things. 2023 May 6:100809.

[119] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024 Jan 1, 152:103322.

[120] Vishwakarma R, Jain AK. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems. 2020 Jan, 73(1):3-25.

[121] de Neira AB, Kantarci B, Nogueira M. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks. 2023 Feb 1, 222:109553.

[122] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[123] Gao S, Peng Z, Xiao B, Hu A, Song Y, Ren K. Detection and mitigation of DoS attacks in software defined networks. IEEE/ACM Transactions on Networking. 2020 Apr 15, 28(3):1419-33.

[124] Obaid HS, Abeed EH. DoS and DDoS attacks at OSI layers. International Journal of Multidisciplinary Research and Publications. 2020, 2(8):1-9.

[125] Chai TU, Goh HG, Liew SY, Ponnusamy V. Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory. Systems. 2023 Apr 20, 11(4):211.

[126] Patel ND, Singh A. Security Issues, Attacks and Countermeasures in Layered IoT Ecosystem. International Journal of Next-Generation Computing. 2023 Mar 1, 14(2).

[127] Batchu RK, Seetha H. An integrated approach explaining the detection of distributed denial of service attacks. Computer Networks. 2022 Oct 24, 216:109269.

[128] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149).

[129] Saad RMA, Anbar M, Manickam S, Alomari E. An Intelligent ICMPv6 DDoS Flooding-Attack Detection Framework (v6IIDS) using Back-Propagation Neural Network. IETE Technical Review. 2015 Oct 27, 33(3):244–55.

[130] Aldhyani TH, Alkahtani H. Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. Mathematics. 2023 Jan 3, 11(1):233.

[131] Kaur Chahal J, Bhandari A, Behal S. Distributed denial of service attacks: a threat or challenge. New Review of Information Networking. 2019 Jan 2, 24(1):31-103.

[132] Al-Juboori SA, Hazzaa F, Jabbar ZS, Salih S, Gheni HM. Man-in-the-middle and denial of service attacks detection using machine learning algorithms. Bulletin of Electrical Engineering and Informatics. 2023 Feb 1, 12(1):418-26.

[133] Guo X, Li Q, Ji L, Wang J. Secured impulsive control for directed networks under denial-of-service attacks. Systems & Control Letters. 2023 Mar 1, 173:105463.

[134] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[135] Kumar V, Sinha D. A robust intelligent zero-day cyber-attack detection technique. Complex & Intelligent Systems. 2021 Oct, 7(5):2211-34.

[136] Jangjou M, Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering. 2022 Oct, 29(6):3587-6

[137] Parrend P, Navarro J, Guigou F, Deruyver A, Collet P. Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection. EURASIP Journal on Information Security. 2018 Apr 24, 2018(1).

[138] Thapa VM, Srivastava S, Garg S. Zero Day Vulnerabilities Assessments, Exploits Detection, and Various Design Patterns in Cyber Software. InAI Tools for Protecting and Preventing Sophisticated Cyber Attacks 2023 (pp. 132-147). IGI Global.

[139] Nair D, Mhavan N. Augmenting Cybersecurity: A Survey of Intrusion Detection Systems in Combating Zero-day Vulnerabilities. InSmart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy 2023 May 29 (pp. 129-153). Emerald Publishing Limited.

[140] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1, 24:100969.

[141] Guo Y. A review of Machine Learning-based zero-day attack detection: Challenges and future directions. Computer Communications. 2023 Jan 15, 198:175-85.

[142] Alhebaishi N, Wang L, Jajodia S. Modeling and mitigating security threats in network functions virtualization (NFV). InData and Applications Security and Privacy XXXIV: 34th Annual IFIP WG 11.3 Conference, DBSec 2020, Regensburg, Germany, June 25–26, 2020, Proceedings 34 2020 (pp. 3-23). Springer International Publishing.

[143] Dissanayake N, Jayatilaka A, Zahedi M, Babar MA. Software security patch management-A systematic literature review of challenges, approaches, tools and practices. Information and Software Technology. 2022 Apr 1, 144:106771.

[144] Nkongolo M, Van Deventer JP, Kasongo SM. Ugransome1819: A novel dataset for anomaly detection and zero-day threats. Information. 2021 Sep 30, 12(10):405.

[145] Chen X, Feng W, Ge N, Zhang Y. Zero trust architecture for 6G security. IEEE Network. 2023 Oct 20.

[146] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[147] Hunter B. 'til the Next Zero-Day Comes: Ransomware, Countermeasures, and the Risks They Pose to Safety. Safety-Critical Systems eJournal. 2022 Jan 27, 1(1).

[148] Lu X, Luong NC, Hoang DT, Niyato D, Xiao Y, Wang P. Secure wirelessly powered networks at the physical layer: Challenges, countermeasures, and road ahead. Proceedings of the IEEE. 2021 Nov 24, 110(1):193-209.

[149] Xu D, Zhu H. Proactive Eavesdropping of Physical Layer Security Aided Suspicious Communications in Fading Channels. IEEE Transactions on Information Forensics and Security. 2023 Jan 11, 18:1111-26.

[150] Li M, Dou Z. Active eavesdropping detection: a novel physical layer security in wireless IoT. EURASIP Journal on Advances in Signal Processing. 2023 Nov 22, 2023(1):119.

[151] Wu H, Zhang Y, Shen Y, Jiang X, Taleb T. Achieving covertness and secrecy: The interplay between detection and eavesdropping attacks. IEEE Internet of Things Journal. 2023 Jul 18.

[152] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[153] Fitsanakis J. Redesigning Wiretapping: The Digitization of Communications Interception. Springer Nature, 2020 Dec 18.

[154] Patil BP, Kharade KG, Kamat RK. Investigation on data security threats & solutions. International Journal of Innovative Science and Research Technology. 2020, 5(1):79-83.

[155] Sianipar B, Zarlis M, Nasution BB. Detection of tapping via wifi. IOP Conference Series: Materials Science and Engineering. 2020 Jan 1, 725(1):012097.

[156] Mughaid A, AlZu'bi S, Alnajjar A, AbuElsoud E, Salhi SE, Igried B, Abualigah L. Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches. Multimedia Tools and Applications. 2023 Apr, 82(9):13973-95.

[157] Yan P, Duan W, Ji X, Zhang G, Li B, Zou Y, Wen M, Ho PH. EH Cognitive Network With NOMA: Perspective on Impact of Passive and Active Eavesdropping. IEEE Internet of Things Journal. 2023 Aug 3.

[158] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[159] Mavrommatis K. Confronting and intrusion detection techniques of cyber-attacks in wired and wireless communication networks. InProceedings of the 26th Pan-Hellenic Conference on Informatics 2022 Nov 25 (pp. 290-295).

[160] Goenka R, Chawla M, Tiwari N. A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy. International Journal of Information Security. 2023 Oct 19:1-30.

[161] Valdovinos IA, Pérez-Díaz JA, Choo KK, Botero JF. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. Journal of Network and Computer Applications. 2021 Aug 1, 187:103093.

[162] Sándor B, Rajnai Z. Smart Building IoT Cybersecurity: A Review of Threats and Mitigation Technique. In2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY) 2023 Sep 21 (pp. 000321-000326). IEEE.

[163] Wu Z, Zhang X, Li F, Wang S, Huang L, Li J. W-Net: A boundary-enhanced segmentation network for stroke lesions. Expert Systems with Applications. 2023 Jun 1:120637.

[164] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[165] Rahman A, Hasan K, Kundu D, Islam MJ, Debnath T, Band SS, Kumar N. On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Computer Systems. 2023 Jan 1, 138:61-88.

[166] Iftikhar A, Qureshi KN, Shiraz M, Albahli S. Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. Journal of King Saud University-Computer and Information Sciences. 2023 Oct 13:101788.

[167] Polese M, Bonati L, D'oro S, Basagni S, Melodia T. Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges. IEEE Communications Surveys & Tutorials. 2023 Jan 23, 25(2):1376-411.

[168] López Martínez A, Gil Pérez M, Ruiz-Martínez A. A comprehensive review of the state-of-the-art on security and privacy issues in healthcare. ACM Computing Surveys. 2023 Mar 28, 55(12):1-38.

[169] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[170] Pandey GK, Gurjar DS, Nguyen HH, Yadav S. Security threats and mitigation techniques in UAV communications: A comprehensive survey. IEEE Access. 2022 Oct 19, 10:112858-97.

[171] Kwon S, Park S, Cho H, Park Y, Kim D, Yim K. Towards 5G-based IoT security analysis against Vo5G eavesdropping. Computing. 2021 Mar, 103:425-47.

[172] DeKoven LF, Randall A, Mirian A, Akiwate G, Blume A, Saul LK, Schulman A, Voelker GM, Savage S. Measuring security practices. Communications of the ACM. 2022 Aug 19, 65(9):93-102.

[173] Barua A, Al Alamin MA, Hossain MS, Hossain E. Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. IEEE Open Journal of the Communications Society. 2022 Feb 7, 3:251-81.

[174] Kouachi AI, Bachir A, Lasla N. Anonymizing communication flow identifiers in the internet of things. Computers & Electrical Engineering. 2021 May 1, 91:107063.

[175] Ali J, Dyo V. Cross hashing: Anonymizing encounters in decentralised contact tracing protocols. In2021 International Conference on Information Networking (ICOIN) 2021 Jan 13 (pp. 181-185). IEEE.

[176] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28, 15(13):10264.

[177] Determe JF, Azzagnuni S, Horlin F, De Doncker P. MAC address anonymization for crowd counting. Algorithms. 2022 Apr 20, 15(5):135

[178] Demir L, Cunche M, Lauradoux C. Analysing the privacy policies of Wi-Fi trackers. InProceedings of the 2014 workshop on physical analytics 2014 Jun 11 (pp. 39-44).

[179] Chakraborty M, Singh M, Balas VE, Mukhopadhyay I, editors. The" Essence" of Network Security: An End-to-End Panorama. Springer Singapore, Imprint: Springer, 2021.

[180] Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things. 2021 Sep 1, 15:100420.

[181] Tamburri DA. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems. 2020 Jul 1, 91:101469.

[182] Baik JS. Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). Telematics and Informatics. 2020 Sep 1, 52.

[183] Glasze G, Cattaruzza A, Douzet F, Dammann F, Bertran MG, Bômont C, Braun M, Danet D, Desforges A, Géry A, Grumbach S. Contested spatialities of digital sovereignty. Geopolitics. 2023 Mar 15, 28(2):919-58.

[184] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[185] Nigam A, Pasricha R, Singh T, Churi P. A systematic review on AI-based proctoring systems: Past, present and future. Education and Information Technologies. 2021 Sep, 26(5):6421-45

[186] Fernández JD, Sabou M, Kirrane S, Kiesling E, Ekaputra FJ, Azzam A, Wenning R. User consent modeling for ensuring transparency and compliance in smart cities. Personal and Ubiquitous Computing. 2020 Aug, 24:465-86.

[187] Nguyen VL, Lin PC, Cheng BC, Hwang RH, Lin YD. Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials. 2021 Aug 30, 23(4):2384-428.

[188] Lv Z, Qiao L, Kumar Singh A, Wang Q. AI-empowered IoT security for smart cities. ACM Transactions on Internet Technology. 2021 Jul 22, 21(4):1-21.

[189] Müller T, Walz A, Kiefer M, Doran HD, Sikora A. Challenges and prospects of communication security in real-time ethernet automation systems. In2018 14th ieee international workshop on factory communication systems (wfcs) 2018 Jun 13 (pp. 1-9). IEEE.

[190] Manimuthu A, Ramesh R. Privacy and data security for grid-connected home area network using Internet of Things. Iet Networks. 2018 Nov, 7(6):445-52.

[191] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[192] Khoussainov R, Patel A. LAN security: problems and solutions for Ethernet networks. Computer Standards & Interfaces. 2000 Aug 1, 22(3):191-202.

[193] Ramezanpour K, Jagannath J, Jagannath A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. Computer Networks. 2023 Feb 1, 221:109515

[194] Gruteser M, Grunwald D. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. InProceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots 2003 Sep 19 (pp. 46-55).

[195] Yahuza M, Idris MY, Ahmedy IB, Wahab AW, Nandy T, Noor NM, Bala A. Internet of drones security and privacy issues: Taxonomy and open challenges. IEEE Access. 2021 Apr 9, 9:57243-70.

[196] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal. 2017 Mar 15, 4(5):1125-42.

[197] Medard M, Marquis D, Barry RA, Finn SG. Security issues in all-optical networks. IEEE network. 1997 May, 11(3):42-8

[198] Jones BE, NAVAL POSTGRADUATE SCHOOL MONTEREY CA. Improving security in the Fiber Distributed Data Interface (FDDI) protocol. MS Thesis Naval Postgraduate School, Monterey, CA.. 1992 Sep 1, 1

[199] Rao PM, Deebak BD. Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing. 2022 Feb 3:1-37.

[200] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[201] Ma PY, Wu B, Shastri BJ, Tait AN, Mittal P, Prucnal PR. Steganographic communication via spread optical noise: A link-level eavesdropping resilient system. Journal of Lightwave Technology. 2018 Sep 27, 36(23):5344-57

[202] Yu H, Li P, Zhang L, Zhu Y, Al-Zahrani FA, Ahmed K. Application of optical fiber nanotechnology in power communication transmission. Alexandria Engineering Journal. 2020 Dec 1, 59(6):5019-30.

[203] Patwary MN, Nawaz SJ, Rahman MA, Sharma SK, Rashid MM, Barnes SJ. The potential short-and long-term disruptions and transformative impacts of 5G and beyond wireless networks: Lessons learnt from the development of a 5G testbed environment. IEEE Access. 2020 Jan 7, 8:11352-79.

[204] Polese M, Bonati L, D'oro S, Basagni S, Melodia T. Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges. IEEE Communications Surveys & Tutorials. 2023 Jan 23.

[205] Al Hayajneh A, Bhuiyan MZ, McAndrew I. Improving internet of things (IoT) security with software-defined networking (SDN). Computers. 2020 Feb 7, 9(1):8.

[206] Long Q, Chen Y, Zhang H, Lei X. Software defined 5G and 6G networks: A survey. Mobile networks and applications. 2022 Oct, 27(5):1792-812.

[207] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[208] Kulin M, Kazaz T, De Poorter E, Moerman I. A survey on machine learning-based performance improvement of wireless networks: PHY, MAC and network layer. Electronics. 2021 Jan 29, 10(3):318.

[209] Sookhak M, Tang H, He Y, Yu FR. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Communications Surveys & Tutorials. 2018 Aug 26, 21(2):1718-43

[210] Zou Y, Zhu J, Wang X, Hanzo L. A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE. 2016 May 10, 104(9):1727-65.

[211] Hoyer WD, Kroschke M, Schmitt B, Kraume K, Shankar V. Transforming the customer experience through new technologies. Journal of interactive marketing. 2020 Aug, 51(1):57-71.

[212] Munirathinam S. Industry 4.0: Industrial internet of things (IIOT). InAdvances in computers 2020 Jan 1 (Vol. 117, No. 1, pp. 129-164). Elsevier.

[213] Kishor A, Chakraborty C. Artificial intelligence and internet of things based healthcare 4.0 monitoring system. Wireless personal communications. 2022 Nov, 127(2):1615-31.

[214] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25, 4(1):10-9.

[215] Haile H, Grinnemo KJ, Ferlin S, Hurtig P, Brunstrom A. End-to-end congestion control approaches for high throughput and low delay in 4G/5G cellular networks. Computer Networks. 2021 Feb 26, 186:107692.

[216] Huang Y, Li YJ, Cai Z. Security and privacy in metaverse: A comprehensive survey. Big Data Mining and Analytics. 2023 Jan 26, 6(2):234-47.

[217] Zhang Y, Love DJ, Krogmeier JV, Anderson CR, Heath RW, Buckmaster DR. Challenges and opportunities of future rural wireless communications. IEEE Communications Magazine. 2021 Dec, 59(12):16-22.

[218] Tan SY, Taeihagh A. Smart city governance in developing countries: A systematic literature review. sustainability. 2020 Jan 25, 12(3):899.

[219] Xie T, Tu GH, Yin B, Li CY, Peng C, Zhang M, Liu H, Liu X. The untold secrets of wifi-calling services: Vulnerabilities, attacks, and countermeasures. IEEE Transactions on Mobile Computing. 2020 May 18, 20(11):3131-47.

[220] Hasan MT, Hossain MR, Pathan AS. Protecting Regular and Social Network Users in a Wireless Network by Detecting Rogue Access Point: Limitations and Countermeasures. InSecuring Social Networks in Cyberspace 2021 Oct 10 (pp. 255-275). CRC Press.

[221] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[222] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, Sarwat AI. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors. 2023 Apr 17, 23(8):4060.

[223] Perwej Y, Abbas SQ, Dixit JP, Akhtar N, Jaiswal AK. A systematic literature review on the cyber security. International Journal of scientific research and management. 2021 Dec 6, 9(12):669-710.

[224] Arora A, Yadav SK, Sharma K. Denial-of-service (dos) attack and botnet: Network analysis, research tactics, and mitigation. InResearch Anthology on Combating Denial-of-Service Attacks 2021 (pp. 49-73). IGI Global.

[225] Shankar SP, Gudadinni SM, Mohta R. A Comprehensive Study of Cyber Threats in the Banking Industry. InStrengthening Industrial Cybersecurity to Protect Business Intelligence 2024 (pp. 244-269). IGI Global.

[226] Gupta BB, Dahiya A. Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC press, 2021 Feb 28.

[227] Kaur G, Habibi Lashkari Z, Habibi Lashkari A, Kaur G, Habibi Lashkari Z, Habibi Lashkari A. Cybersecurity threats in Fintech. Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends. 2021:65-87.

[228] Lehto M. Cyber-attacks against critical infrastructure. InCyber security: Critical infrastructure protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[229] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[230] Seechurn NT, Mungur A, Armoogum S, Pudaruth S. Issues and challenges for network virtualisation. International Journal of Communication Networks and Information Security. 2021 Aug 1, 13(2):206-14.

[231] Bispham M, Creese S, Dutton WH, Esteve-Gonzalez P, Goldsmith M. Cybersecurity in working from home: An exploratory study. InTPRC49: The 49th Research Conference on Communication, Information and Internet Policy 2021 Aug 1.

[232] Buckley B, Dion M. Securing a Remote Workforce. CPM-Capstone, University of New Hampshire. 2021 Jun 15.

[233] Ganesh Keshaorao Yenurkar, Mal S, Nyangaresi VO, Anshul Hedau, Prajwal Hatwar, Shreyas Rajurkar, et al. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering reports. 2023 May 21, 5(12).

[234] Arogundade OR. Network security concepts, dangers, and defense best practical. Computer Engineering and Intelligent Systems. 2023, 14(2).

[235] Majeed A, Hwang SO. A comprehensive analysis of privacy protection techniques developed for COVID-19 pandemic. IEEE Access. 2021 Nov 25, 9:164159-87.

[236] Kumar R, Sharma S, Vachhani C, Yadav N. What changed in the cyber-security after COVID-19?. Computers & security. 2022 Sep 1, 120:102821.

[237] Ferrag MA, Shu L, Choo KK. Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives. IEEE/CAA Journal of Automatica Sinica. 2021 Jul 9, 8(9):1477-99.

[238] Sowmiya B, Abhijith VS, Sudersan S, Sakthi Jaya Sundar R, Thangavel M, Varalakshmi P. A survey on security and privacy issues in contact tracing application of Covid-19. SN computer science. 2021 May, 2:1-1.