World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

A survey of transmission control protocol variants

Lydiah Moraa Machora *

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

World Journal of Advanced Research and Reviews, 2024, 21(03), 1828–1853

Publication history: Received on 08 February 2024; revised on 19 March 2024; accepted on 21 March 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.3.0886

Abstract

TCP (Transmission Control Protocol), is a reliable connection oriented end-to-end protocol. It contains within itself, mechanisms for ensuring reliability by requiring the receiver to acknowledge the segments that it receives. The network is not perfect and a small percentage of packets are lost enroute, either due to network error or due to the fact that there is congestion in the network and the routers are dropping packets. TCP ensures reliability by starting a timer whenever it sends a segment. If it does not receive an acknowledgement from the receiver within the 'time-out' interval then it retransmits the segment. In this paper a review of various TCP is carried out. There are a number of TCP variants for application in the management of network efficiency in terms of network congestion and transmission efficiency. These variants include: - TCP Tahoe, TCP Reno, TCP New Reno, TCP Vegas, TCP SACK, TCP FACK, TCP Asym, TCP RBP, Full TCP and TCP CUBIC. Therefore, the main objective of this paper is to study the tcp types on the network performance variances. All have different features and advantages but with maximal throughput as main objective, which are termed as the clones of TCP, have been incorporated into TCP/IP protocol for handling congestion efficiently in different network scenarios.

Keywords: TCP variants; Attacks, Security; Privacy; Performance

1. Introduction

Transmission Control Protocol (TCP) is the most widely used transport layer protocol in the Internet and one of the most important standards for best effort, reliable data transmission [1]-[4]. In the Internet traffic that is used predominately TCP, applications like HTTP, FTP, SMTP. The performance perceived by users of these Internet applications depends largely depend on the performance of TCP. Considering that the TCP/IP protocol suite is the foundation of the Internet this comes as no surprise. TCP provides a secure and reliable [6] transfer of information. It is used by most of the existing Internet applications today and more than 90% of all data transfers use TCP. The evolution of the Internet has in turn led to evolutions in the TCP protocol. The transport layer can be looked upon as the heart of the whole protocol hierarchy [7], [8]. It provides data transport for the application layer above it. TCP and UDP are two different transport protocols in the TCP/IP protocol suite. The transport protocol used in a particular situation depends on the concerned application. The first implementation of TCP, simply called TCP, was succeeded by a new version: TCP Tahoe. These two versions share the fundamental rules of information transportation, but differ in the solutions. This has led to the expression 'TCP clones'. TCP clones is an expression used for talking about different versions of TCP, considering they all share the same basic functions and purpose. There are many implementations of TCP, each operating slightly differently and even some with significant problems [9], [10]. There are numbers of variants of TCP that are currently deployed. Such as Tahoe, Reno, New Reno, Sack, Vegas, Westwood, Fack and Veno etc. In this paper we will discuss ten version of TCP that is Tahoe, Reno, New Reno, Vegas, SACK, FACK, Asym, RBP, Full TCP and CUBIC on their variants in network performance.

* Corresponding author: Lydiah Moraa Machora

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

1.1. Role of TCP

TCP is the part of the system's kernel. It is responsible for sending/receiving packet in order (FIFO). It resends the missed packet. It also handles error. It is a connection oriented. It is responsible for correct delivery of data.

1.2. TCP variants

Each variation of TCP possesses some special criteria. All the variants look like same, but they have a different technique to deal with congestion. TCP's first variant was Tahoe. A new mechanism called Fast Recovery adds to TCP Tahoe, a new variant is introduced that is TCP Reno [11]. TCP New Reno adds a newest mechanism retransmission to TCP Reno. TCP Vegas also provide its own congestion control techniques and unique retransmission. TCP FACK is same as Reno with Forward Acknowledgment. There are other kinds of TCP variants like SACK, RBP, and Asym etc. We will look at them, on their variants as shown in Figure 1 below. They have a slightly different on their technique to deal with the congestion issue on the network simulation.

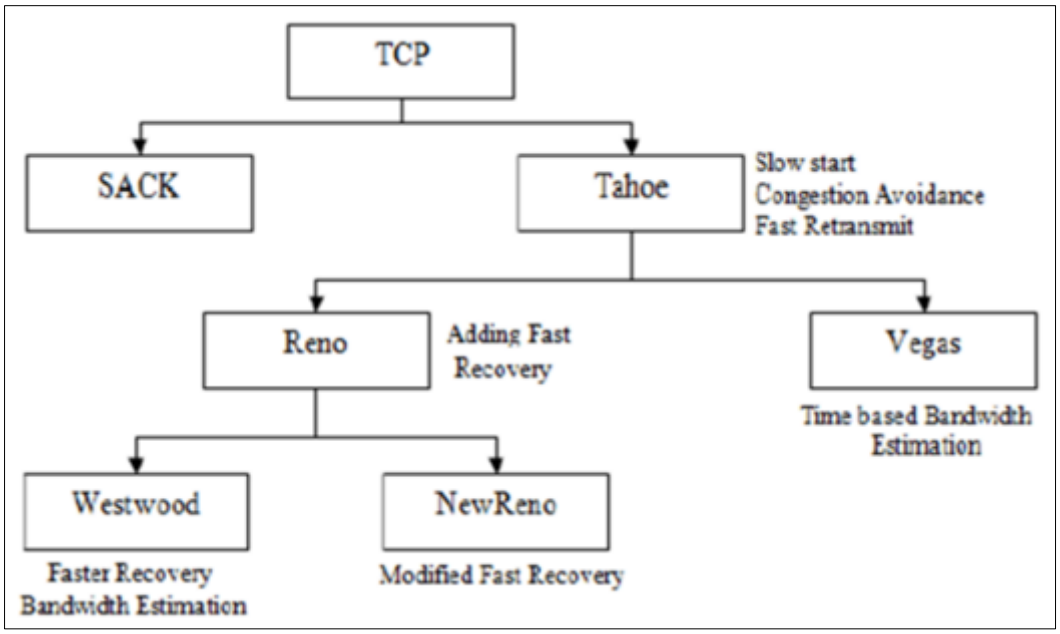

Figure 1 TCP Variants e.g. SACK, Reno, New Reno, Westwood, Vegas

1.2.1. TCP Tahoe

This TCP is based on a principle of conservation of packets, i.e. if the connection is running at the available bandwidth [12] capacity, then a packet is not injected into the network unless a packet is taken out as well. It implements this principle by using the acknowledgements to clock outgoing packets because an acknowledgement means that a packet was taken off the wire by the receiver [13], [14]. It also maintains a congestion window (CWD), to reflect the network capacity. It is a congestion algorithm that utilizes slow start, congestion avoidance, and fast re-transmit. Figure 1 shows congestion control under TCP Tahoe.

According to [15], TCP Tahoe is one of the earliest implementations of the Transmission Control Protocol (TCP) and is characterized by its simplicity and basic congestion control mechanisms. Introduced in the 1980s, TCP Tahoe includes features such as slow start, congestion avoidance, fast retransmit, and fast recovery [16], [17]. Slow start gradually increases the sending rate of data packets [18] until congestion is detected, at which point it enters congestion avoidance mode, slowing down transmission to alleviate network congestion. If packets are lost, TCP Tahoe employs fast retransmit to quickly retransmit the missing packet upon detecting duplicate acknowledgments, while fast recovery helps maintain network throughput by reducing the congestion window upon packet loss [19], [20].

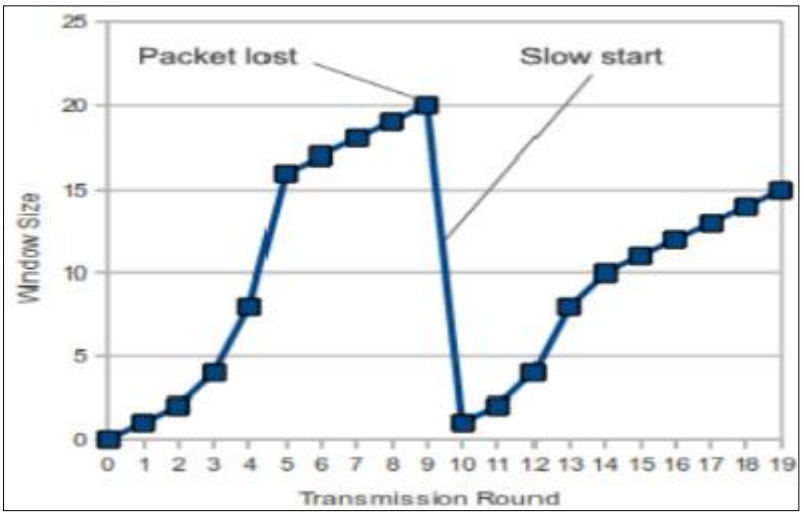

Figure 2 TCP Tahoe congestion control

While TCP Tahoe laid the groundwork for subsequent TCP variants, it lacks more sophisticated congestion control mechanisms found in later implementations, making it less suitable for modern high-speed and high-latency networks.

1.2.2. TCP Reno

This Reno retains the basic principle of Tahoe, such as slow starts and the coarse grain re-transmit timer. However, it adds some intelligence over it so that lost packets are detected earlier and the pipeline is not emptied every time a packet is lost [21]-[23]. Reno requires that it receives immediate acknowledgement whenever a segment is received. The logic behind this, is that whenever it receives a duplicate acknowledgment, then the duplicate acknowledgment could have been received if the next segment in sequence is expected and has been delayed in the network and the segments reached there are out of order or the packet will be lost, its known for its reliability and efficiency [24], incorporates mechanisms like slow start, fast retransmit, and fast recovery. Figure 2 shows the basic operation of TCP Reno.

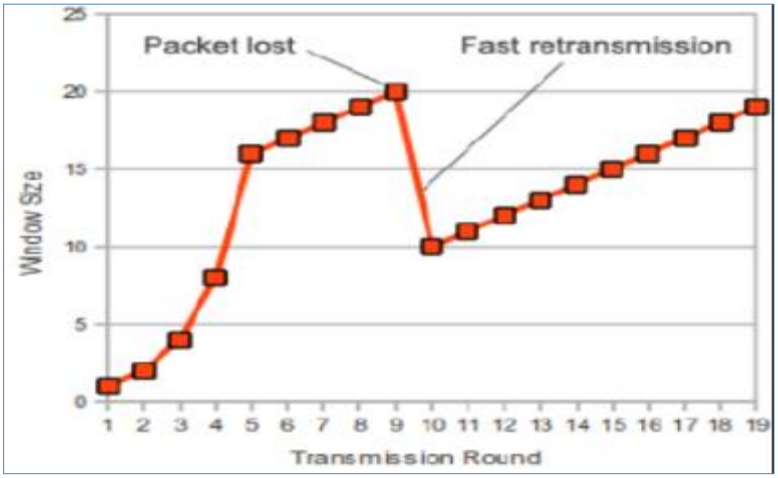

Figure 3 TCP Reno congestion control

According to [25], TCP Reno is a widely used variant of the TCP, a fundamental protocol of the Internet. It is known for its congestion control mechanism, which includes the fast retransmit and fast recovery algorithms. When a packet loss is detected, TCP Reno initiates fast retransmit, resending the packet that was expected to acknowledge the lost one [26]. This is followed by fast recovery, where the sender reduces its congestion window by half and enters a congestion avoidance phase to gradually increase the transmission rate. TCP Reno strikes a balance between efficiency and fairness in handling network congestion, making it a cornerstone of reliable data transfer over the Internet.

1.2.3. TCP New Reno

TCP New Reno is the extension of TCP Reno. It has some advantages over TCP Reno that can detect the multiple packet loss. It does not leave the fast recovery until it receives acknowledgment of all packets, that are present in the window [27]. The fast recovery phase proceeds as in TCP Reno, when a fresh acknowledgment is received. It can detect multiple packet loss. Its congestion avoidance mechanism is very efficient and utilizes network resources much more efficiently [28]. TCP New Reno has few retransmits because of its modified congestion avoidance and slow start. Figure 3 shows the operation of TCP New Reno.

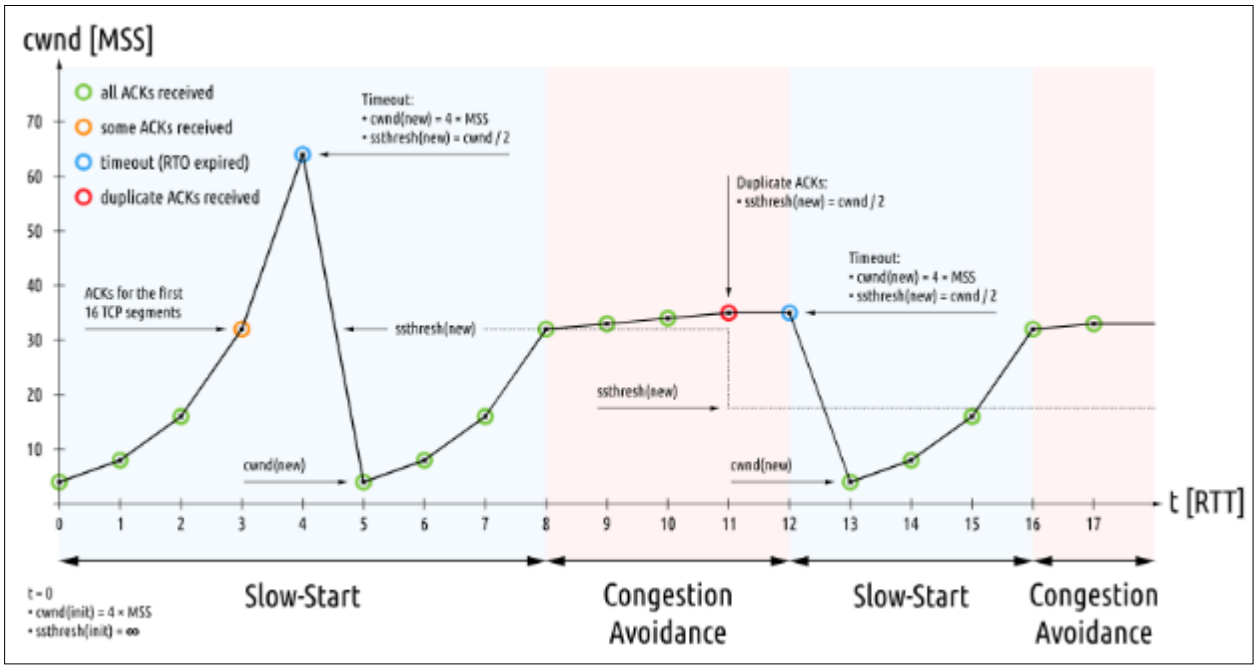

Figure 4 TCP New Reno

As explained in [29], TCP New Reno is an extension of TCP Reno, designed to improve its performance in scenarios involving multiple packet losses within a single window of data. It enhances the fast recovery mechanism of TCP Reno by allowing it to continue sending new packets during the fast recovery phase after the first acknowledgment of a retransmitted packet is received. This optimization reduces unnecessary delays [30] in recovering from multiple packet losses and can lead to more efficient bandwidth utilization. TCP New Reno retains the fundamental congestion control principles of TCP Reno while offering enhanced resilience in facing scenarios with multiple packet losses, making it particularly beneficial in modern network environments with high bandwidth and diverse applications.

1.2.4. TCP Vegas

TCP Vegas is better than the other TCP variants. Like now Reno, Vegas uses triple duplicate acknowledgments always result in packet retransmission [31]. TCP Vegas introduces a new retransmission mechanism for lost packets. It uses fine-grained round trip time measurements for a compute timeout period of each packet. If the timeout period of the oldest unacknowledged packets has expired then, the packet is retransmitted [32]. As shown in Figure 4, TCP Vegas it also provides modified slow start and congestion avoidance.

Vegas exponentially increases its window at every, other round-trip time [33]. It leaves the slow start and enters into the congestion avoidance phase when the actual throughput is lower than the expected throughput. According to [34], TCP Vegas is a congestion control algorithm that differs from traditional TCP variants like Reno by utilizing an explicit measurement of network congestion through the calculation of the round-trip time (RTT) variations. It operates on the principle that an increase in RTT indicates approaching congestion, allowing it to proactively adjust the transmission rate before packet loss occurs [35]. By employing this predictive approach, TCP Vegas aims to achieve better network utilization and reduced packet loss compared to reactive congestion control mechanisms. However, its effectiveness [36] can be influenced by network conditions and the accuracy of RTT measurements, making it a subject of ongoing research and optimization for specific network environments.

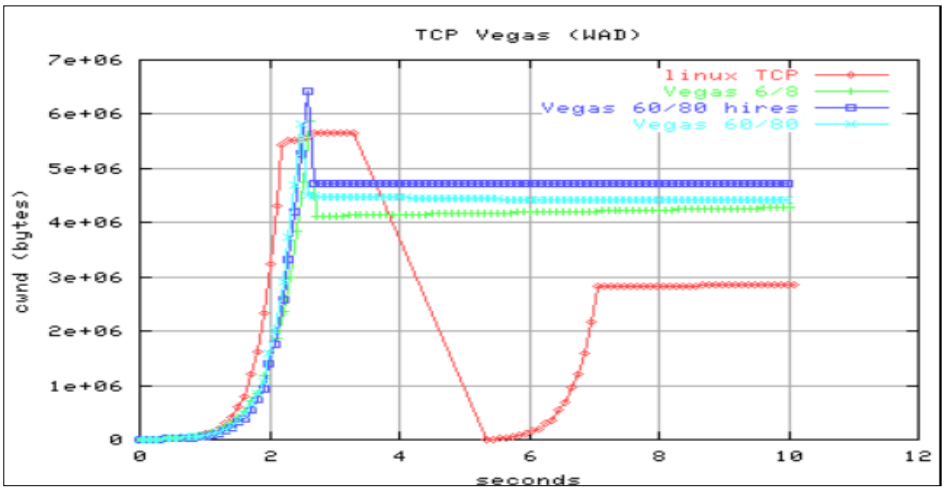

Figure 5 TCP VEGAS

1.2.5. TCP SACK

TCP SACK or selective acknowledgement requires that packets should acknowledge selectively. It is an option that is enabling a receiver to tell the sender the range of non-contiguous packets received [37]. Without SACK, the receiver can only tell the sender about sequentially received packets. The sender uses this information to retransmit selectively only the lost packets. SACK (Selective Acknowledgement) to TCP does not change the basic underlying congestion control algorithms. The main difference between the SACK TCP and the Reno TCP implementation is in the behavior when multiple packets are dropped from one window of data. During the Fast Recovery, SACK maintains a variable called pipe that represents the estimated number of packets outstanding in the path [38]. The use of the pipe variable decouples the decision of when to send a packet from the decision of which packet to send. As shown in Figure 5, the sender maintains a data structure that remembers acknowledgments from previous SACK options.

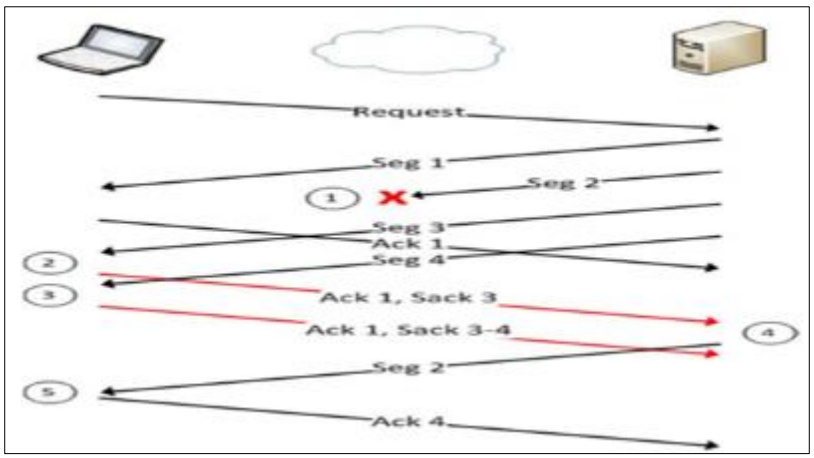

Figure 6 Selective Acknowledgement by SACK

When the sender is allowed to send a packet, it retransmits the next packet from the list of packets inferred to be missing at the receiver. The SACK sender has a special handling for partial ACKs (ACKs received during Fast Recovery that advance the Acknowledgment Number field of TCP header, but do not take the sender out of fast Recovery). The sender decrements pipe by two rather than one for partial ACKs, the SACK sender never recovers more slowly than a Slow-Start. Detailed description of SACK TCP can be found [39].

1.2.6. TCP FACK

TCP FACK (Forward Acknowledgment) is a congestion control mechanism designed to improve the performance of TCP in scenarios with multiple packet losses within a single window. TCP FACK, is used to improve the congestion control during the recovery process, therefore a new algorithm is introduced to help in the congestion control, that is TCP FACK [40], [41]. FACK also called forward acknowledgement that is on top of the selective acknowledgement in the network.

This TCP is therefore, useful in forwarding the selective acknowledgement sequence number as a sign that all the previous unselected acknowledged packets that were lost [42]. This type of TCP Variant it improves the recovery process of packets lost significantly and performance [43] that the traditional approaches when the packets are lost. Figure 6 demonstrates the operation of TCP FACK.

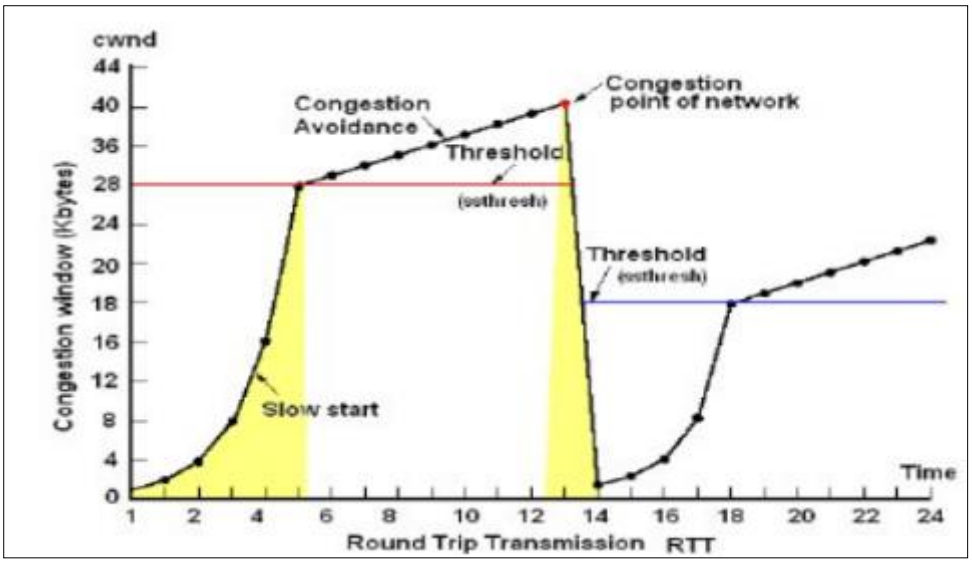

Figure 7 TCP FACK

Unlike traditional TCP variants that rely solely on the acknowledgment of data packets to infer packet loss, TCP FACK utilizes both cumulative acknowledgments (ACKs) and selective acknowledgments (SACKs) to accurately identify lost packets [44]. By leveraging this combination, TCP FACK can more precisely determine the extent of packet loss within a window, allowing for quicker recovery without unnecessarily reducing the sending rate [45]. This approach enhances TCP's efficiency in handling congestion and reduces the impact of packet loss on network throughput, making it particularly beneficial in environments prone to packet loss and congestion.

1.2.7. TCP ASYM

In this type of TCP ASYM, it has the same characteristics of TCP Reno and the TCP New Reno. Therefore, we can say that is analyzed from the above variants of TCP [46]. As shown in Figure 7, TCP Asym is very useful when one is using a high volume in the data transmission application in the network.

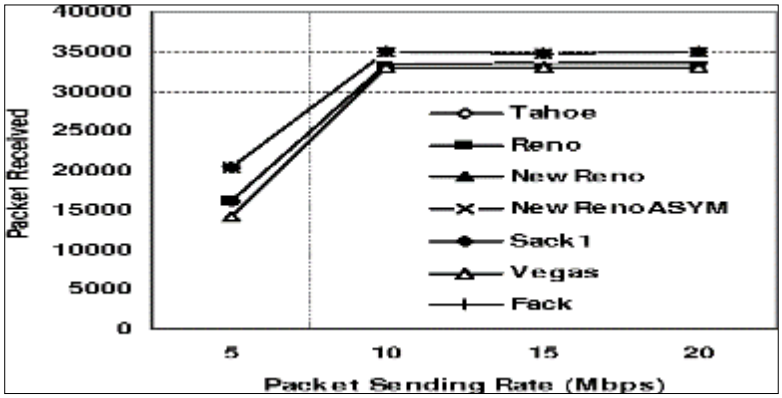

Figure 8 Packet transmission rate comparisons

In FACK and Tahoe, TCP Asym can reset the congestion window to one packet, when it is lost in an event loss. The demerit of the Asym TCP is that it not suitable for the medium or high quality in the real time application on the internet.

1.2.8. TCP RBP

TCP RBP stands for Transmission Control Protocol Rate Based Pacing. The slow start problem that decreases a problem in the performance. This problem is therefore solved by sending the packets at a very few paces until it may get the ACK clock running again [47]. This sender rate of the data transfer is estimated or rated by a nearby estimate of accessible bandwidth, this type of modification is called the Rate Based Pacing [48]. TCP RBP requires clock mechanism segments that can be sent to the RBP. Figure 8 shows the sequence of packet plot of TCP RBP.

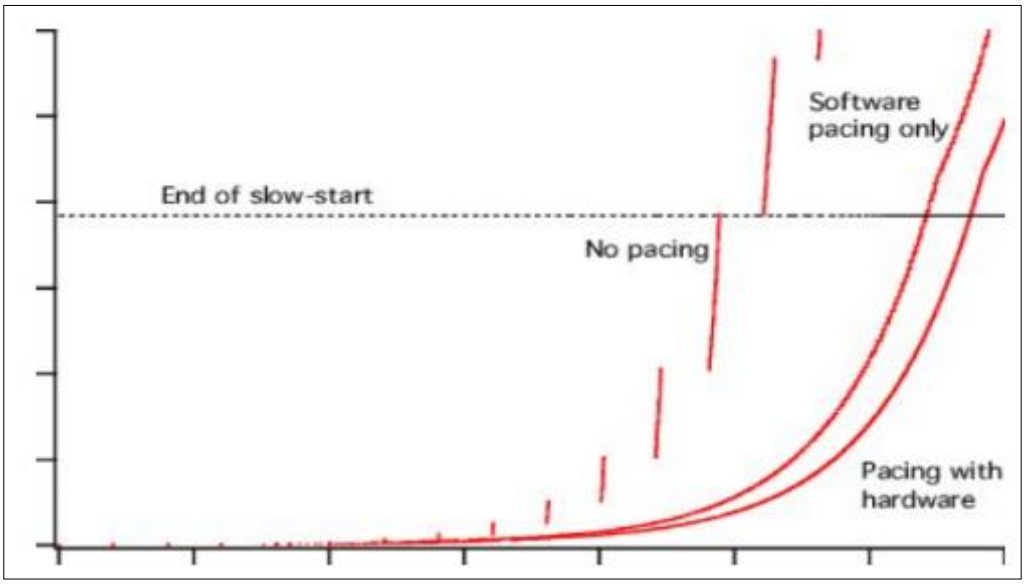

Figure 9 Sequence of packet plot of original TCP, software-only RBP TCP, and RBP with hardware support. (HZ=100)

As explained in [49], Transmission Control Protocol Rate Based Pacing (TCP-RBP) is a congestion control mechanism designed to regulate the sending rate of TCP connections based on the observed network conditions. Unlike traditional TCP variants that rely on packet loss or delay for congestion inference, TCP-RBP employs a proactive approach by pacing the transmission rate according to a pre-defined target rate. By dynamically adjusting the pacing rate based on feedback from the network, TCP-RBP aims to achieve optimal throughput while minimizing congestion and packet loss. This approach is particularly beneficial in high-speed networks [50] where traditional congestion control mechanisms may struggle to maintain efficiency. TCP-RBP offers improved stability, fairness, and predictability in bandwidth utilization, making it well-suited for modern networking environments with diverse traffic patterns and varying link capacities.

1.2.9. FULL TCP

Full TCP (Transmission Control Protocol) refers to the complete implementation of the TCP protocol suite, encompassing all its features and functionalities [51]. It provides a reliable virtual-circuit connection between applications; that is, a connection is established before data transmission begins. Data is sent without errors or duplication and is received in the same order as it is sentAs a fundamental protocol of the Internet, TCP provides reliable, connection-oriented communication between hosts, ensuring data delivery with error detection, flow control, and congestion control mechanisms [52]. Full TCP includes components such as three-way handshake for establishing connections, sliding window for efficient data transmission, acknowledgment mechanism for confirming data receipt, and congestion control algorithms to manage network congestion [53]-[55]. By incorporating these elements, Full TCP enables robust and efficient communication over IP networks [56], facilitating the exchange of data across diverse applications and network environments with reliability and integrity.

1.2.10. TCP CUBIC

This type of TCP, is a network congestion avoidance algorithm that can be used to achieve the high bandwidth connections on the networks faster and relatively in the face of high latency that the earlier congestion algorithms [57]. This supports the optimization of long fat networks. The first CUBIC implementation was released in Linux kernel 2.6.13. We propose a new TCP variant, called CUBIC, for fast and long-distance networks. CUBIC is an enhanced version of BIC-TCP [58], [59]. It simplifies the BIC-TCP window control and improves its TCP-friendliness and RTT-fairness [60]. TCP CUBIC uses a cubic increase function in terms of the elapsed time since the last loss event. In order to provide fairness

to Standard TCP, CUBIC also behaves like Standard TCP when the cubic window growth function is slower than Standard TCP [61]. Figure 9 shows the comparison of TCP CUBIC and TCP BIC.

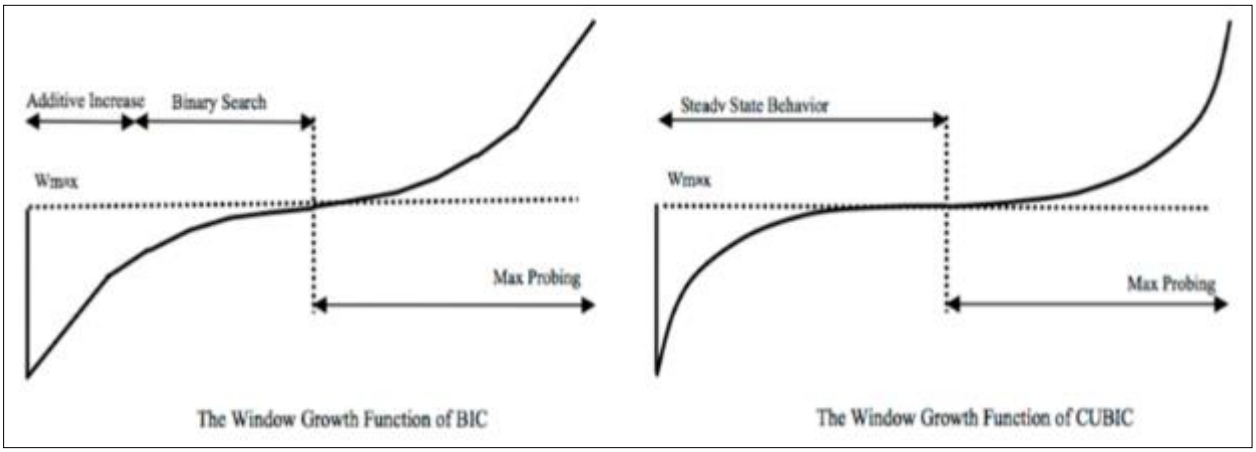

Figure 10 TCP CUBIC and TCP BIC

In the real-time nature of the protocol keeps the window growth rate independent of RTT, which keeps the protocol TCP friendly under both short and long RTT paths. Through extensive testing, we confirm that CUBIC tackles the shortcomings of CUBIC TCP and achieves fairly good Intra-protocol fairness, the RTT fairness and the TCP-friendliness. In addition, CUBIC is a high-speed variant of standard TCP [62].

1.2.11. TCP BIC

TCP BIC, or Binary Increase Congestion control, is a congestion control algorithm designed to optimize network performance [63] by efficiently utilizing available bandwidth while minimizing congestion. Unlike traditional TCP congestion control algorithms like Reno or New Reno, which adjust the congestion window size linearly, TCP BIC operates in a binary search-like manner, doubling or halving the congestion window based on congestion signals from the network [64]. This binary search approach allows TCP BIC to rapidly converge to an optimal congestion window size, thereby achieving higher throughput and better network utilization.

TCP BIC is particularly effective in high-speed and high-delay networks where traditional algorithms may struggle to find the appropriate congestion window size due to their linear adjustments [65]. By using a binary search mechanism, TCP BIC can quickly adapt to changing network conditions, allowing for more efficient data transfer and reduced packet loss. However, TCP BIC may exhibit aggressiveness in certain scenarios, potentially causing unfairness in network bandwidth allocation when competing with other congestion control algorithms [66]. Nonetheless, TCP BIC remains a valuable tool in modern networking environments, especially for optimizing performance in challenging network conditions.

1.3. Privacy issues

Privacy concerns in TCP variants encompass a range of issues stemming from the inherent structure and behavior of TCP, as well as the specific features and optimizations introduced in various TCP variants [67]-[69]. One of the primary concerns revolves around the metadata contained in TCP headers, which can include sensitive information such as source and destination IP addresses, port numbers, sequence numbers, and window sizes. While this metadata is essential for establishing and maintaining TCP connections, it can also be intercepted and analyzed by adversaries to infer details about the communicating parties, the nature of the communication, and potentially even the content being transmitted. For example, analyzing TCP headers could reveal the identities of users, the applications they are using, and their browsing habits, posing risks to individual privacy and security.

Furthermore, certain TCP variants or configurations may introduce additional header fields or behaviors that exacerbate privacy risks. For instance, extensions like Explicit Congestion Notification (ECN) or Timestamps can provide valuable information to network observers but also increase the amount of metadata exposed in TCP headers [70]-[75]. Similarly, optimizations such as Selective Acknowledgment (SACK) or Fast Retransmit/Fast Recovery mechanisms may inadvertently leak information about network conditions or packet loss events, which could be exploited by adversaries to infer details about the communication session or launch targeted attacks. As TCP variants

evolve to address performance or reliability challenges, it is essential to consider the potential privacy implications of these enhancements and implement appropriate safeguards to protect user data.

Another significant privacy concern in TCP variants pertains to traffic analysis and pattern recognition. Adversaries can analyze the timing, size, and frequency of TCP packets to infer various aspects of network activity, including user behavior, application usage, and specific actions such as web browsing or file transfers [71]-[79]. By examining patterns in TCP traffic, attackers can potentially identify relationships between users, organizations, or devices, as well as infer sensitive information such as browsing habits, preferences, or even login credentials. This type of traffic analysis poses significant risks to individual privacy and can be leveraged for various malicious purposes, including surveillance, targeted advertising, or cyber-attacks [80] aimed at compromising systems or extracting sensitive data.

To mitigate privacy risks associated with TCP variants, several strategies can be employed. Firstly, encryption technologies such as Transport Layer Security (TLS) should be implemented to protect the confidentiality and integrity of TCP communications, particularly for sensitive data transmissions over untrusted networks [81], [82]. Encrypting TCP payloads ensures that even if adversaries intercept the traffic, they cannot decipher the content without the appropriate cryptographic keys [83], [84]. Additionally, network administrators should implement traffic obfuscation techniques, such as traffic padding or mixing, to conceal patterns in TCP traffic and make it more challenging for attackers to perform traffic analysis. Furthermore, privacy-preserving protocols [85] and anonymization services can be utilized to anonymize user identities and mask sensitive information in TCP headers, reducing the risks associated with metadata exposure.

According to [86], users and network administrators should be educated about the potential privacy risks associated with TCP communications and encouraged to adopt best practices for securing their networks and systems. This includes staying informed about the latest developments in TCP variants and implementing appropriate security measures to mitigate privacy threats effectively [87]-[90]. By fostering a culture of privacy awareness and promoting responsible data handling practices, organizations can better protect user privacy and ensure the secure transmission of data over TCP networks.

1.4. Security challenges in TCP

Security issues in Transmission Control Protocol (TCP) variants encompass a wide range of vulnerabilities that can be exploited by attackers to compromise network integrity, confidentiality, and availability. One of the primary concerns revolves around TCP's susceptibility to various types of attacks, including TCP session hijacking, spoofing, and packet injection [91]-[96]. TCP's connection-oriented nature, coupled with its reliance on sequence numbers and acknowledgment mechanisms, makes it vulnerable to manipulation by malicious actors seeking to disrupt communications or gain unauthorized access to network resources. For example, attackers can launch TCP session hijacking attacks by intercepting and impersonating legitimate TCP connections, thereby gaining unauthorized access to sensitive information or injecting malicious payloads into communication streams.

Moreover, certain TCP variants or configurations may introduce additional security vulnerabilities or weaknesses that could be exploited by attackers. For instance, extensions like Selective Acknowledgment (SACK) or Timestamps may inadvertently reveal information about network conditions or internal system parameters, which could aid attackers in crafting more effective exploits or launching targeted attacks [97]-[99]. Similarly, optimizations such as Fast Retransmit/Fast Recovery mechanisms may introduce new attack vectors or exacerbate existing vulnerabilities, particularly in scenarios where attackers can manipulate network traffic to trigger abnormal behavior in TCP implementations [100], [101]. As TCP variants evolve to address performance or reliability challenges, it is essential to conduct thorough security assessments and implement appropriate safeguards to mitigate potential risks.

Another significant security concern in TCP variants pertains to denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. TCP's connection establishment process, which involves a series of handshakes and resource allocations, can be exploited by attackers to overwhelm target systems with a flood of malicious connection requests, thereby exhausting available resources and rendering the service inaccessible to legitimate users [102]-[104]. Additionally, vulnerabilities in TCP implementations or configurations may allow attackers to exploit protocol weaknesses or resource limitations to orchestrate more sophisticated DDoS attacks, such as SYN flood attacks or amplification attacks [105, [108]. These attacks can have severe consequences for network availability and performance, highlighting the importance of implementing robust defenses and mitigation strategies at both the network and application layers.

To mitigate security risks associated with TCP variants, organizations should adopt a comprehensive approach to network security that includes implementing strong authentication, access control, and encryption mechanisms [109]-[114]. For example, deploying technologies such as IPsec or TLS can help protect TCP communications against eavesdropping, tampering, and impersonation attacks by encrypting data in transit and authenticating communication endpoints. Additionally, network intrusion detection and prevention systems (IDS/IPS) can be employed to detect and block malicious traffic patterns associated with TCP-based attacks, helping to thwart exploitation attempts and mitigate the impact of security incidents [115], [116]. Furthermore, regular security audits and vulnerability assessments should be conducted to identify and remediate potential weaknesses in TCP implementations, configurations, and network infrastructure, ensuring that security controls remain effective against evolving threats.

Network administrators and users should be educated about common TCP vulnerabilities, attack techniques, and best practices for securing TCP-based communications. This includes understanding the importance of timely software updates and patches, implementing strong password policies, and configuring firewalls and intrusion detection systems to filter and block malicious traffic [117], [118]. By fostering a culture of security awareness and promoting proactive risk management strategies, organizations can better protect their networks and systems against TCP-related security threats.

1.5. Common attacks in TCP

Common attacks targeting TCP variants exploit vulnerabilities in the protocol's design and implementation to compromise network security, integrity, and availability [119], [120]. One prevalent attack is TCP session hijacking, where an attacker intercepts and takes control of an ongoing TCP connection between two parties. By exploiting weaknesses in TCP's sequence number generation or prediction, attackers can inject malicious packets into the communication stream, impersonate one of the parties, or manipulate data exchanged between them [121]-[124]. Session hijacking attacks can lead to unauthorized access to sensitive information, unauthorized transactions, or the injection of malware into network traffic [125].

Another common TCP attack is SYN flooding, a type of Denial of Service (DoS) attack that exploits TCP's three-way handshake mechanism. In a SYN flood attack, the attacker sends a flood of TCP SYN packets with spoofed source addresses to the victim's server, initiating multiple half-open connections [127]-[128]. As the server allocates resources for each incoming connection request and waits for the final ACK packet, it quickly becomes overwhelmed by the volume of incoming SYN packets, exhausting available resources and rendering the service unavailable to legitimate users [129], [131]. SYN flooding attacks can significantly degrade network performance and disrupt service availability, highlighting the importance of implementing countermeasures such as SYN cookies or rate limiting.

Moreover, TCP variants are susceptible to Man-in-the-Middle (MitM) attacks, where an attacker intercepts and alters communication between two parties without their knowledge. In a TCP MitM attack, the attacker inserts themselves between the communicating parties, intercepting and relaying packets while masquerading as the legitimate endpoint to both parties [132]-[135]. This allows the attacker to eavesdrop on sensitive information, manipulate data exchanged between the parties, or even hijack the entire communication session. MitM attacks pose significant risks to data confidentiality, integrity, and privacy, particularly in scenarios where sensitive information such as login credentials or financial transactions are being transmitted [136], [137].

Additionally, TCP variants can be vulnerable to TCP sequence number prediction attacks, where attackers attempt to predict the sequence numbers used in TCP connections to inject malicious packets or hijack ongoing sessions [138], [139]. By analyzing patterns in TCP sequence number generation or exploiting weaknesses in random number generation algorithms, attackers can predict the sequence numbers used in TCP connections, enabling them to inject forged packets into the communication stream or impersonate legitimate endpoints [140]-[143]. Sequence number prediction attacks can lead to unauthorized access, data manipulation, or the injection of malware into network traffic, highlighting the importance of implementing secure sequence number generation algorithms and cryptographic protections.

Furthermore, TCP variants are susceptible to Reflective and Amplification attacks, where attackers exploit certain features of the protocol to amplify the volume of malicious traffic directed at a target [144], [145]. For example, attackers can abuse TCP's connection establishment process to amplify the volume of SYN flood attacks, exploiting the asymmetry between the resources required to initiate a TCP connection and those required to respond to it. Similarly, attackers can abuse TCP's acknowledgment mechanism to amplify the volume of data exchanged between two parties, exploiting vulnerabilities such as TCP ACK spoofing or Blind TCP Reset attacks [146]-[149]. Reflective and Amplification attacks can significantly amplify the impact of DoS attacks, making it more challenging to mitigate them effectively.

Moreover, TCP variants are susceptible to TCP Reset (RST) attacks, where attackers send forged TCP RST packets to terminate ongoing connections or disrupt communication between two parties [150]. By spoofing the source address of the TCP RST packets and injecting them into the communication stream, attackers can cause legitimate connections to be terminated prematurely, leading to service disruption or data loss [151], [152]. TCP RST attacks can be used to target specific services or applications, disrupt critical infrastructure, or sabotage network communications, highlighting the importance of implementing robust defenses such as intrusion detection and prevention systems (IDS/IPS).

Additionally, TCP variants are susceptible to Blind TCP Injection attacks, where attackers inject malicious payloads into ongoing TCP connections without directly observing the communication stream [153], [154]. By predicting or guessing the sequence numbers used in TCP connections, attackers can inject forged packets into the communication stream, impersonate legitimate endpoints, or manipulate data exchanged between parties. Blind TCP Injection attacks can be used to exploit vulnerabilities in network services or applications, bypass security controls, or compromise sensitive information [155], highlighting the importance of implementing secure sequence number generation algorithms and cryptographic protections.

Furthermore, TCP variants are susceptible to TCP Window Size attacks, where attackers manipulate TCP window size values to degrade network performance, disrupt communication, or exhaust available resources [156], [157]. By sending TCP packets with artificially inflated or reduced window size values, attackers can force the target's TCP stack to allocate excessive memory or processing resources, leading to performance degradation or denial of service [158]. TCP Window Size attacks can be used to exploit vulnerabilities in TCP implementations or configurations, bypass security controls, or disrupt critical infrastructure, highlighting the importance of implementing robust defenses such as rate limiting or traffic filtering.

Moreover, TCP variants are susceptible to TCP Connection Hijacking attacks, where attackers gain unauthorized access to ongoing TCP connections by exploiting weaknesses in TCP's connection establishment process or session management mechanisms [159]. By intercepting and manipulating packets exchanged during the three-way handshake or session termination process, attackers can hijack existing TCP connections, impersonate legitimate endpoints, or inject malicious payloads into the communication stream [160, [161]. TCP Connection Hijacking attacks can lead to unauthorized access, data manipulation, or the injection of malware into network traffic, highlighting the importance of implementing secure connection establishment and session management protocols [162].

Lastly, TCP variants are susceptible to TCP Session Termination attacks, where attackers disrupt ongoing TCP connections by sending forged TCP FIN or RST packets to terminate communication between two parties prematurely [163]. By spoofing the source address of the TCP termination packets and injecting them into the communication stream, attackers can cause legitimate connections to be terminated unexpectedly, leading to service disruption or data loss [164]. TCP Session Termination attacks can be used to target specific services or applications, disrupt critical infrastructure, or sabotage network communications, highlighting the importance of implementing robust defenses such as intrusion detection and prevention systems (IDS/IPS).

1.6. Common vulnerabilities in TCP

The TCP variants are fundamental to internet communication, facilitating reliable data transmission across networks. However, they are not without vulnerabilities. One common vulnerability is related to TCP's connection-oriented nature, which makes it susceptible to SYN flooding attacks [165], [166]. During the TCP handshake process, attackers can flood a target server with a barrage of SYN packets, causing it to allocate resources for incomplete connections. As the server's resources become exhausted, it can no longer accept legitimate connection requests, leading to denial of service for legitimate users. SYN flooding exploits TCP's reliance on the three-way handshake, overwhelming servers with excessive connection requests.

Furthermore, TCP variants are vulnerable to session hijacking attacks, which exploit weaknesses in TCP sequence number generation. Attackers intercept and manipulate TCP packets, impersonating one of the communicating parties to gain unauthorized access to sensitive information or inject malicious payloads into the communication stream 167], [168]. Session hijacking is particularly concerning because it can occur without the parties' knowledge, enabling attackers to eavesdrop on confidential conversations, steal credentials, or tamper with data exchanges [169]. This vulnerability underscores the importance of implementing robust cryptographic protocols to authenticate and secure TCP connections.

Another significant vulnerability in TCP variants is related to sequence number prediction attacks. By analyzing TCP packet headers, attackers can predict sequence numbers used in TCP connections, enabling them to inject forged packets into the communication stream or impersonate legitimate endpoints [170]-[173]. Sequence number prediction attacks can compromise the confidentiality and integrity of TCP communications, leading to unauthorized access [174], data manipulation, or the injection of malware. Mitigating this vulnerability requires implementing secure sequence number generation algorithms and cryptographic protections to prevent attackers from tampering with TCP packets.

Moreover, TCP variants are vulnerable to man-in-the-middle (MitM) attacks, where attackers intercept and alter communication between two parties. By inserting themselves between the communicating parties, attackers can eavesdrop on sensitive information, manipulate data exchanges, or hijack entire communication sessions [175], [176]. MitM attacks exploit TCP's lack of built-in authentication and encryption, enabling attackers to masquerade as legitimate endpoints and compromise the confidentiality and integrity of TCP communications [176]. To mitigate this vulnerability, it is essential to implement robust cryptographic protocols such as Transport Layer Security (TLS) to authenticate and encrypt TCP connections.

Additionally, TCP variants are susceptible to TCP RST (reset) attacks, where attackers send forged TCP reset packets to terminate ongoing connections or disrupt communication between two parties. By spoofing the source address of the TCP reset packets and injecting them into the communication stream, attackers can cause legitimate connections to be terminated prematurely, leading to service disruption or data loss [177], [178]. TCP RST attacks can be used to target specific services or applications, disrupt critical infrastructure, or sabotage network communications, highlighting the importance of implementing robust defenses such as intrusion detection and prevention systems (IDS/IPS).

Furthermore, TCP variants are vulnerable to blind TCP injection attacks, where attackers inject malicious payloads into ongoing TCP connections without directly observing the communication stream. By predicting or guessing sequence numbers used in TCP connections, attackers can inject forged packets into the communication stream, impersonate legitimate endpoints, or manipulate data exchanges [179]. Blind TCP injection attacks can exploit vulnerabilities in network services or applications, bypass security controls, or compromise sensitive information. To mitigate this vulnerability, organizations must implement secure sequence number generation algorithms and cryptographic protections [180] to prevent attackers from tampering with TCP packets.

Moreover, TCP variants are vulnerable to TCP window size attacks, where attackers manipulate TCP window size values to degrade network performance, disrupt communication, or exhaust available resources. By sending TCP packets with artificially inflated or reduced window size values, attackers can force the target's TCP stack to allocate excessive memory or processing resources, leading to performance degradation or denial of service [181], [182]. TCP window size attacks can exploit vulnerabilities in TCP implementations or configurations, bypass security controls, or disrupt critical infrastructure, emphasizing the importance of implementing robust defenses such as rate limiting or traffic filtering.

Additionally, TCP variants are vulnerable to TCP connection hijacking attacks, where attackers gain unauthorized access to ongoing TCP connections by exploiting weaknesses in TCP's connection establishment process or session management mechanisms. By intercepting and manipulating packets exchanged during the three-way handshake or session termination process, attackers can hijack existing TCP connections, impersonate legitimate endpoints, or inject malicious payloads into the communication stream [183], [184]. TCP connection hijacking attacks can lead to unauthorized access, data manipulation, or the injection of malware into network traffic, highlighting the importance of implementing secure connection establishment and session management protocols.

Lastly, TCP variants are vulnerable to TCP session termination attacks, where attackers disrupt ongoing TCP connections by sending forged TCP FIN or RST packets to terminate communication between two parties prematurely [185]. By spoofing the source address of the TCP termination packets and injecting them into the communication stream, attackers can cause legitimate connections to be terminated unexpectedly, leading to service disruption or data loss. TCP session termination attacks can be used to target specific services or applications, disrupt critical infrastructure, or sabotage network communications [186], highlighting the importance of implementing robust defenses such as intrusion detection and prevention systems (IDS/IPS).

1.7. Performance indicators analysis

In this section, the ten TCP variants are described in terms of their performance. In this description, different parameters are utilized and on the basis of these parameters, the different descriptions are obtained from all the ten TCP variants. A brief definition about these parameters is given below.

Number of packets dropped: - It is failure of transmitting packets to arrive at their destination. It is calculated as: Number of packets dropped = total no. of packets sent-total no. of packets received.

Number of packets sent: - It is the total number of packets sent by the sender.

Delivery Ratio: - To calculate delivery ratio, we need the total number of packets sent and total number of packets received. Delivery Ratio = no. of packets successfully delivered/ total no. of packets sent

Average Throughput: - throughput is the rate at which packets transferred between the sender and receiver. Where the average throughput is the rate over a longer period of time. Units of average throughput are bytes/Sec or bits/Sec.

Total Delay: - Total delay is the difference between the time at which sender generated the packet and time which the receiver received the packet. Total delay= packet generation time/packet receiving time.

Total Jitter: - Variations in delay of receiving packets, called jitter. It is the variation in latency as measured in the variability over time of the packet latency across a network

Average Delay: - The average delay a packet takes to travel from sender to the receiver side node. A delay is introduced due to the queuing of packets at the interface of node, time transmission and due to buffering during route discovery.

Average Jitter: -It is time variation between subsequent packets arrived. Main causes of jitter are network congestion or route changes.

2. Comparison of TCP variants

From the description above, the following comparison of TCP variants in different parameters in a survey of transmission control protocols are obtained as summarized below.

2.1. Number of Nodes vs. Number of Packets Dropped

It is the difference between the total number of packets sent by the sender and total number of packets received by the receiver. Number of Nodes are related to the number of packets dropped. As we increase the no. of nodes, then the complexity of the network is automatically increased. The complexity may cause of congestion. All variants have the different performance whenever the numbers of nodes are increased. We checked on 10 nodes at this level no. of packets dropped by TCP variants is 0. We double the no. of nodes. There's no complexity arises at this stage so no. of dropped packets is still 0 by all algorithms. Actually, there is simplicity in the network. But when the number of nodes is 40 then packets start to drop.

2.2. Number of nodes vs. Delivery ratio

We can get the delivery ratio by dividing the total number of packets, delivered to the receiver with total number of packets sent by the sender, delivery ratio is 100 percent when numbers of nodes are 10 and 20. But whenever the number of nodes becomes 40 then delivery ratio of all variants is decrease except the TCP Vegas.

2.3. Number of nodes vs. Number of packets sent

It is the rate of packet transmission. Number of nodes also affect the number of packets send by each node. In experiment1 table, where the no. of nodes is 10 then TCP Reno, TCP New Reno, TCP SACK, TCP FACK and TCP Asym has the same output and TCP Vegas sends the highest number of packets. No. of the nodes become 20 and TCP RBP sends the highest number of packets. TCP New Reno sends highest no. of the packet.

2.4. Number of nodes vs. Average throughput

Average throughput is rate over a longer period of time. It is measured in bytes/sec. In first stage every variant has the same throughput. The highest throughput from the all-TCP variants and where the no. of nodes is 40. But it varies as the number of nodes increases.

2.5. Number of nodes vs. Total delay

It is calculated by minus the packet received time from packet generation time There are various reasons for packet delay in TCP. TCP RBP and Vegas both has a lowest delay rate than the others. Where TCP Reno is having highest delay.

2.6. Number of nodes vs. Total jitter

Variations in delay of receiving packets, called jitter. In this paper, we evaluate the Total jitter that is a combination of random jitter and deterministic jitter. All variants have almost same jitter except RBP and Vegas. Jitter difference varies and where 40 nodes are used, Asym has higher jitter and RBP has lower jitter than all other.

2.7. Number of nodes vs. Average Delay

The average delay is based on the total delay. TCP RBP has lowest average delay and TCP Asym has the highest average delay.

2.8. TCP variants on key performance indicators

Table 1 Key Performance Indicators on TCP Variants

TCP Variants ➡ Parameters ⬇	**TAHOE**	**RENO**	**NEW RENO**	**VEGAS**	**SACK**	**FACK**	**ASYM**	**RBP**	**FULL TCP**	**CUBIC**
Delivery Ratio	Decreases	Decreases	Decreases	Increases	Decreases	Decreases	Decreases	Decreases	Decreases	Decreases
Total Delay	Lowest	Highest	Highest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Total Jitter	Lowest	Highest	Highest	Highest	Lowest	Lowest	Highest	Lowest	Lowest	Lowest
Average Delay	Lowest	Lowest	Highest	Lowest	Lowest	Highest	Highest	Lowest	Lowest	Lowest
Number of packets dropped	Lowest	Lowest	Highest	Highest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Average Throughput	Lowest	Highest	Highest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Average Jitter	Lowest	Highest	Highest	Lowest	Lowest	Highest	Highest	Lowest	Lowest	Lowest
Number of Packets Sent	Lowest	Highest	Highest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

3. Result

We select the best TCP on the basis of the above-mentioned parameters. Each variant has different performance of different parameters. If a variant has low performance in a parameter, then it can be possible that the variant has the highest performance in another parameter. The table below shows the brief description about it.

Table 2 Best TCP Variants in different parameters

PARAMETERS	**BEST TCP**
Number of Nodes vs. Number of packets Dropped	Vegas
Number of Nodes vs. Number of packets sent	NewReno
Number of Nodes vs. Average Throughput in bytes/sec	NewReno
Number of Nodes vs. Delay	RBP
Number of Nodes vs. Jitter	RBP

3.1. Open challenges in TCP

Despite its fundamental role in internet communication, TCP faces several open challenges that warrant attention and innovation. One significant challenge is TCP's performance over high-latency and high-bandwidth networks [187]. Traditional TCP variants struggle to fully utilize available bandwidth in such environments due to their conservative congestion control mechanisms. As a result, there's a need for TCP variants that can efficiently handle long round-trip times and large bandwidth-delay products. Researchers are exploring solutions such as TCP Cubic and TCP BBR, which aim to optimize TCP's performance over challenging network conditions by adjusting congestion control algorithms and window management strategies.

Another open challenge in TCP is the proliferation of encrypted traffic, particularly with the widespread adoption of Transport Layer Security (TLS). While encryption enhances data privacy and security, it also poses challenges for network management and performance optimization [188], [189]. Encrypted traffic makes it difficult for network administrators to perform deep packet inspection (DPI) and traffic shaping, potentially impacting network visibility and control. Additionally, encrypted traffic introduces overhead due to encryption and decryption processes, affecting TCP's throughput and latency. Addressing these challenges requires developing efficient techniques for managing encrypted traffic, such as optimizing TLS handshake protocols and integrating encryption-aware congestion control mechanisms into TCP variants.

Furthermore, TCP's congestion control algorithms face challenges in dynamic and heterogeneous network environments. TCP's traditional congestion control mechanisms may not adapt optimally to varying network conditions, leading to suboptimal performance or unfairness in bandwidth allocation [190], [191]. Addressing these challenges requires developing adaptive congestion control algorithms that can dynamically adjust to changes in network congestion, link characteristics, and traffic patterns. Solutions such as TCP CUBIC and TCP BBR incorporate adaptive congestion control mechanisms to improve TCP's responsiveness and fairness in dynamic network environments.

Another significant challenge in TCP is the robustness and resilience of TCP implementations against security threats and attacks. TCP variants are susceptible to various types of attacks, including SYN flooding, session hijacking [192], and TCP injection attacks. Moreover, TCP's lack of built-in authentication and encryption makes it vulnerable to man-in-the-middle attacks and data interception [193]. To address these challenges, TCP implementations must incorporate robust security features such as encryption, authentication, and integrity protection. Additionally, network administrators should deploy intrusion detection and prevention systems (IDS/IPS) to detect and mitigate TCP-based attacks in real-time.

Moreover, TCP faces challenges in supporting emerging applications and technologies, such as Internet of Things (IoT) devices, real-time communication, and multimedia streaming. Traditional TCP variants may not be well-suited for these applications due to their stringent latency and reliability requirements [194]. Addressing these challenges requires developing specialized TCP variants or protocols tailored to the unique characteristics of emerging applications. For example, TCP variants optimized for IoT devices may prioritize energy efficiency and low latency, while those designed for multimedia streaming may prioritize throughput and loss recovery mechanisms.

Another open challenge in TCP is the efficient utilization of network resources in data center environments. Data center networks often exhibit unique characteristics, such as high link speeds, low latency, and dense traffic patterns. Traditional TCP variants may not fully utilize available bandwidth or adapt optimally to dynamic traffic conditions in data center networks [195]. To address these challenges, researchers are developing specialized TCP variants, such as Data Center TCP (DCTCP) and TCP Vegas, which are designed to optimize performance and fairness in data center environments by incorporating congestion control mechanisms tailored to data center traffic patterns.

Furthermore, TCP faces challenges in supporting mobile and wireless networks, where link characteristics are dynamic and unpredictable. Traditional TCP variants may not adapt optimally to wireless network conditions, leading to performance degradation and inefficient resource utilization [196]. Addressing these challenges requires developing TCP variants or protocols specifically designed for mobile and wireless networks. Solutions such as TCP Westwood and TCP New Reno-Mod optimize TCP's performance over wireless networks by incorporating adaptive congestion control mechanisms and error recovery strategies tailored to wireless link characteristics.

Additionally, TCP's performance over satellite networks presents unique challenges due to long propagation delays and high error rates. Traditional TCP variants may not perform well over satellite links, leading to poor throughput and high latency [197]. Addressing these challenges requires developing specialized TCP variants or protocols optimized for

satellite communication. Solutions such as TCP New Reno-Mod and TCP Vegas adapt TCP's congestion control and error recovery mechanisms to satellite link characteristics, improving TCP's performance and efficiency over satellite networks.

Moreover, TCP's performance in asymmetric network environments, where upload and download speeds differ significantly, presents challenges for achieving fairness and efficiency. Traditional TCP variants may not allocate bandwidth fairly between upload and download traffic, leading to suboptimal performance and inefficient resource utilization [198], [199]. Addressing these challenges requires developing TCP variants or protocols that can dynamically adjust to asymmetric network conditions and allocate bandwidth fairly between upload and download traffic. Solutions such as TCP CUBIC and TCP BBR incorporate adaptive congestion control mechanisms to achieve fairness and efficiency in asymmetric network environments.

Finally, TCP's support for multipath communication presents challenges for achieving optimal throughput and reliability. Traditional TCP variants may not effectively utilize multiple network paths or adapt optimally to changing network conditions in multipath environments. Addressing these challenges requires developing TCP variants or protocols specifically designed for multipath communication [200], [201]. Solutions such as Multipath TCP (MPTCP) enable TCP connections to utilize multiple network paths simultaneously, improving throughput and reliability in multipath environments. Additionally, TCP variants optimized for multipath communication incorporate adaptive congestion control mechanisms and error recovery strategies tailored to multipath network conditions.

4. Conclusion

This survey of Transmission Control Protocol (TCP) variants underscores the dynamic nature of network protocols in adapting to evolving networking requirements and challenges. Through a comprehensive examination of diverse TCP variants such as Reno, New Reno, Vegas, FACK, and RBP, it becomes evident that each variant offers unique approaches to congestion control, error recovery, and bandwidth utilization. While traditional variants like Reno and New Reno focus on reactive congestion control mechanisms, newer variants like Vegas and RBP introduce proactive strategies to optimize network performance. Furthermore, variants like FACK enhance TCP's reliability by accurately identifying and recovering from packet losses within a window. Overall, this survey highlights the importance of understanding the intricacies and trade-offs of different TCP variants to effectively design and manage modern network infrastructures.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that she has no any competing interests.

References

[1] Wang G, Ren Y, Li J. An effective approach to alleviating the challenges of transmission control protocol. Iet Communications. 2014 Apr;8(6):860-9.

[2] Liu H. 2024 World Scientific Publishing Company. Practical Guide On Security And Privacy In Cyber-physical Systems, A: Foundations, Applications And Limitations. 2023 Sep 21;3:25.

[3] Bansal P, Agrawal K, Gupta A. Performance Evaluation of Various Transmission Control Protocols in NS2. Computational Network Application Tools for Performance Management. 2020:167-79.

[4] Lim C. Improving congestion control of TCP for constrained IoT networks. Sensors. 2020 Aug 24;20(17):4774.

[5] Abubakar A, Yusof ZM. Streams of Data Flow in Transmission Control Protocol (TCP) Request-Response Cycle Efficiency. International Journal on Perceptive and Cognitive Computing. 2024 Jan 28;10(1):79-89.

[6] 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.

[7] Sella Veluswami JR, Chinnusamy K, Kumar K, Klinge VC, Mohankumar S. Improvement of transmission control protocol for high bandwidth applications. Wireless Personal Communications. 2021 Apr;117:3359-79.

[8] Sung GM, Lee CT, Yan ZY, Yu CP. Ethernet packet to usb data transfer bridge asic with modbus transmission control protocol based on fpga development kit. Electronics. 2022 Oct 11;11(20):3269.

[9] Molia HK, Kothari AD. Fuzzy Logic Systems for Transmission Control Protocol. InInternational Conference on Communication, Devices and Computing 2019 Mar 14 (pp. 553-565). Singapore: Springer Nature Singapore.

[10] Amezcua Valdovinos I, Perez Diaz JA, Garcia Villalba LJ, Kim TH. BATCP: Bandwidth-aggregation transmission control protocol. Symmetry. 2017 Aug 21;9(8):167.

[11] Abdullah S. Enhancing the TCP Newreno Fast RecoveryAlgorithm on 5G Networks. Journal of Computing and Communication. 2024 Jan 31;3(1):33-43.

[12] 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.

[13] Abolfazli E, Shah-Mansouri V. Dynamic adjustment of queue levels in TCP Vegas-based networks. Electronics Letters. 2016 Mar;52(5):361-3.

[14] Ceco A, Mrdovic S. Possible Improvements of TCP Protocol with the Use of Heuristic Methods. Tehnički vjesnik. 2024;31(1):303-15.

[15] Ramos D, Esparza O, Mata-Díaz J, Alins J. Evaluation of TCP Congestion Control Algorithms with traffic control policies in a PEP-based geosynchronous satellite scenario. Computer Networks. 2024 Feb 1;239:110131.

[16] Shenoy SU, Kumari M S, Shenoy UK. Comparative analysis of TCP Variants for video transmission over multi-hop mobile Ad hoc networks. InInternational Conference on Computer Networks and Communication Technologies: ICCNCT 2018 2019 (pp. 371-381). Springer Singapore.

[17] Kiruthiga R, Nithya B. Dynamic Retransmission Count Prediction (DRCP) Algorithm for FANET Using Machine Learning Techniques. InInternational Conference on Advances in Data-driven Computing and Intelligent Systems 2023 Sep 21 (pp. 473-486). Singapore: Springer Nature Singapore.

[18] 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).

[19] Kumar A, Hemrajani N. Congestion Avoidance in TCP Based on Optimized Random Forest with Improved Random Early Detection Algorithm. International Journal of Image and Graphics. 2024 Feb 5:2550055.

[20] Goyal MK, Verma YK, Bassi P, Misra PK. Performance evaluation of TCP congestion control variants using Dynamic State Routing in wireless AD-HOC network. InProceedings of the Third International Conference on Trends in Information, Telecommunication and Computing 2013 (pp. 445-449). Springer New York.

[21] Dhawane PG, Navghare P, Manjre B, Dhule P, Fale P, Kahile M. Wireless TCP Congestion Control Based on Loss Discrimination Approach Using Machine Learning. InInternational Conference on Communications and Cyber Physical Engineering 2018 2024 Feb 5 (pp. 343-349). Singapore: Springer Nature Singapore.

[22] Bisoy SK, Pattnaik PK. Throughput of a network shared by TCP reno and TCP vegas in static multi-hop wireless network. InComputational Intelligence in Data Mining—Volume 1: Proceedings of the International Conference on CIDM, 5-6 December 2015 2016 (pp. 471-481). Springer India.

[23] Rajasekaran S, Narang S, Zabreyko AA, Ghobadi M. MLTCP: Congestion Control for DNN Training. arXiv preprint arXiv:2402.09589. 2024 Feb 14.

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

[25] Ramos D, Esparza O, Mata-Díaz J, Alins J. Evaluation of TCP Congestion Control Algorithms with traffic control policies in a PEP-based geosynchronous satellite scenario. Computer Networks. 2024 Feb 1;239:110131.

[26] Dogar AB, Ullah S, Zhang Y, Alasmary H, Waqas M, Chen S. Resilient TCP variant enabling smooth network updates for software defined data center networks. Tsinghua Science and Technology. 2024 Jan 9.

[27] Shenoy SU, Shenoy UK, Kumari MS. Performance Analysis of Modified TCP New Reno for MANETs. InRecent Advances in Artificial Intelligence and Data Engineering: Select Proceedings of AIDE 2020 2022 (pp. 85-96). Springer Singapore.

[28] Iovlev D, Korikov A. TCP-NEWRENO protocol modification for MANET networks. InInformation Technologies and Mathematical Modelling-Queueing Theory and Applications: 15th International Scientific Conference, ITMM 2016, named after AF Terpugov, Katun, Russia, September 12-16, 2016. Proceedings 15 2016 (pp. 120-131). Springer International Publishing.

[29] Pavani KR, Sreenath N. Performance Evaluation of TCP NewVegas and TCP Newreno on Burstification in an OBS Network. InComputer Networks & Communications (NetCom) Proceedings of the Fourth International Conference on Networks & Communications 2013 (pp. 185-194). Springer New York.

[30] 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.

[31] Liao X, Tian H, Zeng C, Wan X, Chen K. Towards Fair and Efficient Learning-based Congestion Control. arXiv preprint arXiv:2403.01798. 2024 Mar 4.

[32] Sood R, Kang SS. Hybrid Congestion Control Mechanism in Software Defined Networks. International Journal of Intelligent Systems and Applications in Engineering. 2024;12(6s):686-76.

[33] Liu Z, Jiang Y. Design and implementation for a UAV-based streaming media system. Ad Hoc Networks. 2024 Feb 12:103443.

[34] Pi Y, Jamin S, Wei Y. Measuring congestion-induced performance imbalance in Internet load balancing at scale. Computer Networks. 2024 Feb 1;240:110189.

[35] Poorzare R, Calveras A, Abedidarabad S. An improvement over TCP Vegas to enhance its performance in optical burst switching networks. Optical Review. 2021 Apr;28:215-26.

[36] 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).

[37] Wang Z, Feng X, Li Q, Sun K, Yang Y, Li M, Xu K. Off-Path TCP Hijacking in Wi-Fi Networks: A Packet-Size Side Channel Attack. arXiv preprint arXiv:2402.12716. 2024 Feb 20.

[38] Dunaytsev R, Moltchanov D, Koucheryavy Y, Harju J. Modeling TCP SACK performance over wireless channels with completely reliable ARQ/FEC. International Journal of Communication Systems. 2011 Dec;24(12):1533-64.

[39] Kamboj R, Singh G. Various TCP options for congestion evasion. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2015 Apr;4(4):1534-9.

[40] Zhang K, Fu CP. An enhancement of TCP Veno with forward acknowledgement. Computer communications. 2008 Sep 25;31(15):3683-90.

[41] Gital AY, Ismail AS, Chiroma H, Abubakar AI, Abdulhamid BM, Maitama IZ, Zeki A. Performance analysis of cloud-based cve communication architecture in comparison with the traditional client server, p2p and hybrid models. InThe 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M) 2014 Nov 17 (pp. 1-6). IEEE.

[42] Abed GA, Ismail M, Jumari K. Exploration and evaluation of traditional TCP congestion control techniques. Journal of King Saud University-Computer and Information Sciences. 2012 Jul 1;24(2):145-55.

[43] 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.

[44] Bazi K, Nassereddine B. Efficient Congestion Management for Sustainable Wireless Mesh Networks. InEmerging Trends in ICT for Sustainable Development: The Proceedings of NICE2020 International Conference 2021 (pp. 297-305). Springer International Publishing.

[45] Jahan R, Suman P. Reliable and Fast Data Transmission Mechanism for Congested Wireless Sensor Network. InProceeding of International Conference on Intelligent Communication, Control and Devices: ICICCD 2016 2017 (pp. 173-179). Springer Singapore.

[46] Fetoh H, Amin KM, Hamad AM. Packets distribution over asymmetric paths using concurrent multipath transfer. IET Networks. 2024.

[47] Kodama S, Shimamura M, Iida K. Initial CWND determination method for fast startup TCP algorithms. In2011 IEEE Nineteenth IEEE International Workshop on Quality of Service 2011 Jun 6 (pp. 1-3). IEEE.

[48] Kaur H, Singh G. Measuring Performance of Variants of TCP Congestion Control Protocols. Indian J. Comput. Sci. Eng. 2017;8(3):285-96.

[49] Ke J, Williamson C. Towards a Rate-based TCP Protocol for the Web. InProceedings 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (Cat. No. PR00728) 2000 Aug 29 (pp. 36-45). IEEE.

[50] 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.

[51] Al-Jubari AM, Othman M, Mohd Ali B, Abdul Hamid NA. TCP performance in multi-hop wireless ad hoc networks: challenges and solution. EURASIP Journal on Wireless Communications and Networking. 2011 Dec;2011:1-25.

[52] Abed GA, Ismail M, Jumari K. A comparison and analysis of congestion window for HS-TCP, Full-TCP, and TCP-Linux in long term evolution system model. In2011 IEEE Conference on Open Systems 2011 Sep 25 (pp. 358-362). IEEE.

[53] Dollas A, Ermis I, Koidis I, Zisis I, Kachris C. An open tcp/ip core for reconfigurable logic. In13th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'05) 2005 Apr 18 (pp. 297-298). IEEE.

[54] Kim HY, Rixner S. TCP offload through connection handoff. InProceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems 2006 2006 Apr 18 (pp. 279-290).

[55] Kumar S, Andersen MP, Kim HS, Culler DE. TCPlp: System design and analysis of full-scale TCP in low-power networks. arXiv preprint arXiv:1811.02721. 2018.

[56] 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.

[57] Bruhn P, Kuehlewind M, Muehleisen M. Performance and improvements of TCP CUBIC in low-delay cellular networks. Computer Networks. 2023 Apr 1;224:109609.

[58] Lee JY, Kim BC, Kwon Y, Han K. Coupled CUBIC Congestion Control for MPTCP in Broadband Networks. Computer Systems Science & Engineering. 2023 Apr 1;45(1).

[59] Aykurt K, Zerwas J, Blenk A, Kellerer W. When TCP Meets Reconfigurations: A Comprehensive Measurement Study. IEEE Transactions on Network and Service Management. 2023 Oct 25.

[60] Havinal R, Attimarad GV, Prasad MG. Easr: Graph-based framework for energy efficient smart routing in manet using availability zones. International Journal of Electrical and Computer Engineering (IJECE). 2015 Dec;5(6):1381-95.

[61] Krishnappa PK, Babu BP. Investigating open issues in swarm intelligence for mitigating security threats in MANET. International Journal of Electrical and Computer Engineering. 2015 Oct 1;5(5).

[62] Sisodia DS, Singhal R, Khandal V. A performance review of intra and inter-group MANET routing protocols under varying speed of nodes. International Journal of Electrical and Computer Engineering (IJECE). 2017 Oct 1;7(5):2721-30.

[63] 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.

[64] Tsiknas K, Stamatelos G. TCP-BIAD for enhancing TCP performance in broadband wireless access networks. Wireless personal communications. 2014 Sep;78:785-99.

[65] Tsiknas K, Rantos K, Schinas CJ, Soilemes A. Performance evaluation of TCP-BIAD in high-speed, long-distance networks. Computing. 2019 Apr 12;101:319-37.

[66] Amponis G, Lagkas T, Tsiknas K, Radoglou-Grammatikis P, Sarigiannidis P. Introducing a New TCP Variant for UAV networks following comparative simulations. Simulation Modelling Practice and Theory. 2023 Feb 1;123:102708.

[67] Singh UK, Sharma A, Singh SK, Tomar PS, Dixit K, Upreti K. Security and privacy aspect of cyber physical systems. InCyber Physical Systems 2023 Jan 11 (pp. 141-164). Chapman and Hall/CRC.

[68] Abubakar A, Najmuddin NM, Alwi RA, Faizal NA. Examining Potential Threats of Eavesdropping in TCP Stream of Personal Interactive Transmission Session. International Journal on Perceptive and Cognitive Computing. 2024 Jan 28;10(1):98-104.

[69] 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.

[70] 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.

[71] Dikshit P, Sengupta J, Bajpai V. Recent trends on privacy-preserving technologies under standardization at the IETF. ACM SIGCOMM Computer Communication Review. 2023 Jul 19;53(2):22-30.

[72] Hutchinson S, Stanković M, Ho S, Houshmand S, Karabiyik U. Investigating the privacy and security of the SimpliSafe security system on android and iOS. Journal of Cybersecurity and Privacy. 2023 Apr 7;3(2):145-65.

[73] 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.

[74] Mao B, Liu J, Wu Y, Kato N. Security and privacy on 6g network edge: A survey. IEEE communications surveys & tutorials. 2023 Feb 14.

[75] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[76] Korba AA, Boualouache A, Brik B, Rahal R, Ghamri-Doudane Y, Senouci SM. Federated learning for zero-day attack detection in 5g and beyond v2x networks. InICC 2023-IEEE International Conference on Communications 2023 May 28 (pp. 1137-1142). IEEE.

[77] Semantha FH, Azam S, Shanmugam B, Yeo KC. PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management. Journal of Sensor and Actuator Networks. 2023 Apr 13;12(2):36.

[78] Amponis G, Radoglou-Grammatikis P, Nakas G, Goudos S, Argyriou V, Lagkas T, Sarigiannidis P. 5G core PFCP intrusion detection dataset. In2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST) 2023 Jun 28 (pp. 1-4). IEEE.

[79] Latif RM, Jamil M, He J, Farhan M. A Novel Authentication and Communication Protocol for Urban Traffic Monitoring in VANETs Based on Cluster Management. Systems. 2023 Jul;11(7):322.

[80] 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.

[81] Kaushal N, Singh G, Singh J. An addressing techniques for maintaining security and privacy framework for internet of things. In2023 3rd International Conference on Intelligent Technologies (CONIT) 2023 Jun 23 (pp. 1-7). IEEE.

[82] Hadi HJ, Cao Y, Nisa KU, Jamil AM, Ni Q. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. Journal of Network and Computer Applications. 2023 Apr 1;213:103607.

[83] Wang C, Yuan Z, Zhou P, Xu Z, Li R, Wu DO. The Security and Privacy of Mobile Edge Computing: An Artificial Intelligence Perspective. IEEE Internet of Things Journal. 2023 Aug 11.

[84] Alabdulatif A, Thilakarathne NN, Kalinaki K. A Novel Cloud Enabled Access Control Model for Preserving the Security and Privacy of Medical Big Data. Electronics. 2023 Jun 13;12(12):2646.

[85] 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.

[86] Salam A, Ullah F, Amin F, Abrar M. Deep learning techniques for web-based attack detection in industry 5.0: A novel approach. Technologies. 2023 Aug 8;11(4):107.

[87] Jingfu LI. A QoS-aware Mechanism for Reducing TCP Retransmission Timeouts using Network Tomography. International Journal of Advanced Computer Science and Applications. 2023;14(9).

[88] Khan K. User-Centric Algorithms: Sculpting the Future of Adaptive Video Streaming. International Transactions on Electrical Engineering and Computer Science. 2023 Dec 30;2(4):155-62.

[89] Laštovička M, Husák M, Velan P, Jirsík T, Čeleda P. Passive operating system fingerprinting revisited: Evaluation and current challenges. Computer Networks. 2023 Jun 1;229:109782.

[90] 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.

[91] Muzammil MB, Bilal M, Ajmal S, Shongwe SC, Ghadi YY. Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking. IEEE Access. 2024 Jan 5.

[92] Pan Y, Rossow C. TCP Spoofing: Reliable Payload Transmission Past the Spoofed TCP Handshake. In2024 IEEE Symposium on Security and Privacy (SP) 2024 Feb 1 (pp. 179-179). IEEE Computer Society.

[93] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

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

[95] Pour MS, Nader C, Friday K, Bou-Harb E. A comprehensive survey of recent internet measurement techniques for cyber security. Computers & Security. 2023 May 1;128:103123.

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

[97] Craven R, Beverly R, Allman M. A middlebox-cooperative TCP for a non end-to-end Internet. ACM SIGCOMM Computer Communication Review. 2014 Aug 17;44(4):151-62.

[98] Dahiya Y, Sangwan MS. Developing and Enhancing the Security of Digital Evidence Bag. International Journal of Research Studies in Computer Science and Engineering (IJRSCSE). 2014 Jun;1(2):14-25.

[99] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[100] Paliwal G, Mudgal AP, Taterh S. A study on various attacks of tcp/ip and security challenges in manet layer architecture. InProceedings of Fourth International Conference on Soft Computing for Problem Solving: SocProS 2014, Volume 2 2015 (pp. 195-207). Springer India.

[101] Popat K, Kapadia VV. Multipath TCP security issues, challenges and solutions. InInformation, Communication and Computing Technology: 6th International Conference, ICICCT 2021, New Delhi, India, May 8, 2021, Revised Selected Papers 6 2021 (pp. 18-32). Springer International Publishing.

[102] Shang W, Yu Y, Droms R, Zhang L. Challenges in IoT networking via TCP/IP architecture. NDN Project. 2016 Feb 10;2.

[103] Volkova A, Niedermeier M, Basmadjian R, de Meer H. Security challenges in control network protocols: A survey. IEEE Communications Surveys & Tutorials. 2018 Sep 26;21(1):619-39.

[104] 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.

[105] Pearce C, Zeadally S. Ancillary impacts of multipath TCP on current and future network security. IEEE Internet Computing. 2015 Jul 13;19(5):58-65.

[106] Cao Y, Qian Z, Wang Z, Dao T, Krishnamurthy SV, Marvel LM. Off-path TCP exploits of the challenge ACK global rate limit. IEEE/ACM Transactions on Networking. 2018 Feb 2;26(2):765-78.

[107] Zhang Y. A multilayer IP security protocol for TCP performance enhancement in wireless networks. IEEE Journal on selected areas in communications. 2004 May 4;22(4):767-76.

[108] 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.

[109] Ali I, Sabir S, Ullah Z. Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309. 2019 Jan 9.

[110] Pereira PP, Eliasson J, Delsing J. An authentication and access control framework for CoAP-based Internet of Things. InIECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society 2014 Oct 29 (pp. 5293-5299). IEEE.

[111] Kahani N, Elgazzar K, Cordy JR. Authentication and access control in e-health systems in the cloud. In2016 IEEE 2nd international conference on big data security on cloud (BigDataSecurity), IEEE international conference on high performance and smart computing (HPSC), and IEEE international conference on intelligent data and security (IDS) 2016 Apr 9 (pp. 13-23). IEEE.

[112] Patel S, Patel DR, Navik AP. Energy efficient integrated authentication and access control mechanisms for Internet of Things. In2016 International Conference on Internet of Things and Applications (IOTA) 2016 Jan 22 (pp. 304-309). IEEE.

[113] El Sibai R, Gemayel N, Bou Abdo J, Demerjian J. A survey on access control mechanisms for cloud computing. Transactions on Emerging Telecommunications Technologies. 2020 Feb;31(2):e3720.

[114] 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.

[115] Möller DP. Intrusion detection and prevention. InGuide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 131-179). Cham: Springer Nature Switzerland.

[116] Garbis J, Chapman JW, Garbis J, Chapman JW. Intrusion Detection and Prevention Systems. Zero Trust Security: An Enterprise Guide. 2021:117-26.

[117] West M. Preventing system intrusions. InNetwork and System Security 2014 Jan 1 (pp. 29-56). Syngress.

[118] Kizza JM. System intrusion detection and prevention. InGuide to computer network security 2024 Jan 20 (pp. 295-323). Cham: Springer international publishing.

[119] Jero S, Hoque ME, Choffnes DR, Mislove A, Nita-Rotaru C. Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach. InNDSS 2018 Jul 16.

[120] 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.

[121] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems. 2020 Sep 1;77:103201.

[122] Prabhu S. Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic–A Review of Literature. Sangeetha Prabhu, & Subramanya Bhat.(2020). Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic–A Review of Literature. International journal of case studies in business, IT, and education (IJCSBE). 2020 Aug 11;4(2):40-64.

[123] Rupprecht D, Kohls K, Holz T, Pöpper C. IMP4GT: IMPersonation Attacks in 4G NeTworks. InNDSS 2020 Feb.

[124] Gilad Y, Herzberg A, Shulman H. Off-path hacking: The illusion of challenge-response authentication. IEEE Security & Privacy. 2013 Oct 10;12(5):68-77.

[125] 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.

[126] Yoo S, Chen X, Rexford J. SmartCookie: Blocking Large-Scale SYN Floods with a Split-Proxy Defense on Programmable Data Planes. InUSENIX Security 2024.

[127] Bensaid R, Labraoui N, Abba Ari AA, Maglaras L, Saidi H, Abdu Lwahhab AM, Benfriha S. Toward a real-time tcp syn flood ddos mitigation using adaptive neuro-fuzzy classifier and sdn assistance in fog computing. Security and Communication Networks. 2023 Nov 27;2024.

[128] Zamrai MA, Yusof KM, Azizan A. Dissecting Denial of Service (DoS) Syn Flood Attack Dynamics and Impacts in Vehicular Communication Systems. InITM Web of Conferences 2024 (Vol. 63, p. 01008). EDP Sciences.

[129] Dang VT, Huong TT, Thanh NH, Nam PN, Thanh NN, Marshall A. Sdn-based syn proxy—a solution to enhance performance of attack mitigation under tcp syn flood. The Computer Journal. 2019 Apr 1;62(4):518-34.

[130] Shirsath VA, Chandane MM, Lal C, Conti M. SYNTROPY: TCP SYN DDoS attack detection for software defined network based on Rényi entropy. Computer Networks. 2024 Mar 12:110327.

[131] 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.

[132] Tyagi V, Saraswat A, Bansal S. An Analysis of Securing Internet of Things (IoT) Devices from Man-in-the-Middle (MIMA) and Denial of Service (DoS). InSmart Cities 2023 Nov 30 (pp. 337-357). CRC Press.

[133] Al-Abadi AA, Mohamed MB, Fakhfakh A. Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks. Computers. 2023 Dec 17;12(12):262.

[134] 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.

[135] Bruschi D, Di Pasquale A, Lanzi A, Pagani E. Ensuring cybersecurity for industrial networks: A solution for ARP-based MITM attacks. Journal of Computer Security. 2024(Preprint):1-29.

[136] Martins T, Oliveira SV. Enhanced Modbus/TCP security protocol: Authentication and authorization functions supported. Sensors. 2022 Oct 20;22(20):8024.

[137] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[138] Vajrobol V, Gupta BB, Gaurav A, Chuang HM. Adversarial learning for Mirai botnet detection based on Long Short-Term Memory and XGBoost. International Journal of Cognitive Computing in Engineering. 2024 Mar 3.

[139] Wang W, Yi P, Jiang J, Zhang P, Chen X. Transformer-based framework for alert aggregation and attack prediction in a multi-stage attack. Computers & Security. 2024 Jan 1;136:103533.

[140] Parmar A, Lamkuche H. Distributed Denial of Service Attack Detection Using Sequence-To-Sequence LSTM. InThe International Conference On Global Economic Revolutions 2023 Feb 27 (pp. 39-53). Cham: Springer Nature Switzerland.

[141] Harris B, Hunt R. TCP/IP security threats and attack methods. Computer communications. 1999 Jun 25;22(10):885-97.

[142] Bitit R, Derhab A, Guerroumi M, Khan FA. DDoS attack forecasting based on online multiple change points detection and time series analysis. Multimedia Tools and Applications. 2023 Nov 23:1-31.

[143] 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.

[144] Gondim JJ, Albuquerque RD. Reflector Saturation in Amplified Reflection Denial of Service Attack Abusing CLDAP and Memcache Protocols. InInternational Conference on Advanced Research in Technologies, Information, Innovation and Sustainability 2023 Oct 18 (pp. 248-263). Cham: Springer Nature Switzerland.

[145] Nawrocki M, Kristoff J, Hiesgen R, Kanich C, Schmidt TC, Wählisch M. SoK: A Data-driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots. In2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P) 2023 Jul 3 (pp. 576-591). IEEE.

[146] Gondim JJ, de Oliveira Albuquerque R, Orozco AL. Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols. Future Generation Computer Systems. 2020 Jul 1;108:68-81.

[147] Fachkha C, Bou-Harb E, Debbabi M. Inferring distributed reflection denial of service attacks from darknet. Computer Communications. 2015 May 15;62:59-71.

[148] Liu B, Li J, Wei T, Berg S, Ye J, Li C, Zhang C, Zhang J, Han X. SF-DRDoS: The store-and-flood distributed reflective denial of service attack. Computer communications. 2015 Sep 15;69:107-15.

[149] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[150] Huang YF, Chang SW, Lin CB, Chen CJ, Li SJ, Chen CM. An Improved Light Weight Countermeasure Scheme to Efficiently Mitigate TCP Attacks in SDN. InInternational Computer Symposium 2022 Dec 15 (pp. 501-511). Singapore: Springer Nature Singapore.

[151] Rahman A, Mustafa G, Khan AQ, Abid M, Durad MH. Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms. International Journal of Critical Infrastructure Protection. 2022 Dec 1;39:100568.

[152] Raj SA, Amritha PP, Sethumadhavan, Seshadhri S. Hybrid Intrusion Detection System for Industrial Control System. InWorld Conference on Information Systems for Business Management 2023 Sep 7 (pp. 573-583). Singapore: Springer Nature Singapore.

[153] Wang YC, Zhang GL, Zhang YL. Analysis of SQL Injection Based on Petri Net in Wireless Network. Journal of Information Science & Engineering. 2023 Jan 1;39(1).

[154] Alarfaj FK, Khan NA. Enhancing the performance of SQL injection attack detection through probabilistic neural networks. Applied Sciences. 2023 Mar 29;13(7):4365.

[155] 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.

[156] Alyami M, Alghamdi A, Alkhowaiter MA, Zou C, Solihin Y. Random Segmentation: New Traffic Obfuscation against Packet-Size-Based Side-Channel Attacks. Electronics. 2023 Sep 9;12(18):3816.

[157] Sudar KM, Deepalakshmi P, Singh A, Srinivasu PN. TFAD: TCP flooding attack detection in software-defined networking using proxy-based and machine learning-based mechanisms. Cluster Computing. 2023 Apr;26(2):1461-77.

[158] Zhang H, Min Y, Liu S, Tong H, Li Y, Lv Z. Improve the Security of Industrial Control System: A Fine-Grained Classification Method for DoS Attacks on Modbus/TCP. Mobile Networks and Applications. 2023 Apr;28(2):839-52.

[159] Jajula SK, Tripathi K, Bajaj SB. Review of Detection of Packets Inspection and Attacks in Network Security. InEmerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 1 2022 Sep 29 (pp. 597-604). Singapore: Springer Nature Singapore.

[160] Li S, Shi S, Xiao Y, Zhang C, Hou YT, Lou W. Bijack: Breaking Bitcoin Network with TCP Vulnerabilities. InEuropean Symposium on Research in Computer Security 2023 Sep 25 (pp. 306-326). Cham: Springer Nature Switzerland.

[161] Kowalski M, Mazurczyk W. Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. Computer Networks. 2023 Apr 23:109778.

[162] 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).

[163] Tripathi N. Delays have dangerous ends: Slow http/2 dos attacks into the wild and their real-time detection using event sequence analysis. IEEE Transactions on Dependable and Secure Computing. 2023 May 15.

[164] Gierlings M, Brinkmann M, Schwenk J. Isolated and exhausted: attacking operating systems via site isolation in the browser. In32nd USENIX Security Symposium (USENIX Security 23) 2023 (pp. 7037-7054).

[165] Boger AM, Sokolov AN. Detection of Vulnerabilities in the Perimeter of the ICS Network Infrastructure Using TCP/IP Protocols. In2023 International Russian Automation Conference (RusAutoCon) 2023 Sep 10 (pp. 703-708). IEEE.

[166] Zografopoulos I, Hatziargyriou ND, Konstantinou C. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Systems Journal. 2023 Sep 1.

[167] Hwang WS, Shon JG, Park JS. Web session hijacking defense technique using user information. Human-centric Computing and Information Sciences. 2022 Apr 15;12.

[168] 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.

[169] Almuflih AS, Popat K, Kapdia VV, Qureshi MR, Almakayeel N, Mamlook RE. Efficient key exchange using identity-based encryption in multipath TCP environment. Applied Sciences. 2022 Jul 27;12(15):7575.

[170] Cheng Z, Sun D, Wang L, Lv Q, Wang Y. MMSP: A LSTM Based Framework for Multi-Step Attack Prediction in Mixed Scenarios. In2022 IEEE Symposium on Computers and Communications (ISCC) 2022 Jun 30 (pp. 1-6). IEEE.

[171] Mihoub A, Fredj OB, Cheikhrouhou O, Derhab A, Krichen M. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering. 2022 Mar 1;98:107716.

[172] Saurabh K, Sood S, Kumar PA, Singh U, Vyas R, Vyas OP, Khondoker R. Lbdmids: LSTM based deep learning model for intrusion detection systems for IOT networks. In2022 IEEE World AI IoT Congress (AIIoT) 2022 Jun 6 (pp. 753-759). IEEE.

[173] Abou El Houda Z, Brik B, Senouci SM. A novel iot-based explainable deep learning framework for intrusion detection systems. IEEE Internet of Things Magazine. 2022 Jun;5(2):20-3.

[174] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[175] Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. IEEE communications surveys & tutorials. 2016 Mar 29;18(3):2027-51.

[176] Pingle B, Mairaj A, Javaid AY. Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use. In2018 IEEE International Conference on Electro/Information Technology (EIT) 2018 May 3 (pp. 0192-0197). IEEE.

[177] Luckie M, Beverly R, Wu T, Allman M, claffy K. Resilience of deployed TCP to blind attacks. InProceedings of the 2015 Internet Measurement Conference 2015 Oct 28 (pp. 13-26).

[178] Schuba CL, Krsul IV, Kuhn MG, Spafford EH, Sundaram A, Zamboni D. Analysis of a denial of service attack on TCP. InProceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097) 1997 May 4 (pp. 208-223). IEEE.

[179] Siwakoti YR, Bhurtel M, Rawat DB, Oest A, Johnson RC. Advances in IOT security: Vulnerabilities, enabled Criminal Services, attacks and countermeasures. IEEE Internet of Things Journal. 2023 Mar 6.

[180] 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.

[181] Neto EC, Dadkhah S, Ferreira R, Zohourian A, Lu R, Ghorbani AA. CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors. 2023 Jun 26;23(13):5941.

[182] Vedula V, Lama P, Boppana RV, Trejo LA. On the detection of low-rate denial of service attacks at transport and application layers. Electronics. 2021 Aug 30;10(17):2105.

[183] Alamleh H. Counter-surveillance Technique by Diversifying Transmission Links. In2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) 2023 Mar 8 (pp. 1046-1050). IEEE.

[184] Court A, Alamleh H. Multi-path Data Transmission to Protect Data in Transit. In2023 IEEE International Conference on Consumer Electronics (ICCE) 2023 Jan 6 (pp. 1-6). IEEE.

[185] Kuo EC, Chang MS, Kao DY. User-side evil twin attack detection using time-delay statistics of TCP connection termination. In2018 20th International Conference on Advanced Communication Technology (ICACT) 2018 Feb 11 (pp. 211-216). IEEE.

[186] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[187] Lee C, Jung J, Chung JM. DEFT: Multipath TCP for high speed low latency communications in 5G networks. IEEE Transactions on Mobile Computing. 2020 Jun 4;20(12):3311-23.

[188] Peralta G, Cid-Fuentes RG, Bilbao J, Crespo PM. Homomorphic encryption and network coding in iot architectures: Advantages and future challenges. Electronics. 2019 Jul 25;8(8):827.

[189] Liang C, Zhang Q, Ma J, Li K. Research on neural network chaotic encryption algorithm in wireless network security communication. EURASIP Journal on Wireless Communications and Networking. 2019 Jun 6;2019(1):151.

[190] Lorincz J, Klarin Z, Ožegović J. A comprehensive overview of TCP congestion control in 5G networks: Research challenges and future perspectives. Sensors. 2021 Jun 30;21(13):4510.

[191] Li W, Zhou F, Chowdhury KR, Meleis W. QTCP: Adaptive congestion control with reinforcement learning. IEEE Transactions on Network Science and Engineering. 2018 May 11;6(3):445-58.

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

[193] Alqahtani AH, Iftikhar M. TCP/IP attacks, defenses and security tools. International Journal of Science and Modern Engineering (IJISME). 2013 Sep;1(10):42-7.

[194] Said O, Albagory Y, Nofal M, Al Raddady F. IoT-RTP and IoT-RTCP: Adaptive protocols for multimedia transmission over internet of things environments. IEEE access. 2017 Jul 28;5:16757-73.

[195] Raiciu C, Barre S, Pluntke C, Greenhalgh A, Wischik D, Handley M. Improving datacenter performance and robustness with multipath TCP. ACM SIGCOMM Computer Communication Review. 2011 Aug 15;41(4):266-77.

[196] Poorzare R, Augé AC. Challenges on the way of implementing TCP over 5G networks. IEEE access. 2020 Sep 24;8:176393-415.

[197] Zhu J, Roy S, Kim JH. Performance modelling of TCP enhancements in terrestrial–satellite hybrid networks. IEEE/ACM Transactions on Networking. 2006 Aug 21;14(4):753-66.

[198] Siddiqi SJ, Naeem F, Khan S, Khan KS, Tariq M. Towards AI-enabled traffic management in multipath TCP: A survey. Computer Communications. 2022 Jan 1;181:412-27.

[199] Abdelsalam A, Luglio M, Patriciello N, Roseti C, Zampognaro F. TCP Wave over Linux: a disruptive alternative to the traditional TCP window approach. Computer Networks. 2021 Jan 15;184:107633.

[200] Chao L, Wu C, Yoshinaga T, Bao W, Ji Y. A brief review of multipath tcp for vehicular networks. Sensors. 2021 Apr 15;21(8):2793.

[201] Kimura BY, Lima DC, Loureiro AA. Packet scheduling in multipath TCP: Fundamentals, lessons, and opportunities. IEEE Systems Journal. 2020 Jan 27;15(1):1445-57.