Positioning Integrity via Uncertainty Quantification

Stefania Bartoletti, *Member, IEEE*, Ivan Palamà, *Student Member, IEEE*, Luca Chiaraviglio, *Senior Member, IEEE*, Sara Modarres Razavi, Yuxin Zhao, Giuseppe Bianchi, and Nicola Blefari-Melazzi

***Abstract*—The integrity and reliability of the positioning information are crucial for applications, including safety-critical ones, that rely on cellular network users' locations. Release 18 of the Third Generation Partnership Project (3GPP) broadens the notion of integrity, which was initially applied only to positioning based on Global Navigation Satellite System (GNSS), to include positioning based on Radio Access Technology (RAT). This paper presents a general 3GPP-compliant framework to assess 5G positioning integrity. The framework is based on uncertainty quantification and is applied to classical time-difference-of-arrival positioning algorithms and to more advanced positioning methods that rely on machine learning. In the event of an integrity alert, error mitigation techniques are also proposed to enable resilient positioning through the selection of reliable network nodes. Results obtained by using a 3GPP-compliant dataset of position estimates in an indoor open-office scenario demonstrate promising detection and resilience capabilities in the presence of integrity breaches.**

***Index Terms*—5G Positioning, Positioning Integrity, Uncertainty Quantification, Localization, Positioning Reliability**

I. Introduction

Mobile positioning is fundamental to several applications and services that rely on the location of users served by cellular networks [1]–[3]. Starting with Release 16, the 3rd Generation Partnership Project (3GPP) is enhancing 5G networks and devices with localization capabilities targeting a very high level of location accuracy and dedicated 5G core network functions [4], making the 5G network system a catalyst for a plethora of new applications in various fields such as rail, maritime, unmanned autonomous vehicles (drones), autonomous driving, vehicle-to-anything (V2X), e-health and Industial Internet of Things (IIoT) [5]–[17]. Release 17 further improves 5G positioning to meet more stringent use case requirements such as centimeter-level accuracy.

While accuracy and latency are key performance indicators for positioning, for many use-cases, the certainty, reliability, and attack awareness (i.e., jamming attack and spoofing attack) [18], [19] in the positioning system is crucial. Indeed, for all mission-critical applications in which positioning error could cause harm, safety hazards, or erroneous legal decisions, positioning integrity, which in short is the measure of trust in the correctness of the positioning information, needs to be assessed [20]–[23].

A key component of 3GPP's standardization process is position integrity for Global Navigation Satellite System (GNSS), while the positioning integrity concept is being introduced only with Release 18, given the more recent yet rapid development of positioning with radio access technologys (RATs) [24]. The definition and measurement of integrity metrics for cellular networks are challenging, as integrity depends on a number of intrinsic characteristics of the positioning system: (i) network deployment and signaling; (ii) type of location-dependent measurements used for positioning (e.g., time, angle, power); and (iii) localization algorithms adopted to process such measurements, e.g., through classical approaches such as trilateration or more advanced ones, such as those based on machine learning.

This paper proposes a general 3GPP-compliant framework for monitoring 5G positioning integrity and enabling mitigation techniques based on the quantification of positioning uncertainty. More concretely, we leverage traditional integrity indicators (e.g., used in satellite systems), which we apply in the mobile network domain. Moreover, we introduce novel approaches to quantify uncertainty in a collective way. The main contributions of this paper are:

- the mathematical formalization of positioning integrity for cellular networks;
- the definition of integrity indicators that rely on uncertainty quantification and are fully 3GPP-compliant;
- the design of a framework for collective integrity monitoring and detection of integrity failures over time;
- the proposal of mitigation techniques to enable resilient positioning through leveraging a subset of reliable network nodes.

We assess the performance of the 5G integrity framework in a TDOA-based 5G positioning use case. In particular, the generality of the proposed framework is showcased using two localization algorithms with very different performance and computational complexity: (i) a basic grid-based least-square positioning algorithm to solve the multi-lateration problem; and (ii) an advanced ML-based algorithm based on Gaussian process (GP). Results demonstrate that the suggested approach for uncertainty quantification and collective monitoring is extremely promising for assessing the integrity of cellular positioning. In addition, the proposed mitigating technique can greatly improve positioning accuracy, thus considerably lessening the effects of an integrity violation.

The remainder of the paper is organized as follows. Sec. II provides an overview of the main related works. In Sec. III, we briefly recall the fundamentals of 5G positioning and present the system model. Sec. IV presents the integrity assessment based on uncertainty quantification. The collective approach for uncertainty monitoring is presented in Sec. V. In Sec. VI, a case study is shown in which the presented framework is applied in a simulated positioning environment.

S. Bartoletti, I. Palamà, L. Chiaraviglio, G. Bianchi, and N. Blefari Melazzi are with CNIT and University of Rome Tor Vergata, Italy.

Y. Zhao and S. Modarres Razavi are with Ericsson Research, Sweden.

This work was supported by the European Union's Horizon 2020 R&I program under Grant no. 871249.

II. RELATED WORKS

Integrity is a fundamental concept in secure systems concerned with the assurance that data is accurate, complete, and unchanged during transmission. In the context of network technologies, there are two types of integrity: (i) cryptography or physical layer integrity; and (ii) statistical integrity. Cryptography and physical layer integrity ensure that the data is protected from malicious attacks, unauthorized alterations, and eavesdropping through the use of encryption, authentication, and other security mechanisms [25]–[31]. Statistical integrity, on the other hand, is focused on ensuring that the received data is consistent with the expected behavior of the system and that any anomalies are detected and corrected [32]–[40].

This paper focuses on statistical integrity, which is particularly important in positioning systems where a range of environmental unintentional factors such as multipath effects, limited satellite visibility and interference, or intentional factors such as spoofing can affect the accuracy and reliability of the position estimation, see, e.g., [26].

In 3GPP Release 17 [41], the necessary solutions to support the integrity and reliability of positioning assistance data were studied, specifically in identifying positioning integrity Key Performance Indicators (KPIs) and error sources for GNSS, which is a RAT-independent positioning technology [24]. This demonstrates the importance of statistical integrity and its integration into the 3GPP standardization process. Nevertheless, most of the existing works in the literature are focused on GNSS systems to provide security against uncertainties that can affect GNSS performance [38], [42]–[47].

Receiver Autonomous Integrity Monitoring (RAIM) is a technique used to ensure the statistical integrity of GNSS positioning performance. Specifically, RAIM uses a set of algorithms that allow the receiver to check the consistency of the measurements received from multiple satellites and detect any anomalies, thus providing an additional layer of security for the GNSS positioning performance. RAIM can be divided into two types: traditional RAIM methods and Bayesian RAIM methods. Traditional RAIM uses statistical consistency checks on range residuals and position estimates to eliminate faulty measurements [38]. This approach is based on redundant measurements and does not provide a direct instantaneous probability distribution of position error. On the other hand, Bayesian RAIM uses prior information and actual measurements to calculate the posterior probability distribution of position error [40], [48]. This approach can result in a more accurate probability of loss but can be computationally complex, especially when the number of unknown parameters is large.

Another example of positioning integrity is Cooperative Integrity Monitoring (CIM) [46], [49]. CIM is a real-time approach that involves cooperation between multiple devices in a distributed system to detect and mitigate errors in the location information provided by the mobile network. CIM is an effective approach for real-time error detection and mitigation but requires the devices to be in close proximity to each other for effective cooperation, which can limit its applicability in certain situations. Additionally, CIM can be resource-intensive, as it requires continuous communication between devices.

Despite the recognized importance of RAIM and CIM techniques for RAT-independent technologies, their employment for cellular systems has only recently started [50], [51]. As a matter of fact, cellular positioning is evolving rapidly in 5G and beyond leading to an urgent need for expanding and assessing positioning integrity in cellular networks. Nevertheless, there is still a lack of mathematical formalization of the issue and a general approach for calculating integrity based on measurements carried out within the network for the user's positioning. In [52], a promising RAIM-based methodology is presented, while preliminary numerical results support this without providing mitigation techniques in case of integrity breaches.

The scope of this paper is to fill the existing gap in the definition of a general framework that permits integrity techniques to be applied to cellular positioning systems. On the one hand, example methodologies used in the GNSS will be revised by considering recent advancements in 5G positioning so as to be fully compliant with the 3GPP standards. Furthermore, a new approach will be proposed, which leverages integrity-related information from multiple UEs connected to the same network and machine learning (ML) techniques to enable a collective integrity assessment. Such a collective approach will allow the network to monitor positioning integrity over space and time, not only to detect any breach but also to develop mitigation strategies aimed at enhancing positioning accuracy.

III. FUNDAMENTALS OF 5G POSITIONING AND INTEGRITY

We initially provide a concise overview of the main positioning measurements and methods in 5G networks – useful for the non-experts in the field. In the following, we sketch the system model to formalize the network topology and measurements, which constitute the foundation of our integrity framework. Finally, we define and model the target integrity risk as a performance metric for 5G positioning.

A. 5G Positioning Methods

The user equipment (UE) position in 5G is estimated based on location-dependent measurements (e.g., time of arrivals or angles) performed between the UE and one or multiple 5G radio network nodes called gNode-Bs (gNBs), either in uplink or downlink. In particular, the Sounding Reference Signals (SRS) for the uplink and an enhanced Positioning Reference Signal (PRS) for the downlink positioning are introduced as new NR reference signals. Although other downlink signals can be used, the PRS has better correlation properties to improve positioning accuracy than existing reference signals, thanks to the diagonal or staggered PRS Resource Element (RE) pattern. Moreover, the PRS signal provides better coverage and robustness against interference from adjacent cells [41], [53], [54].

3GPP Release 16 introduced several positioning methods for 5G: (i) Downlink Time Difference of Arrival (DL-TDOA), (ii) Uplink Time Difference of Arrival (UL-TDOA), (iii) Downlink Angle-of-Departure (DL-AOD), (iv) Uplink Angle-of-Arrival

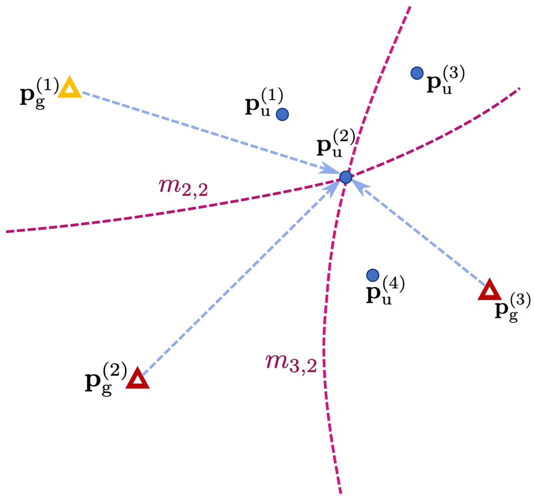


Fig. 1: Example network deployment with $N_{\mathrm{g}} = 3$ gNBs (triangles) and $N_{\mathrm{u}} = 4$ UEs (circles). The TDOA $m_{3,2}$ and $m_{2,2}$ are measured considering the first anchor as the reference one (yellow triangle). The corresponding hyperbolas are illustrated in magenta.

(UL-AOA), and (iv) Multi-Round Trip Time (Multi-RTT) positioning. Such methods are defined based on the type of measurements used, i.e., time measurements (DL-TDOA, UL-TDOA, Multi-RTT) or angle measurements (DL-AOD, UL-AOA), as well as whether the measurement is uplink or downlink using the appropriate reference signal.

In this paper, we mainly focus on DL-TDOA without loss of generality, as the integrity framework proposed can be easily extended to other RAT-dependent positioning methods. In the DL-TDOA scheme, the UE measures the TDOA of the DL-PRS of a set of gNBs according to the positioning assistance information received from the network's Location Management Function (LMF), i.e., a network function dedicated to the positioning service, and sends the Reference Signal Timing Difference (RSTD) measurements to the location management function (LMF), i.e. the network function that calculates the position estimate. An illustration of the main measurements used for DL-TDOA is proposed in Fig. 1 according to the system model presented in the following.

B. System Model

We consider a network of N_{g} gNBs that are operating in a monitored area. The nth gNB is at $\mathbf{p}_{\mathrm{g}}^{(n)}$, with $n \in \mathcal{N}_{\mathrm{g}} = \{1, 2, \dots, N_{\mathrm{g}}\}$. The positioning service is active for N_{u} users within a certain observation time window T_{obs}. The true unknown position of the ith UE is at $\mathbf{p}_{\mathrm{u}}^{(i)}$, with $i \in \mathcal{N}_{\mathrm{u}} = \{1, 2, \dots, N_{\mathrm{u}}\}$. Fig. 1 illustrates a network deployment example with this system model.

We consider that all the gNBs are serving all the UEs and therefore, a measurement is performed between each gNB with respect to each UE. According to the DL-TDOA method, the gNBs are synchronized and the UE measures the TOA $t_{n,i}$ for the DL-PRS signal transmitted from the nth gNB, with $n \in \mathcal{N}_{\mathrm{g}}$. In ideal conditions (no error sources) and free-space propagation, $t_{n,i} = \|\mathbf{p}_{\mathrm{g}}^{(n)} - \mathbf{p}_{\mathrm{u}}^{(i)}\|/c$, where c is the speed-of-light. Then, the TDOA for the nth gNB with respect to the reference rth gNB is calculated at the UE as $t_{n,i} - t_{r,i}$.

In real scenarios, the measurement model for the TDOA is

$$m_{n,i} = \|\mathbf{p}_{\mathrm{g}}^{(n)} - \mathbf{p}_{\mathrm{u}}^{(i)}\|/c - \|\mathbf{p}_{\mathrm{g}}^{(r)} - \mathbf{p}_{\mathrm{u}}^{(i)}\|/c + w_{r,n,i} \quad (1)$$

where the measurement noise $w_{n,i}$ is generally dependent on the position of the nodes, the line-of-sight (LOS) conditions between each transmitter and receiver, and the signal-to-noise ratio (SNR) of the two received signals. Therefore, $w_{n,i}$ is a random variable that depends on many nuisance parameters.

Then, the positioning algorithm, deployed within the LMF, estimates the ith UE position as $\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}$, by processing the measurements vector $\mathbf{m}_i = [m_{1,i}, m_{2,i}, \dots, m_{N_{\mathrm{g}},i}]$, that includes the TDOA measurements from all the gNBs with respect to the reference one. Specifically for the DL-TDOA, $\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}$ is obtained as the point that intersects $N_{\mathrm{g}} - 1$ hyperbolas, where the nth hyperbola is defined as the set of points $\{\mathbf{p} : \|\mathbf{p}_{\mathrm{g}}^{(n)} - \mathbf{p}\|/c + \|\mathbf{p}_{\mathrm{g}}^{(r)} - \mathbf{p}\|/c = m_{n,i}\}$. The positioning error is defined as the Euclidean distance between the true and estimated UE position, i.e.

$$e_i = \|\mathbf{p}_{\mathrm{u}}^{(i)} - \hat{\mathbf{p}}_{\mathrm{u}}^{(i)}\|\,. \quad (2)$$

The specific positioning algorithm adopted to find the intersection of hyperbolas further impacts the final positioning accuracy. Classical, low-complexity solutions are based on least squares (LS) algorithm. More recently, ML algorithms have been considered to solve the positioning problems [55]–[57]; in such a case the measurement model in eq. (1) is learned during a training phase, i.e., for learning the statistical distribution of $n_{n,i}$, and then used for position estimation in the online phase.

C. Target Integrity Risk

As part of the 5G service requirements specified in [58], the reliability of position-related data and the level of uncertainty or confidence must be determined. Positioning integrity is defined as a measure of trust in the accuracy of the position estimate and the capability of providing timely and valid warnings when the positioning system does not fulfill the conditions for the intended operation.

Such a condition for intended operation is defined through the alert limit (AL), here denoted as e_{al}, i.e., the maximum allowable value for the positioning error (denoted by e_i and defined in (2)) such that the positioning system is available for the intended application. Specifically, if the positioning error is beyond the AL, i.e., $e_i > e_{\mathrm{al}}$ the positioning system should be declared unavailable for the intended application to prevent loss of positioning integrity. Furthermore, a possibility could be to detect the source of error for the integrity failure and refine the position estimation based on a subset of reliable measurements.

We define an integrity indicator $\beta_{\mathrm{al}}^{(i)}$ as a Boolean variable that is flagged to 1 when an integrity alert is issued. Based on the AL e_{al} and such integrity alert $\beta_{\mathrm{al}}^{(i)}$, the target integrity risk (TIR) R_{TIR} is defined as the probability that the positioning error exceeds the AL without warning the user within the

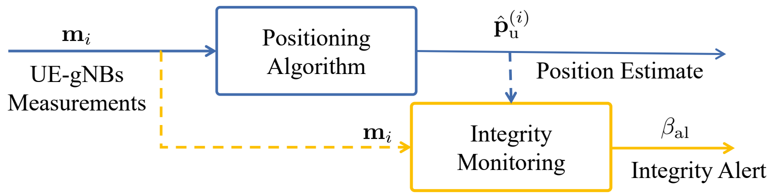


Fig. 2: Building blocks of measurement processing for integrity assessment.

required time-to-alert (TTA). The IR is usually defined as a probability rate per some time unit (e.g., per hour, per second, or per independent sample). In our framework, we consider the position estimates for all the UEs with index $i \in \mathcal{N}_{\text{u}}$, i.e., the positions $\mathcal{N}_{\text{u}}$ represents an independent sample of the users, and we define the IR as

$$R_{\text{TIR}} = \mathbb{P}_{i\in\mathcal{N}_{\text{u}}}\Big\{\{e_i > e_{\text{al}}\} \cap \{\beta_{\text{al}}^{(i)} = 0\}\Big\} \tag{3}$$

which is the probability that the errors e_i in the independent sample $i \in \mathcal{N}_{\text{u}}$ are above the e_{al} limit while the integrity indicator is 0, i.e., no warning is provided. Note that the value of R_{TIR} depends on the positioning process, including the positioning algorithm, through the positioning error as well as by the specific definition for the integrity indicator, which is left to the implementation.

IV. Uncertainty Quantification for Integrity Assessment

In this section, we introduce the integrity assessment framework. The main blocks are illustrated in Fig. 2. Intuitively, the output of the positioning system with integrity assessment is the estimated position $\hat{\mathbf{p}}_{\text{u}}^{(i)}$ together with an integrity alert $\beta_{\text{al}}^{(i)}$. The estimated position is obtained from the measurement vector $\mathbf{m}$ containing the measurements between each gNB and the ith UE through a positioning algorithm. The integrity alert is obtained by processing both the measurement vector and the estimated position; therefore, the integrity alert depends on the specific positioning algorithm considered. Note that the evaluation of the positioning algorithm is out of the scope of this paper; therefore, we selected two example algorithms that are very different in terms of computational complexity and positioning performance to demonstrate the generality of the integrity framework.

In an ideal condition, the Boolean variable $\beta_{\text{al}}^{(i)}$ would be flagged to 1 when $\{e_i > e_{\text{al}}\}$ and 0 otherwise, i.e., leading the TIR to zero. Nevertheless, this would require the perfect knowledge of the positioning error, which is unknown in real operating conditions. While the true error cannot be measured, there exist multiple ways to measure the uncertainty associated with the position estimate [50], [51]. Therefore, we assume that for each position estimate $\hat{\mathbf{p}}_{\text{u}}^{(i)}$ with $i \in \mathcal{N}_{\text{u}}$ we are able to measure an uncertainty level u_i associated with the estimation. In the next two subsections, we will define how to set $\beta_{\text{al}}^{(i)}$ for two categories of positioning algorithms for DL-TDOA: classical positioning and ML-based algorithms.

Algorithm 1 Classical Positioning and Uncertainty Quantification

---

1) The distances from the ith UE to all the N_{g} gNBs are computed as: $\mathbf{m}_i$ with nth element $m_{n,i}$ and $n = 1, 2, \ldots, N_{\text{g}}$.
2) Compute the position estimation as
$$\hat{\mathbf{p}}_{\text{u}}^{(i)} = \arg\min_{\mathbf{p}} \left(\sum_{n=1}^{N_{\text{g}}} m_{n,i} - \|\mathbf{p}_{\text{g}}^{(n)} - \mathbf{p}\|/c - \|\mathbf{p}_{\text{g}}^{(r)} - \mathbf{p}\|/c\right)^2 \tag{4}$$
3) Compute the residuals as:
$$r_{n,i} = m_{n,i} - \|\mathbf{p}_{\text{g}}^{(n)} - \hat{\mathbf{p}}_{\text{u}}^{(i)}\|/c - \|\mathbf{p}_{\text{g}}^{(r)} - \hat{\mathbf{p}}_{\text{u}}^{(i)}\|/c \tag{5}$$
4) Compute the uncertainty as:
$$u_i = \left[\frac{1}{N_{\text{g}} - 2} \sum_{n\in\mathcal{N}_{\text{g}}} r_{n,i}^2\right]^{1/2} \tag{6}$$

A. Classical Positioning

a) Positioning Algorithm: As a classical positioning algorithm, we consider a basic LS algorithm, which aims at solving the system of equations given by the TDOA-based hyperbolas by minimizing the sum of squared residual errors as reported in Algorithm 1 [59].

b) Integrity Indicator: Given the UE estimated position $\hat{\mathbf{p}}_{\text{u}}^{(i)}$ and the measurement vector $\mathbf{m}_i$, for the ith gNB, we can consider the residual $r_{n,i}$ as in [51]

$$r_{n,i} = m_{n,i} - \|\mathbf{p}_{\text{g}}^{(n)} - \hat{\mathbf{p}}_{\text{u}}^{(i)}\|/c + \|\mathbf{p}_{\text{g}}^{(r)} - \hat{\mathbf{p}}_{\text{u}}^{(i)}\|/c \tag{7}$$

which represents the difference between the ideal distance that would be expected if the UE was $\hat{\mathbf{p}}_{\text{u}}^{(i)}$ and the value $m^{(i)}(\mathbf{p}_{\text{u}})$ that is actually measured. This quantity $r_{n,i}$ represents the residual error for the measurement model (1) given the estimated position.

A possible uncertainty measurement in the absence of measurement models is the standard error calculated as [51]

$$u_i = \left[\frac{1}{N_{\text{g}} - 2} \sum_{n\in\mathcal{N}_{\text{g}}} r_{n,i}^2\right]^{1/2}. \tag{8}$$

Then, a simple integrity indicator for the single, ith UE is

$$\beta_{\text{al}}^{(i)} = \mathbb{1}\{u_i > u_{\text{th}}\} \tag{9}$$

which is equal to 1 when the uncertainty level is above a threshold u_{th} and 0 otherwise.

B. ML-based Positioning

a) Positioning Algorithm: In real scenarios, the measured time-of-arrival (TOA) is a random variable that depends on many nuisance parameters, e.g., related to multipath propagation. Thus, in general, the statistical distribution of the generic measurement $m_{n,i}$ in (1) is unknown and hard to be derived. There are many regression tools, including ML-based ones, that can be employed to learn the statistical characterization of the TOA or TDOA measurements [60].

GP-based models are widely adopted in a plethora of applications thanks to their outstanding performance in function approximation with a self-contained uncertainty bound [61]. The gist of GP is to impose a Gaussian prior on the function/system $f(x)$ and then compute the posterior distribution over the function given the observed data. One advantage of using GP is that there is no need to have prior assumptions about the function itself. The training data set fully determines the function. To be more specific, a GP is a generalization of the Gaussian probability distribution. In a GP, every point in some continuous input space is associated with a normally distributed random variable. Moreover, every finite collection of those random variables has a multivariate normal distribution. The distribution of a GP is the joint distribution of all those (infinitely many) random variables. In GP, the joint distribution of the distances is still Gaussian [50], [62].

In [50], a generic model for the true distance $d_{n,i}$ between the nth gNB and ith UE is assumed, i.e.

$$d_{n,i} = f_n(t_{n,i}) + z_{n,i}, \tag{10}$$

where $z_{n,i}$ is a zero mean Gaussian random variable with variance $\sigma^2_{n,i}$, and the function $f_n(t_{n,i})$ is modeled by a GP. In particular, the GP can be formulated as

$$f_n(t_{n,i}) \sim \mathcal{GP}\big(\mu_n(t_{n,i}), k_n(t_{n,i}, t'_{n,i})\big). \tag{11}$$

where $\mu_n(t_{n,i})$ is the mean function, and $k_n(t_{n,i}, t'_{n,i})$ is the covariance/kernel function which indicates the correlation between two TOA measurements $t_{n,i}$ and $t'_{n,i}$.

Using a supervised ML approach, during the training phase, a set of TOA measurements $t_{n,i}$ for the nth gNB are collected in known positions $\mathbf{p}_{\text{u}}^{(i)}$, with index $i \in \mathcal{N}_{\text{u}}^{(\text{tr})}$. Then, a probability model $f(d_{n,i}|t_{n,i}, \mathcal{T}_n)$ for each gNB is trained based on the dataset of measurements and true distances $\mathcal{T}_n \triangleq \{(t_{n,i}, d_{n,i})\}_{i\in\mathcal{N}_{\text{u}}^{(\text{tr})}}$. Parameters such as $\sigma^2_{n,i}$, and hyperparameters in the kernel function can be learned during the training phase by maximizing the log-likelihood function $\log f(d_{n,i}|t_{n,i}, \mathcal{T}_n)$ according to [62].

In the prediction/positioning phase, we make use of the trained GP models to predict the true distances from the UE to gNBs based on the TOA estimations. For a new TOA measurement $t^\star_{n,i}$, the predicted true distance $d^\star_{n,i}$ is modeled as

$$f(d^*_{n,i}|t^*_{n,i}, \mathcal{T}_n) \sim \mathcal{N}(\hat{\mu}_{\mathcal{T}_n}(t^*_{n,i}), \hat{k}_{\mathcal{T}_n}(t^*_{n,i})), \tag{12}$$

and therefore, its estimate is obtained as

$$\hat{d}_{n,i} \sim \mathcal{N}(\hat{\mu}_{\mathcal{T}_n}(t_{n,i}), \hat{k}_{\mathcal{T}_n}(t_{n,i})), i = n, \ldots, N_{\text{g}}\,. \tag{13}$$

Finally the estimated time-difference-of-arrival (TDOA) with the rth gNB acting as the reference gNB is obtained as

$$\hat{m}_{n,i} = (\hat{d}_{r,i} - \hat{d}_{n,i})/c\,. \tag{14}$$

This way, a new vector is obtained as $\hat{\mathbf{m}}_i = [\hat{m}_{1,i}, \hat{m}_{2,i}, \ldots, \hat{m}_{N_{\text{g}},i}]$ of predicted measurements. With the above derivations, the estimated position of UE is computed through Algorithm 2, where the measurements $\hat{\mathbf{m}}_i$ predicted through the GP are used to feed the LS algorithm introduced in Algorithm 1.

b) Integrity Indicator: To measure the uncertainty level u_i, we can sample the distribution of the estimated distance $\mathcal{N}(\hat{\mu}_{\mathcal{T}_n}(t_{n,i}), \hat{k}_{\mathcal{T}_n}(t_{n,i}))$ and collect N_{s} sampled distances $\hat{d}_{n,i,k}$ and therefore N_{s} measurement vectors $\hat{\mathbf{m}}_{i,k}$, with $k = 1, 2, \ldots, N_{\text{s}}$. From the kth measurement vector, we compute the position estimates $\hat{\mathbf{p}}_{\text{u}}^{(i,k)}$ using the LS algorithm approach. The uncertainty vector is then calculated using the N_{s} position estimates as

$$\mathbf{v}(\hat{\mathbf{p}}_{\text{u}}^{(i)}) = \frac{1}{N_{\text{s}}-1}\sum_{n_{\text{s}}=1}^{N_{\text{s}}}(\hat{\mathbf{p}}_{\text{u}}^{(i,k)} - \hat{\mathbf{p}}_{\text{u}}^{(i)})^2 \tag{17}$$

and the uncertainty level as

$$u_i = \sqrt{v_x + v_y}, \tag{18}$$

where $\mathbf{v}(\hat{\mathbf{p}}_{\text{u}}^{(i)}) \triangleq [v_x, v_y]^T$, v_x and v_y denote the uncertainty in x and y coordinate, respectively. Then, an integrity indicator for the single, ith UE is obtained as in (9).

Algorithm 2 ML-based Positioning and Uncertainty Quantification

1) The distances from the ith UE to all the N_{g} gNBs are predicted as: $\hat{\mathbf{m}}_i$ where the nth element is $\hat{m}_{n,i}$ and $n = 1, 2, \ldots, N_{\text{g}}$.
2) Compute the position estimation as
$$\hat{\mathbf{p}}_{\text{u}}^{(i)} = \arg\min_{\mathbf{p}} \Big(\sum_{n=1}^{N_{\text{g}}} \hat{m}_{n,i} - \|\mathbf{p}_{\text{g}}^{(n)} - \mathbf{p}\|/c - \|\mathbf{p}_{\text{g}}^{(r)} - \mathbf{p}\|/c\Big)^2 \tag{15}$$
3) For $k = 1, \ldots, N_s$, do
   - Take samples from the Gaussian distribution $\mathcal{N}(\hat{\mu}_{\mathcal{T}_n}(t_{n,i}), \hat{k}_{\mathcal{T}_n}(t_{n,i}))$
   - Denote the sampled distances as $\hat{d}_{n,i,k}$ and obtain $\hat{\mathbf{m}}_{i,k}$
   - Use $\hat{\mathbf{m}}_{i,k}$ to feed the LS algorithm (see Sec. IV-A and compute the kth position estimate $\hat{\mathbf{p}}_{\text{u}}^{(i,k)}$
4) Compute the uncertainty vector as $\mathbf{v}(\hat{\mathbf{p}}) = [v_x, v_y]$ from (17)
5) Compute the uncertainty as:
$$u_i = \sqrt{v_x + v_y}, \tag{16}$$

V. Collective Integrity Monitoring

In this section, we introduce a general framework for collective integrity monitoring. The idea behind the framework

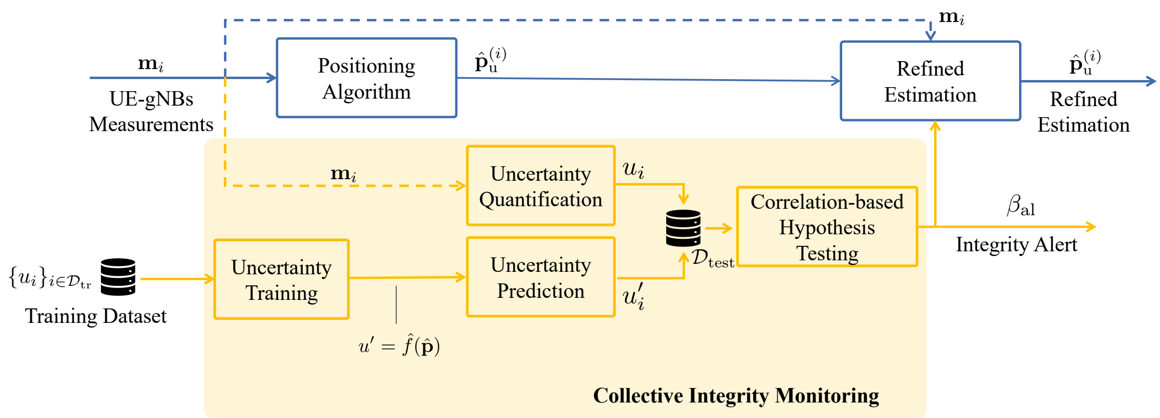


Fig. 3: Building blocks of measurement processing for collective integrity monitoring.

is that the positioning system is expected to guarantee the required level of accuracy when operating in normal conditions, i.e., in the absence of integrity problems. In such conditions, the positioning error is spatially correlated among users, as the error sources are due to channel conditions. Therefore, by gathering the uncertainty level from multiple users, we could train a spatial model and build the uncertainty map in a collective way. Then, it would be possible to monitor the uncertainty map over time to detect any significant change, e.g., due to an integrity breach, and possibly mitigate its effect.

Fig. 3 summarizes the main building blocks of collective integrity monitoring, which are then specified in the next subsections. We first present the collective process for uncertainty modeling and training. Then, building on the trained model, we elaborate further on the integrity indicators defined in Sec. IV for detecting integrity failures collectively. Finally, we propose mitigation techniques to refine the position estimate in case an anomaly is detected.

A. Uncertainty Modelling and Training

a) Uncertainty Model: The uncertainty value is a function of the estimated position, and therefore we can model it as a random variable

$$u_i = f(\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}) + \varepsilon_i \,. \tag{19}$$

where we are considering the uncertainty measure u_i as a generic one, disregarding the specific positioning algorithm. As the model for the uncertainty is unknown and depends on multiple factors (e.g., network deployment and configuration, signal propagation environment, positioning algorithm), we propose the use of a regression tool to learn the probability model $f(\hat{\mathbf{p}})$. Then, we model $f(\hat{\mathbf{p}})$ in as a GP, i.e.

$$f(\hat{\mathbf{p}}) \sim \mathcal{GP}\big(\mu(\hat{\mathbf{p}}), k(\hat{\mathbf{p}}, \hat{\mathbf{p}}')\big). \tag{20}$$

where $\mu(\hat{\mathbf{p}})$ is the mean function, and $k(\hat{\mathbf{p}}, \hat{\mathbf{p}}')$ indicates the correlation between two uncertainty measurements corresponding to two estimated positions $\hat{\mathbf{p}}$ and $\hat{\mathbf{p}}'$.

b) Uncertainty Training: Specifically, a training dataset $\mathcal{D}_{\mathrm{tr}}$ is collected. The dataset contains the position estimates and uncertainty measures associated with a set of users, i.e., $\mathcal{D}_{\mathrm{tr}} = \{(\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}, u_i)\}_{i\in\mathcal{S}_{\mathrm{tr}}}$. The measurements and estimates with index set $\mathcal{S}_{\mathrm{tr}}$ are used to obtain the probability model $f(\hat{\mathbf{p}})$ for the uncertainty u_i as a function of the position estimate $\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}$. A geometrical interpretation of $\hat{f}(\hat{\mathbf{p}})$ is that it represents a probabilistic map of the positioning uncertainty as a function of the estimated position in normal conditions, i.e., in the absence of integrity breaches. Then, in the uncertainty prediction phase, when a new position estimate is obtained as $\hat{\mathbf{p}}^*$, the predicted uncertainty u^* is estimated as

$$f(u^*|\hat{\mathbf{p}}^*, \mathcal{D}_{\mathrm{tr}}) \sim \mathcal{N}(\hat{\mu}_{\mathcal{D}_{\mathrm{tr}}}(\hat{\mathbf{p}}^*), \hat{k}_{\mathcal{D}_{\mathrm{tr}}}(\hat{\mathbf{p}}^*)). \tag{21}$$

The kernel function used in this work is the Squared Exponential (SE) kernel:

$$k(\hat{\mathbf{p}}, \hat{\mathbf{p}}') = \sigma_k^2 \exp(-\frac{||\hat{\mathbf{p}} - \hat{\mathbf{p}}'||^2}{2l^2}), \tag{22}$$

where σ_k and l are hyperparameters, which can be estimated by maximizing the likelihood function calculated with the trained dataset $\mathcal{D}_{\mathrm{tr}}$.

B. Integrity Indicator based on Collective Uncertainty

In the next Sections, we will specify the uncertainty prediction and goodness-of-fit blocks in Fig. 3. In particular, these will be specified for the 1 and 2 as case studies.

a) Uncertainty Prediction: When an integrity failure is experienced, the predicted uncertainty can deviate from the expected one. Note that we can always measure the single uncertainty value u_i for any position estimate $\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}$ during the positioning system operation. Meanwhile, if the uncertainty model has been trained as in (21), we can predict the uncertainty value associated with the estimated position, which, according to the GP model, is distributed as

$$u'_i \sim \mathcal{N}\big(\hat{\mu}_{\mathcal{D}_{\mathrm{tr}}}(\hat{\mathbf{p}}_{\mathrm{u}}^{(i)}), \hat{k}_{\mathcal{D}_{\mathrm{tr}}}(\hat{\mathbf{p}}_{\mathrm{u}}^{(i)})\big) \,. \tag{23}$$

b) Goodness-of-fit Test: Then, for the ith user, we have a measured uncertainty value u_i and a predicted one u'_i. We carry out a goodness-of-fit test for any independent sample of position estimates to evaluate if the model still fits the observed data. Specifically, if the model does not fit the observed data, this should trigger an integrity alert for the position estimation process (e.g., a gNB is not working properly or the propagation conditions have changed substantially) and eventually can trigger an integrity mitigation process to refine the position estimate.

There are several tests for goodness-of-fit, which depend on the available information and on the definition of the uncertainty itself. Let's assume an independent sample of position estimates and associated uncertainty measures are collected online, i.e., $\mathcal{D}_{\text{on}} = \{(\hat{\mathbf{p}}_{\text{u}}^{(i)}, u_i, u_i')\}_{i\in\mathcal{N}_{\text{u}}}$ where the UEs are indexed by $i \in \mathcal{N}_{\text{u}}$, u_i is the uncertainty level measured online, while u_i' is the uncertainty level that is predicted according to (23). A simple yet effective goodness-of-fit test is the fraction of variance unexplained (FVU), which corresponds to the fraction of variance of the uncertainty level in the observed dataset that can be explained by a regression model. Considering the uncertainty model, the FVU is calculated as

$$\Phi_{\text{vu}}^{(\mathcal{N}_u)} = \frac{\sum_{i\in\mathcal{N}_{\text{u}}}\left(u_i' - u_i\right)^2}{\sum_{i\in\mathcal{N}_{\text{u}}}\left(u_i' - \overline{u}\right)^2} \tag{24}$$

where $\overline{u} = \frac{1}{N_{\text{u}}}\sum_{i\in\mathcal{N}_{\text{u}}} u_i$. Specifically, small values for Φ_{vu} indicate that the regression model considered is able to explain most of the variance of the observed data. Then, a threshold Φ_{th} can be set such that the integrity indicator is

$$\beta_{\text{al}}^{(\mathcal{N}_{\text{u}})} = \mathbb{1}\left\{\Phi_{\text{vu}} \geq \Phi_{\text{th}}\right\} \tag{25}$$

where $\mathbb{1}\{\mathcal{A}\}$ is equal to 1 if the event $\mathcal{A}$ is true, and 0 otherwise.

Despite the design for the value of Φ_{th} is not the scope of this paper, this can be chosen on the basis of the value of Φ_{vu} under normal conditions (i.e., by collecting an additional independent sample during the training phase). Alternatively, in the presence of a prior model on the positioning error, the value of Φ_{th} can be chosen to satisfy the desired risk level R_{TIR}.

C. Mitigation of Integrity Failure

When an integrity alert warning is provided, i.e., $\beta_{\text{al}}^{(i)} = 1$, the position estimate $\hat{\mathbf{p}}_{\text{u}}^{(i)}$ for each $i \in \mathcal{N}_{\text{u}}$. In particular, the refined position is obtained by selecting a subset of measurements, i.e., the ones obtained through gNB that are believed to be more reliable based on the residual error.

Specifically, in the case of classical positioning, a subset of gNBs with index $\mathcal{S}_{\text{g}}^{(i)} \subset \mathcal{N}_{\text{g}}$ is selected as the subset of anchors with lower residual error. The positioning estimation is then refined as

$$\hat{\mathbf{p}}_{\text{u}}^{(i)} = \arg\min_{\mathbf{p}} \sum_{n\in\mathcal{S}_{\text{g}}^{(i)}} \left(m_{n,i} - \|\mathbf{p}_{\text{g}}^{(n)} - \mathbf{p}\|/c - \|\mathbf{p}_{\text{g}}^{(r)} - \mathbf{p}\|/c\right)^2. \tag{26}$$

In the ML-based positioning, if an integrity alert is issued, i.e., $\beta_{\text{al}}^{(\mathcal{N}_u)} = 1$, the position estimate $\hat{\mathbf{p}}_{\text{u}}^{(i)}$ for each $i \in \mathcal{N}_{\text{u}}$ can be updated by selecting a subset of measurements, i.e., the ones obtained through gNB that are believed to be more reliable based on the residuals with respect to the estimated position. Then, the GP process is trained on $\mathcal{T}_n$ by only considering $n \in \mathcal{S}_{\text{g}}^{(i)}$, i.e., the measurements in the training dataset from the most reliable anchors. A new model is obtained, and the position estimate is updated as in (26).

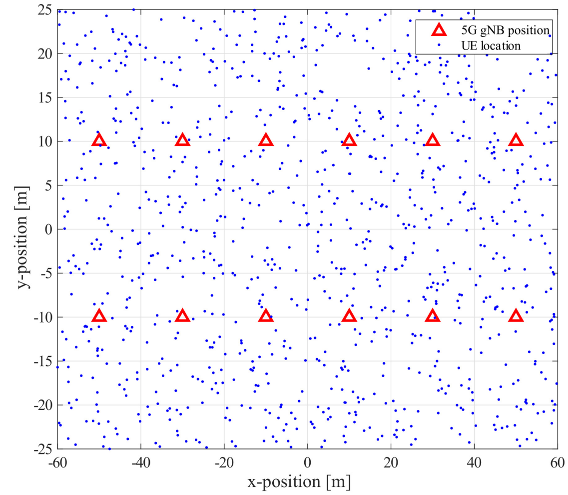


Fig. 4: Indoor open office deployment.

VI. Case Study

This Section presents the simulation results in a case study representing a standard Indoor Open Office (IOO) scenario. First, the simulation settings are introduced. Then, the results in terms of integrity assessment are presented. Finally, the mitigation techniques are evaluated for both the classical and ML-based positioning.

A. Simulation Settings

a) Operating Scenario: For the purpose of evaluation we consider a standard Indoor Open Office (IOO) scenario defined by 3GPP [63]. The standard IOO scenario considers an indoor area of 120 m × 50 m where 12 gNBs are deployed, maintaining a 20 m inter-site distance as shown in Fig. 4. All 12 gNBs are anchored to the ceiling at a height of 3 m and transmit PRS using an isotropic antenna. The radio links between UE and gNB follow multi-path propagation and are subjected to both LOS and NLOS conditions (depending on how far the UE is located from a gNB) and following the LOS probability distribution function defined in [63]. In total, 1000 UEs (at the height of 1.5m) are randomly dropped within the deployment area. In the simulation, UEs measure the DL PRS signals and the TOA measurements between each UE and all 12 gNBs are estimated and recorded. The estimated TOA corresponds to the time of flight of the PRS transmitted from a gNB and reaching UE via the first significant path, regardless of whether the radio link between UE and gNB is in LOS or NLOS condition.

b) Integrity Breach Simulation: For the integrity assessment evaluation, we start by defining an integrity breach related to a single gNB. Specifically, a random bias is added to the TOA from the nth gNB so that

$$t_{n,i}' = t_{n,i}(1 + b(\delta)) \tag{27}$$

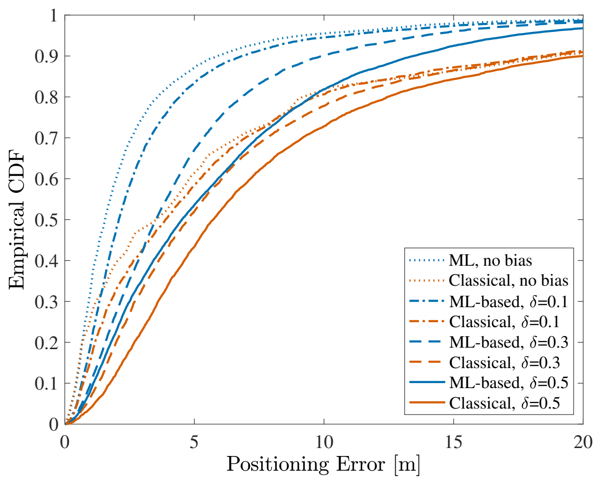


Fig. 5: cumulative distribution function (CDF) versus positioning error with unbiased condition $b(\delta) = 0$ (dotted line) and varying δ, in both classical and ML-based positioning.

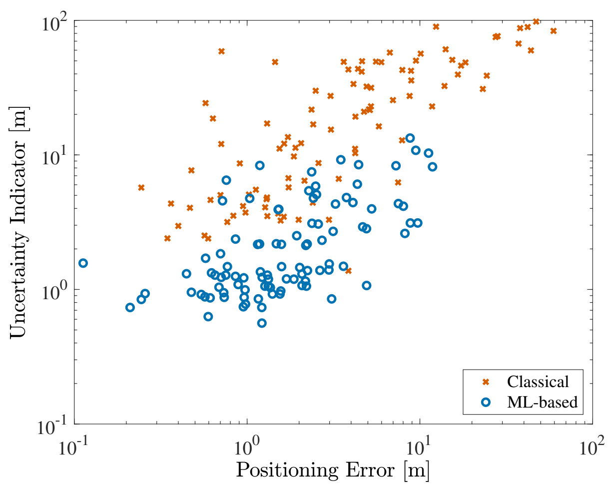


Fig. 6: Scatterplot of the uncertainty indicator u_i as a function of the positioning error e_i for the Classical and ML-based positioning algorithms.

where the bias $b(\delta)$ is uniformly distributed as $b(\delta) \sim \mathcal{U}(\delta, \delta+0.1)$. Results are obtained by varying $\delta = \{0.1, 0.2, \ldots, 0.5\}$. Therefore, the parameter δ indicates the extent of the integrity breach. For each value of δ, simulation results are obtained with 10^4 simulations for each biased gNB, for a total of 12×10^4 position estimates.

Fig. 5 shows the CDF for the positioning error under default conditions and in the presence of an integrity breach by varying the value of δ. As expected, the positioning error is increased with larger values of δ. Moreover, for a given bias setting, the ML-based CDF is always on the left compared to the classical positioning approach, with a distance of several meters between the two CDFs for the majority of the distribution. Consequently, the ML-based approach outperforms the classical one in terms of positioning error. For example, the ML-based positioning error is less than 5 meters in 90% of the cases with $b(\delta) = 0$, and only in 70% and 57% of the cases with $\delta = 0.3$ and $\delta = 0.5$, respectively; while the classical positioning error is less than 5 meters in 65% of the cases with $b(\delta) = 0$, and only in 50% and 40% of the cases with $\delta = 0.3$ and $\delta = 0.5$, respectively. The difference in terms of performance between the two approaches will be used in the next subsections to demonstrate the generality of the integrity monitoring mechanism.

c) Training of ML-based Positioning: The training phase of the ML-based positioning is based on 700 UE random positions, which are known for the purpose of learning the TOA distribution. Under default conditions, all the anchors are considered for the GP model learning. In the mitigation case, the GP model is re-trained based on the same UE positions but considering only the selected subset of reliable gNBs.

d) Uncertainty Quantification: For both the classical and ML-based positioning, a dataset of 100 position estimates and associated uncertainties are used for the ML-based regression of the uncertainty model.

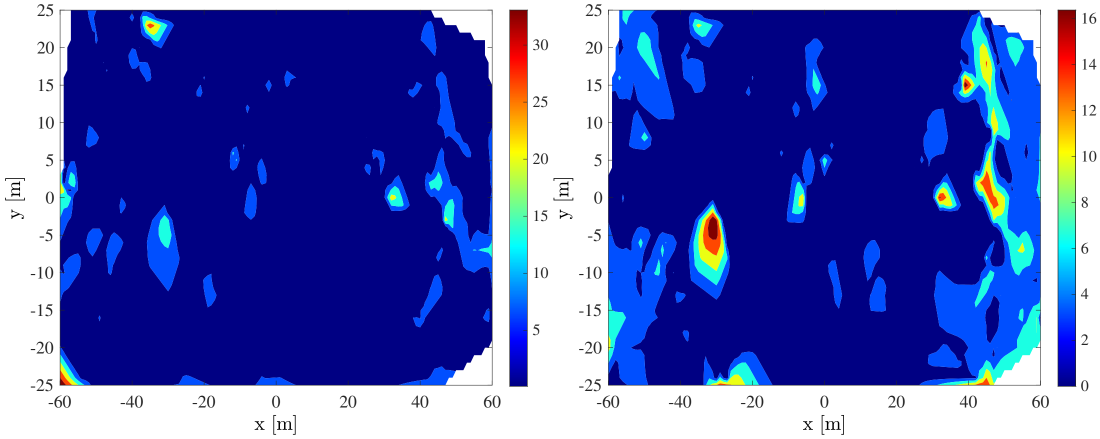
e) Integrity Indicator: Once the uncertainty model is trained, the integrity assessment is performed based on a set of $N_\mathrm{u} = 100$ position estimates and associated uncertainties, with index set $\mathcal{N}_\mathrm{u}$. Specifically, the integrity indicator $\beta_\mathrm{al}^{(\mathcal{N}_u)}$ is flagged to one when the associated FVU value $\Phi_\mathrm{vu}^{(\mathcal{N}_u)}$ overcomes the threshold $\Phi_\mathrm{vu,th} = 0.85$. Such a threshold is set to 0.85 based on the results in the absence of the integrity breach.

B. Integrity Assessment

In this section, we focus on the integrity assessment by employing the proposed indicators with the two algorithms simulated in the 3GPP-compliant scenario. First, we evaluate the performance of uncertainty quantification and its correlation with the positioning error, also in terms of spatial correlation. Then, we focus on the TIR as a performance metric to show how in the presence of an integrity breach, the proposed approach for collective integrity monitoring is able to detect an integrity failure and alert the system.

Fig. 6 shows the scatterplot of the uncertainty indicator u_i as a function of the positioning error e_i for the Classical and ML-based positioning algorithms. The plot also shows, as expected, that for the same dataset, the error obtained with the ML-based positioning algorithms is lower. From such bivariate data, we can measure the correlation between the uncertainty value and the position estimation's Root-Mean-Square Error (RMSE). The correlation coefficients vary between 0 and 1, in which 1 indicates the strongest correlation. As the correlation coefficient gets closer to 1, it indicates a more accurate uncertainty estimation. For both algorithms, a positive correlation is experienced, with correlation coefficients equal to 0.82 for the classical positioning and 0.68 for the ML-based positioning. This result is relevant in our context, as a classical positioning approach can be preferred in those applications where a higher error can be accepted when detected, while the ML-based approach should be adopted viceversa.

In Fig. 7, we evaluate the spatial distribution for both the positioning error e_i and the uncertainty indicator u_i as a function



(a) Error Heatmap

(b) Uncertainty Heatmap

Fig. 7: Heatmap of positioning error and uncertainty in the monitored area.

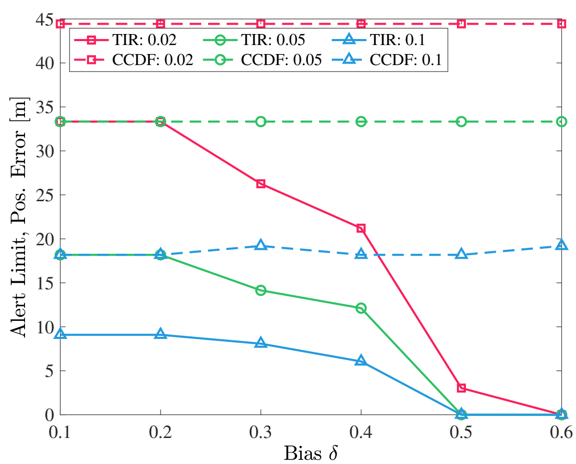


Fig. 8: Minimum alert limit e_{al} (solid lines) to guarantee different values of TIR; error value e_{th} (dashed lines) corresponding to a CCDF, i.e. $\mathbb{P}\{e_i > e_{\mathrm{th}}\}$, equal to the TIR value. Results are obtained by varying the bias δ with the LS algorithm.

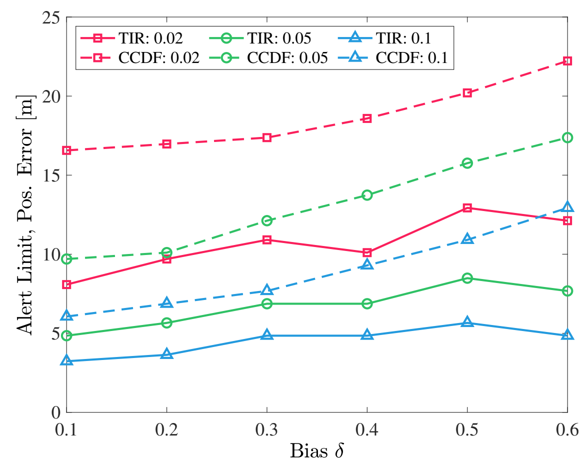


Fig. 9: Minimum alert limit e_{al} (solid lines) to guarantee different values of TIR; error value e_{th} (dashed lines) corresponding to a CCDF, i.e. $\mathbb{P}\{e_i > e_{\mathrm{th}}\}$, equal to the TIR value. Results are obtained varying the bias δ with the ML algorithm.

of the user position, i.e., collected in the simulated scenario for a set of N_{u}. The figure demonstrates the very high correlation between the uncertainty indicator and the positioning error also on the spatial map. The spatial variability depends on the position of the gNBs (see Fig. 4) and specifically of the reference gNB (which is at coordinates $(-50\,\mathrm{m}, -10\,\mathrm{m})$, but also on the channel conditions. By building an uncertainty heatmap based on a collective collection of uncertainty values, we can predict what zones of the monitored area are more susceptible to positioning errors. Moreover, an uncertainty map can be used to train uncertainty in space and time so that anomalies can be detected.

Fig. 8 shows, with solid lines, the minimum alert limit e_{al} that should be accepted with a target integrity risk of 0.02, 0.05, and 0.1. Results are obtained by varying the bias δ with the LS algorithm. For example, when the bias factor is $\delta = 0.2$, there is a risk of 5% that the error overcomes $18\,\mathrm{m}$ without an integrity breach being detected. Conversely, when the bias factor is $\delta = 0.6$, an integrity alert is always issued.

The alert limit is compared, with dashed lines, to the general positioning error corresponding to a CCDF equal to 0.02, 0.05, and 0.1. For example, when the bias factor is $\delta = 0.3$, there is a general probability of 5% that the error overcomes $34\,\mathrm{m}$, regardless if an integrity monitoring mechanism is adopted. In the same conditions, there is a general probability of 5% that the error overcomes $14\,\mathrm{m}$ without the error being detected. Note that δ has a small impact on the positioning error in general, as the accuracy is already low for those values of probability. However, even under such low performances in terms of positioning, the higher the extent of the integrity breach, i.e., δ increases, the more often an integrity alert is issued.

Similarly, Fig. 9 compares the minimum alert limit e_{al} (solid lines) to guarantee different values of TIR and the general positioning error corresponding to a CCDF, with the ML algorithm varying δ. Differently from LS-based positioning and uncertainty quantification, in this case, the alter limit does not strictly decrease as δ increases. This is due to the fact that even the small values considered for δ are sufficient to increase the general positioning error (i.e., the dashed curves are increasing). For example, when $\delta = 0.1$, there is a probability of 5% that the error overcomes 10 m. Under the same conditions, when an integrity indicator is used, there is a target integrity risk of 5% that the error overcomes 5 m without the error being detected. When δ increases, the difference between the general error and the minimum alert limit increases. For example, when $\delta = 0.6$, there is a probability of 5% that the error overcomes 17 m. Under the same conditions, when an integrity indicator is used, there is a target integrity risk of 5% that the error overcomes 7.5 m without the error being detected.

As a matter of fact, observing Fig. 8 and Fig. 9, we conclude that when the bias extent increases, for the considered probability values, the positioning error increases only for the ML algorithm, while the accuracy of LS-based positioning is already low. However, the collective integrity monitoring framework is able to detect the integrity breach, i.e., a lower alert limit is guaranteed for the same TIR value.

C. Uncertainty-based Mitigation

In this section, we evaluate the mitigation techniques presented in Sec. V-C. The scope is to understand if the integrity indicators proposed in the papers can be used to select a subset of more reliable gNB for refining the position estimation.

Fig. 10 shows the effect of the mitigation on the classical positioning when an integrity breach is detected, and varying the value of δ. The mitigation approach is beneficial even in the absence of an integrity problem. Specifically, even with no bias $b(\delta) = 0$, the error is below 5 m in the 60% of cases when no mitigation is performed, while such a rate increases to 80% when the subset of most reliable gNB is selected. Such an improvement holds also for $\delta = 0.4$ and $\delta = 0.5$.

Fig. 11 shows the mitigation effect on the ML-based positioning when an integrity breach is detected, and the value of δ is varying. Specifically, when there is no bias $b(\delta) = 0$, the positioning performance is the same with and without mitigation. However, with $\delta = 0.4$ and $\delta = 0.5$, the mitigation improves the positioning performance with a behavior that is very similar to the case with no bias, except for the tail of the curve. For example, for $\delta = 0.4$, the error is below 5 m in the 70% of cases when no mitigation is performed, while such a rate increases to 82% when the subset of most reliable gNB is selected.

VII. 5G Positioning Integrity Support

With the integrity assessment framework and case studies presented in this paper, we point out that a systematic framework is needed to support the 5G UE with RAT-dependent positioning integrity support. In this paper, for clarity and without loss of generality, we considered integrity breaches in one of the gNBs and evaluated the impact of a network with integrity alert support. The integrity breach of the targeted gNB could be from lack of synchronization, incorrect location information, high NLOS condition, or any other potential error sources.

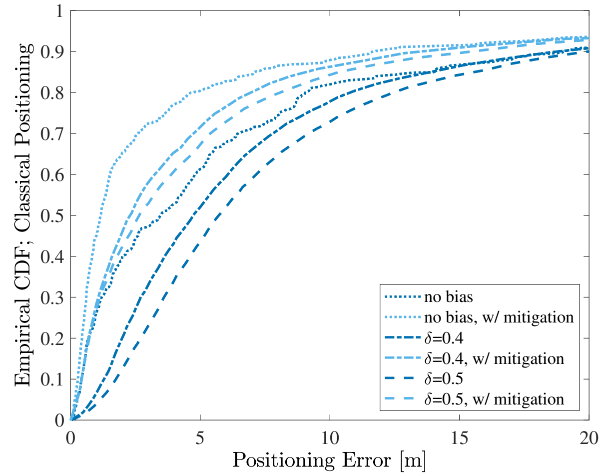


Fig. 10: CDF of the positioning error with (light blue) and without (blue) mitigation after an integrity alert is provided, for the classical positioning, varying the bias δ.

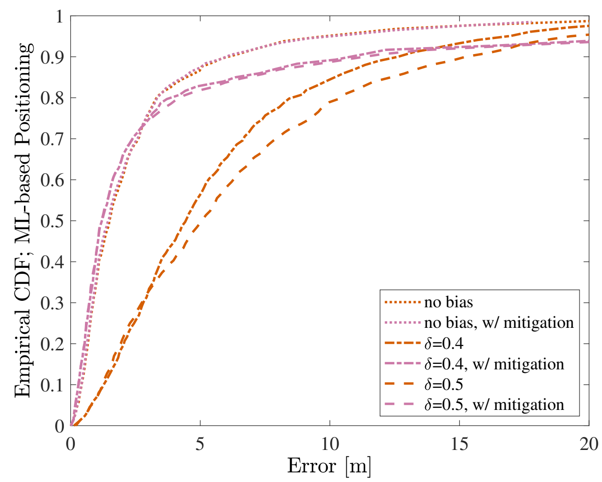


Fig. 11: CDF of the positioning error with (pink) and without (orange) mitigation after an integrity alert is provided, for the ML-based positioning, varying the bias δ.

There are different error sources in each of the RAT-dependent positioning methods, and in Release 18 a list of these error sources is identified for both the *LMF-based positioning integrity mode* and the *UE-based positioning integrity mode* [41]. For example in the IIoT scenario, one of the main contributors in indoor positioning performance is the deployment planning of the indoor nodes. Again, considering the assumed different zones in a factory, one should consider that the number of nodes and how they are deployed in that particular zone would identify the level of accuracy, reliability and integrity of the positioning service within that zone. In terms of DL-TDOA, while the UE does the positioning measurements, it is important that the LMF provides proper integrity assistance information regarding any error sources in the UE's region, the alert limit and the target integrity risk.

VIII. Final Remarks

In this paper, a general framework for the assessment of the integrity of position estimation is presented, focusing on RAT-dependent techniques. First, integrity indicators based on uncertainty quantification are introduced. Then, the applicability of such indicators is verified by considering classical measurement-based algorithms and trained models based on explainable ML techniques. A new approach based on collective integrity monitoring is presented, for assessing the integrity of the positioning system based on multiple users. Based on such collective integrity monitoring, error mitigation techniques are proposed to mitigate the impact of integrity failures by refining the estimated position through a subset of most reliable measurements. The proposed framework is evaluated in a 3GPP-compliant scenario and shows promising performance in terms of integrity risk, even considering different case studies and positioning algorithms.

References

[1] N. Blefari-Melazzi, S. Bartoletti, L. Chiaraviglio, F. Morselli, E. Baena, G. Bernini, D. Giustiniano, M. Hunukumbure, G. Solmaz, and K. Tsagkaris, "Locus: Localization and analytics on-demand embedded in the 5g ecosystem," in *2020 European Conference on Networks and Communications (EuCNC)*, 2020, pp. 170–175.

[2] Z. Wang, Z. Liu, Y. Shen, A. Conti, and M. Z. Win, "Location awareness in beyond 5g networks via reconfigurable intelligent surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 7, pp. 2011–2025, 2022.

[3] Y. Ruan, L. Chen, X. Zhou, G. Guo, and R. Chen, "Hi-Loc: Hybrid indoor localization via enhanced 5G NR CSI," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–15, 2022.

[4] *NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN*, 3rd Generation Partnership Project 3GPP™ 3GPP TS 38 305 V17.2.0 (2022-09), Sep. 2022, release 17.

[5] P. Hammarberg, J. Vinogradova, G. Fodor, R. Shreevastav, S. Dwivedi, and F. Gunnarsson, "Architecture, protocols, and algorithms for location-aware services in beyond 5g networks," *arXiv preprint arXiv:2211.14781*, 2022.

[6] F. Gunnarsson and R. Shreevastav, "3GPP GNSS positioning and integrity: The latest trials and developments," *Ericsson Blogpost*, 2022.

[7] *Study on positioning use cases*, 3rd Generation Partnership Project 3GPP™ 3GPP TR 22 872 V16.1.0 (2018-09), Sep. 2018, release 16.

[8] *Service requirements for cyber-physical control applications in vertical domains*, 3rd Generation Partnership Project 3GPP™ 3GPP TR 22 104 V18.3.0 (2021-12), Dec. 2021, release 18.

[9] A. Frankó, G. Vida, and P. Varga, "Reliable identification schemes for asset and production tracking in industry 4.0," *Sensors*, vol. 20, no. 13, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/13/3709

[10] J. Lenz, E. MacDonald, R. Harik, and T. Wuest, "Optimizing smart manufacturing systems by extending the smart products paradigm to the beginning of life," *Journal of Manufacturing Systems*, vol. 57, pp. 274–286, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278612520301709

[11] E. J. Khatib and R. Barco, "Optimization of 5g networks for smart logistics," *Energies*, vol. 14, no. 6, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/6/1758

[12] H. Laaki, Y. Miche, and K. Tammi, "Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery," *IEEE Access*, vol. 7, pp. 20 325–20 336, 2019.

[13] M. Patnaik and S. Mishra, *Indoor Positioning System Assisted Big Data Analytics in Smart Healthcare*. Cham: Springer International Publishing, 2022, pp. 393–415.

[14] H. Bagheri, M. Noor-A-Rahim, Z. Liu, H. Lee, D. Pesch, K. Moessner, and P. Xiao, "5g nr-v2x: Toward connected and cooperative autonomous driving," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 48–54, 2021.

[15] S. Bartoletti, H. Wymeersch, T. Mach, O. Brunnegård, D. Giustiniano, P. Hammarberg, M. F. Keskin, J. O. Lacruz, S. M. Razavi, J. Rönnblom, F. Tufvesson, J. Widmer, and N. Blefari-Melazzi, "Positioning and sensing for vehicular safety applications in 5g and beyond," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 15–21, 2021.

[16] A. Fouda, R. Keating, and A. Ghosh, "Dynamic selective positioning for high-precision accuracy in 5g nr v2x networks," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 2021, pp. 1–6.

[17] H. N. Qureshi, M. Manalastas, A. Ijaz, A. Imran, Y. Liu, and M. O. Al Kalaa, "Communication Requirements in 5G-Enabled Healthcare Applications: Review and Considerations," *Healthcare*, vol. 10, no. 2, 2022. [Online]. Available: https://www.mdpi.com/2227-9032/10/2/293

[18] D. Orlando, S. Bartoletti, I. Palamà, G. Bianchi, and N. B. Melazzi, "Innovative attack detection solutions for wireless networks with application to location security," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2022.

[19] Y. Li, S. Liu, Z. Yan, and R. H. Deng, "Secure 5G Positioning with Truth Discovery, Attack Detection and Tracing," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[20] A. K. Dutta and M. Singh, "Challenges and opportunities in enabling secure 5g positioning," in *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2023, pp. 498–504.

[21] X. Cui, T. A. Gulliver, J. Li, and H. Zhang, "Vehicle Positioning Using 5G Millimeter-Wave Systems," *IEEE Access*, vol. 4, pp. 6964–6973, 2016.

[22] V. Bottino, G. de Alteriis, R. Schiano Lo Moriello, and D. Accardo, "system architecture design of a uav for automated cinematography in gnss-challenging scenarios," in *2022 IEEE 9th International Workshop on Metrology for AeroSpace (MetroAeroSpace)*.

[23] S. Bartoletti, N. Decarli, and B. M. Masini, "Sidelink 5G-V2X for integrated sensing and communication: the impact of resource allocation," in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2022, pp. 79–84.

[24] 3GPP, "New SID on NR positioning enhancements," no. RP-193237, 2019, meeting #86.

[25] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[26] M. Singh, M. Roeschlin, A. Ranganathan, and S. Capkun, "V-range: Enabling secure ranging in 5g wireless networks," in *NDSS*, 2022.

[27] P. Leu, M. Singh, M. Roeschlin, K. G. Paterson, and S. Čapkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 500–516.

[28] M. Singh, P. Leu, and S. Capkun, "Uwb with pulse reordering: Securing ranging against relay and physical-layer attacks," *Cryptology ePrint Archive*, 2017.

[29] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[30] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 410–419.

[31] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005*. IEEE, 2005, pp. 7–pp.

[32] D. Orlando, I. Palamà, S. Bartoletti, G. Bianchi, and N. B. Melazzi, "Design and experimental assessment of detection schemes for air interface attacks in adverse scenarios," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1989–1993, 2021.

[33] S. Bartoletti, G. Bianchi, D. Orlando, I. Palamà, and N. Blefari-Melazzi, "Location security under reference signals' spoofing attacks: Threat model and bounds," in *The 16th International Conference on Availability, Reliability and Security*, ser. ARES 2021, 2021.

[34] J. Al Hage, P. Xu, P. Bonnifait, and J. Ibanez-Guzman, "Localization integrity for intelligent vehicles through fault detection and position error characterization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 4, pp. 2978–2990, 2020.

[35] J. Gabela, A. Kealy, M. Hedley, and B. Moran, "Case study of bayesian raim algorithm integrated with spatial feature constraint and fault detection and exclusion algorithms for multi-sensor positioning," *Navigation*, vol. 68, no. 2, pp. 333–351, 2021.

[36] T. G. Reid, S. E. Houts, R. Cammarata, G. Mills, S. Agarwal, A. Vora, and G. Pandey, "Localization requirements for autonomous vehicles,"

SAE International Journal of Connected and Automated Vehicles, vol. 2, no. 12-02-03-0012, 2019.

[37] S. Gupta and G. X. Gao, "Particle raim for integrity monitoring," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, 2019, pp. 811–826.

[38] N. Zhu, J. Marais, D. Bétaille, and M. Berbineau, "Gnss position integrity in urban environments: A review of literature," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 9, pp. 2762–2778, 2018.

[39] Q. Zhang and Q. Gui, "A new bayesian raim for multiple faults detection and exclusion in gnss," *The Journal of Navigation*, vol. 68, no. 3, pp. 465–479, 2015.

[40] H. Pesonen, "A framework for bayesian receiver autonomous integrity monitoring in urban navigation," *NAVIGATION: Journal of the Institute of Navigation*, vol. 58, pp. 229–240, 09 2011.

[41] *Study on NR positioning enhancements*, 3rd Generation Partnership Project 3GPP™ 3GPP TR 38 857 V17.0.0 (2021-03), Mar. 2021, release 17.

[42] L. Bai, C. Sun, A. G. Dempster, H. Zhao, J. W. Cheong, and W. Feng, "Gnss-5g hybrid positioning based on multi-rate measurements fusion and proactive measurement uncertainty prediction," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–15, 2022.

[43] C. Sun, H. Zhao, L. Bai, J. W. Cheong, A. G. Dempster, and W. Feng, "Gnss-5g hybrid positioning based on toa/aoa measurements," in *China Satellite Navigation Conference (CSNC) 2020 Proceedings: Volume III*, J. Sun, C. Yang, and J. Xie, Eds. Singapore: Springer Singapore, 2020, pp. 527–537.

[44] J. A. Del Peral-Rosado, P. Nolle, S. M. Razavi, G. Lindmark, D. Shrestha, F. Gunnarsson, F. Kaltenberger, N. Sirola, O. Särkkä, J. Roström, K. Vaarala, P. Miettinen, G. Pojani, L. Canzian, H. Babaroglu, E. Rastorgueva-Foi, J. Talvitie, and D. Flachs, "Design considerations of dedicated and aerial 5g networks for enhanced positioning services," in *2022 10th Workshop on Satellite Navigation Technology (NAVITEC)*, 2022, pp. 1–12.

[45] V. Bottino, G. de Alteriis, R. Schiano Lo Moriello, and D. Accardo, "System architecture design of a uav for automated cinematography in gnss-challenging scenarios," in *2022 IEEE 9th International Workshop on Metrology for AeroSpace (MetroAeroSpace)*, 2022, pp. 627–632.

[46] H. Jing, Y. Gao, S. Shahbeigi, and M. Dianati, "Integrity monitoring of gnss/ins based positioning systems for autonomous vehicles: State-of-the-art and open challenges," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[47] P. Zabalegui, G. De Miguel, A. Perez, J. Mendizabal, J. Goya, and I. Adin, "A review of the evolution of the integrity methods applied in gnss," *IEEE Access*, vol. 8, pp. 45 813–45 824, 2020.

[48] J. Gabela, A. Kealy, M. Hedley, and B. Moran, "Case study of bayesian raim algorithm integrated with spatial feature constraint and fault detection and exclusion algorithms for multi-sensor positioning," *NAVIGATION: Journal of the Institute of Navigation*, vol. 68, no. 2, pp. 333–351, 2021. [Online]. Available: https://navi.ion.org/content/68/2/333

[49] J. Xiong, J. W. Cheong, Z. Xiong, A. G. Dempster, S. Tian, and R. Wang, "Integrity for multi-sensor cooperative positioning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 2, pp. 792–807, 2019.

[50] Y. Zhao and D. Shrestha, "Uncertainty in position estimation using machine learning," in *2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2021, pp. 1–7.

[51] S. Bartoletti, G. Bernini, I. Palamà, M. D. Angelis, L. M. Monteforte, T. E. Kennouche, K. Tsagkaris, G. Bianchi, and N. B. Melazzi, "Uncertainty quantification of 5g positioning as a location data analytics function," in *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2022, pp. 255–260.

[52] L. Ding, G. Seco-Granados, H. Kim, R. Whiton, E. G. Ström, J. Sjöberg, and H. Wymeersch, "Bayesian integrity monitoring for cellular positioning – a simplified case study," 2022.

[53] *Study on NR positioning support*, 3rd Generation Partnership Project 3GPP™ 3GPP TR 38 855 V16.0.0 (2019-03), Mar. 2019, release 16.

[54] S. Dwivedi, R. Shreevastav, F. Munier, J. Nygren, I. Siomina, Y. Lyazidi, D. Shrestha, G. Lindmark, P. Ernström, E. Stare, S. M. Razavi, S. Muruganathan, G. Masini, A. Busin, and F. Gunnarsson, "Positioning in 5G networks," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 38–44, 2021.

[55] M. M. Butt, A. Pantelidou, and I. Z. Kovács, "ML-Assisted UE Positioning: Performance Analysis and 5G Architecture Enhancements," *IEEE Open Journal of Vehicular Technology*, vol. 2, pp. 377–388, 2021.

[56] J. Gante, L. Sousa, and G. Falcao, "Dethroning GPS: Low-Power Accurate 5G Positioning Systems Using Machine Learning," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 10, no. 2, pp. 240–252, 2020.

[57] A. Conti, F. Morselli, Z. Liu, S. Bartoletti, S. Mazuelas, W. C. Lindsey, and M. Z. Win, "Location awareness in beyond 5g networks," *IEEE Communications Magazine*, vol. 59, no. 11, 2021.

[58] *Service requirements for the 5G system*, 3rd Generation Partnership Project 3GPP™ 3GPP TS 22 261 V19.0.0 (2022-09), Sep. 2022, release 19.

[59] H. L. Van Trees, *Detection, Estimation, and Modulation Theory*, 1st ed. New York, NY 10158-0012: John Wiley & Sons, Inc., 1968.

[60] A. Conti, S. Mazuelas, S. Bartoletti, W. C. Lindsey, and M. Z. Win, "Soft information for localization-of-things," *Proc. IEEE*, vol. 107, no. 11, pp. 2240–2264, Nov. 2019.

[61] F. Perez-Cruz, S. Van Vaerenbergh, J. J. Murillo-Fuentes, M. Lazaro-Gredilla, and I. Santamaria, "Gaussian processes for nonlinear signal processing: An overview of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 4, pp. 40–50, 2013.

[62] C. E. Rasmussen and C. K. I. Williams, *Gaussian Processes for Machine Learning*. Cambridge, MA, USA: MIT Press, 2006.

[63] 3GPP, "Study on channel model for frequencies from 0.5 to 100 GHz (Release 16)," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 38.901, V16.1.0, 2019.