A Multi-Slice Lawful Interception Framework for Beyond-5G Networks: Design and Evaluation of a Standard-Compliant Emulation Testbed

Ingrid Huso*†, Angelo Calia*, Giuseppe Piro*†, Gennaro Boggia*†
*Dept. of Electrical and Information Engineering - Politecnico di Bari, Bari, Italy,
†CNIT, Consorzio Nazionale Interuniversitario per le Telecomunicazioni
Email: {name.surname}@poliba.it

***Abstract*—Network slicing enables the creation of logically isolated, service-specific virtual networks over a shared infrastructure, supporting differentiated Quality of Service (QoS) and security guarantees. However, the dynamic and encrypted nature of these slices introduces new challenges for Lawful Interception (LI). Current 3GPP and ETSI specifications do not fully support multi-slice interception, particularly in the presence of end-to-end encryption (E2EE). This paper presents a standards-compliant LI framework tailored for B5G slicing environments. The Lawful Interception (LI) Framework is deployed on a containerized testbed built with Open5GS and OpenLI, enabling reproducible experimentation in controlled multi-slice scenarios. The system supports per-slice interception of file transfers and encrypted VoIP traffic. A secure, identity-based key escrow scheme enables lawful decryption while preserving user privacy and slice isolation. Experimental results show a latency overhead below 10 ms in all test scenarios, demonstrating the feasibility of low-impact, compliant interception in modern B5G networks.**

***Index Terms*—5G, Network Slicing, Lawful Interception, Open5GS, OpenLI.**

I. Introduction

Network slicing represents a fundamental architectural innovation in future mobile communication systems , allowing the dynamic partitioning of a shared physical infrastructure into multiple logically isolated virtual networks. Each network slice can be customized to meet the specific requirements of diverse service types and industry verticals [1]. By integrating key enabling technologies such as Network Function Virtualization (NFV), Software-Defined Networking (SDN), and Multi-access Edge Computing (MEC), this paradigm facilitates the provisioning of differentiated services with tailored Quality of Service (QoS) and security guarantees [2].

To meet public safety and regulatory needs, bodies such as 3rd Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI) have standardized a comprehensive set of specifications for LI in 5G. In particular, TS 33.126, 33.127, and 33.128 define functional, procedural, and interface-level requirements [3], [4], [5]. However, these frameworks are predominantly based on centralized and static network architectures, which increasingly conflict with the dynamic, distributed, and service-oriented nature of contemporary Fifth Generation (5G) deployments. Specifically, in 5G and Beyond 5G (B5G) networks, the disaggregation of control and user planes, along with the pervasive and dynamic placement of User Plane Functions (UPFs), introduces significant challenges in the orchestration and enforcement of LI functions. These challenges are intensified in network slicing environments, where slices may adopt independent deployment strategies tailored to the specific application needs. Furthermore, the growing use of End-to-End Encryption (E2EE) limits the visibility of Communications Service Providers (CSPs) into Intercept Related Informations (IRIs) and Communication Contents (CCs) unless supported by secure key management frameworks [6], [7]. Consequently, intercepted traffic often remains inaccessible, undermining the operational utility of LI as defined by current standards.

Although recent studies have addressed aspects of privacy, trust, and encryption, they fall short of delivering practical, standards-compliant LI capabilities that integrate seamlessly with virtualized B5G network slicing infrastructures [8]. This paper addresses these challenges by proposing a standards-compliant framework for LI in a virtualized multi-slice 5G network environment. By leveraging open-source platforms, such as Open5GS [9], OpenLI [10], and UERANSIM [11], the solution implements a fully containerized testbed supporting per-slice LI of both file transfers and encrypted VoIP traffic. Thus, the main contributions of this work are:

- Extension of our prior LI framework [12] to support multi-slice LI in B5G network environments.
- Design and deployment of a container-based, multi-slice testbed that emulates LI of encrypted communication flows in realistic 5G scenarios, via open-source platforms.
- Evaluation of interception latency and system overhead to assess performance and scalability.

The remainder of this paper is organized as follows. Section II reviews background concepts and related works. Section III presents the proposed methodology, for the per-slice interception procedures. Section IV describes the proof-of-concept implementation and discusses performance evaluations. Finally, Section V concludes the paper and outlines future research directions.

II. Background and Related Work

A. Background concepts

Lawful Interception in 5G. LI refers to the standardized frameworks and processes that enable CSPs to collect, preserve, and deliver communication data to authorized LEAs upon proper legal authorization [3]. Within 5G networks, LI is specified across 3GPP TS 33.126 (requirements) [3], TS 33.127 (architecture) [4], and TS 33.128 (protocols) [5] standards. Specifically, LI functions are distributed across multiple network components. In detail, the Administration Function (ADMF) oversees the lifecycle of interception, including the management of warrants and Point of Interceptions (POIs) via the System Information Retrieval Function (SIRF) and interfaces defined in the standards. POIs are typically deployed within UPFs to detect target communications, extract IRI and CC, and forward them to the Mediation and Delivery Function (MDF). It then splits and delivers the intercepted data to the Law Enforcement Monitoring Facilitys (LEMFs) through standardized HI2 and HI3 interfaces, ensuring authorized LEAs can access communications in compliance with regulatory requirements.

Network Slicing. Network slicing is a foundational capability of 5G networks, enabling the deployment of multiple logically isolated virtual networks over a common physical infrastructure. Each slice can be individually configured to meet specific service requirements, thereby supporting diverse use cases such as enhanced Mobile Broadband (eMBB), ultra-Reliable Low Latency Communications (URLLC), and massive Machine-Type Communications (mMTC) [1], [2]. The 3GPP defines standardized slice types and associated parameters—such as bandwidth, latency, and reliability—to ensure service differentiation and adherence to application-specific constraints [13], [2]. This architecture facilitates efficient resource allocation, service-level isolation, and secure multi-tenancy within a unified 5G infrastructure.

B. Related Work on LI

LI in B5G networks has been extensively studied, with particular focus on the challenges introduced by E2EE and stringent privacy requirements. In this context, several works have explored key escrow-based frameworks that reconcile lawful access with encryption. Notably, [14], [12] propose solutions enabling controlled decryption of intercepted traffic within the core network, ensuring LEA access while maintaining compliance and feasibility. These studies also emphasize the importance of legal protections to prevent misuse and protect user privacy. Complementary approaches based on privacy-preserving mechanisms have also been investigated. For instance, [15] introduces P3LI5, which leverages Private Information Retrieval (PIR) to enable identifier resolution with reduced data exposure and latency during interception.

Moreover, integrity and non-repudiation of intercepted data remain critical concerns. The architecture in [16] addresses non-frameability through formal verification, preventing malicious attribution by compromised actors. Similarly, [17] ensures completeness, correctness, and freshness of captured data to reinforce trust in LI systems.

While, at the system level, [18] presents LiaaS, an AI-driven interception platform built on big data and cloud-native paradigms to handle heterogeneous multimedia traffic. Thus, it employs machine learning for traffic classification but lacks decryption capabilities for E2EE content.

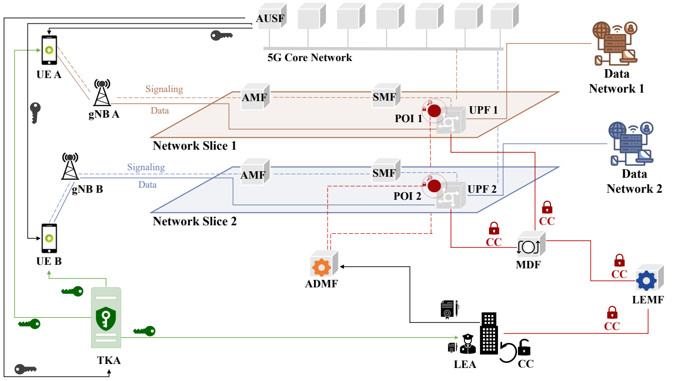


Fig. 1: High-level architecture of the proposed LI framework in a multi-slice 5G network.

Finally, position papers [19], [20], [21] underline ongoing regulatory and standardization challenges, calling for harmonized legal frameworks to support LI in future virtualized infrastructures. However, these contributions remain conceptual and do not propose deployable technical solutions.

Despite these advances, existing work does not address the integration of LI within dynamic, multi-slice B5G environments. In particular, orchestration, isolation, and compliance issues remain unresolved in contexts where each slice may impose distinct security and performance requirements. This gap highlights the need for LI frameworks that are cryptographically robust, standards-compliant, and natively deployable across virtualized, multi-slice infrastructures without undermining the isolation guarantees of network slicing.

III. The Proposed Multi-slice LI Methodology

The proposed LI framework builds upon our previously designed architecture [12]. It enhances the standardized 3GPP LI architecture with the capability to lawfully intercept application-layer E2EE traffic within a multi-slice environment, differently from our previous work. Thus, by integrating the concept of network slicing, the model provides a flexible and efficient interception framework for managing heterogeneous traffic types in logically isolated network slices. This section details the key entities and the LI framework workflow.

A. LI Framework - Principles and Entities.

The proposed LI framework is natively designed to integrate network slicing as a core architectural principle within B5G networks. By partitioning the physical infrastructure into multiple logically independent virtual networks, each slice is provisioned with dedicated resources and customized configurations tailored to the specific QoS requirements of diverse application types—such as high-throughput file transfers or ultra-low-latency call sessions. This architectural partitioning enables advanced service and traffic differentiation, allowing critical network functions—particularly the UPF—to be instantiated on a per-slice basis. This segregation is crucial for LI, ensuring that interception within one slice does not compromise the performance or confidentiality of traffic in other slices. Furthermore, to address the challenges posed by encrypted communications, the proposed LI framework incorporates a secure application-layer Key Escrow mechanism. This procedure, in line with [12], enables authorized LEAs to perform controlled and lawful decryption of E2EE traffic, while maintaining the confidentiality of users outside the scope of legal mandates.

Fig. 1 depicts the high-level architecture of the proposed LI framework, which comprises the following key entities [12]:

- *Subscribers* : end-users (e.g., UE A and UE B) engaged in encrypted E2EE communications.
- *Law Enforcement Agency (LEA)*: the legally authorized government entity responsible for issuing warrants and receiving both IRI and Content of Communication CC.
- *Authentication Server Function (AUSF)*: a standard 5G Core Network (5GCN) function for subscriber authentication, extended here to securely distribute application-layer encryption materials to both User Equipments (UEs) and the LEA.
- *Trusted Key Authority (TKA)*: a trusted third-party entity, functionally similar to a Certification Authority (CA), responsible for managing the application-layer cryptosystem. The TKA employs a Key Escrow mechanism based on an ID-based Cryptosystem (IDBC) scheme [22] to generate session-specific encryption keys. Notably, the TKA retains only its master secret.
- *POIs*: dynamically instantiated within the network, in charge of conducting the interception procedure. Specifically, POI instances in the Access and Mobility Management Function (AMF) generate IRI, whereas those colocated with per-slice UPF instances are responsible for intercepting the CC.

B. LI framework workflow in a multi-slice Network

This section illustrates the operational workflow of the proposed LI framework, which integrates the lawful interception procedure defined in [12] within each isolated network slice. The workflow is structured into the following four phases:

1) Key Negotiation Phase. During this phase, the AUSF and TKA collaboratively perform cryptographic operations using application-level primitives, including hash functions $\mathcal{H}(\cdot)$ and bilinear pairings $e(\cdot,\cdot)$, as specified by the Key Escrow scheme in [22]. The AUSF engages in a secure nonce exchange with the communicating UEs, allowing them to independently generate the session key k_{AB}. Concurrently, the key derivation information is securely relayed to the TKA, which subsequently transfers it to the LEA, ensuring that the session key is accessible solely to authorized parties. Crucially, this mechanism guarantees that subscribers remain unaware of the interception by respecting the non-engagement principle.

2) Per-slice Interception Phase. Upon receiving a valid warrant, the ADMF initiates the interception process targeting a specific network slice identified by its Single - Network Slice Selection Assistance Information (S-NSSAI). This phase leverages both session- and slice-specific identifiers to accurately confine interception to authorized traffic flows. Each session is uniquely identified using the International Mobile Subscriber Identity (IMSI) combined with the S-NSSAI, ensuring that only relevant communications are subject to interception. The UE traffic is captured and filtered by the POI integrated within the UPF node assigned to the targeted slice. The POI further decapsulates the GPRS Tunneling Protocol User Plane (GTP-U) traffic to extract the encrypted CC and corresponding IRI metadata, which are then processed by the MDF and forwarded to the LEMF via standardized HI2 and HI3 interfaces.

3) Decryption Phase. In the final phase, the LEA utilizes the application session key, previously established through the key escrow mechanism, to decrypt the intercepted CC received from the LEMF. Specifically, the session key is derived as $k_{AB} = e(\eta \cdot M\mathcal{H}(ID_A), \mathcal{H}(ID_B))$. Moreover, since this key is generated using unique nonces for each session, it ensures that keys cannot be reused, thereby guaranteeing adherence to warrant validity requirements. For further cryptographic details on the key escrow mechanism, refer to [22] and [12].

IV. Proof-of-Concept and Performance Evaluation

This section details the proof-of-concept implementation and evaluation of the proposed multi-slice LI framework in a 5G environment, for intercepting encrypted and slice-isolated traffic. Specifically, in the implemented scenario, distinct network slices are employed to deliver differentiated services: one slice hosts the File Transfer Protocol (FTP) server, while another is dedicated to Voice over IP (VoIP) communication.

A. Proof-of Concept Implementation

Fig. 2 illustrates the proof-of-concept of the proposed multi-slice LI framework in a 5G environment, by leveraging Docker containerization.

5G Network. The 5GCN is implemented using Open5GS [9], which provides the essential core functions, including the AMF, Session Management Function (SMF), Network Repository Functions (NRF), and two distinct UPF instances. Each UPF is bound to a dedicated network slice, allowing for service-based traffic separation. The testbed integrates UERANSIM [11] to emulate the behavior of both the Next Generation Node B (gNB) and the UEs, enabling support for registration, session management, and traffic generation in compliance with 3GPP specifications.

Network slicing configuration. Network slicing is realized through tailored configurations of the AMF and SMF, where S-NSSAI parameters, specifically `sst` and `sd`, are explicitly defined in YAML configuration files (i.e., `amf.yaml` and `smf.yaml`) to distinguish FTP and VoIP service classes. Traffic associated with the FTP slice is routed through UPF1, while VoIP traffic is directed through UPF2. Thus, ensuring logical and functional isolation between services across slices.

LI environment. The LI framework is implemented using OpenLI [10], deployed as four dedicated microservices (i.e.,

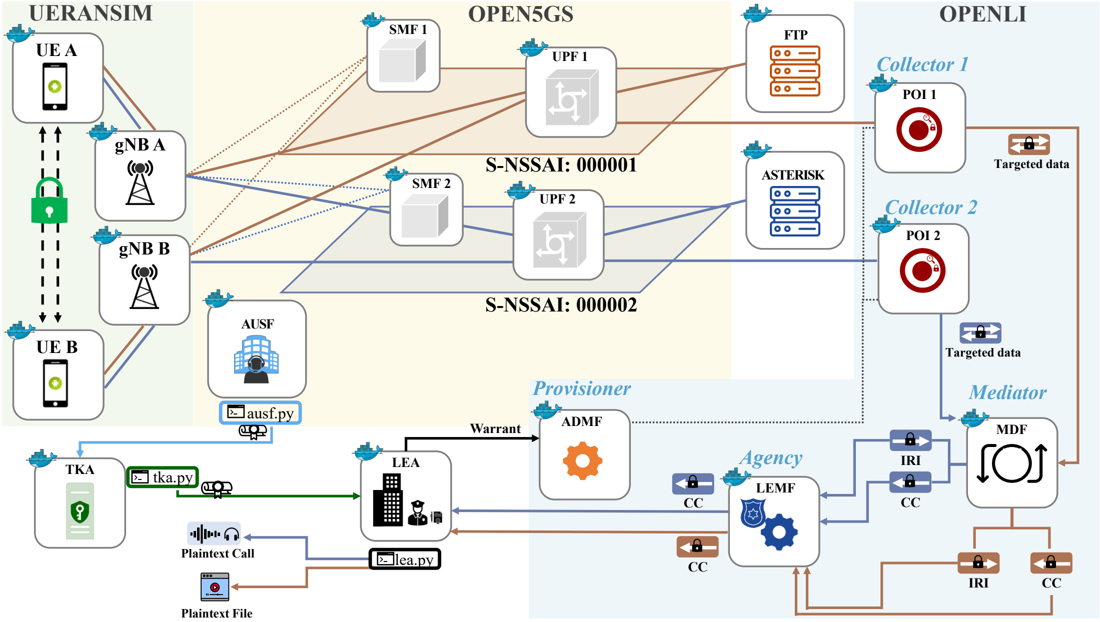


Fig. 2: Containerized proof-of-concept of the proposed multi-slice LI framework.

Provisioner, Collector, Mediator, and Agency) each instantiated within isolated Docker containers and interconnected via dedicated virtual bridges. The Provisioner handles warrant-based provisioning through a RESTful API. The Collector interfaces with the UPFs to capture mirrored traffic and generate ETSI-compliant IRI and CC records. To ensure reliable and ordered delivery, the records are buffered using RabbitMQ [10].

Interception of encrypted traffic. To enable lawful access to encrypted communications, the architecture incorporates a key escrow mechanism based on cryptographic primitives from the PyCryptodome library and bilinear pairings via the Tate library. Keys are generated and securely distributed using dedicated scripts (`generate_keys.py` and `copy_key.sh`). This mechanism enables the Agency component to decrypt both Secure Real-time Transport Protocol (SRTP) and FTP traffic, thus maintaining lawful access capabilities while preserving the integrity of end-to-end encryption.

Application-layer services. FTP traffic is served through a Pure-FTPd instance associated with the first slice (SD:000001). While the VoIP communication is handled by a second slice (SD:000002) where an Asterisk server is configured to support SRTP VoIP call.

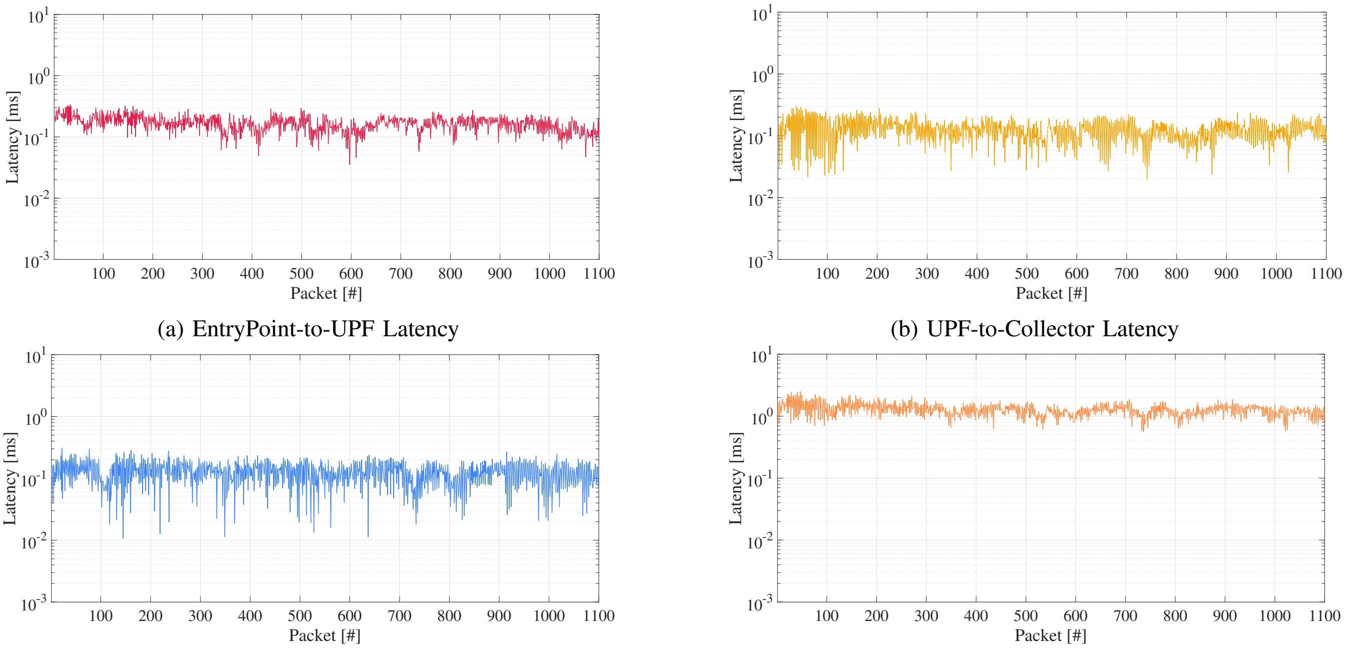
Deployment Workflow. A dedicated orchestration script manages the end-to-end deployment of the testbed, including configuration loading, Docker container instantiation, and service registration across the 5GCN and LI layers. Each UE is configured to establish two simultaneous Packet Data Unit (PDU) sessions, with virtual tunnel interfaces (e.g., `uesimtun0` and `uesimtun1`) mapped to different slices and subnets. This design enables fine-grained traffic separation and routing through independent UPF instances. Thus, mirroring of intercepted traffic is performed directly at the UPF level using port mirroring rules, forwarding copies of packets to the Collector component, which embodies the POI. Upon capture, traffic is parsed and relayed via standard ETSI HI interfaces (i.e., HI2 for IRI and HI3 for CC) to the Agency, which embodies here the LEMF. Captured data is post-processed using a combination of `libtrace`, `Scapy`, and custom Python scripts. These tools enable full reassembly of intercepted streams, extraction of metadata, and verification of decryption correctness. Allowing the Agency to obtain and decrypt the captured CC data.

B. *Performance Evaluation*

This section evaluates the performance of the proposed multi-slice LI framework in a 5G environment. The primary focus lies in assessing latency overheads and service isolation across network slices, particularly for FTP traffic and for VoIP communications. Performance metrics are derived from controlled testbed experiments employing two disjoint UPF and SMF instances per service slice. Specifically, FTP, transfers were conducted using three different file sizes (i.e., 1 MB, 10 MB, and 100 MB) while VoIP scenarios involved SRTP-encrypted calls of varying durations (i.e., 15 s, 30 s, and 45 s).

In line with [12], to quantify the system performance the following Key Performance Indicators (KPIs) are considered:

1) **EntryPoint-to-UPF Latency**: Time elapsed for a packet to reach the UPF, marking the first Collector.
2) **UPF-to-Collector Latency**: Delay introduced during mirroring and capturing of packets by the OpenLI Collector.
3) **Collector-to-Agency Latency**: Transmission latency from the Collector to the Agency.
4) **Aggregate LI Latency**: Aggregated latency introduced across all interception stages.



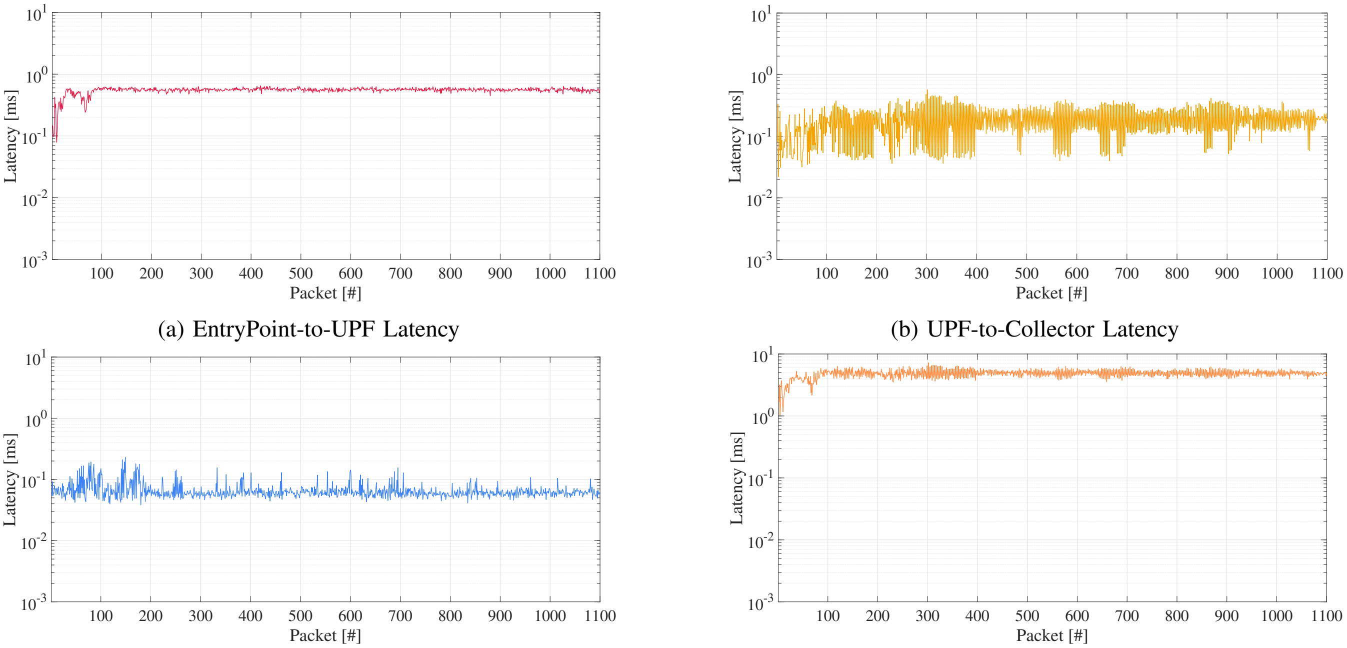
(a) EntryPoint-to-UPF Latency

(b) UPF-to-Collector Latency

(c) Collector-to-Agency Latency

(d) Aggregate LI Latency

Fig. 3: Packet latency across different LI components of a 10 MB FTP file transfer in a dedicated 5G network slice.



(a) EntryPoint-to-UPF Latency

(b) UPF-to-Collector Latency

(c) Collector-to-Agency Latency

(d) Aggregate LI Latency

Fig. 4: Packet latency across different LI components of a 30 seconds VoIP call in a dedicated 5G network slice.

To assess the latency impact of the proposed LI framework, two representative scenarios were analyzed: a 10 MB encrypted FTP file transfer over the first network slice and a 30-second SRTP VoIP call over the second network slice. In both cases, the services were assigned to distinct UPF nodes (i.e., UPF 1 and UPF 2) and POI nodes to enforce strict slice-level isolation. Fig. 3 shows latency measurements of the FTP scenario over the first network slice. The average per-packet delay at the UPF 1 remained around 0.84 ms, while the latency observed at the OpenLI Collector 1 and the Agency interface each stayed well below 1 ms. According to the aggregated data shown in Fig. 3d, the end-to-end interception latency never exceeded 10 ms, even under transient conditions, and remained under 3 ms in the vast majority (95%) of samples. These results confirm that the LI framework scales well and introduces negligible overhead, even when processing medium-sized file transfers. Fig. 4 shows latency measurements of the VoIP scenario over the second network slice. The UPF 2 acquisition latency consistently remained below 0.9 ms. The delay added by the OpenLI Collector 2 and the Agency component was again under 1 ms each. Fig. 4d illustrates that the total LI-induced latency across all interception stages remained within 4 ms, thereby meeting the stringent requirements imposed by real-time call services. Importantly, the overall end-to-end user latency remained below the 10 ms threshold, thus ensuring also compliance with real-time communications. Overall, the latency trends across both network slice scenarios confirm the lightweight nature of the proposed multi-slice LI framework.

V. Conclusion

This work introduced a practical, standards-compliant framework for LI in multi-slice B5G networks, explicitly designed to operate within multi-slice and end-to-end encrypted communication environments. By leveraging open-source platforms such as Open5GS, OpenLI, and UERANSIM, the proposed system enables fine-grained, per-slice Lawful Interception while ensuring service-level isolation. The integration of an application-layer key escrow mechanism allows authorized LEAs to access encrypted content in a controlled manner, without undermining the privacy of users outside the legal scope. Experimental results confirm that the overall latency overhead introduced by the framework remains minimal—even for latency-sensitive services—demonstrating its feasibility for real-world deployment. Future work will carry a security evaluation test, explore support for multi-domain and multi-tenant slicing scenarios, as well as investigate LI functionalities at the network edge in the context of future mobile communication systems.

Acknowledgments

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, Mission 4, Component 2, in the context of partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART", CUP:D93C22000910001), national center on "Sustainable Mobility" (CN00000023-program "MOST", CUP: D93C22000410001), and partnership on "Cybersecurity" (PE00000007 - program "SERICS", CUP:D33C22001300002, project ISP5G+). It was also supported by the PRIN 2022 projects INSPIRE (grant no. 2022BEXMXN 01) and HORUS (grant no. 2022P44KA8) funded by the Italian MUR, and by the HORIZON MSCA project BRIDGITISE (grant no. 101119554).

References

[1] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, "Network slicing to enable scalability and flexibility in 5g mobile networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, 2017.

[2] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.

[3] 3GPP, "Lawful interception (li) requirements," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 33.126, November 2022, Release 18.0.0.

[4] ——, "Lawful interception (li) architecture and functions," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 33.127, September 2023, Release 18.5.0.

[5] ——, "Protocol and procedures for lawful interception (li)," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 33.128, September 2023, Release 18.5.0.

[6] M. Vidoni, E. Senior Course, and F. Police, "5g technology: New challenges for law enforcement agencies to face," *European Law Enforcement Research Bulletin*, vol. 22, pp. 157–171, October 2022.

[7] Scientists4Crypto, "Academic letter to the european commission on "encryption — security through encryption and security despite encryption"," *Scientists4Crypto*, December 2020.

[8] Council of the European Union and EUROPOL, "Position paper on 5G," The European Commission, Tech. Rep., April 2019.

[9] S. Kim and J. Lee, "Open5gs: An open-source 5g core network implementation," *IEEE Access*, vol. 8, pp. 142 447–142 456, 2020.

[10] O. Project, "Openli: An open-source lawful interception system," https://www.openli.nz/, 2023.

[11] W. Zhou and A. Smith, "Ueransim: A 5g nr simulator for research and development," *IEEE Access*, vol. 9, pp. 17 823–17 835, 2021.

[12] I. Huso, M. Olivieri, L. Galgano, A. Rashid, G. Piro, and G. Boggia, "Design and implementation of a looking-forward lawful interception architecture for future mobile communication systems," *Computer Networks*, vol. 249, p. 110518, 2024.

[13] 3GPP, "3gpp technical specification group services and system aspects; telecommunication management; study on management and orchestration of network slicing for next generation network," in *3GPP TR 28.801 V15.1.0*, 2018.

[14] G. Ungaro, F. Ricchitelli, I. Huso, G. Piro, and G. Boggia, "Design and implementation of a lawful interception architecture for b5g systems based on key escrow," in *2022 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2022, pp. 207–207.

[15] F. Intoci, J. Sturm, D. Fraunholz, A. Pyrgelis, and C. Barschel, "P3li5: Practical and confidential lawful interception on the 5g core," in *2023 IEEE Conference on Communications and Network Security (CNS)*, 2023.

[16] F. Boeira, M. Asplund, and M. Barcellos, "Provable non-frameability for 5g lawful interception," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023.

[17] F. Buccafurri, A. Consoli, C. Labrini, and A. M. Nesurini, "A solution to support integrity in the lawful interception ecosystem," in *Electronic Government and the Information Systems Perspective*, A. Kö, E. Francesconi, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds. Springer International Publishing, 2021.

[18] M. Monshizadeh, V. Khatri, M. Varfan, and R. Kantola, "Liaas: Lawful interception as a service," in *2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2018.

[19] M. Säily, O. N. C. Yilmaz, D. S. Michalopoulos, E. Pérez, R. Keating, and J. Schaepperle, "Positioning technology trends and solutions toward 6g," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021.

[20] D. Giustiniano, G. Bianchi, A. Conti, S. Bartoletti, and N. B. Melazzi, "5g and beyond for contact tracing," *IEEE Communications Magazine*, vol. 59, no. 9, pp. 36–41, 2021.

[21] V. Doronin, ""lawful interception – a market access barrier in the european union"?" *Computer Law & Security Review*, vol. 51, p. 105867, 2023.

[22] K. Han, C. Y. Yeun, T. Shon, J. Park, and K. Kim, "A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication," *International Journal of Communication Systems*, vol. 24, no. 4, 2011.