Orchestrating Security Measures for Legacy Devices in Far-Edge Computing Scenarios*

Gaetano Francesco Pittalà[1], Gianluca Davoli[1], Davide Borsatti[1], and Walter Cerroni[1]

University of Bologna, Bologna, Emilia Romagna, Italia
francesco.pittala/gianluca.davoli/davide.borsatti/walter.cerroni@unibo.it

Abstract

The study assesses the effects of different security enforcement levels on overall service orchestration performance through a series of simulations carried out in a 10-node edge computing scenario. The results show that static, one-size-fits-all approaches frequently degrade performance, especially on constrained nodes, and highlight the trade-offs between confidentiality mechanisms and service provisioning efficiency. On the other hand, by strategically modifying protection levels in response to new threats, the suggested adaptive orchestration approach strikes a more effective balance, optimizing both security and operational efficiency. The framework's versatility makes it a viable option for protecting diverse and resource-constrained edge environments.

-keywords: physical layer security, edge computing, service provisioning

1 Introduction

The growth of Edge Computing (EC) has enabled deploying services closer to end users, reducing latency and improving responsiveness. However, many far-edge nodes rely on legacy or resource-limited hardware lacking modern security features, making it difficult to maintain confidentiality, integrity, and availability across such heterogeneous infrastructures. Physical Layer Security (PLS) offers a lightweight confidentiality solution by exploiting inherent channel characteristics (such as noise and fading), to secure data at the physical transmission level. Its minimal computational overhead makes it well suited for constrained far-edge devices, unlike traditional cryptographic methods that require significant processing resources. Still, because PLS depends on variable channel conditions, it cannot always provide strong or consistent protection, while conventional security frameworks may impose prohibitive computational costs. To overcome these challenges, this study proposes an adaptive orchestration strategy that dynamically coordinates service provisioning and security mechanisms. By continuously adjusting protection levels in response to network conditions and threat dynamics, the approach seeks to balance strong security with high performance in far-edge environments. Recent research increasingly applies machine learning and AI to intrusion analysis and threat detection in networked systems. In [3], an adaptive edge-security framework combines trust-based management, decentralized decisions, and microservice controls to strengthen protection in distributed environments. The work in [2] proposes a reconfigurable IoT security framework that leverages edge devices as security agents to support multi-layer defenses while reducing computational overhead. SAFENet [1] introduces an AI-driven, multilayered security architecture for 6G edge networks, enabling real-time, adaptive protection in decentralized and resource-limited settings.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-33, December 16-18, 2025, Sapporo, Japan.

However, these approaches primarily target threat detection and its distribution, without addressing adaptive security mechanisms during service provisioning. In far-edge systems (characterized by fluctuating resources and heterogeneous device capabilities), more context-aware, self-adjusting security strategies are needed.

2 System Overview and Performance

In far-edge environments, the proposed orchestration architecture provides a unified framework that balances security and service efficiency. It integrates two core layers: the Service Orchestration (SO) layer, which deploys and manages service components based on user demands, constraints, and available resources; and the Security Measures Orchestration (SMO) layer, which dynamically adjusts security functions across the network, transport, and physical layers. The SMO adapts encryption, integrity checks, and authentication to current node capabilities and threat levels. A CSI-based threat detection subsystem identifies malicious users by analyzing wireless signal anomalies. When threats arise, an adaptive response module strengthens or adjusts security mechanisms to maintain confidentiality and integrity without overloading constrained devices. A Security Intelligence Module coordinates both layers by monitoring network conditions, evaluating attack windows, and tuning orchestration parameters in real time. This closed-loop control enables fine-grained adaptation, ensuring strong protection while preserving service quality under resource limitations and evolving threats.

To evaluate the proposed approach, we conducted a simulation with 10 edge nodes processing 1000 service requests in a controlled environment. An attack window spanning requests 450–550 tested the system's adaptability under active threat. Key metrics included blocking probability, service activation delay, and security overhead across different orchestration setups. As shown in Figure 1, nodes first operate with TLS, then with PLS, and finally with the proposed adaptive mechanism. In the adaptive case, far-edge nodes use PLS until request 450, switch to TLS during the detected intrusion, and revert to PLS after request 550.

Results show a 6.73% rise in blocking probability when moving from mixed (MIX) to full TLS, illustrating the trade-off between strong security and responsiveness. Overhead also increased by 9.22% (TLS vs MIX) and 14.89% (TLS vs PLS), confirming that heavier encryption significantly impacts performance on legacy devices. Despite this, the orchestrator effectively limited performance degradation by adjusting security parameters according to threat level.

These findings highlight that static, uniform security models are inadequate for heterogeneous far-edge settings. Adaptive orchestration offers a scalable, intelligent alternative that balances security assurance and service performance, even under resource constraints and dynamic threat conditions.

Acknowledgments

This work was partially supported by the European Union - Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP J33C22002880001 and CUP E13C22001870001, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

References

[1] Khandakar Rabbi Ahmed et al. Ai-enhanced adaptive network security for 6g and edge computing. In *2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)*.

[2] Ruei-Hau Hsu et al. Reconfigurable security: Edge-computing-based framework for iot. *IEEE Network*.

[3] Kuznetsov Oleksandr et al. Chapter 2 - architectural foundations for adaptive security in edge computing systems. In *Cybersecurity Defensive Walls in Edge Computing*.