

However, two other key performance metrics have received less attention, further affecting the positioning accuracy itself:

- **Positioning availability:** AML solutions operate under a "send us what you have now" timeout rule, meaning they often receive the best available data within a limited timeframe. Similarly, NILR protocol requires a time-consuming traffic exchange with the PSAP before the network operator initiates the process of positioning the smartphone. Unfortunately, this often results in no position being delivered or positions that are not optimally accurate. Official EU monitoring data indicate that the share of AML messages received within 15 seconds varies widely – from 12% to 94% – while a significant number of Member States reported not timing data at all, indicating a persistent lack of performance monitoring [10].
- **Energy consumption:** mobile Operating Systems (OSs) perform a battery check before computing the user's location. This process can drain the battery, a vital resource during emergencies. In practice, handset-derived location may be delayed or degraded under critical battery states or OS energy-saving policies (e.g., GNSS activation is subject to battery checks), which can impact the timeliness of AML payloads [2, 10]. Similarly, network-initiated approaches such as NILR rely on active handset measurements, while device-hybrid services like Android's ELS are likewise energy constrained, reducing location availability.

In summary, emergency-location provisioning remains *fragmented* across regions (e.g., network-initiated, used-based, or hybrid approaches) and among PSAP integrations (e.g., AML transport over SMS/HTTPS, heterogeneous timeouts and confidence semantics). The efforts of different entities have mainly focused on improving positioning accuracy, while positioning availability and energy consumption have received less attention in real settings.

In contrast, 3rd Generation Partnership Project (3GPP) specifies a *standardized* architecture for cellular networks. We find that the use of 5G New Radio (NR) signals can enhance localization with network-based methods. However, network-based methods such as NILR protocol are too slow. **This gap motivates our RAN-first, standards-aligned approach.** In order to address this problem, we propose a framework to provide early notification of user position without wasting user resources. Our concept leverages 5G and Open-RAN (O-RAN) capabilities to enable earlier delivery of positioning data, using only standard-compliant communication signaling already exchanged when a User Equipment (UE) initiates an emergency call. A high-level illustration of this approach is shown in Figure 1.

Upon detecting an emergency session during the initial control-plane exchange in the Radio Resource Control (RRC) layer, we perform Radio Access Network (RAN) analytics exposed via the near-real-time RAN Intelligent Controller (RIC) to coordinate multi-gNB sensing and derive location estimates with minimal device overhead. We implement a proof of concept based on OAI to validate feasibility. Our contributions are:

- A standards-aligned architecture that leverages early RRC signaling for extracting user status and providing ranging measurements, and O-RAN interfaces to trigger RAN-based positioning;
- A control-plane workflow that enables multi-gNB collection of time/angle features without modifying PSAP infrastructure;

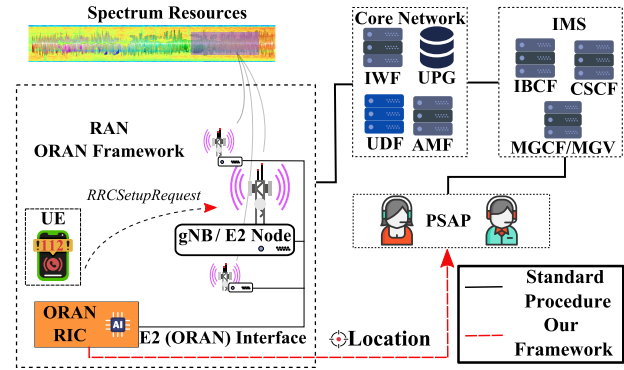


Figure 2: Proposed relation among 3GPP, ORAN and emergency architecture.

- A proof-of-concept with OAI demonstrating the interception of signals in the RAN from a real smartphone, and showing the feasibility of using early messages sent by the caller to speed up the positioning process.

2 Background

In this section, we present the relevant background on 5G system architecture and emergency services. We provide a high-level illustration for emergency in Figure 2.

5G System architecture and O-RAN. The 5G system architecture comprises three key components: UE, 5G-Radio Access Network (5G-RAN), and 5G-Core Network (5G-CN). UEs, such as smartphones and Internet of Things (IoT) devices. The 5G-RAN, consisting of base stations known as Next Generation NodeBs (gNBs), is responsible for connecting UEs to the 5G-CN using 5G radio technologies.

The O-RAN Alliance [3] complements these efforts by driving innovation in the RAN through its principles of openness, softwarization, and disaggregation. A key innovation in O-RAN is the introduction of the RIC, programmable components designed to host optimization routines and Artificial Intelligence (AI) algorithms to enable advanced capabilities such as real-time network optimization. Furthermore, the E2 Interface is the open interface between two endpoints, the near-real time RIC and the E2Nodes. It enables the collection of metrics from the RAN. Finally, an E2Node is a logical node and offers a variety of RAN functions, and supports the connection with E2 Interface [17].

Emergency Services. 5G, 4G, and even legacy 3G systems, provide access to emergency services such as 911 or 112 calls. In modern networks, the services are delivered to PSAPs via the Packet-Switched (PS) core, where the 5G-CN routes traffic through the IP Multimedia Subsystem (IMS). The IMS facilitates emergency voice and text services over IP or Public Switched Telephone Network (PSTN) through three key components:

- The Call Session Control Function (CSCF), or IMS server, manages Session Initiation Protocol (SIP) signaling to establish and control emergency sessions;

- The Media Gateway Control Function (MGCF) and Media Gateway (MGW) connect IMS to PSAPs via PSTN for legacy telephony interoperability;
- The Interconnect Border Control Function (IBCF) ensures secure inter-connectivity between PS Core, IMS and PSAPs.

To initiate an emergency call, the UE follows a structured process. First, the UE establishes an emergency connection to the PS Core Network by creating a session with the User-Plane Gateway (UPG), which routes traffic between RAN and IMS. Next, the UE performs emergency registration and authentication with the IMS server, ensuring secure access to the network. Finally, the UE initiates an emergency session with the PSAP by sending a Session Initiation Protocol (SIP) INVITE message via the IMS.

3 Architecture Design

In the vision of the designed architecture, tracking the user for emergency location requires to provide earlier position notification to the PSAP, before other methods such as AML or NILR are initiated. The solution has to be compatible with current and emerging standards, avoiding the need for implementing new or unfeasible features on users' devices (that is, just using commercial smartphones) or in the infrastructure side (no changes on the public safety service and its infrastructure). Finally, it should leverage existing emerging paradigms such as O-RAN.

In what follows, we present the key steps of the proposed framework for accelerating the acquisition of positioning data, referring to the workflow presented in Fig. 3.

3.1 Early emergency detection

The first step for the caller is to gain access to the spectrum resources via the 5G-RAN. Let us refer to Fig. 4. When a UE initiates an emergency call with the gNB, specific protocol messages are sent by the mobile device to request network resources. One key message is the RRCSetupRequest, which contains a field indicating the reason for the request. This field enables the 5G-RAN to immediately detect that the connection request is related to an emergency.

According to 3GPP, when the RRCSetupRequest message includes the establishment cause set to *emergency*, the gNB must handle it with the highest priority. In this case, access is guaranteed even if the network is congested or the UE is in a limited service state. The limited service state occurs when the UE is not permitted to use normal services, for example, when no valid SIM is present or when the network has denied registration for regular services.

In our view, *the goal is for the 5G RAN to take actions as early as possible, gaining valuable time before the emergency call is received and acted upon by a PSAP assistant. Early detection enables the RAN to augment the the location data shared with the PSAP.*

3.2 Multi-gNB time/angle feature collection

Once the serving gNB detects an emergency UE, it notifies the near-RT RIC (via E2 service models) and share the *uplink scheduling decisions* such as time-frequency resource blocks (RBs) and Modulation and Coding Scheme (MCS) used by that UE's uplink transmissions. Neighboring gNBs may then adjust their schedulers where feasible: e.g., by avoiding to allocate or use resources used by

other UEs to facilitate opportunistic monitoring of the emergency UE's uplink signals.

Once all the gNBs (or E2Node, see Sec. 2) involved by the RIC are coordinated to use only the resources related to the emergency session, they can extract low-layer features from known portions of the physical signals that can be leveraged for positioning the emergency caller. These features include both time-based and angle-based measurements.

A key enabler here is the Demodulation Reference Signal (DMRS) embedded within the Physical Uplink Shared Channel (PUSCH). Because DMRS sequences are deterministic and known to the network, nearby gNBs that are aware of the uplink scheduling can correlate with the DMRS to obtain precise timing for Time-of-Arrival (ToA) or Time-Difference of Arrival (TDoA) measurements, as well as channel-phase information for Angle-of-Arrival (AoA) estimation in Multi Input Multi Output (MIMO)-enabled 5G deployments. In this way, other gNBs can sense the emergency UE's uplink messages without requiring any additional power-hungry transmissions from the UE, as DMRS is already part of the standard uplink data channel used during the call setup.

We note that, unlike prior work that explores Open RAN as a general-purpose sensing infrastructure [19], we specifically focus on emergency caller localization, leveraging early RRC emergency signaling and multi-gNB feature collection to deliver preliminary position estimates directly to PSAPs.

Immediate observability. The RRCSetupComplete + NAS message is carried on PUSCH and it is scheduled by the serving gNB through a *DCI 0_1 uplink grant* sent over the Physical Downlink Control Channel (PDCCH). Therefore, its DMRS spans *exactly the frequency-time resources allocated in that grant*. To speed up observability of accurate positioning measurements for localizing the caller, the serving gNB can issue a *wide uplink grant* for this first transmission, such that the subsequent RRCSetupComplete uses DMRS over a larger bandwidth. The parameters that define the usable uplink bandwidth such as Bandwidth Part (BWP) and numerology are provided to the UE in the preceding RRCSetup message, while the specific resource allocation is realized by the subsequent DCI 0_1.

The time between RRCSetupRequest and RRCSetupComplete allows the nearby gNBs to reconfigure their resource allocation for listening to the emergency caller. This time window *offers a low-latency opportunity for early positioning augmentation without additional UE overhead or Core involvement.*

Positioning. Once each gNB in range of the UE passively computes its local measurements, those are forwarded to the O-RAN controller (or an associated xApp) where they are fused into a preliminary position estimate, and sent directly to the PSAP over a standard HTTPS endpoint.

This workflow complements, rather than replaces, existing AML/NILR data flows, avoiding changes to PSAP infrastructure and minimizing device energy consumption. It also decouples accuracy improvements from GNSS availability by exploiting measurements available in the cellular access already required to place the emergency call. Finally, while the 5G Core Network and the Location Management Function (LMF) can support both commercial and emergency positioning services [18], our approach provides a faster

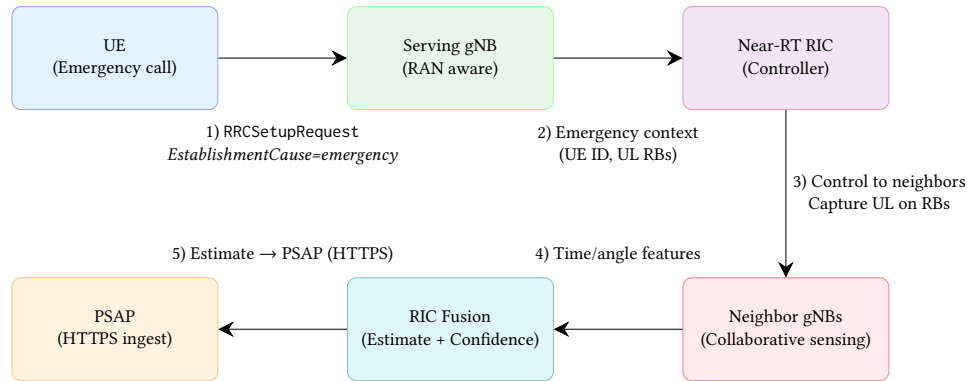


Figure 3: Proposed signaling workflow for emergency.

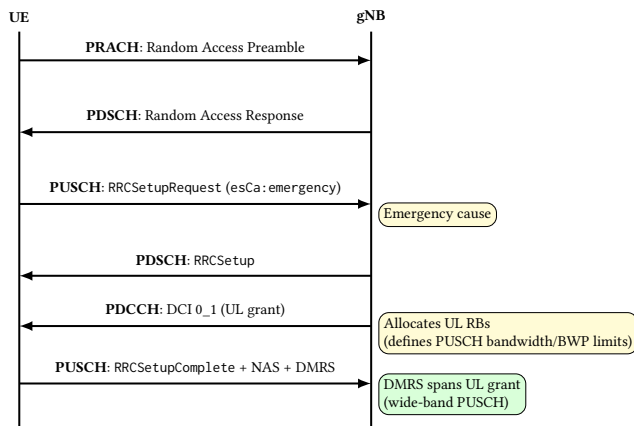


Figure 4: Emergency RRC signaling and their physical channels, and proposed uplink allocation.

preliminary location estimate directly from the RAN, ahead of any LMF-based positioning procedures.

4 Preliminary Results

This section presents initial experimental results aimed at validating the framework in realistic 5G scenarios, focusing on signaling-level feasibility and integration within existing network infrastructures.

4.1 Testbed

To validate the proposed architecture and demonstrate its feasibility, we initiated a study by developing a testbed using OAI, an open-source 3GPP-compliant platform for running 5G-RAN and 5G-CN components. As UE, we use the Google Pixel 7 Pro with a 5G USIM card. This smartphone is powered by the Google Tensor G2 chip.

4.2 Interception of RRCSetupRequest

We study a realistic call initialization scenario. During the call setup process, we successfully intercept the RRC Setup Request (*RRCSetupRequest*) message transmitted from the UE to the gNB.

```

message: c1 (0)
  <Choice Index: 0>
  v c1: rrcSetupRequest (0)
    v rrcSetupRequest
      v rrcSetupRequest
        <Choice Index: 1>
        v ue-Identity: randomValue (1)
          randomValue: 15663f4590 [bit length
          <Enumerated Index: 3>
          establishmentCause: mo-Signalling (3)
  
```

Figure 5: RRCSetupRequest message format highlighting the *EstablishmentCause* field used to signal connection requests (3GPP TS 38.331).

This message is a critical component of the connection establishment procedure in the RAN, as it specifies the reason for the UE’s request for network resources.

Notably, we are able to identify the *EstablishmentCause* field within the *RRCSetupRequest* message at runtime in the gNB, which indicates the reason for requesting the connection [8]. Fig. 5 illustrates the relevant portion of the *RRCSetupRequest* message format, highlighting the *EstablishmentCause* information element used to signal connection requests. This key field provides an explicit reason for the connection setup and serves as a reliable trigger for the RIC controller within the O-RAN architecture. While in these first tests, we did not create an emergency call to the PSAP for ethical reasons, it is possible to extend our framework using the app developed in [14], that allows to block the traffic exchange before the UE communicates to the PSAP.

4.3 RRC procedure delay

To assess the practical feasibility of reconfiguring the 5G-RAN for computing the positioning of the UE with the DMRS within the *SetupComplete* message, the time interval between the transmission of the *RRCSetupRequest* and the *RRCSetupComplete* are analyzed by repeatedly establishing the connection between the UE to the gNB.

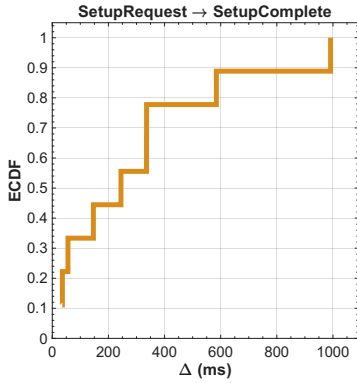


Figure 6: Experimental RRC procedure delay in LOS and NLOS conditions.

Figure 6 presents the ECDF of this delay. The majority of connection setups (over 90%) are completed within 200 ms. Two prominent clusters emerge: a first one below 50 ms, and a second broader group in the 150–200 ms range. The first cluster corresponds to Line-of-Sight (LoS) conditions, where uplink synchronization and signaling complete promptly with minimal contention or retransmissions. In contrast, Non-Line-of-Sight (NLoS) environments induce longer delays, which can be attributed to several physical-layer effects.

The hypothesis is that the main contributor to the second cluster is the activation of retransmissions at the physical layer. During the tests, multiple re-transmissions of the RRCSetup message from the gNB to the UE under NLoS conditions are observed. These retransmissions occur when the gNB fails to receive an acknowledgment on the Physical Uplink Control Channel (PUCCH) from the UE. In such cases, the gNB resends the RRCSetup message, potentially adjusting redundancy parameters to improve decoding probability. This increases the total delay between request and completion, shifting the observed setup delay towards higher values while still remaining within sub-second bounds.

While occasional outliers with delays approaching 1 s were recorded, these remain rare. Overall, the results validate the existence of a stable and usable window—typically tens to hundreds of milliseconds—within which the RAN can opportunistically collect time and angle-based features from uplink transmissions. These findings confirm that the approach remains feasible even under challenging radio conditions.

4.4 Time of Arrival with single Base Station

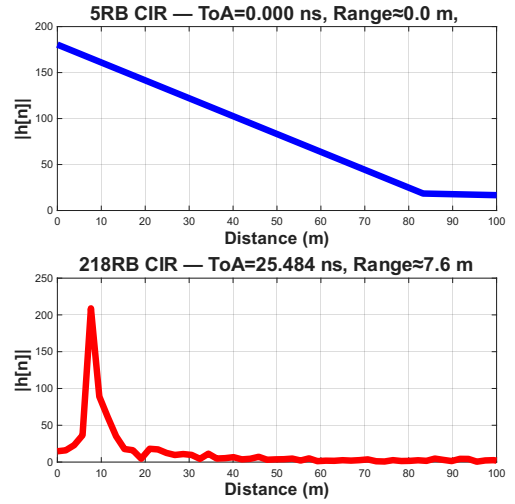
Finally, we study whether DMRS can be used for ranging measurements between the gNB and the UE. We can estimate the Time of Arrival (ToA) t_i of DMRS signal as

$$t_i = \frac{\tilde{n}}{B} \quad (1)$$

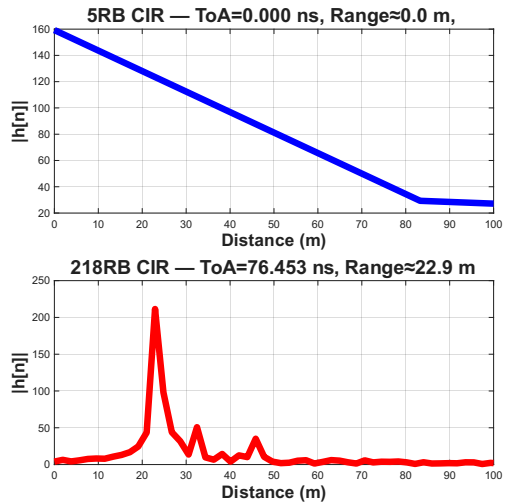
where B is the bandwidth allocated to the DMRS signal and

$$\tilde{n} = \arg \max_n |\hat{h}[n]| \quad (2)$$

Here, $|\hat{h}[n]|$ denotes the magnitude of the estimated Channel Impulse Response (CIR) in the time domain obtained from the DMRS.



(a) Comparison of CIR at 5RB and 218RB at distance ≈ 9 m, with x axis from 0 to 100 m.



(b) Comparison of CIR at 5RB and 218RB at distance ≈ 20 m, with x axis from 0 to 100 m.

Figure 7: Channel Impulse Response $|h[n]|$ vs. distance in two bandwidth configurations (default and wideband DMRS for RRCSetupComplete message).

The index \tilde{n} therefore corresponds to the sample with the maximum channel magnitude, which is used to estimate the ToA.

We can then compute the distance estimate \hat{d} as:

$$\hat{d} = \frac{1}{2} \frac{\tilde{n}}{B} c \quad (3)$$

where c is the speed of light and the factor 2 considers that the UE is time-synchronized with the gNB, with a synchronization offset equal to the propagation time.

We consider two experimental scenarios: at ground truth distance of 9 m and 20 m, indoor and outdoor respectively. In the default configuration, the DMRS uses only a few physical resource blocks (PRBs)—5 in our tests—since they suffice to transmit the

RRCSetupComplete message. As shown in the top of Fig. 7a, this results in poor distance estimation: due to the large quantization error, the gNB cannot discern the two scenarios and provides a 0 m estimate (peak of $|\hat{h}[n]|$ at $\tilde{n} = 0$) in both cases.

Conversely, by increasing PRBs to 218 (resulting in $B = 78.48$ MHz), the RRCSetupComplete message carries a wider DMRS bandwidth, enabling the gNB to discern between the two scenarios. We observe that the estimated distances are 7.6 m and 22.9 m for the 9 m and 20 m ground-truth scenarios, respectively. The residual discrepancy between estimated and true distances is primarily due to the fundamental time-resolution limitation imposed by the finite DMRS bandwidth. In fact, for $B = 78.48$ MHz, the distance quantization error is $\Delta d \approx 1.9$ m.

This study proves the effectiveness of increasing bandwidth of the RRC messages for estimating the range to the UE. The effective time resolution may be improved by oversampling of the estimated CIR or by applying interpolation techniques to the correlation peak.

5 Practical Considerations

The proposed approach has some key practical constraints that must be considered in real deployments.

First, since DMRS is embedded within the PUSCH and mapped to resources allocated dynamically by the uplink scheduler, collisions may occur if other UEs in neighbouring cells are scheduled on the same REs. Such interference can degrade or prevent successful DMRS detection at non-serving gNBs. Coordinated scheduling or partial resource reservation for emergency scenarios may therefore be necessary to guarantee reliable multi-gNB reception.

Second, successful DMRS decoding at non-serving gNBs depends on their knowledge of the relevant uplink configuration parameters – including RNTI (Radio Network Temporary Identifier), scrambling identifiers, and resource allocation details – which are typically internal to the serving cell's MAC scheduler [5–7]. We foresee two solutions: i) mechanisms for securely sharing this information across gNBs or through the RIC must be established to support this functionality; ii) centralizing this operation, sharing the received DMRS sequence with the controller, which will be then in charge of computing the required features (Sec. 3.2).

Third, the proposed methods may be extended to federation across multiple network operators. Existing approaches such as MORAN (Multi-Operator RAN) already enable shared access to radio resources among different providers while maintaining independent cores. Building on this, O-RAN interfaces such as E2 could support trusted data sharing between operators' RICs, allowing gNBs from different domains to contribute to DMRS-based timing and angle features. Such cross-operator cooperation would enhance localization accuracy and resilience in emergency situations, especially where a single network has limited coverage.

6 Conclusion

We presented a 5G/O-RAN-based framework for accelerating emergency caller localization by leveraging early access signaling and RAN analytics. A proof of concept with OAI demonstrated feasibility of detecting messages at RRC setup, evaluating delays in the process that can be leveraged to reconfigure the 5G-RAN and

performed a preliminary assessment of RRC messages in the call initiation for early inference of UE location. The approach is standards-compliant and complements AML and NILR, offering a practical path to more timely and robust emergency location.

Appendix A. Ethical Considerations: Use of Generative AI Tools

Generative AI tools and technologies were used exclusively to support grammar and minor text polishing during the preparation of this manuscript. They were also used in part to improve the visual quality of some figures. No Generative AI tools were used to generate, alter, or fabricate experimental results, data, or conclusions.

Acknowledgments

Francesco Pigato's work has been funded by Comunidad de Madrid predoctoral grant PIPF-2024/COM-35499. This paper has been funded by project PID2022-136769NB-I00 (6th-SENSE_ELSA) funded by MICIU/AEI /10.13039/501100011033/ and by the ERDF, EU.

References

- [1] [n. d.]. Advanced Mobile Location mandatory on EU smartphones. <https://www.etsi.org/newsroom/press-releases/2040-2022-03-etsi-advanced-mobile-location-standard-now-mandatory-on-all-european-smartphones-for-emergency-calls>.
- [2] [n. d.]. Android Developers: Background location and battery life. <https://developer.android.com/develop/sensors-and-location/location/battery>.
- [3] [n. d.]. O-RAN ALLIANCE e.V. <https://www.o-ran.org/>.
- [4] 2025. FCC Proposes Improvements to Wireless E911 Location Accuracy Rules. Federal Communications Commission.
- [5] 3rd Generation Partnership Project (3GPP). 2024. *5G NR; Physical channels and modulation (Release 18)*. Technical Report TS 38.211.
- [6] 3rd Generation Partnership Project (3GPP). 2024. *5G NR; Physical layer procedures for control (Release 18)*. Technical Report TS 38.213. 3GPP.
- [7] 3rd Generation Partnership Project (3GPP). 2024. *5G NR; Physical layer procedures for data (Release 18)*. Technical Report TS 38.214. 3GPP.
- [8] 3rd Generation Partnership Project (3GPP). 2024. *NR; Radio Resource Control (RRC) protocol specification (Release 18)*. Technical Report TS 38.331. 3GPP.
- [9] Apple Inc. 2020. Enhanced Emergency Data: Technical Paper for Public Safety. Technical report, Apple Public Safety Resources. https://www.apple.com/government/docs/resources/Enhanced_Emergency_Data_Tech_Paper_for_Public_Safety_092020.pdf
- [10] European Emergency Number Association (EENA). 2023. *AML Report Card: 2023 Update*. Technical Report. EENA. https://eena.org/wp-content/uploads/2023/05/2023_15_05-AML-Report-Card-FINAL.pdf
- [11] European Emergency Number Association (EENA). 2023. *EENA Recommendation on Emergency Caller Location Information Criteria for Mobile-Originated Emergency Communications*. Technical Report. European Emergency Number Association.
- [12] Federal Communications Commission. 2011. FCC Strengthens E911 Location Accuracy for Wireless Services. <https://www.fcc.gov/document/fcc-strengthens-e911-location-accuracy-wireless-services>
- [13] Google LLC. 2023. Emergency Location Service (ELS): How it works. <https://www.android.com/safety/emergency-help/emergency-location-service/how-it-works/>
- [14] Yiwen Hu, Min-Yue Chen, Haitian Yan, Chuan-Yi Cheng, Guan-Hua Tu, Chi-Yu Li, Tian Xie, Chunyi Peng, Li Xiao, and Jiliang Tang. 2024. Uncovering Problematic Designs Hindering Ubiquitous Cellular Emergency Services Access. In *ACM Mobicom*.
- [15] Mobile World Live. 2023. Location Has Never Been So Precise. Mobile World Live. <https://www.mobileworldlive.com/location-has-never-been-so-precise/>
- [16] National Emergency Number Association. 2021. *9-1-1 Statistics*. <https://www.nena.org/page/911Statistics>
- [17] O-RAN Alliance. 2023. WG3: Near-real-time RIC and E2 Interface Workgroup Specification. <https://www.o-ran.org/specifications>.
- [18] Ivan Palamà, Yago Lizarribar, Lorenzo Maria Monteforte, Giuseppe Santaromita, Stefania Bartoletti, Domenico Giustiniano, Giuseppe Bianchi, and Nicola Blefari Melazzi. 2024. 5G positioning with software-defined radios. *Computer Networks* 250 (2024), 110595.
- [19] Qingrui Pan, Mahesh K. Marina, and Thanos Triantafyllou. 2025. On NextG Open RAN as a Sensing Infrastructure. In *ACM HotMobile*.