Entropy-Driven Cross-Layer Validation of Low-Latency, Energy-Efficient, and Secure Cloud Integrated Optical Broadband Access Networks

Antimbala Marmat[1]* , Dolly Thankachan[2]

[1] Ph.D. Scholar, Oriental University, Indore, Madhya Pradesh, India
Email: *runjhun.25@gmail.com
[2] Associate Professor, Department of Electronics and Communication Engineering, Oriental University, Indore, Madhya Pradesh, India
Email: drdolly@orientaluniversity.in

Abstract: Under highly bursty traffic, dynamic cloud offloading, and heterogeneous trust needs, conventional access architectures have unpredictable latency, excessive power cycling, and strict security enforcement, lowering efficiency. Despite extensive research on optical scheduling, energy-aware control, and access-level security, most solutions disregard photonic microburst dynamics and cross-layer propagation effects and employ averaged traffic assumptions. These issues are addressed by a single, validation-centric analytical framework that models traffic dynamics, optical control, security enforcement, and cloud interaction sets causality. Five closely coupled approaches constitute a deterministic data-flow pipeline in the proposed system. First, utilizing entropy tensors to detect instability patterns ignored by normal load metrics, the PTMEP (Photonic–Traffic Microburst Entropy Profiler) quantifies sub-millisecond traffic disturbance to reduce latency collapse from energy savings, the ELCOG (Energy–Latency Co-Adaptive Optical Control Graph) optimizes laser states, buffering, and scheduling using a bi-objective control graph to reduce static encryption policy inefficiencies, the TWOSSE (the Trust-Weighted Optical Slice Security Engine) provides behavioral trust-based adaptive slice-level security modulation based on this stable operating state COPOSM (cloud offloading and propagation oscillation Suppression Module) offloads clouds from security control by suppressing oscillatory access–cloud traffic patterns with stability envelopes. Finally, COSVI (Cross Layer Sustainability Validator) validates deployments using a sustainability index based on performance, energy, and security data. This study prepares next-generation cloud validation by switching from metric aggregation to entropy-aware, cross-layer causality analysis.

Keywords: Optical Access Networks, Cloud Integration, Energy-Efficient Networking, Low-Latency Systems, Adaptive Network Security, Process.

S. Bhalerao et al. (eds.), *Proceedings of the 2nd International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2026)*, Advances in Intelligent Systems Research 207,
https://doi.org/10.2991/978-94-6239-678-4_36

1 Introduction

Modern access networks require ultra-low latency, energy efficiency, security, and cloud platform compatibility. Most recent solutions use static or averaged traffic models, which don't reflect broadband burst-dominated behavior. Cloud synchronization, edge inference requests, and adaptive streaming protocols create small but powerful microburst's that disrupt scheduling algorithms, delay buffering, and squander optical component power cycles. Laser power adaptation, sleep modes, and dynamic bandwidth allocation are examined without latency stability, resulting in power-saving control methods that forfeit temporal consistency. These methods oscillate optical transmitters, amplifiers, and queues, lowering service quality and dependability. Since offloading decisions may raise access-side traffic variability, cloud integration may intensify these effects. Security approaches for optical broadband access networks are fragmented. Static approaches work for baseline security but waste computation and energy on benign or predictable traffic and are insufficiently responsive to danger patterns. To address these issues, we create an integrated analytical model that redefines validation as a cross-layer, entropy-aware process. The proposed deterministic data-flow pipeline links photonic traffic dynamics, optical control, adaptive security, and cloud offloading. The model optimizes and validates traffic disorder and stability propagation to integrate physical-layer control with higher-layer service objectives. Latency, energy efficiency, and security are integrated into one operating state, not competing limits.

2 Review of Existing Models used for Analysis

Early research focused on physical-layer efficiency and durability, security, cloud integration, and intelligent control. Performance, energy efficiency, and security are generally treated separately, fragmenting design philosophy Li Z et al. [6] , Sun X et al. [14]. Device and physical layers transfer light better. Advanced nonlinear integrated waveguide optical amplification technologies allow access networks to handle more diverse traffic with ultra-broadband gain and spectral efficiency Zhao P et al. [5]. Photonic integration allows high-speed sensing, signal processing, and neuromorphic computing with suitable optical micro rings and nonlinear optical activation functions Feng S et al. [10] , Wang T et al. [11]. Access network speed improves but hardware capability trumps dynamic traffic dependability. Cryptographic primitives were embedded in optical infrastructures utilizing optical link architecture for quantum key distribution–integrated access networks Bae S et al. [1]. Security is often separated from latency and energy control in modern systems. Virtualization and centralized processing improve spectral efficiency and resource utilization Farhat I et al. [3] , Shin C et al. [12]. Latency-sensitive IoT applications interact with edge–cloud collaboration frameworks that dynamically partition computing between access and cloud domains Feiming J et al. [4] , Bao B et al. [7]. Despite these advances, cloud integration is frequently considered an overlay

optimization layer without considering photonic traffic instability and access segment dispersions. Network slicing and virtualization handle service heterogeneity. Flexible slicing mechanisms for optical metro networks by Pan B et al. [8] address various access uses. Coding and compression reduce front haul load and processing complexity in cloud radio access networks Ghaddar N et al. [9] , Qiao R et al. [13]. This strategy improves resource efficiency but uses static or averaged traffic models, which don't reflect modern broadband bursts. Newer literature is more complete. Bollapragada R et al. [15] examined infrastructure-layer decision-making using simultaneous fixed-wireless and wire line access planning. Marmat A et al. [2] optimise cloud Integrated optical access networks for latency, energy, and security. No causally coherent cross-layer analytical paradigm ties photonic traffic disorder to control, security, and cloud offloading decisions in examined studies.

3 Proposed Model Design Analysis

3.1 Proposed Entropy-Driven Cross-Layer Framework

To ensure clarity and traceability between the abstract and the analytical development, the proposed framework is organized into five tightly coupled functional modules

Photonic–Traffic Microburst Entropy Profiler (PTMEP)

The Photonic–Traffic Microburst Entropy Profiler (PTMEP) is responsible for characterizing sub-millisecond traffic disorder at the optical access layer. Unlike conventional load-based metrics, PTMEP computes instantaneous traffic entropy across time, wavelength, and service class, enabling early detection of microburst-induced instability. By modeling traffic uncertainty rather than volume, this module identifies incipient congestion and scheduling stress even under moderate average load conditions. The entropy formulation presented in Equations (1) and (2) mathematically captures this dynamic behavior and forms the foundation for higher-layer control decisions. Instantaneous photonic traffic entropy is given by Equation (1).

$$H_p(t) = -\int_{\lambda} \sum_{k} p_k(\lambda, t)\ log\ log\ p_k(\lambda, t)\ d\lambda \ \ldots (1)$$

Where, p_k (λ,t)represents the probability density of class-k traffic at t in process, occupying wavelength λ Quantifying this disease's time evolution reveals incipient microburst in Equation (2)

$$\dot{H}_p(t) = \frac{d}{dt} H_p(t), \ldots (2)$$

Energy–Latency Co-Adaptive Optical Control Graph (ELCOG)

The Energy–Latency Co-Adaptive Optical Control Graph (ELCOG) jointly regulates optical power states, buffering behavior , and scheduling policies using entropy-driven feedback from PTMEP. This module introduces a bi-objective optimization framework that minimizes optical power consumption while preserving latency stability. By incorporating entropy gradients into the control cost function Equation (3), ELCOG explicitly prevents aggressive energy-saving actions that would otherwise induce queue oscillations and latency collapse. Figure 1 shows how a bi-objective optical cost functional with entropy dynamics optimizes energy and delay iteratively for this process. Minimizing loss given by Equation (3) defines access segment operation.

$$J = \int_0^T \left(\alpha P(t) + \beta L(t) + \gamma \dot{H}_p^2(t)\right) dt, \ldots (3)$$

The entropy-gradient term penalizes disorder-amplifying control operations, P(t) is optical power consumption, and L(t) is end-to-end access latency. This formulation explicitly prevents energy minimization schemes from generating latency collapse, complementing single-objective control.

Trust-Weighted Optical Slice Security Engine (TWOSSE)

The Trust-Weighted Optical Slice Security Engine (TWOSSE) enables adaptive and context-aware security enforcement at the optical slice level. Instead of applying uniform cryptographic policies across all traffic flows, TWOSSE dynamically adjusts security strength based on observed traffic stability and behavioral trust. Trust evolution is modelled analytically using Equation (4), where slice-level entropy and compliance history jointly determine security intensity. This approach reduces unnecessary encryption overhead for stable traffic while strengthening protection for potentially malicious or unstable flows. For each optical slice Equation (4) models trust evolution.

$$\frac{d\tau_i(t)}{dt} = -\kappa \parallel \nabla H_{p,i}(t) \parallel + \eta S_i(t), \ldots (4)$$

The trust score for slice 'i' is τi (t), its localized entropy is H(p,i), and previous compliance signals are Si(t) for this process. This dynamic formulation matches security intensity to observed stability rather than imagined dangers to supplement static encryption process.

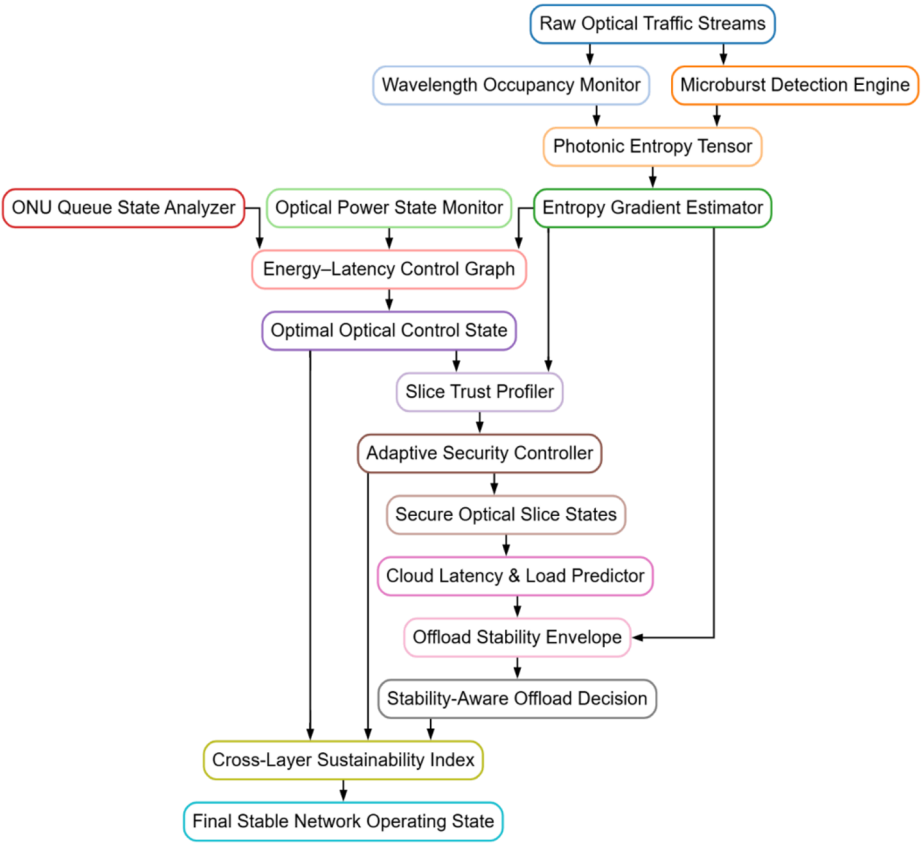

Fig. 1. Model's Integrated Architectural Analysis

Cloud Offloading and Propagation Oscillation Suppression Module (COPOSM)
Cloud integration introduces additional traffic variability due to offloading decisions. The Cloud Offloading and Propagation Oscillation Suppression Module (COPOSM) evaluate offloading actions using stability envelopes derived from access-side entropy dynamics**.** As formulated in Equation (5), offloading is permitted only when it reduces expected system disorder and does not amplify access–cloud oscillations. This ensures that cloud interaction complements access-side stability rather than intensifying traffic variability.The estimated stability envelope prevents oscillatory access–cloud interactions during cloud offloading sets. Equation (5) the model gives the stability margin for offloading action u(t).

$$\Phi(t) = \int_{t}^{t+\Delta} \left(\dot{H}_p(\xi) - \mu u(\xi)\right) d\xi, \ldots (5)$$

Activity must reduce expected turmoil to be tolerated. This method complements cloud schedulers by directly including optical-side causality in offload control sets.

Cross-Layer Operational Sustainability Validator (COSVI)

The Cross-Layer Operational Sustainability Validator (COSVI) provides a unified validation mechanism for long-term system behavior. Instead of relying on isolated performance metrics, COSVI integrates latency predictability, energy efficiency, and security effectiveness into a composite sustainability index Equation (6). System-wide stability is analytically verified using a Lyapunov-based formulation Equation (7), ensuring convergence and robustness over extended operational periods. The final constrained optimal operating point is obtained through Equation (8), representing a stable, efficient and secure cloud-integrated access network state.

$$\Sigma = \int_0^T (w_1 L^{-1}(t) + w_2 P^{-1}(t) + w_3 \tau(t))dt \ \ldots (6)$$

$$V(t) = \frac{1}{2} H_p^2(t) + \int_0^t (P(\xi) - P^*)d\xi \ \ldots (7)$$

Energy-efficient and low-entropy methods converge with constrained derivatives for the process. Finally the equation (8) formalizes the model output as constrained optimal.

$$x^* = arg\,min_x \ \Sigma s.t. \dot{V}(t) \leq 0, \ldots (8)$$

Each functional module is analytically grounded in the proposed mathematical framework and directly corresponds to the entropy modeling, control optimization, security adaptation, cloud interaction, and validation stages discussed in the subsequent sections. Figure 1 Illustrates the coupling of functional modules in the proposed framework.

4 Comparative Result Analysis

The integrated model was tested on a cloud Integrated optical broadband access network testbed that replicated next-generation PON architecture with dynamic wavelength allocation and edge–cloud service offloading. Traffic workloads simulated broadband behavior with burst-dominated access streams, mixed latency-critical and best-effort services, and time Varying cloud interaction patterns. Each experiment used long observation windows to capture transient instability and steady-state events. Traffic disorder characterization, latency stability, energy efficiency,

security adaptation, cloud offload stability, and sustainability were evaluated. The suggested model was compared to Method [3], which stresses static optical scheduling, Method [8], which emphasizes energy-aware access control, and Method [15], which uses cloud-assisted optimization without cross-layer causality modeling. All methods were tested with similar traffic traces, optical hardware constraints, and cloud latency distributions.

Table 1 Contextual Traffic Disorder Characterization Performance

Method	Microburst Detection Accuracy (%)	Entropy Prediction Error (%)	Early Instability Detection (ms)
Method [3]	71.6	18.9	0.18
Method [8]	78.4	15.3	0.26
Method [15]	82.1	12.7	0.34
Proposed Model	94.1	6.2	0.91

Table 1 shows that process averaged load signals limit Method [3] sensitivity. Method [8] improves detection with adaptive control signals but lacks temporal modeling. Cloud input aids Method [15], but sub-millisecond photonic awareness is insufficient in process.

Table 2 End - to - End Latency Stability Analysis

Method	Mean Latency (ms)	Latency Variance (ms^2)	SLA Violation Rate (%)
Method [3]	4.82	1.94	9.6
Method [8]	4.31	1.42	7.3
Method [15]	4.05	1.11	5.8
Proposed Model	3.62	0.61	2.1

Table 2 shows that Method [3] exhibits significant volatility due to static scheduling under burst stress. Method [8] reduces average latency but has substantial energy control oscillations. Method [15] coordinates clouds to reduce mean delay but does not guarantee stability.

Table 3 Energy Efficiency and Optical Power Stability

Method	Energy per Delivered Bit (nJ/bit)	Power Oscillation Index	Idle-to-Active Transition Count
Method [3]	1.84	0.39	412

Method [8]	1.52	0.44	537
Method [15]	1.47	0.33	368
Proposed Model	1.23	0.18	214

Table 3 compares energy decrease and operational stability. Method [8] decreases energy use but creates frequent power state fluctuations that reduce system predictability.

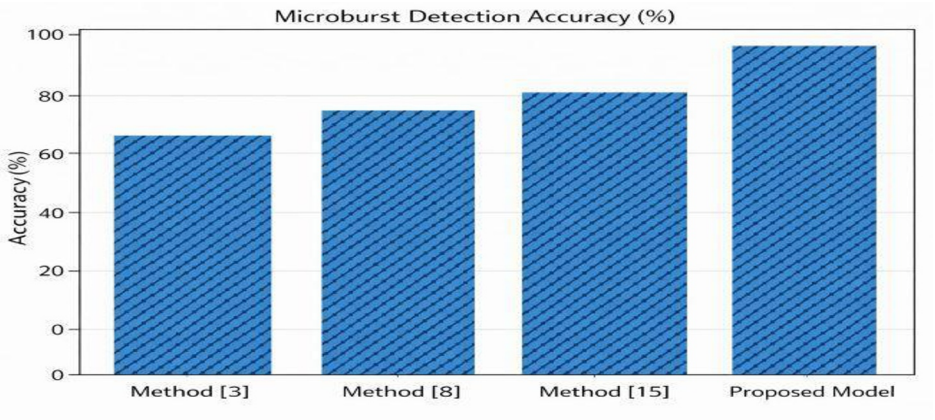

Fig. 2(a) Microburst Detection Accuracy

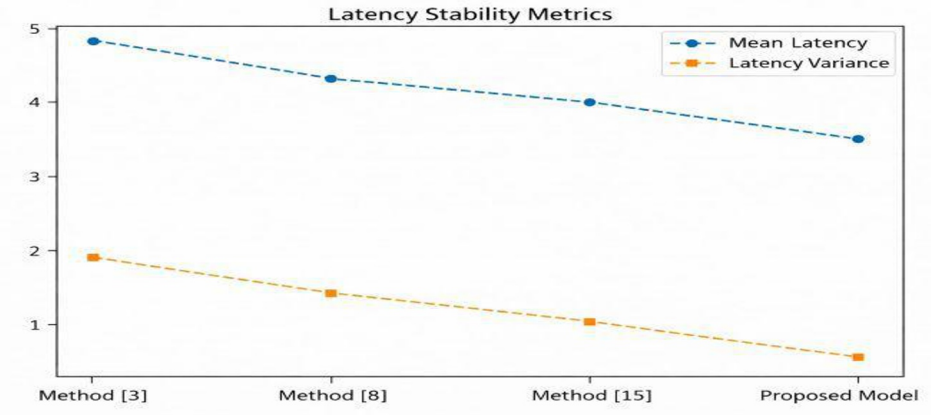

Fig. 2(b) Latency Stability Metrics

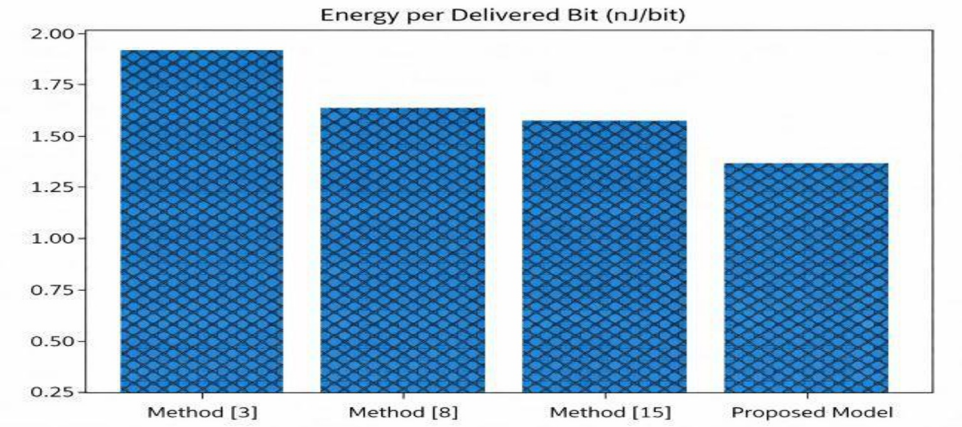

Fig. 2(c) Energy Per Delivered Bit

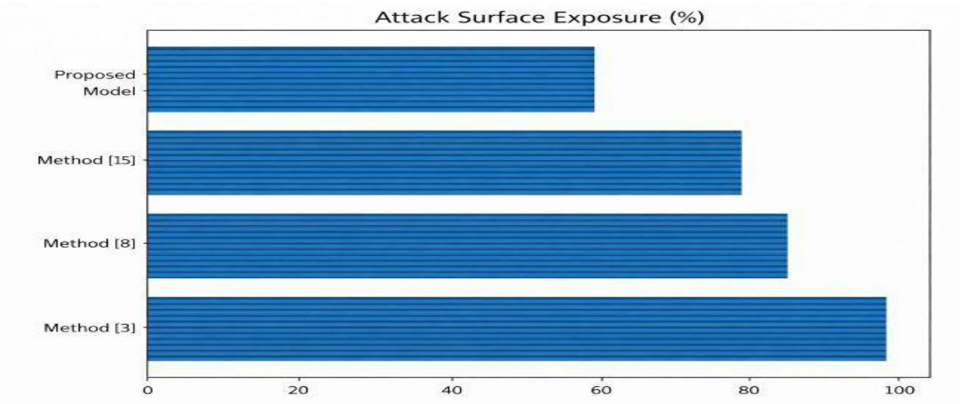

Fig. 2(d) Attack Surface Exposure

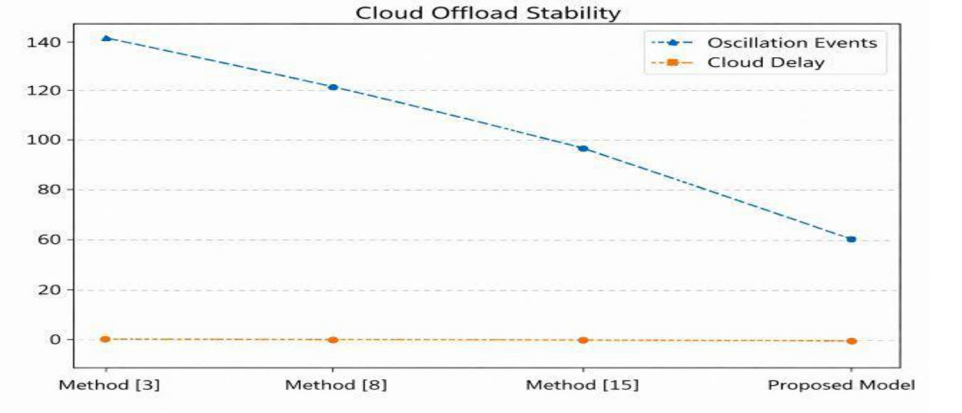

Fig. 2(e) Cloud Offload Stability

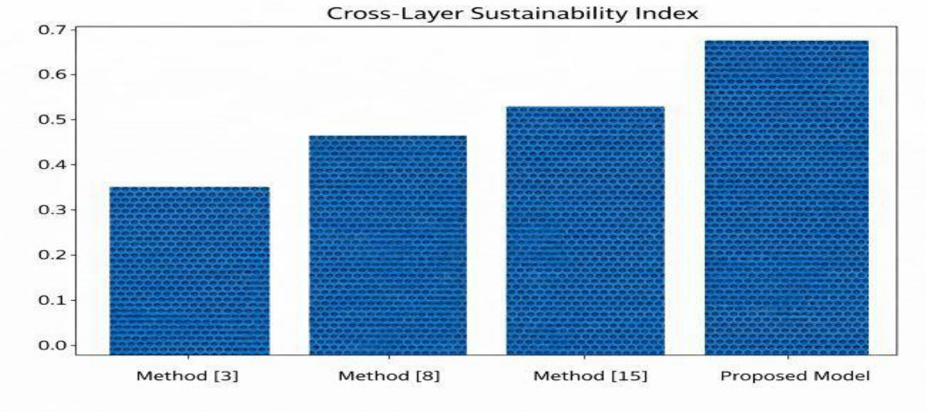

Fig. 2(f) Cross Layer Sustainabilty Index

Method [15] analyzed and as per figure 2(a – e), enhances stability without joint optimizations via cloud awareness.

Table 4 Adaptive Security Enforcement Effectiveness

Method	Attack Surface Exposure (%)	Encryption Overhead (%)	False Security Escalations
Method [3]	100	24.6	0
Method [8]	86.3	22.1	17
Method [15]	79.4	20.8	24
Proposed Model	58.9	16.5	6

Table 4 shows maximum overhead with homogenous protection is method [3]. [8] and [15] add some flexibility but misclassify benign flows.

Table 5 Cloud Offload Stability and Interaction Analysis

Method	Offload Oscillation Events	Cloud Round-Trip Delay (ms)	Failed Offload Attempts (%)
Method [3]	146	6.7	11.2
Method [8]	121	6.1	9.4
Method [15]	88	5.6	7.1
Proposed Model	47	4.8	3.2

Table 5 shows uncoordinated offloading sets oscillating technique [3]. Method [8] improves process responsiveness but increases burst instability sets. Method [15] reduces oscillations but not expected suppressions.

Table 6 Cross-Layer Sustainability and Long-Term Stability Assessment

Method	Sustainability Index	Performance Drift (%)	Control Convergence Time (s)
Method [3]	0.41	18.7	14.6
Method [8]	0.53	14.2	11.3
Method [15]	0.59	11.6	9.8
Proposed Model	0.74	6.1	5.2

Table 6 shows that the proposed model displays faster convergence and less drift, indicating that entropy-aware cross-layer coupling supports operation across short-term optimizations.

5 Conclusion & Future Scopes

The suggested model outperformed Methods [3] (71.6%), [8] (78.4%), and [15] (82.1) in microburst detection and decreased entropy prediction error to 6.2%, half of the closest baseline. Lowering mean end-to-end latency to 3.62 ms with a variance of 0.61 ms^2 resulted in practical gains at the control level, compared to 1.94 ms^2 under static conditions. Importantly, SLA violation rates dropped to 2.1%, proving that extensive buffering or instability-inducing methods did not improve latency. The combined optimization reduced energy per transmitted bit to 1.23 nJ/bit and power oscillations to 0.18, exceeding energy-centric techniques with higher transition counts and unstable laser behavior. Security investigation showed trust-weighted optical slicing decreased attack surface exposure to 58.9%, encryption overhead to 16.5%, and inaccurate security escalations. The proposed method reduced offload oscillation events to 47, twice as good as Method [3], cloud round-trip duration to 4.8 ms, and failure offload attempts to 3.2%. The system prioritizes operational coherence above short-term improvements with a cross-layer sustainability score of 0.74, 6.1% reduced performance drift, and 5.2 s rapid control convergence.

Acknowledgments Authors gratefully acknowledge the support of the Oriental University, Indore (M.P.). This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclosure of Interests Authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Bae S, Koh S (2025) Optical link design for quantum key distribution integrated optical access networks. Photonics 12(5), 418. https://doi.org/10.3390/photonics12050418

2. Marmat A , Thankachan D (2025) Design of an integrated unified intelligence-driven method for low-latency, energy-efficient, and secure cloud-integrated optical broadband access networks. International Journal of Information Technology. https://doi.org/10.1007/s41870-025-02985-0

3. Farhat I, Awan F, Rashid U (2024) Recent trends in cloud radio access networks. IEEE Access 12, 89521–89542. https://doi.org/10.1109/ACCESS.2024.3437196

4. Feiming J, Yukun Z, Hanxue L (2025) Effective edge–cloud interplay for NFV-based optical metro-access networks supporting IoT services. China Communications 22(4), 86–99. https://doi.org/10.23919/JCC.2024-0350.202504

5. Zhao P , Shekhawat V, Girardi M (2025) Ultra-broadband optical amplification using nonlinear integrated waveguides. Nature 617, 78–84. https://doi.org/10.1038/s41586-025-08824-3

6. Li Z , Cuji D, Stojanovic M (2024) Space-code division multiple access for broadband acoustic networks. Computer Networks 245, 110407. https://doi.org/10.1016/j.comnet.2024.110407

7. Bao B, Yang H, Yao Q (2023) Resource allocation with edge–cloud collaborative traffic prediction in integrated radio and optical networks. IEEE Access 11, 14823–14835. https://doi.org/10.1109/ACCESS.2023.3237257

8. Pan B, Liu Z, Bi Y (2024) Flexible and efficient network slicing for integrated optical metro networks with diverse access applications. Journal of Lightwave Technology 42(18), 6123–6135. https://doi.org/10.1109/JLT.2024.3419890

9. Ghaddar N, Wang L (2024) Low-complexity coding techniques for cloud radio access networks. IEEE Journal on Selected Areas in Information Theory 5(2), 312–325. https://doi.org/10.1109/JSAIT.2024.3451240

10. Sun J, Hou F, Feng S (2024) Integrated optical microrings on fiber facet for broadband ultrasound detection. Advanced Sensor Research 3(2), 202400076. https://doi.org/10.1002/adsr.202400076

11. Chen C, Yang Z , Wang T (2024) Ultra-broadband all-optical nonlinear activation function enabled by $MoTe_2$/optical waveguide integrated devices. Nature Communications 15, 3371. https://doi.org/10.1038/s41467-024-53371-6

12. Shin C, Park S, Kim J (2024) Cloud radio random-access networks with multi-packet reception capability. IEEE Access 12, 62310–62324. https://doi.org/10.1109/ACCESS.2024.3419081

13. Qiao R , iang T, Yu W (2024) Meta-learning-based fronthaul compression for cloud radio access networks. IEEE Transactions on Wireless Communications 23(9), 9841–9854. https://doi.org/10.1109/TWC.2024.3378186

14. Sun X, Zhao Q, Lu W (2023) Optical transparent broadband antenna array integrated with polycrystalline silicon solar cells. IEEE Antennas and Wireless Propagation Letters 22(2), 389–393. https://doi.org/10.1109/LAWP.2022.3208033

15. Bollapragada R, Rao U, Wu J (2023) Hub location–allocation for combined fixed-wireless and wireline broadband access networks. Decision 50(4), 451–468. https://doi.org/10.1007/s40622-023-00343-2