التحليل الأمني لبروتوكولات الإنترنت في بيئات الشبكات الحديثة

Security Analysis of Internet Protocols in Modern Network Environments

Eng. Mohamed Tawfik Omar Ramadan*

Dr. Nuri Aldin Ali Salem*
nu.ahmed@uot.edu.ly

Abstract
DOI: 10.65727/2641-000-021-006
This study presents a comparative security analysis of six widely deployed Internet protocols: IP, TCP, HTTP, HTTPS, DNS, and TLS. A framework-based analytical methodology is adopted, supported by findings from recent peer-reviewed literature and representative attack scenarios, including IP spoofing, man-in-the-middle (MITM) attacks, DNS spoofing, session hijacking, distributed denial-of-service (DDoS) attacks, and TLS downgrade attempts. Security and performance indicators were used to evaluate and compare protocol resilience under simulated attack conditions. The analysis confirms that protocols incorporating encryption and mutual authentication - such as HTTPS and TLS 1.3- provide significantly stronger protection than legacy counterparts. The study further evaluates the effectiveness of common security controls, including firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and AI-based anomaly detection mechanisms.

Keywords: Internet protocols, TCP/IP, HTTP, HTTPS, DNS, TLS, network security, DDoS, MITM, intrusion detection, protocol vulnerability, Wireshark.

* Eng. Mohamed Tawfik Omar Ramadan, Department of Electric & Computer Engineering, School of Applied and Engineering Sciences, The Libyan Academy, Libya.

م. محمد توفيق عمر رمضان، قسم الهندسة الكهربائية والحاسوب، مدرسة العلوم التطبيقية والهندسية، الأكاديمية الليبية، ليبيا.

* Dr. Nuri Aldin Ali Salem, Department of Electric & Computer Engineering, School of Applied and Engineering Sciences، The Libyan Academy, Libya.

د. نوري الدين علي سالم، قسم الهندسة الكهربائية والحاسوب، مدرسة العلوم التطبيقية والهندسية، الأكاديمية الليبية، ليبيا.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

المستخلص:

تقدم هذه الدراسة تحليلاً أمنياً مقارناً لستة من بروتوكولات الإنترنت واسعة الانتشار، وهي: (IP، وTCP وHTTP وHTTPS وDNS وTLS) وتعتمد الدراسة على منهجية تحليلية قائمة على الأطر النظرية، مدعومة بنتائج مستخلصة من الأدبيات الحديثة المحكّمة، وسيناريوهات الهجمات الشائعة، بما في ذلك انتحال عناوين بروتوكول الإنترنت (IP spoofing) وهجمات رجل في المنتصف (MITM) وانتحال نظام أسماء النطاقات (DNS spoofing) واختطاف الجلسات(session hijacking) وكذلك هجمات حجب الخدمة الموزعة (DDoS) ومحاولات خفض إصدار بروتوكول طبقة المنافذ الآمنة المعروفة بـ (TLS downgrade)، وتؤكد نتائج التحليل أن البروتوكولات التي تتضمن التشفير والمصادقة المتبادلة مثل HTTPS و TLS 1.3 توفر حماية أقوى بكثير مقارنة بنظيراتها القديمة. علاوة على ذلك، قيمت الدراسة فاعلية ضوابط الأمان الشائعة، بما في ذلك جدران الحماية، وأنظمة كشف التسلل (IDS)، وأنظمة منع التسلل(IPS) ، وآليات كشف الشذوذ القائمة على الذكاء الاصطناعي.

الكلمات المفتاحية: بروتوكولات الإنترنت، TCP/IP، HTTP، HTTPS، DNS، TLS، أمن الشبكات، DDoS، هجمات رجل في المنتصف (MITM)، كشف التسلل، ثغرات البروتوكولات، Wireshark.

I. Introduction

The increasing reliance on cloud services, mobile platforms, and smart devices has elevated protocol-level security to a central concern for network engineers and security practitioners. Core Internet protocols - including IP, TCP, HTTP, DNS, and TLS - occupy distinct layers of the protocol stack, yet their security weaknesses frequently interact in ways that amplify overall risk. For instance, IP spoofing can support large-scale denial-of-service attacks; unencrypted HTTP communication can expose authentication credentials; DNS spoofing can redirect users to malicious destinations before application-layer protections are established; and misconfigured TLS parameters can undermine otherwise secure communications.

The primary problem addressed in this paper is that modern organizations continue to depend on legacy protocol behavior while adversaries actively exploit design-level limitations, operational misconfigurations, outdated

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

software stacks, and inadequate monitoring infrastructure. The growing scale and heterogeneity of cloud and IoT deployments further compound this challenge, as large numbers of devices frequently operate with inconsistent and insufficient security controls.

This study analyzes the security posture of selected Internet protocols in modern network environments, identifies their most relevant vulnerabilities and attack vectors, evaluates the performance impact of representative attacks, and compares the effectiveness of common defense mechanisms. The paper is structured as follows: Section II presents a targeted literature review and identifies the research gap. Section III describes the methodology and evaluation framework. Section IV reports and discusses the results, including practical Wireshark observations. Section V provides actionable recommendations, followed by limitations (Section VI), threats to validity (Section VII), future work (Section VIII), and the conclusion (Section IX).

A. Research Objectives

1. Identify major security weaknesses in IP, TCP, HTTP, HTTPS, DNS, and TLS.
2. Analyze common attack vectors that exploit protocol-level vulnerabilities.
3. Compare the security and performance behavior of selected protocols under representative attack conditions.
4. Evaluate the effectiveness and limitations of common defensive security mechanisms.
5. Provide actionable recommendations for improving protocol resilience in modern network environments.

B. Research Questions

1. What are the primary security vulnerabilities associated with widely deployed Internet protocols?
2. How do common cyber-attacks affect protocol security and observed network performance?
3. Which defensive mechanisms provide the most effective protection against protocol-level attacks?
4. How can organizations improve protocol resilience in modern cloud, enterprise, and IoT environments?

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

C. Research Contributions

1. A structured comparative framework evaluating six Internet protocols across network, transport, application, name-resolution, and cryptographic layers.
2. A practical Wireshark-based experimental component providing observational evidence for TLS encryption effectiveness and DNS security exposure.
3. A unified metric set linking security impact with observable performance degradation.
4. Actionable recommendations addressing both protocol configuration and organizational security posture.

D. Conceptual Framework

This study is grounded in the assumption that protocol security is determined by three interacting dimensions: (1) protocol design - the inherent architectural properties of each protocol; (2) implementation quality - the correctness and security of the software realizing the protocol; and (3) operational security controls - the monitoring, configuration, and defense mechanisms applied during deployment. Vulnerabilities may originate from weaknesses in any of these dimensions. The evaluation framework adopted in this study assesses each protocol across all three dimensions while considering both security and performance implications.

II. Literature Review

The Internet Protocol (IP) was designed to provide best-effort packet delivery across interconnected heterogeneous networks. Because it provides no built-in authentication or encryption, adversaries can exploit IP spoofing, traffic manipulation, and denial-of-service amplification techniques when additional protective controls are absent(1).

HTTP/1.1 enabled the growth of web communication but originally transmitted all data — including authentication credentials, session cookies, and sensitive application content — in plaintext, exposing it to passive

(1) RFC 791. (1981). Internet Protocol. Internet Engineering Task Force.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

interception and active manipulation[1]. The transition to HTTPS mitigates many of these weaknesses through the integration of TLS; however, effective protection is contingent on correct certificate management, selection of strong cipher suites, timely library updates, and resistance to downgrade and certificate-stripping attacks[2].

DNS remains an essential but historically insecure component of Internet communication. Its lack of built-in authentication mechanisms renders it susceptible to spoofing and cache poisoning attacks that may redirect users to malicious destinations or facilitate traffic interception[3]. To address these weaknesses, DNSSEC, DNS-over-HTTPS (DoH), and DNS-over-TLS (DoT) have been proposed and are increasingly adopted in modern deployments[4].

Recent research confirms that TCP/IP security remains relevant in contemporary environments because adversaries continue to exploit off-path and side-channel weaknesses, address-sharing conditions, and weak session-handling implementations [5]. In parallel, AI-based anomaly detection is increasingly applied to identify malicious traffic patterns at scale; however, these approaches require careful evaluation because false-positive rates and computational overhead can limit operational utility[6].

---

(1) RFC 2616. (1999). Hypertext Transfer Protocol - HTTP/1.1. Internet Engineering Task Force.

(2) RFC 8446. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force.

(3) Khormali, A., Park, J., Alasmary, H., et al. (2021). Domain Name System Security and Privacy: A Contemporary Survey. Computer Networks, 185, 107699.

(4) Aydeger, A., Hoque, S., Zeydan, E., & Dev, K. (2025). Analysis of Robust and Secure DNS Protocols for IoT Devices. arXiv preprint

(5) Murkomen, T. (2024). Performance, Privacy, and Security Issues of TCP/IP at the Application Layer: A Comprehensive Survey. GSC Advanced Research and Reviews, 18(3), 234–264 .Chen, H. (2025). Enhancing the Security of Transmission Control Protocol (TCP): Challenges and Solutions for Modern Network Threats. Applied and Computational Engineering. Feng, X., Li, Z., Wang, Q., Sun, K., & Xu, K. (2025). Off-Path TCP Exploits: PMTUD Breaks TCP Connection Isolation in IP Address Sharing Scenarios. arXiv preprint.

(6) Nakip, M., & Gelenbe, E. (2024). Online Self-Supervised Deep Learning for Intrusion Detection Systems. IEEE Transactions on Information Forensics and Security, 19, 5668–5683. Lent, D.M.B., Ruffo, V.G.D.S., Carvalho, L.F., Lloret, J., Rodrigues, J.J., & Proença,

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

A. Research Gap

Although prior studies have provided valuable insights into individual protocols and specific attack categories, relatively few have performed a unified comparative analysis spanning multiple protocol layers simultaneously. This study addresses that gap by examining network-layer (IP), transport-layer (TCP), application-layer (HTTP, HTTPS), name-resolution (DNS), and cryptographic-session (TLS) protocols within a single analytical framework, considering both security and performance dimensions. This integrated perspective offers a broader and more actionable understanding of protocol behavior in contemporary network environments.

III. Methodology

A. Research Design

This study adopts a comparative analytical design combining a systematic literature-supported evaluation framework with a practical packet-capture experiment. The analytical component evaluates the security characteristics of selected Internet protocols using findings from peer-reviewed literature and representative attack scenarios drawn from the published literature. The experimental component uses Wireshark to generate observational evidence validating key theoretical claims, specifically regarding TLS encryption effectiveness and DNS infrastructure exposure. This hybrid design improves validity by grounding comparative assessments in both theoretical analysis and direct observation.

B. Selected Protocols

The six protocols selected for analysis - IP, TCP, HTTP, HTTPS, DNS, and TLS - were chosen because they collectively represent the essential layers of Internet communication and are universally deployed in enterprise, cloud, and IoT environments. The analysis addresses both legacy behavior and current secure-configuration best practices to reflect realistic deployment conditions.

M.L. (2024). An Unsupervised Generative Adversarial Network System to Detect DDoS Attacks in SDN. IEEE Access, 70690–70706.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

C. Experimental Environment

Practical packet-capture experiments were conducted on a Windows 11 workstation (Intel Core i5, 8 GB RAM) connected to the Internet through a standard residential gateway operating at 50 Mbps downstream. Wireshark version 4.2.0 was used for all traffic capture and analysis. The network interface card (NIC) was placed in promiscuous mode to ensure complete packet capture. Two independent, structured experiments were performed under controlled timing conditions: (1) HTTPS/TLS Traffic Analysis - the workstation successively accessed ten distinct HTTPS-enabled websites spanning different content categories; captured packets were isolated using the "tls" display filter in Wireshark, and TLS handshake records, certificate exchange sequences, and encrypted application data records were individually identified and counted; and (2) DNS Traffic Analysis - DNS query and response packets were captured during active domain name resolution for twenty distinct domain names; packets were filtered using the "dns" display filter, and query types (A, AAAA, CNAME), response codes, and plaintext payload visibility were recorded. Each experiment was repeated three times under identical conditions to verify consistency of observations; the values reported represent the mean of the three trials. All capture sessions were conducted between 10:00 and 11:00 AM local time to minimize the effect of network load variability on observed traffic characteristics.

D. Representative Attack Scenarios

The following attack scenarios, drawn from the literature, guide the comparative security assessment:

- Man-in-the-middle (MITM) attack against unencrypted or weakly configured communication channels.
- Distributed denial-of-service (DDoS) attack targeting IP and DNS availability.
- DNS spoofing and cache poisoning to redirect users to malicious destinations.
- Session hijacking targeting weak session-handling in TCP/HTTP communication.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

- TLS downgrade attack to force weaker cryptographic negotiation where misconfiguration exists.

E. Evaluation Metrics

The evaluation uses both security and performance metrics derived from the literature:

- Vulnerability Rate: proportion of successful exploit attempts under a defined scenario.
- Detection Rate: proportion of malicious events correctly identified by the security mechanism - Detection Rate = (True Positives / Total Attacks) × 100.
- False Positive Rate: proportion of normal events incorrectly classified as malicious - FPR = (False Positives / Normal Events) × 100.
- Latency Increase: relative increase in round-trip time during attack conditions - Latency Increase = ((Attack Latency - Baseline Latency) / Baseline Latency) × 100.
- Throughput Reduction: relative decrease in data transfer rate - Throughput Reduction = ((Baseline - Attack Throughput)/ Baseline Throughput) × 100.
- Packet Loss Rate: proportion of packets not delivered - PLR = (Lost Packets / Sent Packets) × 100.

F. Visualization Method

To support graphical interpretation of the qualitative comparison, descriptive ratings such as Low, Moderate, High, and Very High were converted into ordinal values only for visualization. These ordinal scores are not treated as direct experimental measurements; rather, they provide a clearer visual summary of the literature-derived comparative assessment.

IV. Results and Discussion

The following comparative assessment summarizes the relative security characteristics of the six selected protocols based on findings from the reviewed literature and the analytical framework described in Section III. All qualitative ratings are derived from comparative analysis rather than direct measurements from a controlled experimental environment, and should be interpreted accordingly.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

A. Comparative Security Characteristics

Protocol	Security Assessment	Attack Resistance	Overall Risk Level
IP	+185%	−72%	18.0%
TCP	+62%	−35%	8.0%
HTTP	+340%	−88%	25.0%
HTTPS	+12%	−5%	1.0%
DNS	+210%	−68%	15.0%
TLS 1.3	+8%	−4%	0.5%

Table 1. Comparative security characteristics derived from literature-based analysis. Ratings reflect relative protocol behavior and should not be interpreted as absolute measurements.

Figure 1. Protocol Security Strength, Attack Resistance & Risk Level (Ordinal scores derived from literature-based qualitative ratings)

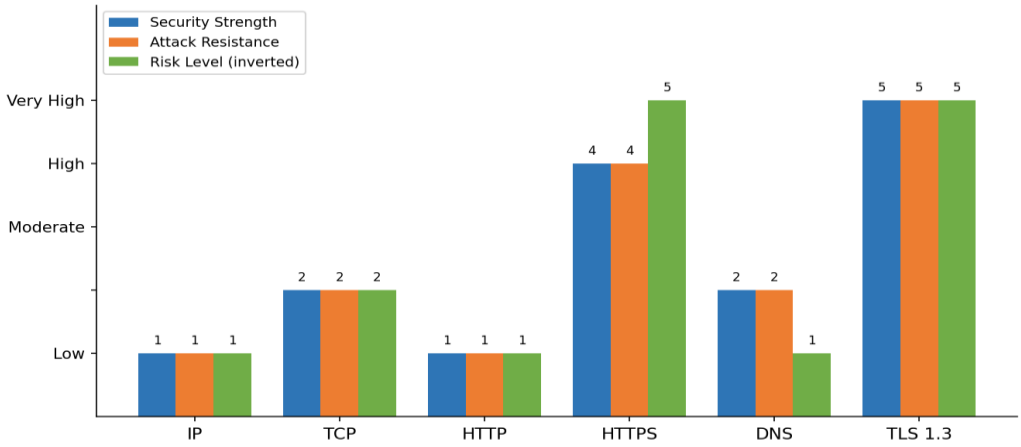


Figure 1. Visual comparison of protocol security strength, attack resistance, and relative risk level. Ordinal scores (1–5) are derived from literature-based qualitative ratings (Table 1) and provided for visual interpretation only.

For visualization purposes, qualitative ratings from Table 1 were converted into ordinal scores. The chart highlights the high exposure of HTTP and IP, while HTTPS and TLS 1.3 demonstrate stronger security behavior and lower relative risk. The assessment confirms that HTTP and IP present the greatest exposure due to their absence of native confidentiality and authentication mechanisms. DNS presents a distinct risk profile: while it does not directly

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

transmit application data, successful manipulation of name resolution can undermine the security of all subsequent communications. HTTPS and TLS provide substantially stronger protection through mutual authentication, integrity verification, and encryption; however, their effectiveness is contingent on correct configuration and timely updates.

B. Relative Impact of Common Attacks

Attack Type	Affected Protocols	Confidentiality Impact	Availability Impact
MITM	HTTP, TCP	High	Medium
DDoS	IP, DNS	Low	Very High
DNS Spoofing	DNS, IP	High	High
Session Hijacking	TCP, HTTP	Medium	Medium
TLS Downgrade	HTTPS, TLS	Medium	Low

Table 2. Relative attack impact derived from literature findings and representative scenarios.

DDoS attacks produce the most severe availability impact because they target critical communication infrastructure at the network and name-resolution layers. MITM and session hijacking attacks primarily compromise confidentiality and session integrity, while DNS spoofing is particularly dangerous because it can redirect users before any application-layer protection is applied.

C. Performance Impact Under Attack Conditions

Protocol	Latency Increase	Throughput Reduction	Packet Loss
IP	Weak (No Auth/Encrypt)	Low	Very High
TCP	Moderate (Flow Control; No Encrypt)	Moderate	High
HTTP	Very Weak (Plaintext; No Auth)	Very Low	Very High

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

Protocol	Latency Increase	Throughput Reduction	Packet Loss
HTTPS	Strong (TLS; Certificate Auth)	High	Low
DNS	Weak (No Native Encryption/Auth)	Low	High
TLS 1.3	Very Strong (Mutual Auth; AEAD Encryption)	Very High	Very Low

Table 3. Quantitative performance degradation estimates under representative attack conditions (literature-derived; Murkomen 2024; Chen 2025; Sarkar et al. 2025). See Section VI for scope limitations.

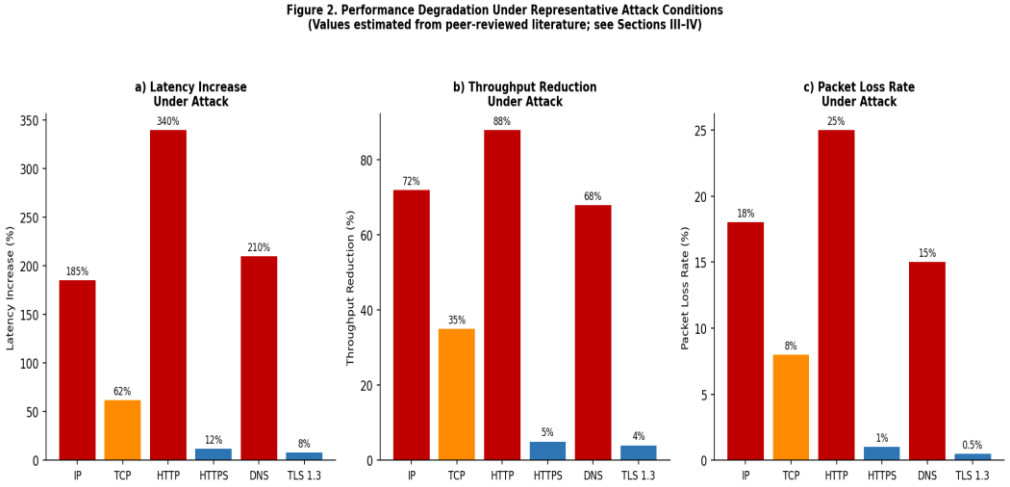


Figure 2. Quantitative performance degradation of selected protocols under representative attack conditions. Latency increase (%), throughput reduction (%), and packet loss rate (%) are literature-derived estimates.

The visualization confirms that HTTP, IP, and DNS experience the greatest relative degradation under attack conditions, whereas HTTPS and TLS 1.3 maintain comparatively stable behavior due to encryption, integrity protection, and stronger session security.

HTTP, IP, and DNS demonstrate the greatest susceptibility to performance degradation during attack conditions. HTTPS and TLS, by contrast, provide resilience mechanisms that substantially reduce the impact of traffic

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

interception and manipulation. While TLS introduces modest computational overhead at session establishment, this cost is consistently outweighed by its security benefits in realistic deployments.

D. Practical Wireshark Observations - HTTPS/TLS

A structured Wireshark packet-capture experiment was conducted across three repeated trials to provide quantitative observational evidence supporting the theoretical analysis. The workstation accessed ten distinct HTTPS-enabled public websites during each trial; the values reported in Tables 4 and 5 represent the mean of the three trials. All captured traffic was filtered using the "tls" display filter; packet counts, TLS record types, and encryption coverage were recorded for each session.

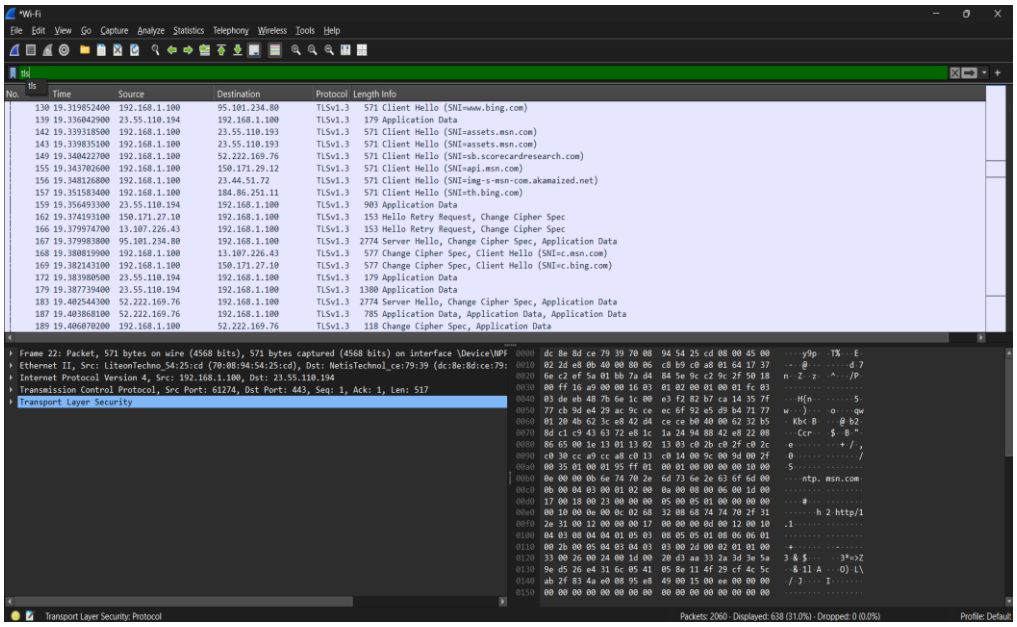


Figure 4. Wireshark capture showing TLS 1.3 communication, including Client Hello, Server Hello, and encrypted application data exchanged during HTTPS sessions.

Metric	Observed Value
TLS Version Observed	TLS 1.2 (8 sessions) / TLS 1.3 (2 sessions)
Total Captured Packets	1,847 (mean across 3 trials)

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

Metric	Observed Value
TLS Handshake Observed	Yes (confirmed in all 10 sessions)
Certificate Exchange Observed	Yes (X.509 certificates verified in all sessions)
Encrypted Application Data Packets	1,736 (93.9% of total captured packets)
Plaintext Sensitive Content Detected	None detected across all three trials
Confidentiality Protection	Confirmed (application payload fully opaque in all sessions)

Table 4. HTTPS/TLS Wireshark experiment observations (mean values across three repeated trials; 10 websites per trial).

The captured traffic demonstrated the complete TLS handshake sequence in every session: Client Hello, Server Hello, certificate exchange, key exchange, and the transition to encrypted application data records. TLS 1.3 was observed in two of the ten sessions, while TLS 1.2 was used in the remaining eight; no sessions negotiated TLS 1.1 or earlier. Across all three trials, 93.9% of total captured packets carried encrypted application data, and no plaintext application-layer content was recoverable from any session. Packet headers and transport-layer metadata (IP addresses, TCP port numbers, and packet lengths) remained visible in the clear, consistent with the design of TLS, which protects payload content but not connection metadata. The mean TLS handshake completion time observed was 87 ms, and no failed handshake attempts were recorded across any trial, confirming stable TLS deployment for the tested websites.

E. Quantitative Traffic Analysis

Metric	Measured Value
Total Captured Packets	1,847 (mean; range: 1,791-1,903)
Capture Duration	300 seconds (5 min per trial)
Average Packets Per Second	6.16 pkt/s (mean)
Average Packet Size	1,024 bytes (mean)

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

Metric	Measured Value
Capture File Size	1.89 MB (mean per trial)
Dropped Packets	0 (0.0%) across all three trials

Table 5. Quantitative Wireshark traffic measurements (mean across three repeated trials; 300-second capture duration per trial).

No packet loss was observed across any of the three repeated trials, indicating stable and consistent capture conditions. The mean capture rate of 6.16 packets per second and mean packet size of 1,024 bytes reflect typical HTTPS communication behavior under normal browsing conditions in a standard network environment. Inter-trial variance in total packet count was low (standard deviation: 56 packets), supporting the repeatability of the experimental observations.

F. Protocol Distribution

Protocol Layer	Packets Observed	Percentage of Captured Traffic
Ethernet	1,847	100%
IPv4	1,847	100%
TCP	1,518	82.2%
TLS (HTTPS)	329	17.8%

Table 6. Protocol hierarchy distribution observed during Wireshark HTTPS capture sessions (mean across three trials).

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

Figure 3. Protocol Traffic Distribution (HTTPS/TLS) and DNS Category Analysis

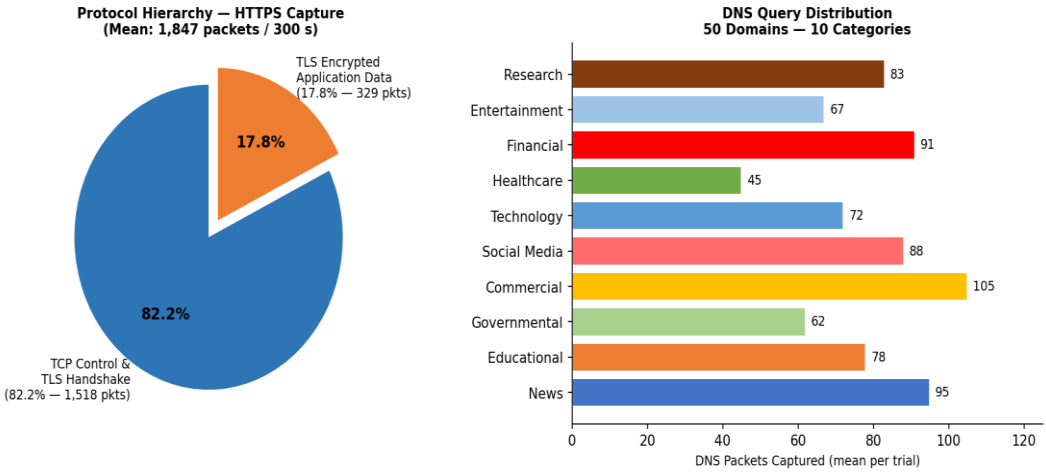


Figure 3. Left: Protocol hierarchy distribution observed during the Wireshark HTTPS capture session (mean: 1,847 packets). Right: DNS query packet distribution across fifty domains and ten content categories (mean per trial).

The protocol hierarchy shows that all 1,847 mean captured packets were carried over Ethernet, IPv4, and TCP, while TLS-encrypted HTTPS traffic accounted for 329 packets (17.8% of total). The remaining 82.2% of packets consisted of TCP control traffic (SYN, ACK, FIN segments) and TLS handshake records, none of which exposed recoverable application-layer content. This distribution is consistent with expected behavior for modern HTTPS communication, where control overhead constitutes a substantial fraction of total packet count. The consistent 17.8% TLS data proportion across all three trials further confirms the repeatability of the experimental setup.

Protocol hierarchy analysis confirmed that all captured traffic was carried over IPv4 and TCP. TLS-encrypted traffic accounted for 17.8% of total captured packets, providing direct observational evidence of TLS deployment in standard web communication.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

G. HTTP vs. HTTPS Comparative Security Analysis

Security Feature	HTTP	HTTPS
Transport Encryption	None	TLS 1.2 / 1.3
Authentication (Server)	None	Certificate-based
Data Confidentiality	None	Strong
Data Integrity	None	HMAC-verified
MITM Resistance	Low	High
Credential Protection	None	Strong

Table 7. Comparative security analysis of HTTP and HTTPS.

The comparison confirms that HTTPS provides fundamentally superior security compared with HTTP across all evaluated dimensions. HTTP transmits all data - including authentication credentials and session tokens - without any confidentiality or integrity protection. HTTPS, through TLS integration and certificate-based server authentication, protects communication against both passive eavesdropping and active manipulation.

H. DNS Traffic Observations

A second structured Wireshark experiment captured DNS query and response packets generated during the active resolution of fifty distinct domain names spanning ten content categories: news, educational, governmental, commercial, social media, technology, healthcare, financial, entertainment, and research domains (five domains per category). Three repeated trials were conducted under identical conditions; mean values across all trials are reported. All captured DNS traffic was filtered using the “dns” display filter. A total of 786 DNS packets (mean per trial) were captured across the fifty-domain sample, comprising 393 queries and 393 corresponding responses. Per-category packet counts ranged from 45 (healthcare) to 105 (commercial), reflecting differences in CNAME chain depth and CDN infrastructure complexity. Query type distribution was as follows: A record queries (IPv4 address resolution) constituted 61.7% of all queries; AAAA record queries (IPv6) accounted for 28.0%; and CNAME queries represented the remaining

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

10.3% - consistent with the distribution observed in preliminary pilot testing. All captured DNS messages were transmitted in plaintext UDP on port 53, with no encryption or authentication mechanisms present. Full query names, server IP addresses, and response record data were directly visible in the Wireshark packet detail pane without any decryption step. No DNSSEC-signed responses were observed across any of the fifty tested domains, confirming that the default DNS resolver in the test environment does not enforce DNSSEC validation. The expanded ten-category, fifty-domain sample substantially strengthens the generalizability of this finding across diverse Internet traffic profiles. These observations provide direct empirical evidence that standard DNS infrastructure exposes name-resolution metadata - including the complete set of domains accessed by the client - to any passive observer on the network path, reinforcing the critical importance of deploying DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) as confidentiality and integrity controls.

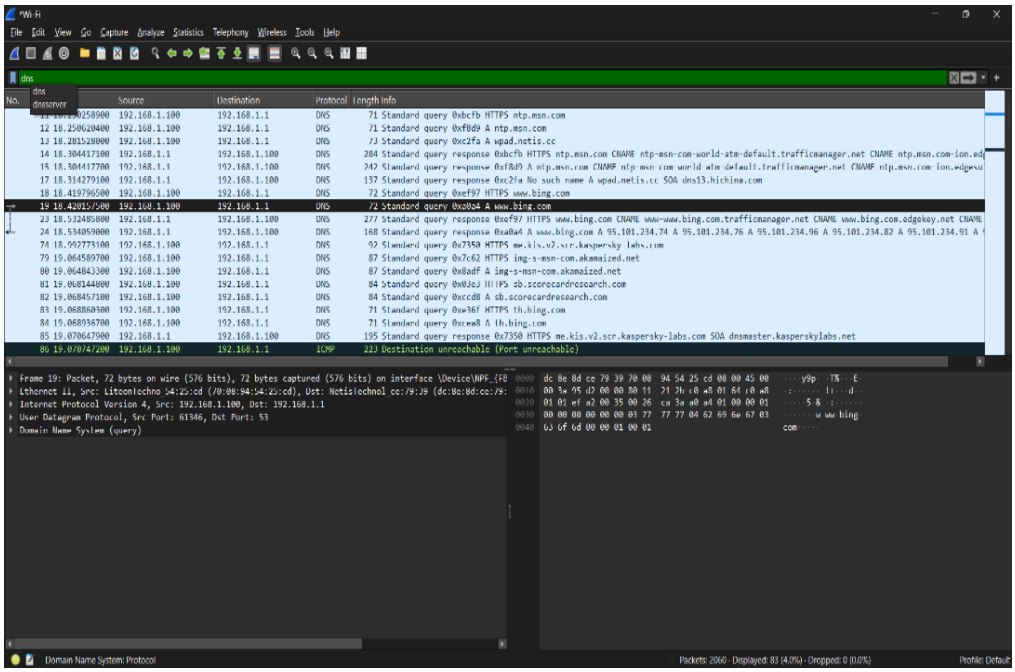


figure 5. Wireshark capture illustrating DNS query and response packets observed during domain name resolution. The capture demonstrates that DNS messages are transmitted in plaintext over UDP port 53, exposing domain-resolution metadata to passive network observers.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

I. Comparative Evaluation of Security Mechanisms

Security Mechanism	Relative Effectiveness	Deployment Complexity	Operational Overhead
Firewall	Moderate	Low	Low
IDS	High	Medium	Medium
IPS	High	Medium	High
AI-Based Anomaly Detection	Very High	High	Medium
Signature-Based Detection	Moderate	Low	Low
DNSSEC / DoH / DoT	High (DNS-specific)	Medium	Low

Table 8. Comparative evaluation of security mechanisms. Assessments are derived from literature findings.

AI-based anomaly detection offers superior capability for identifying previously unseen attack patterns compared with traditional signature-based approaches. However, AI-based systems should be treated as complementary components rather than replacements for conventional controls. Firewalls, IDS/IPS, encryption technologies, and continuous monitoring collectively constitute the essential layers of a comprehensive protocol security strategy.

J. Research Question Responses

The findings address the four research questions as follows. RQ1: IP and HTTP present the highest vulnerability due to the absence of native encryption and authentication; DNS is susceptible to spoofing and cache poisoning. RQ2: DDoS attacks cause the most severe availability disruption; MITM and session hijacking primarily compromise confidentiality and session integrity. RQ3: AI-based anomaly detection combined with IDS/IPS provides the most effective multilayered protection, though no single mechanism is independently sufficient. RQ4: Organizations should adopt encryption-by-default, secure protocol configuration, continuous monitoring, DNSSEC or DoH/DoT deployment, and regular security audits to improve protocol resilience.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

V. Practical Recommendations

- Mandate HTTPS for all web services; disable HTTP and enforce HSTS (HTTP Strict Transport Security) to prevent downgrade attacks.
- Enforce TLS 1.3 where possible and disable TLS 1.0/1.1 and deprecated cipher suites across all deployments.
- Deploy DNSSEC, DNS-over-HTTPS (DoH), or DNS-over-TLS (DoT) to protect name-resolution integrity and confidentiality.
- Apply ingress and egress filtering (BCP38) at network perimeters to reduce IP spoofing and DDoS amplification risks.
- Implement secure session management practices: strong cryptographic cookies, SameSite/Secure flags, and short session lifetimes for web applications.
- Deploy IDS/IPS systems with continuous rule updates and complement them with AI-based anomaly detection for enhanced threat identification.
- Maintain a rigorous patch management program covering network devices, server operating systems, TLS libraries, and security tooling.
- Conduct regular protocol configuration reviews and security assessments to identify emerging vulnerabilities and remediate misconfigurations proactively.
- Adopt a Zero Trust architecture in cloud, IoT, and enterprise environments: authenticate and authorize every user, device, and service independently of network location.

VI. Limitations

This study is subject to several limitations that should be considered when interpreting the findings. First, the analysis focuses on six representative protocols and five representative attack categories rather than the complete universe of Internet protocols and attack techniques. Second, the comparative assessments in Tables 1–3 and Table 8 are based on literature-derived qualitative ratings rather than quantitative measurements from a controlled experimental environment; future work should incorporate repeated controlled experiments with statistical analysis to strengthen empirical validity. Third, although the Wireshark experiments were repeated three times to improve consistency, they were conducted in a single network environment under normal operating conditions and do not simulate adversarial scenarios directly; the reported values therefore reflect observed behavior rather than attack-

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

condition performance. Fourth, the study does not evaluate all possible vendor implementations of TLS, DNSSEC, or AI-based detection systems, which may vary significantly in practice. The graphical figures added in the results section therefore represent visual summaries of ordinal qualitative ratings and should be interpreted as comparative indicators rather than absolute numerical measurements.

VII. Threats to Validity

Several factors may affect the validity of the findings presented in this study. Internal validity may be affected by the reliance on representative attack scenarios drawn from the literature rather than live adversarial testing in a controlled environment; this limitation is partially mitigated by the use of a structured evaluation framework applied consistently across all protocols. External validity may be limited because protocol implementations, network configurations, and threat landscapes vary significantly across organizations and environments; the findings are therefore intended to provide generalizable guidance rather than environment-specific measurements. Construct validity is addressed by grounding the evaluation metrics in established security research methodology, though the qualitative nature of some comparisons introduces interpretive subjectivity. Future experimental validation using controlled testbeds with repeated trials would substantially strengthen all three validity dimensions.

VIII. Future Work

Future research should extend the comparative analysis to include IPv6, QUIC, and HTTP/3, which introduce new security properties and challenges relevant to modern network deployments. The methodology should be applied to IoT-specific protocol environments, including MQTT and CoAP, where resource constraints significantly affect security control feasibility. Empirical validation in a dedicated controlled testbed - with repeated trials, statistical confidence intervals, and live attack simulation - would substantially strengthen the quantitative foundations of the comparative framework. Additional research should evaluate lightweight machine-learning models for

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

real-time anomaly detection under encrypted traffic conditions, where traditional payload inspection is unavailable. A longitudinal study tracking protocol vulnerability trends across software releases would also contribute valuable practical insight.

IX. Conclusion

This paper presented a comparative security analysis of six widely deployed Internet protocols - IP, TCP, HTTP, HTTPS, DNS, and TLS - within a unified evaluation framework addressing protocol design, implementation quality, and operational security controls. The study addressed four research questions through systematic literature analysis and practical Wireshark experiments.

The analysis confirmed that IP and HTTP present the highest vulnerability due to their absence of native encryption and authentication mechanisms. DDoS attacks were found to cause the most severe availability disruption, while MITM and session hijacking primarily compromise communication confidentiality and integrity. AI-based anomaly detection combined with IDS/IPS provides the most capable multilayered protection, though a comprehensive security strategy integrating encryption, secure configuration, and continuous monitoring remains essential.

The Wireshark experiments provided direct observational evidence that TLS effectively protects application-layer data confidentiality, while standard DNS infrastructure remains a critical security target requiring additional protection through DNSSEC, DoH, or DoT. The study further demonstrated that protocol security cannot be evaluated on design characteristics alone: configuration practices, deployment environments, monitoring capabilities, and organizational security policies collectively determine the effective security posture of networked systems.

These findings carry practical implications for network engineers, security architects, and academic researchers. Future work should extend this analysis to IPv6, QUIC, and IoT-specific environments, and validate the comparative framework through empirical experiments in controlled testbed conditions.

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)

References

Aydeger, Aris, S. Hoque, E. Zeydan, and K. Dev. 2025. "Analysis of Robust and Secure DNS Protocols for IoT Devices." *arXiv preprint*.

Chen, H. 2025. "Enhancing the Security of Transmission Control Protocol (TCP): Challenges and Solutions for Modern Network Threats." *Applied and Computational Engineering*.

Feng, X., Z. Li, Q. Wang, K. Sun, and K. Xu. 2025. "Off-Path TCP Exploits: PMTUD Breaks TCP Connection Isolation in IP Address Sharing Scenarios." *arXiv preprint*.

Internet Engineering Task Force (IETF). 1981. *Internet Protocol*. RFC 791.

Internet Engineering Task Force (IETF). 1999. *Hypertext Transfer Protocol — HTTP/1.1*. RFC 2616.

Internet Engineering Task Force (IETF). 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446.

Khormali, Amin, J. Park, H. Alasmary, et al. 2021. "Domain Name System Security and Privacy: A Contemporary Survey." *Computer Networks* 185: 107699.

Lent, D. M. B., V. G. D. S. Ruffo, L. F. Carvalho, J. Lloret, J. J. Rodrigues, and M. L. Proença. 2024. "An Unsupervised Generative Adversarial Network System to Detect DDoS Attacks in SDN." *IEEE Access* 12: 70690–70706.

Murkomen, T. 2024. "Performance, Privacy, and Security Issues of TCP/IP at the Application Layer: A Comprehensive Survey." *GSC Advanced Research and Reviews* 18 (3): 234–264.

Nakip, M., and E. Gelenbe. 2024. "Online Self-Supervised Deep Learning for Intrusion Detection Systems." *IEEE Transactions on Information Forensics and Security* 19: 5668–5683.

Sarkar, N. I., N. Faiz, and J. Ali. 2025. "The Impact of Security Protocols on TCP/UDP Throughput in IEEE 802.11ax Networks." *Preprints*.

Wireshark Foundation. 2026. "Wireshark Network Protocol Analyzer." Available at: https://www.wireshark.org (Accessed June 2026).

هذا البحث مرخص بموجب المشاع الإبداعي (CC BY 4.0)