Alqalam Journal of Medical and Applied Sciences. 2026;9(6):1785-1792
https://doi.org/10.54361/ajmas.269646

Original article

Protocol Layering in Computer Networks: A Comparative Survey on OSI and TCP/IP Applications, Security Vulnerabilities, and Cross-Layer Directions

Aya Asswaie*[1], Nuredin Ahmed[2], Abdulrahman Ashtawi[3]

[1]*Department of Information Technology Engineering, Libyan Academy for Graduate Studies, Janzour, Libya*
[2]*Department of Computer Engineering, Faculty of Engineering, University of Tripoli, Tripoli, Libya.*
[3]*Libyan Authority for Scientific Research, Tripoli, Libya.*
Corresponding email. *ayaalmadhony8@gmail.com*

Abstract
This paper presents a systematic literature review (SLR) of protocol layering architectures, comparing the OSI seven-layer model with the TCP/IP four-layer suite based on literature published between 2022 and 2026. The review finds that strict protocol layering creates systemic vulnerabilities. Informational isolation between layers enables DHCP starvation attacks, where servers accept spoofed requests due to a lack of link-layer authentication. Additionally, HTTP/TCP performance suffers when transport protocols misinterpret reconfiguration events as congestion. In response, the study examines Cross-Layer Design (CLD) as an alternative paradigm. CLD enables controlled information sharing across non-adjacent layers but introduces trade-offs, including loss of modularity and increased complexity.
Keywords: Protocol Layering, OSI Model, TCP/IP, DHCP Starvation, Cross-Layer Design, SLR

Introduction

Protocol layering is a fundamental principle in computer network design. By partitioning communication into discrete layers, network architectures become more manageable and interoperable. Two reference architectures have shaped modern networking: the OSI seven-layer model (conceptual) and the TCP/IP four-layer suite (operational foundation of the Internet). However, emerging environments—IoT, MANETs, cloud, and 5G/6G—demand greater flexibility than strict layering provides. Rigid layer separation restricts cross-layer information exchange, causing increased latency, energy consumption, and security vulnerabilities. Many application-layer protocols operate with limited awareness of lower-layer conditions, creating risks that attackers can exploit. Cross-Layer Design (CLD) has emerged as a promising alternative, enabling controlled information sharing between non-adjacent layers.

Research on protocol layering has evolved considerably over the past decade, shifting from structural comparisons toward performance optimization, security analysis, and cross-layer integration. The literature can be organized into three thematic areas that reflect this evolution.

Several foundational studies have compared the OSI and TCP/IP models from architectural and operational perspectives. Abdulmonim and Zainab (2024) conducted a comprehensive structural comparison, concluding that TCP/IP offers greater practical efficiency due to its simplified four-layer design, while the OSI model remains valuable primarily as a theoretical and pedagogical framework [1]. Janighorban and Kaveh (2025) extended this comparative analysis by examining encapsulation, decapsulation, and session management processes across both models, highlighting the competitive dimensions that influence adoption in different networking contexts [2]. From a security standpoint, Khan and Atif (2025) analyzed layered defense strategies for securing the OSI model through protocol management and advanced cyber techniques, though their work remained focused on the OSI framework and did not extend to TCP/IP or cross-layer considerations [3]. While these studies provide valuable structural and security-focused comparisons, they exhibit a notable limitation: none address cross-layer solutions or integrate application-layer vulnerability analysis into their comparative frameworks. This gap is particularly significant given the increasing recognition that security vulnerabilities often arise precisely at the interfaces between layers.

The application layer has emerged as a critical focal point for understanding the limitations of strict protocol layering. Murkomen (2024) conducted a comprehensive survey of privacy and performance challenges affecting HTTP, DNS, and DHCP, concluding that strict layering fundamentally limits application adaptability and increases security risks through informational isolation [6]. Cevallos-Salas et al. (2024) provided a systematic classification of application-layer security threats for Internet communications, categorizing attacks, control mechanisms, and emerging trends [7]. Dawood et al. (2024) analyzed the specific impact of DNS over HTTPS on cybersecurity, revealing persistent privacy vulnerabilities in DNS and HTTP communications even when encryption is employed [8]. Of particular relevance to the present study, Ramprasad et al. (2023) extended these findings to IoT environments, demonstrating through simulation that DHCP performance degrades severely as device density increases, directly attributable to the absence of cross-layer signaling between the application and link layers [5]. This finding is especially significant because it suggests that the performance degradation observed in high-density IoT deployments is not merely an implementation issue but a systemic consequence of strict layering.

Received: *25-04-2026* - ***Accepted***: *23-06-2026* - ***Published***: *29-06-2026*

Despite the breadth of these studies, a consistent limitation emerges: none propose structured cross-layer solutions to mitigate the identified vulnerabilities. The literature remains largely diagnostic, identifying problems without offering architectural remedies.

Cross-Layer Design (CLD) has gained substantial attention as a potential solution to the limitations of strict layering. Kushwaha and Mishra (2022) surveyed cross-layer optimization techniques in wireless networks, concluding that cross-layer architectures have demonstrated significant performance improvements and may shape the future of wireless networking [4]. Feng et al. (2025) provided empirical evidence of cross-layer vulnerabilities in the TCP/IP protocol suite, demonstrating how off-path attackers can exploit forged ICMP error messages to manipulate network traffic, affecting over 20% of popular websites and more than 89% of public Wi-Fi networks [9]. Mustafa et al. (2024) conducted an extensive survey of cross-layer secure and energy-efficient frameworks for IoT networks, reviewing over 100 research articles and identifying three primary information sharing paradigms: bottom-up signaling, top-down control, and joint optimization through an information sharing plane [10]. Naeem et al. (2025) proposed redesigning cross-layer architectures for performance optimization in ad hoc networks, arguing that the traditional OSI model is being replaced by cross-layer approaches in environments characterized by dynamic topologies and poor radio conditions [11]. Malik et al. (2023) provided a parametric survey on cross-layer design for wireless sensor networks, identifying latency, energy consumption, and overhead as key limitations of strict layering that CLD can potentially address [12]. Beckett and Gupta (2022) introduced KATRA, a real-time verification tool for multilayer networks, demonstrating that efficient verification of arbitrarily layered network data planes is achievable but requires specialized algorithms that account for cross-layer interactions [13]. This work is significant because it addresses one of the key challenges to CLD adoption: the difficulty of verifying correctness when layers are no longer independent. The CLD literature, however, exhibits its own limitations. While individual studies demonstrate performance improvements or identify vulnerabilities, none fully address the architectural trade-offs of CLD—such as modularity loss, increased complexity, and standardization challenges—across all network types. There remains a disconnect between the theoretical promise of CLD and its practical deployment.

The reviewed literature reveals a clear and consistent shift toward adaptive networking approaches that recognize the limitations of strict protocol layering. However, a significant gap persists in the existing body of knowledge: performance limitations, security vulnerabilities, and cross-layer solutions have been examined predominantly in isolation, with few studies integrating these dimensions within a unified analytical framework. Most existing work falls into one of three categories. First, structural comparisons of OSI and TCP/IP (e.g., [1][2]) provide architectural insights but lack vulnerability analysis or CLD considerations. Second, application-layer security surveys (e.g., [6][7][8]) identify problems but do not propose architectural solutions. Third, CLD surveys (e.g., [4][10][11]) demonstrate performance improvements but do not systematically evaluate trade-offs or integrate vulnerability analysis. Specifically, none of the reviewed studies simultaneously address: (1) comprehensive architectural comparison between OSI and TCP/IP, (2) systematic analysis of application-layer vulnerabilities arising from strict layering, and (3) critical evaluation of CLD solutions with their associated trade-offs. This fragmentation limits the ability of researchers and practitioners to make informed decisions about when and how to adopt cross-layer approaches. The present survey fills this gap by providing an integrated analysis that bridges all three dimensions within a unified framework.

To achieve this, the present survey is driven by four primary objectives. The first objective is to conduct a systematic comparison between the OSI seven-layer model and the TCP/IP four-layer suite, examining their structural differences, operational characteristics, and respective strengths and weaknesses in contemporary networking environments. The second objective is to identify and analyze the performance bottlenecks and security vulnerabilities that arise specifically at the application layer, with particular focus on HTTP, DNS, and DHCP protocols, and to understand how strict layering boundaries contribute to these vulnerabilities. The third objective is to evaluate Cross-Layer Design (CLD) as an alternative architectural paradigm, assessing its mechanisms, benefits, and inherent trade-offs including modularity loss, increased complexity, and verification challenges. The fourth objective is to highlight open challenges and future research directions, particularly regarding the standardization of secure CLD frameworks and the integration of emerging technologies such as AI-driven optimization and quantum-safe cryptography.

Methods

Study design

This paper adopts a Systematic Literature Review (SLR) methodology to analyze peer-reviewed literature published between January 2022 and March 2026. The review process followed three phases: (1) search and identification, (2) screening and selection, and (3) synthesis and analysis.

Literature Search Strategy and Selection Criteria

Four digital databases were searched: IEEE Xplore, ACM Digital Library, Scopus (Elsevier), and Springer Link. The primary search string combined keywords related to protocol layering ("OSI model" OR "TCP/IP"

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*

OR "protocol layering"), security vulnerabilities ("DHCP starvation" OR "application layer attack" OR "privacy"), and cross-layer design ("cross-layer design" OR "CLD" OR "cross-layer optimization").
Studies were included if they were: (1) peer-reviewed journal articles or conference proceedings, (2) published in English between 2022 and 2026, and (3) directly relevant to at least one research question. Exclusion criteria included non-peer-reviewed sources, duplicates, and studies focused exclusively on hardware-level protocols. The initial database search yielded 347 records. After duplicate removal, 289 unique records remained. Title and abstract screening excluded 198 records, leaving 91 records for full-text assessment. Full-text review excluded a further 37 records, resulting in 54 eligible studies. Snowballing (citation tracking) added 12 additional records, bringing the total corpus to 66 studies, of which 17 core studies were finally cited as the most representative works. The following PRISMA flow diagram illustrates the study selection process.

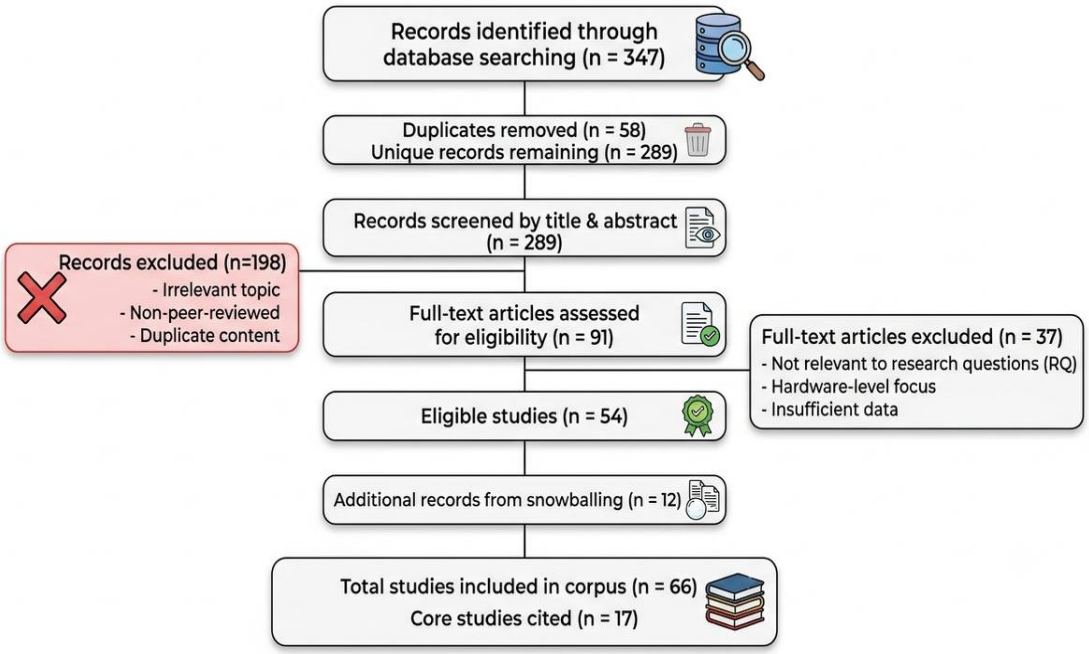

Figure 1. PRISMA Flow Diagram of Study Selection process

Classification Framework

The reviewed literature was organized into three thematic areas consistent with the research objectives: (1) architectural comparison (OSI vs. TCP/IP), (2) application-layer vulnerabilities, and (3) cross-layer design solutions and trade-offs. This classification enabled systematic analysis of findings across different architectural paradigms.

Evaluation Metrics

Each architecture and approach was evaluated across four dimensions, with specific measurement proxies drawn from the reviewed literature:

· Scalability: Maximum supported nodes or prefixes before performance degradation; routing table size growth; control-plane message volume.

· Convergence: Time from topology-change event to stable forwarding state, measured in seconds or milliseconds post-event.

· Stability: Frequency of route changes; oscillation duration; route flapping events per hour.

· Control-Plane Overhead: CPU utilization; memory consumption; bandwidth dedicated to routing traffic under both steady-state and reconvergence conditions.

Statistical Synthesis

A qualitative thematic synthesis was applied, grouping findings into the three thematic areas identified in the classification framework. Data extraction focused on core objectives, methodologies, key findings, and identified gaps for each reviewed study.

Results

This section presents the findings derived from the systematic literature review, organized according to the three thematic areas identified in the methodology.

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*

Architectural Comparison: OSI versus TCP/IP

The comparative analysis reveals fundamental differences between the two architectures that extend beyond their structural representations.

The OSI model consists of seven granular layers conceived through a formal top-down approach, with each layer interacting exclusively with its immediate neighbors through standardized service access points. The hierarchy descends from the Application, Presentation, and Session layers, through the Transport and Network layers, down to the Data Link and Physical layers. This granularity enables precise functional decomposition and pedagogical clarity but is accompanied by increased protocol overhead and reduced commercial adoption.

In contrast, the TCP/IP suite adopts a bottom-up philosophy shaped by real-world deployment rather than formal standardization. It comprises four consolidated layers: the Application layer (which subsumes OSI's top three layers), the Transport layer, the Internet layer (aligned with OSI's Network layer), and the Network Access layer (combining OSI's Data Link and Physical layers). This pragmatic consolidation reduces protocol overhead and has driven TCP/IP's widespread adoption as the foundation of the modern Internet [1][2].

The encapsulation process is fundamental to both architectures and merits specific attention. Data traversing downward is successively wrapped with layer-specific headers. At the receiving end, each layer processes and strips its corresponding header before passing the remaining data upward. This mechanism enables interoperability across heterogeneous platforms but, as later sections will demonstrate, also enforces informational isolation that constrains performance and security. Beckett and Gupta (2022) introduced KATRA, a real-time verification tool for multilayer networks, demonstrating that efficient verification of arbitrarily layered network data planes is achievable [13].

Application-Layer Vulnerabilities

The review identified consistent patterns of vulnerabilities across application-layer protocols, directly attributable to strict layering boundaries. Table 1 summarizes these vulnerabilities around four representative protocols: HTTP/TCP, DHCP, IoT-oriented DHCP, and DNS/HTTP.

Table 1: Performance, Security, and Privacy Matrix of TCP/IP Application Layer Protocols

Target Protocol	Vulnerability Category	Real-World Operational Impact	Reference Study
HTTP/TCP	Performance Bottleneck	Transport protocols misinterpret reconfiguration events as congestion triggering unnecessary back-off mechanisms and reducing throughput	Kushwaha& Mishra (2022) [4]; Malik et al. (2023) [12]
DHCP	Critical Security flaw	Enables DHCP starvation attacks via spoofed MAC addresses exhausting the available IP pool	Ramprasad et al. (2023) [5]
DHCP/IoT	Resource Constraint	Causes severe address allocation delays and increased latency in high-density loT deployments due to absence of cross-layer signaling	Ramprasad et al. (2023) [5]
DNS/HTTP	Privacy Vulnerability	Exposes user metadata through plaintext DNS queries; metadata leakage persists even with HTTPS	Murkomen (2024) [6]; Dawood et al (2024) [8]

Performance Bottlenecks in HTTP/TCP: Kushwaha and Mishra (2022) noted that cross-layer optimization addresses challenges such as QoS, mobility, handover, link adaptation, and energy constraints in wireless networks [4]. Similarly, Malik et al. (2023) highlighted that while strict layer boundaries in TCP/IP and OSI models provide excellent modularity, their performance is limited due to latency, energy consumption, and overhead [12]. These performance penalties are direct consequences of strict layer isolation, which prevents protocols from adapting to dynamic network conditions.

Critical Security Flaw in DHCP: Ramprasad et al. (2023) show that attackers can exploit DHCP address allocation mechanisms to exhaust available IP addresses. By generating requests with spoofed MAC addresses, the DHCP server—operating without access to link-layer authentication—treats each request as legitimate. Once the address pool is exhausted, legitimate clients cannot obtain network access. This vulnerability is not a mere implementation bug but a systemic consequence of strict layering that blinds application-layer services to link-layer context [5].

Resource Constraints in High-Density IoT Deployments: Ramprasad et al. (2023) further investigate DHCP performance in large-scale IoT deployments. Their simulation-based analysis reveals that traditional DHCP mechanisms cause severe address allocation delays as device density increases. The absence of cross-layer signaling means the DHCP server has no awareness of physical link conditions, forcing it to operate

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*

conservatively. Future IoT systems require more adaptive addressing strategies that incorporate lower-layer information [5].

Privacy Vulnerabilities in DNS and HTTP: Murkomen (2024) highlights privacy concerns in DNS and HTTP communications. DNS queries are traditionally transmitted in plaintext, exposing user behavior to network intermediaries. While HTTPS has addressed many concerns through TLS encryption, metadata leakage persists through DNS queries. Dawood et al. (2024) further analyze the impact of DNS over HTTPS on cybersecurity, noting that strict separation between application-layer protocols and lower-layer privacy mechanisms limits comprehensive privacy protection without modifying multiple layers simultaneously [6][8]. Collectively, the vulnerabilities documented in Table 1 demonstrate a consistent pattern: strict layering creates informational blind spots that degrade performance, enable security exploits, and expose user privacy. These findings motivate the exploration of Cross-Layer Design as a potential corrective paradigm, examined in the following section.

Cross-Layer Design Solutions

Cross-Layer Design (CLD) offers an adaptive approach that allows non-adjacent layers to exchange runtime parameters, potentially enabling joint optimization across the protocol stack and mitigating the vulnerabilities identified in the previous section.

Kushwaha and Mishra (2022) noted that cross-layer architectures have shown great performance improvement and may shape the future of wireless networks. They discussed standardization, complex architecture, and implementation issues for building cross-layer stacks, emphasizing that cross-layer optimization addresses challenges such as QoS, mobility, handover, link adaptation, energy constraints, and security [4].

Naeem et al. (2025) argued that the traditional OSI model is being replaced in ad hoc networks by a cross-layer approach due to dynamic topologies and poor radio conditions. Their work proposes a simpler, goal-oriented classification of cross-layer methods to enhance protocol efficiency and guide future research [11].

Malik et al. (2023) provided a parametric survey on cross-layer design for wireless sensor networks, concluding that while strict layer boundaries provide excellent modularity, performance is limited by latency, energy consumption, and overhead. Therefore, cross-layer designs have been proposed to achieve better performance [12].

Information Sharing Modes in CLD

Mustafa et al. (2024) conducted a comprehensive survey of cross-layer secure and energy-efficient frameworks for IoT networks, identifying three primary information sharing paradigms in CLD [13]:

1. Bottom-Up Signaling: Lower layers pass runtime metrics up the stack. For example, the Physical layer can notify TCP of wireless signal fluctuations. If packet loss occurs due to fading rather than congestion, TCP can avoid unnecessary back-off mechanisms, maintaining throughput.
2. Top-Down Control: Upper layers pass QoS requirements down the stack. The Application layer specifies latency boundaries, allowing lower layers to prioritize traffic accordingly.
3. Joint Optimization (Information Sharing Plane): A vertical management plane is established parallel to the protocol stack, enabling all layers to access and adjust operational parameters simultaneously in real time.

Mitigating Vulnerabilities via Cross-Layer Solutions

Performance Optimization: Bottom-up signaling enables application-layer protocols to adapt to channel states without waiting for higher-level detection. Ramprasad et al. (2023) show that dynamic DHCP implementations informed by link-layer metrics can significantly reduce address allocation latency in dense IoT networks [5]. Security Coordination: Breaking layer isolation enables unified security infrastructure. Feng et al. (2025) demonstrated that understanding cross-layer interactions is essential for identifying and mitigating off-path attacks. Their proposed countermeasures include protocol header consistency checks, anomaly detection at multiple layers, and coordinated defense mechanisms [9].

Architectural Trade-offs of CLD

Despite its benefits, CLD introduces significant trade-offs that must be carefully considered: Loss of Modularity: Cross-layer dependencies mean changes in one layer can cause unexpected effects across non-adjacent layers. Aggressive CLD can compromise modular independence, which enables incremental innovation and multi-vendor interoperability. This trade-off is particularly significant because modularity has been a key advantage of protocol layering since its inception.

Increased System Complexity: Unregulated information sharing creates interdependent parameter loops that are difficult to debug. Improper coupling between layers can lead to oscillations, instability, or even system failure under certain conditions. The complexity introduced by CLD may offset its performance benefits in some contexts.

Verification Challenges: Traditional network verification tools assume layer isolation. Extending these tools to handle cross-layer interactions remains an open research problem. Beckett and Gupta (2022) introduced

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*

KATRA, demonstrating that efficient verification of cross-layer interactions is possible but requires specialized algorithms [13].
Standardization Gaps: Standardization bodies have been slow to adopt CLD principles, leaving most solutions proprietary or application-specific. This lack of standardization hinders interoperability and widespread adoption.

Open Issues and Future Trends
The review identified several open challenges that warrant future investigation:
Next-Generation Transport: QUIC and HTTP/3: The deployment of QUIC and HTTP/3 represents a significant shift in transport layer architecture. Unlike TCP, QUIC integrates encryption, connection establishment, and multiplexing within a unified layer over UDP, reducing latency and mitigating head-of-line blocking. Bondar (2025) analyzed next-generation internet transport protocols, concluding that QUIC, WebTransport, and HTTP/3 offer substantial performance improvements over traditional TCP-based approaches [14]. However, open questions remain regarding attack surfaces, middlebox interaction, and integration with CLD frameworks in wireless environments. Eckert et al. (2022) provided an overview of technical developments for the future of networking, discussing post-IP networking and the drivers for reimagining IP for 5G/6G and beyond [15].
Artificial Intelligence for Cross-Layer Optimization: Gustafsson (2026) demonstrated that AI-driven cross-layer resource management using deep reinforcement learning (PPO) can effectively balance latency, throughput, and energy efficiency in 5G and beyond networks. Future research should explore the integration of federated learning, generative AI, and large language models for adaptive CLD frameworks [16]. Quantum-Safe and Secure CLD Frameworks: A significant barrier to CLD adoption is the absence of standardized frameworks that balance adaptive optimization with security compliance. Future research should develop security verification methodologies, create reference implementations, and engage standardization bodies like IETF and IEEE. Mustafa et al. (2024) emphasize that cloud and edge topologies require particular attention due to their high dynamics and multi-tenancy, highlighting the need for integrating blockchain, artificial intelligence, and quantum-safe cryptography in CLD frameworks [10].

Discussion
The findings synthesized from the literature reveal a recurring limitation in strict protocol layering. While historically effective for maintaining modularity and interoperability, strict layering can also function as an informational barrier that constrains performance and security in certain network contexts. This section interprets the findings, discusses their implications, and situates them within the broader research landscape. The comparative analysis confirms that while the OSI model offers pedagogical benefits through its seven-layer structure, TCP/IP has achieved global adoption due to its pragmatic four-layer design and scalability. However, TCP/IP's advantages come with limitations in dynamic environments. The encapsulation process, while fundamental to interoperability, also enforces informational isolation that prevents protocols from adapting to changing network conditions. Beckett and Gupta's (2022) introduction of KATRA demonstrates that efficient verification of network data planes is possible [13], but this does not address the fundamental rigidity of strict layering.
The finding that TCP/IP has achieved commercial dominance while OSI remains primarily pedagogical reflects a broader pattern in networking: architectures that emerge from practical deployment often succeed over those designed through formal standardization. This pattern has implications for CLD adoption, suggesting that cross-layer approaches are more likely to gain traction through demonstrated practical benefits than through formal standardization alone.
The documented vulnerabilities demonstrate a consistent pattern: strict layering creates informational blind spots that degrade performance, enable security exploits, and expose user privacy. Application-layer vulnerabilities such as DHCP starvation attacks are not merely implementation bugs but systemic weaknesses spawned by informational isolation between layers. Because the application layer is decoupled from low-level parameters like MAC address validity, it remains blind to spoofing tactics until resource exhaustion occurs. The DHCP server accepts allocation requests without verifying underlying MAC addresses precisely because strict layering prevents access to link-layer authentication information.
Similarly, cross-layer vulnerabilities in TCP/IP can be exploited by off-path attackers to manipulate network traffic. Feng et al. (2025) demonstrated that such vulnerabilities—including information leakage, desynchronization, semantic gaps, and identity spoofing—affect over 20% of popular websites and more than 89% of public Wi-Fi networks [9]. These findings indicate that enforcing rigid boundaries in softwarized, high-density environments may introduce significant performance and security challenges.
The finding that DHCP starvation attacks affect over 89% of public Wi-Fi networks is particularly concerning because it suggests that strict layering vulnerabilities are not confined to theoretical scenarios but have widespread practical impact. This emphasizes the urgency of developing cross-layer solutions that can mitigate these vulnerabilities. The analysis of Cross-Layer Design reveals that controlled information sharing between non-adjacent layers offers a promising evolutionary path. The three identified information sharing paradigms—bottom-up signaling, top-down control, and joint optimization—enable performance

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*

optimization and security coordination that strict layering cannot achieve. AI-driven CLD approaches represent an emerging direction for 5G/6G networks, as demonstrated by Gustafsson (2026) using deep reinforcement learning (PPO) to balance latency, throughput, and energy efficiency [16]. However, the study has also critically examined CLD's architectural trade-offs. Loss of modularity, increased system complexity, feedback loop instability, and verification challenges remain significant barriers to widespread adoption. The choice between strict layering and CLD is not binary but exists on a continuum, depending on environmental dynamics, performance requirements, security constraints, and deployment scale.

The trade-off between modularity and performance is particularly noteworthy. The modularity of strict layering has been a key factor in the Internet's success, enabling incremental innovation and multi-vendor interoperability. CLD approaches that sacrifice modularity may gain performance benefits but at the cost of these advantages. This suggests that hybrid approaches, which selectively apply CLD where benefits outweigh costs, may be more practical than wholesale replacement of strict layering.

Implications for Practice

The findings have several implications for network architects and security practitioners. First, organizations deploying high-density IoT environments should consider adaptive addressing strategies that incorporate lower-layer information, as traditional DHCP mechanisms cause severe performance degradation [5]. This may involve implementing dynamic DHCP systems that can adjust allocation strategies based on link-layer metrics. Second, security frameworks should be designed with cross-layer awareness to mitigate off-path attacks, as demonstrated by Feng et al. (2025) [9]. This suggests that security monitoring and response should consider information from multiple layers rather than operating within layer boundaries.

Third, the evolution toward QUIC and HTTP/3 requires careful attention to new attack surfaces and integration with CLD frameworks [14][15]. Organizations adopting these protocols should consider their cross-layer implications and potential vulnerabilities. Finally, the integration of AI-driven cross-layer optimization presents opportunities for dynamic resource management in 5G/6G networks [16]. Network operators should explore AI-driven approaches but remain mindful of the complexity and verification challenges they introduce.

This survey extends previous comparative studies by integrating architectural analysis, vulnerability assessment, and cross-layer solutions within a unified framework. Unlike Abdulmonim and Zainab (2024) and Janighorban and Kaveh (2025), who focused primarily on structural comparison [1][2], this study incorporates empirical evidence of vulnerabilities from Murkomen (2024) [6], Ramprasad et al. (2023) [5], and Feng et al. (2025) [9]. Unlike Kushwaha and Mishra (2022) and Naeem et al. (2025), who focused on wireless networks and ad hoc environments respectively [4][11], this survey provides a broader analysis applicable to IoT, cloud, and 5G/6G contexts. The contribution of this survey lies in its synthesis of these previously disconnected threads. By demonstrating that the vulnerabilities identified in application-layer studies are systemic consequences of strict layering, and that CLD offers potential remedies but with significant trade-offs, the survey provides a more complete picture than previous work.

Limitations

Several limitations of the discussion should be acknowledged. The interpretation of findings is constrained by the limitations of the reviewed literature, including heterogeneous experimental methodologies and limited production-scale evidence for certain approaches. The discussion of CLD trade-offs is necessarily general, as specific trade-offs depend on implementation details and deployment contexts. Finally, the pace of development in AI-driven networking means that some recent advances may not be fully reflected in the discussion.

Conclusion

This systematic review compared the OSI and TCP/IP architectures, analyzed application-layer security vulnerabilities, and evaluated Cross-Layer Design (CLD) as a potential evolutionary path. The findings confirm that strict protocol layering, while historically effective for modularity and interoperability, creates informational blind spots that degrade performance, enable attacks such as DHCP starvation, and expose user privacy. In response, CLD offers a promising alternative through bottom-up signaling, top-down control, and joint optimization, yet it introduces significant trade-offs including loss of modularity, increased system complexity, and verification challenges. The choice between strict layering and CLD is not absolute but depends on environmental dynamics, performance demands, and deployment scale. Future research should prioritize the integration of QUIC/HTTP3, AI-driven optimization, and quantum-safe cryptography within standardized CLD frameworks.

References

1. Abdulmonim DA, Zainab HM. Comparative study between the OSI model and the TCP/IP model: Architecture and protocols in computer networking systems. Int J Eng Comput Sci. 2024 Aug;13(8):26358-72. doi:10.6084/ijecs.v13i8.4880.

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*

2. Janighorban A, Kaveh N. Competitive analysis of OSI and TCP/IP models: Architecture and protocols in networking systems. Glob J Bus Integr Secur. 2025 Dec;8(1). Available from: https://www.gbis.ch/index.php/gbis/article/view/925
3. Khan HS, Atif SM. Layered defenses: Securing the OSI model through protocol management and advanced cyber strategies. J Eng Comput. 2025 Sep;10(2):1-18. doi:10.21621/ijec.20250102.01.
4. Kushwaha BS, Mishra PK. A survey on cross-layer optimization in wireless networks. J Adv Comput Netw. 2022;10:1-9.
5. Ramprasad R, Narayanan J, Balaji D, Kishor S. A DHCP based approach to IP address management and allocation in a network using VLSM. In: Proc 9th Int Conf Adv Comput Commun Syst (ICACCS). Coimbatore, India; 2023. p. 882-7. doi:10.1109/ICACCS57279.2023.10142094.
6. Murkomen T. Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey. GSC Adv Res Rev. 2024;18(3):234-64.
7. Cevallos-Salas D, Estrada-Jimenez J, Guaman DS. Application layer security for Internet communications: A comprehensive review, challenges, and future trends. Comput Electr Eng. 2024;118:109498. doi:10.1016/j.compeleceng.2024.109498.
8. Dawood M, Tu S, Xiao C, Haris M, Alasmary H, Nadeem MW. The impact of Domain Name Server (DNS) over Hypertext Transfer Protocol Secure (HTTPS) on cyber security: Limitations, challenges, and detection techniques. Comput Mater Continua. 2024;80(3):4513-42.
9. Feng X, Li Q, Sun K, Xu K, Wu J. Exploiting cross-layer vulnerabilities: Off-path attacks on the TCP/IP protocol suite. Commun ACM. 2025 Mar;68(3):48-59. doi:10.1145/3689819.
10. Mustafa R, Sarkar NI, Mohaghegh M, Pervez S. A cross-layer secure and energy-efficient framework for the Internet of Things: A comprehensive survey. Sensors. 2024;24(22):7209. doi:10.3390/s24227209.
11. Naeem M, Ameer S, Shahzad MS, Afzal A, Aslam A. Redesigning cross-layer architectures for performance optimization in ad hoc networks. J Curr Sign. 2025;8(1):1-12. Available from: https://currentsignjournal.com/index.php/JCS/index
12. Malik PS, Singh RP, Singh Y, Mittal N. Parametric survey on cross-layer design approach for wireless sensor networks. AIP Conf Proc. 2023 May;2535(1):020017. doi:10.1063/5.0125515.
13. Beckett R, Gupta A. KATRA: Realtime verification for multilayer networks. In: Proc 19th USENIX Symp Netw Syst Des Implement (NSDI). Renton, WA, USA; 2022 Apr. p. 617-34. Available from: https://www.usenix.org/conference/nsdi22/presentation/beckett
14. Bondar O. Analysis of next-generation internet transport protocols: QUIC, WebTransport, HTTP/3. Inf Technol Syst. 2025 Dec;6(6):52-63. doi:10.15407/intechsys.2025.06.052.
15. Eckert T, Han L, Li R, Westphal C. An overview of technical developments and advancements for the future of networking. ITU J Future Evol Technol. 2022 Dec;3(3):645-69. doi:10.52953/NFNJ2582.
16. Gustafsson BJ. Cross-layer resource management in 5G and beyond networks using PPO-based AI models. J Adv Artif Intell Res. 2026;5(1):1-15.

Received*: 25-04-2026 -* ***Accepted****: 23-06-2026 -* ***Published****: 29-06-2026*