The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 09 2025
PAGE NO. 88-93

Comparative Performance, Electromagnetic Compatibility, and Security Advancements in High-Speed Ethernet for Modern Distributed and Automotive Systems

Arvind Das
Department of Electrical and Computer Engineering, Horizon Institute of Technology, India

Received: 09 September 2025; **Accepted:** 20 September r 2025; **Published:** 30 September 2025

Abstract: High-speed Ethernet has evolved into a foundational communication backbone in modern distributed systems, from traditional high-performance computing environments to emerging automotive platforms. Research over the past two decades has examined Ethernet's latency characteristics, bandwidth scalability, electromagnetic compatibility constraints, energy considerations, and security limitations under increasing system complexity. Early comparative studies such as the evaluation of Ethernet versus Myrinet for message-passing interface (MPI) communication demonstrated the tension between low-latency interconnects and commodity-grade networking technologies, motivating Ethernet's evolution from 1 Gb/s to 10 Gb/s architectures (Mujumder & Rixner, 2004). Subsequent improvements in 10-Gigabit Ethernet—including TCP offload engines, optimized NIC designs, and commodity hardware acceleration—have significantly improved end-to-end throughput (Feng et al., 2005; Maeda et al., 2018). Yet electrical and optical domains present challenges, particularly under real-world electromagnetic interference (EMI), bandwidth limitations of copper-based physical layers, and the performance trade-offs between modulation formats (Kolahi & Soorty, 2011; Browning et al., 2011).

Parallel to these performance advancements, the rise of automotive Ethernet for advanced driver-assistance systems (ADAS), camera networks, and in-vehicle communication created new security and functional-safety concerns. The survey of automotive Ethernet vulnerabilities highlights risks such as spoofing, replay attacks, and protocol-layer compromise (Douss et al., 2023). Emerging countermeasures include TLS-based in-vehicle authentication (Zelle et al., 2017), privacy-preserving data exchange (Mi et al., 2018), and enhanced controller-area network (CAN-FD) security architectures (Woo et al., 2016; Lin & Sangiovanni-Vincentelli, 2012). Furthermore, automotive EMC standards such as CISPR-25:2021 outline measurement limits to safeguard sensitive on-board receivers, prompting system designers to adopt shielding solutions validated through simulation frameworks such as HyperLynx (Karim, 2025).

This article synthesizes the evolution of high-speed Ethernet through the lenses of performance, EMI resilience, hardware design, and cyber-security, offering a deep theoretical framing of how these factors collectively shape modern distributed and automotive communication networks. The extensive discussion identifies gaps, practical system design considerations, and a forward-looking perspective for high-speed and automotive Ethernet research.

Keywords: High-speed Ethernet, Automotive Ethernet, EMI, MPI performance, 10-Gigabit Ethernet, In-vehicle security, Hardware system design

INTRODUCTION:

Catabolism represents a complex of biochemical Ethernet has undergone profound evolution since its origins as a shared-medium networking technology. The emergence of gigabit-class and 10-gigabit-class Ethernet systems positioned it as not merely a data-center or enterprise communication option but as a core transport mechanism for distributed computation, high-performance scientific workloads, and automotive embedded systems. This transformation was driven by a combination of hardware innovations, protocol-level optimizations,

and industry pressures demanding higher throughput, lower latency, and trustworthy system behavior under complex operating environments.

Early comparative research, such as the study comparing Ethernet and Myrinet for MPI communication, illustrated the limitations of commodity Ethernet in supporting tightly coupled parallel computation workloads (Mujumder & Rixner, 2004). Myrinet's lightweight protocol stack and low-latency routing made it a strong candidate for supercomputing clusters, but the cost and market penetration of commodity Ethernet provided significant economic incentives for industry adoption. As application demands increased—high-fidelity simulation, real-time data processing, distributed rendering—the need to elevate Ethernet's performance became undeniable.

Gigabit Ethernet (GbE) provided a transitional technology enabling organizations to upgrade from Fast Ethernet while maintaining backward compatibility. Research showed, however, that electrical gigabit Ethernet links could suffer from bandwidth limitations stemming from channel properties and physical-layer impairments (Kolahi & Soorty, 2011). Meanwhile, optical links demonstrated distinct performance advantages, especially under advanced modulation schemes such as OFDM with optical injection (Browning et al., 2011), but optical Ethernet added cost and complexity.

The next significant leap came with 10-Gigabit Ethernet (10GbE). Evaluations of 10GbE TCP offload engines demonstrated considerable reductions in CPU utilization and improved throughput for distributed applications (Feng et al., 2005). As commodity hardware matured, further studies assessed end-to-end performance under practical system constraints such as NIC architecture, PCI-Express bandwidth, and OS-level handling of network stacks (Maeda et al., 2018).

Today, Ethernet is no longer confined to data-center or enterprise environments. Automotive Ethernet has become a key enabler for ADAS, autonomous driving sensors, camera networks, and zonal architectures. However, this has introduced new challenges including electromagnetic compatibility, cyber-security vulnerabilities, and functional-safety requirements. Surveys of in-vehicle protocols and vulnerabilities show that modern automotive Ethernet systems are prone to attacks affecting availability, confidentiality, and integrity (Douss et al., 2023). Standards such as CISPR-25:2021 emerged to ensure that in-vehicle networks remain resilient under high EMI conditions, and recent work highlights EMI-aware PCB design as a critical factor for ADAS camera modules (Karim, 2025).

Across all these domains, researchers have gradually shifted focus from raw throughput to nuanced, system-level concerns: electromagnetic behavior, multi-layer security, hardware efficiency, thermal effects, and environmental robustness. Recent work in hardware design emphasizes the importance of balancing high-speed signaling with power constraints, signal integrity, and manufacturability (Desai & Shah, 2025). Similarly, visualization frameworks help system designers understand signal interfaces and their interactions within complex hardware ecosystems (Bergquist, 2025).

Despite significant progress, there is still a need for integrated, cross-domain analysis. Most studies approach Ethernet performance, electromagnetic implications, and security concerns independently. Yet emerging applications—particularly autonomous vehicles and distributed AI systems—demand simultaneous optimization across performance, reliability, and trust. This article fills that gap by synthesizing research findings across computing, hardware design, and automotive security, offering a unified, theoretically rich understanding of high-speed Ethernet's present and future.

Methodology

This article adopts a qualitative synthesis methodology grounded strictly in the referenced works provided. The research process involves several structured stages to ensure methodological rigor, interpretive depth, and alignment with academic publishing standards.

First, all references were thoroughly reviewed and categorized into thematic clusters: (1) performance studies of gigabit and 10-gigabit Ethernet, (2) electromagnetic and physical-layer constraints, (3) optical modulation and high-speed signaling enhancements, (4) automotive Ethernet security and protocol-level vulnerabilities, (5) electromagnetic compatibility and measurement standards, and (6) hardware design and system-level implementation concerns. Categorization allows detailed comparison of the research across separate application domains while also identifying intersections.

Second, a longitudinal perspective was applied to track the evolution of Ethernet research over time. Early studies from the 2000s emphasized performance bottlenecks, low-latency communication, and distributed system efficiency, while recent research has shifted toward cyber-

security, electromagnetic behavior, and system-level engineering challenges. This chronological perspective helps identify how the problem space changed due to hardware trends, application demands, and emerging security threats.

Third, thematic cross-analysis was conducted by examining how findings from one domain influence or constrain another. For example, improvements in 10GbE NIC designs may enhance raw throughput but still lead to EMI vulnerability in automotive environments unless reinforced by shielding. Similarly, research on CAN-FD security informs potential automotive Ethernet security strategies by highlighting attack surfaces, response mechanisms, and protocol-level shortcomings.

Fourth, theoretical elaboration was used to expand upon the underlying implications of each study. Because the goal is not to summarize the references but to develop a deep theoretical narrative, each cited study was contextualized within broader concepts such as signal integrity theory, electromagnetic compatibility frameworks, distributed system communication models, and cryptographic protocol design. This facilitates richer academic interpretation aligned with research article expectations.

Finally, all insights were synthesized into a cohesive narrative structure—introduction, results, discussion, and conclusion—to produce a publication-ready scholarly article. Throughout the methodology, citations were strictly drawn from the provided reference list, and no external references or numerical data were introduced.

Results

The synthesis of research reveals several major findings regarding the progression, strengths, limitations, and emerging challenges of high-speed Ethernet technologies. These results span performance evaluation, electromagnetic behavior, security considerations, and system-level engineering factors.

One key finding is that Ethernet's early limitations for distributed computing were largely rooted in protocol stack inefficiencies and CPU overhead. Studies comparing Ethernet and Myrinet for MPI communication showed that Myrinet provided substantially lower latency and higher throughput due to its lightweight protocols and optimized network interface hardware (Mujumder & Rixner, 2004). Commodity Ethernet's reliance on TCP/IP and CPU-bound processing hindered its suitability for tightly coupled cluster workloads, resulting in performance gaps that motivated further technological advancement.

Research on electrical Gigabit Ethernet (Kolahi & Soorty, 2011) highlighted physical-layer bandwidth constraints that limited effective throughput even in nominally gigabit-class links. Copper cabling, electrical noise, and channel dispersion created performance bottlenecks that could only be addressed through improved cable characteristics, error handling mechanisms, or migration to optical media.

Optical signaling research introduced new avenues for enhancing Ethernet speed and reliability. Studies demonstrated that optical injection using monolithically integrated discrete mode lasers improved the performance of 10Gb/s OFDM signals (Browning et al., 2011). The findings emphasized that optical Ethernet systems could benefit from advanced modulation techniques to achieve higher spectral efficiency and enhanced resilience to signal degradation.

The introduction of 10-Gigabit Ethernet brought significant architectural changes. Performance evaluations of TCP offload engines (TOEs) showed reductions in CPU utilization and improved end-to-end throughput under high-speed workloads (Feng et al., 2005). Subsequent investigations into commodity 10GbE systems revealed that NIC architecture, interrupt moderation, PCI-Express bandwidth, and kernel-level optimizations strongly influenced real-world throughput (Maeda et al., 2018). These findings collectively illustrate that hardware-software co-optimization is essential for achieving the full potential of 10GbE bandwidth.

In the automotive domain, emerging research identifies Ethernet as a key enabler for ADAS and autonomous vehicle data flow. Surveys of automotive Ethernet vulnerabilities show that the protocol stack is susceptible to attacks including spoofing, message injection, replay attacks, and denial-of-service (Douss et al., 2023). Security enhancements investigated include deploying TLS within in-vehicle networks (Zelle et al., 2017) and developing robust CAN-FD-based architectures (Woo et al., 2016; Lin & Sangiovanni-Vincentelli, 2012). These findings underscore that while Ethernet offers superior bandwidth compared to CAN, its security and protocol-layer complexity introduce new risks.

Electromagnetic compatibility research further strengthens this conclusion. EMC standards such as CISPR-25:2021 mandate strict limits on radiated and conducted emissions in vehicles to protect radio

receivers, highlighting the need for robust shielding and EMI-resilient design. EMI-aware PCB design research shows that simulated validation tools—such as HyperLynx—can significantly improve shielding effectiveness in high-speed automotive camera systems (Karim, 2025).

Complementary research on hardware system design stresses the need to balance high-speed performance with power constraints, signal integrity, and manufacturability (Desai & Shah, 2025). Visualization tools for understanding signal interaction within hardware systems further contribute to system-level efficiency (Bergquist, 2025).

Overall, the results reveal an ecosystem where Ethernet performance improvements interact in complex ways with physical-layer characteristics, electromagnetic behavior, and security vulnerabilities. High-speed Ethernet's evolution has succeeded in addressing early performance limitations, but new domains such as automotive systems expose challenges that require holistic engineering solutions.

Discussion

The integrated findings from the referenced works highlight a multilayered evolution of Ethernet technology, reflecting not only improvements in throughput but also the increasing complexity of its operational environments. The discussion below elaborates on the deeper theoretical implications and cross-domain insights that emerge from the synthesis.

Early Ethernet's struggles in high-performance computing contain important lessons for present-day applications. The comparison with Myrinet (Mujumder & Rixner, 2004) demonstrated that low-latency communication is not achieved through raw bandwidth alone but through careful optimization of protocol overhead, hardware offloading, and minimal context switching. These same principles reappear in modern 10GbE systems, where TCP offload engines (Feng et al., 2005) and optimized NIC architectures (Maeda et al., 2018) serve analogous roles to Myrinet's custom hardware pathways. Thus, Ethernet's evolution can be interpreted as a convergence toward design principles long established in specialized HPC interconnects.

Electrical Gigabit Ethernet's bandwidth limitations (Kolahi & Soorty, 2011) reveal persistent challenges in copper-based media. Unlike optical channels—where dispersion and nonlinearity are dominant factors—electrical channels suffer from crosstalk, attenuation, and EMI susceptibility. These constraints become especially pronounced in automotive environments where cable routing is tightly constrained, temperature varies significantly, and power distribution networks introduce noise. This reinforces the need for system-wide EMC considerations, as codified in CISPR-25:2021. The standard's emphasis on protecting radio receivers highlights a broader engineering reality: high-speed signaling must coexist with sensitive analog systems in confined spaces.

Optical injection research (Browning et al., 2011) further clarifies that future high-speed Ethernet may benefit from hybrid electro-optical architectures, especially in domains requiring extreme bandwidth, low noise, and long-distance signaling. Optical Ethernet's superior signal integrity suggests potential applications in next-generation automotive backbones, although cost and environmental robustness remain barriers.

The automotive security findings (Douss et al., 2023) present a fundamental shift in Ethernet's role. Historically, Ethernet was considered a best-effort, insecure medium used for non-critical communication. In vehicles, however, Ethernet becomes responsible for safety-critical functions such as camera data transmission, LiDAR communication, and radar fusion. This introduces severe consequences for packet manipulation or denial-of-service attacks. Consequently, security architectures such as TLS-based in-vehicle authentication (Zelle et al., 2017) and CAN-FD-based enhancements (Woo et al., 2016) represent not optional add-ons but essential safety components.

The cross-domain synergy between electromagnetic compatibility (Karim, 2025) and security emerges as a noteworthy theme. EMI can induce frame errors, desynchronization, or packet loss, which may resemble intentional tampering or degrade the performance of security protocols relying on timing assumptions. Therefore, EMI-resilient design indirectly improves security by reducing the likelihood of misinterpreting environmental noise as adversarial activity.

Theoretical analysis of hardware system design (Desai & Shah, 2025) and system-interface visualizations (Bergquist, 2025) illustrates that achieving reliable high-speed Ethernet requires multi-layer co-design. Signal integrity, thermal behavior, and power constraints must be balanced with protocol complexity, security requirements, and real-time performance demands. The holistic view offered by these references implies that future Ethernet systems—whether automotive or data-center

oriented—will require collaborative engineering spanning electrical design, embedded software, physical-layer modeling, and security analysis.

Another important implication is the shift toward commodity hardware. Early research (Maeda et al., 2018) emphasized that 10GbE performance can be achieved on commodity systems with appropriate optimization. This democratization of high-speed networking has contributed to its adoption in automotive systems. Yet commodity hardware also introduces challenges including inconsistent EMC performance, unpredictable thermal characteristics, and varied security postures. Thus, achieving reliable and secure operation in demanding environments requires careful validation, simulation, and shielding strategies, as exemplified by the HyperLynx-validated shielding approach (Karim, 2025).

Taken together, these insights underscore that Ethernet's future success in high-speed and safety-critical domains hinges not merely on increasing data rate but on integrating performance, EMI resilience, and security into a unified architecture. The increasing convergence of distributed computing, embedded systems, and automotive networks suggests that Ethernet will remain a central communication technology—but only if addressed through multidisciplinary engineering frameworks.

Conclusion

The evolution of Ethernet from a basic networking technology to a robust backbone for high-performance computing and automotive communication has been shaped by advancements across hardware, software, and system-level design. The research synthesis reveals several themes: the importance of minimizing protocol overhead for low-latency communication, the persistent challenges of electrical-layer bandwidth limitations, the promise of optical modulation for high-speed links, and the critical need for enhanced security and electromagnetic compatibility in automotive applications.

High-speed Ethernet's future will depend on balancing throughput with system integrity, environmental resilience, and cyber-security. Automotive Ethernet's emergence highlights the urgency of addressing these concerns, as safety-critical applications demand both reliability and trustworthiness. EMI-aware design, shielding validation, robust security protocols, and hardware-software co-optimization will be essential components of next-generation Ethernet systems.

By integrating findings across disparate research domains, this article emphasizes that the next era of Ethernet innovation must pursue multidisciplinary collaboration that unites performance engineering, cyber-security analysis, and electromagnetic compatibility. Such integrated approaches will be essential as Ethernet continues expanding into autonomous vehicles, industrial automation, distributed AI platforms, and emerging edge-computing environments.

References

1. Achar, R., Derat, B., Khazaka, R., Koul, S., & Frazeir, K. (2024). Four New Distinguished Lecturers for 2024–2025. IEEE Electromagnetic Compatibility Magazine, 12(4), 87-90.
2. Abdul Salam Abdul Karim. (2025). Thermal-Aware Functional Safety Analysis of Automotive LED Drivers: FMEDA for Junction Temperature-Induced Failures. International Journal of Computational and Experimental Science and Engineering, 11(3).
3. Bergquist, M. (2025). Visualizing Signal Interfaces For Machine Simulation.
4. Browning, C., Shi, K., Latkowski, S., Anandarajah, P., Smyth, F., Cardiff, B., Phelan, R., & Barry, L. (2011). Performance improvement of 10Gb/s direct modulation OFDM by optical injection using monolithically integrated discrete mode lasers.
5. Desai, K., & Shah, K. (2025). Mastering High-speed and Low Power Hardware System Design.
6. Douss, A. B. C., Abassi, R., & Sauveron, D. (2023). State-of-the-art survey of in-vehicle protocols and automotive Ethernet security and vulnerabilities. Mathematical Biosciences and Engineering, 20(9), 17057-17095.
7. Feng, W. C., Balaji, P., Baron, C., Bhuyan, N. L., & Panda, D. K. (2005). Performance characterization of a 10-Gigabit Ethernet TOE.
8. International Electrotechnical Commission. (2021). CISPR 25:2021 – Vehicles, boats, and internal combustion engines: Radio disturbance characteristics – Limits and methods of measurement for the protection of on-board receivers.
9. Karim, A. S. A. (2025). Mitigating Electromagnetic Interference in 10G Automotive Ethernet: HyperLynx-validated shielding for camera PCB design in ADAS lighting control. International Journal of Applied Mathematics, 38(2s), 1257-

1268.

10. Kolahi, S. S., & Soorty, B. K. (2011). Bandwidth Limitation of Electrical Gigabit Ethernet.
11. Lee, G., Kwon, Y., Cho, K., Seok, W., & Kwak, J. (2008). Performance Evaluation of Gigabit Ethernet Interfaces.
12. Lin, C.-W., & Sangiovanni-Vincentelli, A. (2012). Cyber-Security for the Controller Area Network (CAN) Communication Protocol.
13. Maeda, K., Norimatsu, T., Kohmu, N., Nishimura, K., & Fukasaku, I. (2018). End-to-end performance of 10-gigabit Ethernet on commodity systems.
14. Mi, B., Huang, D., & Wan, S. (2018). NTRU implementation of efficient privacy-preserving location-based querying in VANET.
15. Mujumder, S., & Rixner, S. (2004). Comparing Ethernet and Myrinet for MPI communication.
16. Woo, S., Jo, H. J., Kim, I. S., & Lee, D. H. (2016). A Practical Security Architecture for In-Vehicle CAN-FD.
17. Zelle, D., Krauß, C., Strauß, H., & Schmidt, K. (2017). On Using TLS to Secure In-Vehicle Networks.