PROJECT "LOCUS": LOCalization and analytics on-demand embedded in the 5G ecosystem, for Ubiquitous vertical applicationS

Grant Agreement Number: 871249
(https://www.locus-project.eu/)

DELIVERABLE D2.3

"Security and Privacy, final version"

Deliverable Type:	R
Dissemination Level:	Public
Contractual Date of Delivery to the EU:	30/04/2021
Actual Date of Delivery to the EU:	29/04/2021
WP contributing to the Deliverable:	WP2 – Use cases, requirements, security, system architecture
Editor(s):	CNIT: Domenico Garlisi, Nicola Blefari Melazzi
Author(s):	CNIT: Stefania Bartoletti, Domenico Garlisi, Ivan Palamà, Francesco Mancini, Danilo Orlando, Nicola Blefari Melazzi Ericsson AB: Sara Modarres Razavi OTE: Maria Belesioti
Internal Reviewer(s):	Incelligent: Kostas Tsagkaris

Short Abstract:	The goal of this deliverable is to present a study of security/privacy issues as well as solutions to mitigate security attacks and ensure data privacy for the LOCUS system.
Keyword List:	Localization, 5G, security, privacy, LBS, catcher, jamming detector, integrity.

Executive Summary

This document is the final deliverable concerning the security and privacy aspects of the LOCUS project. LOCUS pays the highest attention to both location security and privacy to make sure that the technical solutions will process secure location data in compliance with users' privacy rights.

The activities presented within D2.2 (that is preliminary to D2.3) have been further developed and suitably adapted according to the evolution of LOCUS architecture (Task2.3) and use cases (Task2.1). In this deliverable, we devise the main techniques and algorithms related to the security and privacy aspects for localization in LOCUS. Their performances are firstly investigated under design assumptions resorting to simulated data and then resorting to real datasets/measurements. A subset of these algorithms will be further refined and validated within WP6. Finally, we also discuss the main roadmap of the 3GPP through the definition of location data integrity, as LOCUS is participating to the standardization discussion within RAN2 WG through Ericsson representatives.

VERSION CONTROL TABLE			
VERSION N.	**PURPOSE/CHANGES**	**AUTHOR (S)**	**DATE**
1.0	First draft and document structure	Domenico Garlisi, Stefania Bartoletti	22/03/2021
1.1	Add inputs contribute for privacy section	Domenico Garlisi, Francesco Mancini	29/03/2021
1.2	Add inputs contribute for security section	Danilo Orlando, Ivan Palamà,	31/03/2021
1.3	Add inputs contribute for security mitigation	Stefania Bartoletti	10/04/2021
2.0	Add common parts document	Domenico Garlisi, Stefania Bartoletti	15/04/2021
2.1	Internal review	Kostas Tsagkaris	25/04/2021
3.0	Complete version	Danilo Orlando, Stefania Bartoletti, Domenico Garlisi	27/04/2021
3.1	Final revision	Nicola Blefari Melazzi	28/04/2021

Table of Contents

1 Background

1.1 List of Abbreviations

ABBREVIATION	FULL NAME
3GPP	3rd Generation Partnership Project
AN	Access Node
BS	Base Station
DoA	Direction of Arrival
DoS	Denial of Service
EM	Expectation Maximization
GLRT	Generalized Likelihood Ratio Test
IMSI	International Mobile Subscriber Identity
LBS	Location Based Service
LPP	LTE Positioning Protocol
LVM	Latent Variable Model
MIMO	Multiple Input Multiple Output
MLE	Maximum Likelihood Estimates
MNC	Mobile Network Code
MME	Mobility Management Entity
MS	Mobile Station
NLJ	Noise-like Jammer
BNLJ	Barrage Noise-like Jammer
SNLJ	Smart Noise-like Jammer
NR	New Radio
OAI	Open Air Interface
OTDoA	Observed Time Difference of Arrival
PMF	Probability Mass Function
PDF	Probability Density Function
RBS	Rogue Base Station

RSRP	Reference Signal Received Power
RSS	Received Signal Strength
SDR	Software Defined Radio
SINR	Signal-to-Noise-plus-Interference Ratio
SNR	Signal-to-Noise Ratio
SPEB	Squared Position Error Bound
SUCI	Concealed Identifier
TDoA	Time Difference of Arrival
ToA	Time of Arrival
UE	User Equipment
USRP	Universal Software Radio Peripheral

Table 1: Abbreviation List

2 Introduction

In the incoming fifth generation mobile communication network (5G), localization services, which in the past were mainly provided by non-cellular technologies, are now combined with solutions based upon cellular technologies and integrated within 5G architecture [1] [2]. As a consequence, the 5G architecture can improve the performance of the localization system but at the cost of new security and privacy vulnerabilities that need to be investigated and mitigated.

This document finalizes the research activities described in deliverable D2.2 for what concerns the security and privacy aspects related to the LOCUS platform. We focus on main or still unresolved issues. Specifically, the deliverable develops functions and algorithms to detect attacks over the air interface providing alerts that can be used for mitigation purposes. Additionally, this deliverable also considers the privacy and the 3GPP positioning integrity aspects.

From the LOCUS architecture prospective, security and privacy functionalities are separated from the location-based application modules. This allows the LOCUS platform modules to focus on specific localization features using a common approach to retrieve security and privacy functions. In this context, all transactions between location application and security and privacy functions use a suitable function interface. In fact, the latter acts as a connection between the Security/Privacy module and those APIs exposing functionalities, 3rd party applications for network management as well as other vertical applications that shall exploit localization analytics as a service provided by the LOCUS platform.

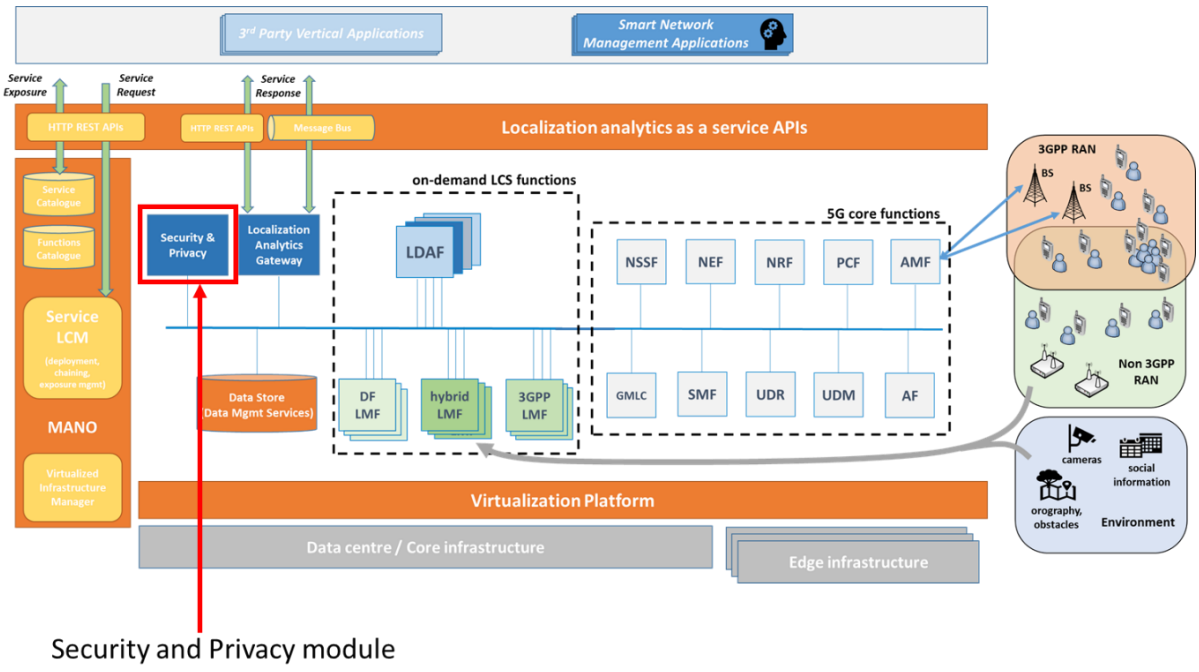

Figure 1 – LOCUS architecture with where Security and Privacy module is emphasised

Figure 1 shows the latest version of the LOCUS architecture as defined in WP2, where the security and privacy module is highlighted. Such a module is directly connected with the Localization Analytics Gateway (to support 3rd party applications) and with the on-demand Location Service (LCS) functions. They can use security and privacy functionalities through security and privacy APIs interface.

The remainder of this document is organized into four main sections. Section 3 provides the results of the activity focused on the design of detection strategies for over the air attacks. By exploiting theoretically-founded design criteria, we come up with decision schemes fed by location data that are made available by the location infrastructure or power measurements collected by the UE. We consider three kinds of attacks: jamming, spoofing and Rogue Base Station (RBS) attacks. The proposed methods are evaluated over simulated data and in a real-world situation where jammers and RBSs attack the UE. To this end, Software Defined Radios (SDRs) are exploited to build up the experimental playground.

Section 4 investigates to what extent false measurements degrade the location performance. More precisely, we focus on localization tampering attacks where the information of anchor nodes (e.g., base stations or access points) are tampered undermining the user's localization accuracy. We provide a mathematical model and derive the squared position error bound (SPEB) to quantify the effects on the localization error.

Section 5 deals with privacy concerns in location base service (LBS). We consider the study of specific functionalities that reduce the risk to produce privacy threats in user data

management. We assess the proposed method via extensive experiments on real dataset provided by network operator.

Finally, Section 6 provides specification on the positioning integrity in 3GPP; after a brief introduction we report the positioning integrity error categories.

3 Detection of attacks over the air interface

In this section, we present the results of the activity focused on threat detection. More precisely, we consider three kinds of malicious agents capable of perpetrating an attack against the UE and/or network infrastructure, namely [3] [4]:

1. (possibly smart) jammers (that inject noise-like signals into the receiver);
2. spoofers (that generate counterfeit signals);
3. Rogue Base Stations (that replace legitimate BSs).

The aim of this activity is twofold. First, we design theoretically-founded decision rules fed by location data that are made available by the location infrastructure and we assess their performance over simulated data whose parameters and distributions are set according to real scenarios. Second, we adapt the ideas behind this approach to a real-world situation where jammers and RBSs attack the UE. Specifically, we build up a real-world experimental playground setup using Software Defined Radios respectively instrumented as a jamming device, as an RBS, and as a UE receiver. In such a scenario, we exploit high-level data measured by the UE without the aid from the infrastructure and suitably adapt change detection algorithms based upon well-established design criteria to process these data.

Notation

In the sequel, vectors and matrices are denoted by boldface lower-case and upper-case letters, respectively. Symbols det(·), Tr (·), and $(\cdot)^{\mathsf{T}}$ denote the determinant, trace, and transpose, respectively. As to the numerical sets, $\mathbb{R}$ is the set of real numbers and $\mathbb{R}^{N\times M}$ is the Euclidean space of $(N \times M)$-dimensional real matrices (or vectors if $M = 1$). The Euclidean norm of a generic vector $\boldsymbol{x}$ is denoted by $\|\boldsymbol{x}\|$ whereas the modulus of a real number x is denoted by $|x|$. For any N-dimensional vector $\boldsymbol{x}$, $\boldsymbol{X} = diag(\boldsymbol{x})$ is a $(N \times N)$-dimensional diagonal matrix whose principal diagonal contains the elements of $\boldsymbol{x}$. Symbols $\boldsymbol{I}$ and $\boldsymbol{0}$ indicate the identity matrix and the null matrix or vector, respectively, whose size depends on the context. The curled inequality symbol $\succcurlyeq$ (and its strict form $\succ$) is used to denote generalized matrix inequality: for any N-dimensional Hermitian matrix $\boldsymbol{A}$, $\boldsymbol{A} \succcurlyeq \boldsymbol{0}$ means that A is a positive semi-definite matrix ($\boldsymbol{A} \succ \boldsymbol{0}$ for positive definiteness). Finally, we write $\boldsymbol{x} \sim \mathcal{N}_N(\boldsymbol{m}, \boldsymbol{M})$ if x is a N-dimensional Gaussian vector with mean $\boldsymbol{m}$ and covariance matrix $\boldsymbol{M} \succ \boldsymbol{0}$, whereas, given $\boldsymbol{X} \in \mathbb{R}^{N\times K}$, $\boldsymbol{x} \sim \mathcal{N}_N(\boldsymbol{m}, \boldsymbol{M}, \boldsymbol{I})$ means that the columns of $\boldsymbol{X}$ are Independent and Identically Distributed (IID) random vectors following the Gaussian distribution with mean $\boldsymbol{m}$ and covariance matrix $\boldsymbol{M}$.

3.1 Background and Motivation

In the fifth generation mobile communication network, localization services will play a crucial role in several scenarios envisioned for 5G, including self-driving cars, unmanned aerial vehicles, smart logistics, emergency services, and many more [5] [6] [7]. At the same time, the ability to exploit location signals emitted by 5G base stations comes with a bleak side: many literature works [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] show how easy is for a tech savvy opponent to build ultra-low cost Jammers or even LTE/5G RBSs [4] capable of generating fake signals or interfering with legitimate ones (Figure 2).

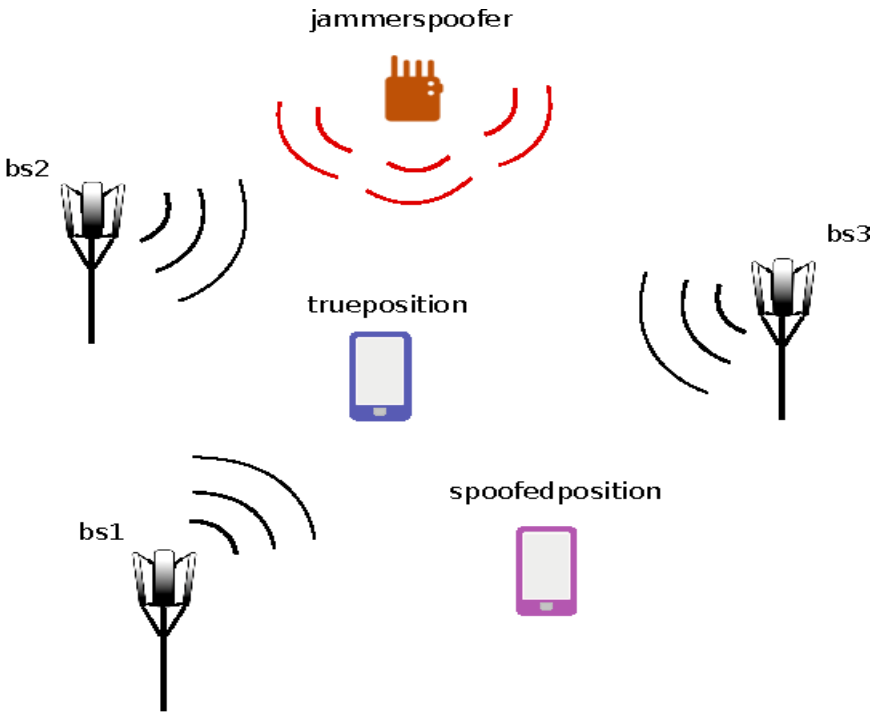

Figure 2. Operating scenario for a cellular network under the attack of a jammer or spoofer which leads to inaccurate or counterfeit location estimates.

In this context, most of the radio interface attacks rely on the suitable combination of targeted jamming signals [3] [16] to force the UE to abandon the (interfered) legitimate operator signal and make it connect to a (fake) RBS controlled by the adversary. At this time, the opponent may suitably spoof unauthenticated protocol/signalling messages so as to steer the victim into: Man-In-The-Middle scenarios such as downgrade/bid-down attacks [18] [19]; location privacy threats such as tracking or International Mobile Subscriber Identity (IMSI) catching [20], [17]; device capability information gathering [16], and so on. The evolving 3GPP standards have devised solutions to most of these threats. The latest example is the public-key-based SUbscriber Concealed Identity (SUCI) recently standardized [21] in 5G to ultimately

solve the IMSI catching problem. However, attackers can leverage practical concerns that force operators to deploy next-generation cellular technologies slowly and incrementally (in fact, as we write, 2G systems are still active!) and convince the UE to believe that the only base station available in a coverage area is a fake one implementing a past generation standard, thereby circumventing the new protections. It turns out that thwarting air interface attacks to cellular networks becomes of crucial importance.

Therefore, in the next subsections, we develop compelling techniques and systems which detect the early-warning signs of their appearance, namely (possibly smart) jamming, spoofing, and RBS activities, etc. To this end, we draw upon decision theory and apply well-known design criteria to come up with adaptive decision schemes fed by either high-level location data that are made available by the network infrastructure or power measurements collected by the UE.

3.2 Spoofer and jammer detection algorithms for location data

In this subsection, we focus on the design of decision schemes fed by location data to face either spoofing or jamming attacks. To this end, notice that the general effect of a spoofing or jamming action is the breakage of the location data homogeneity due to false positioning information or depleted estimation quality. Thus, we can formulate the detection problem at hand in terms of a binary hypothesis test where data under the null hypothesis are homogeneous, whereas, under the alternative hypothesis, there exists a discontinuity in data distribution parameters. The discontinuity point is assumed unknown and is estimated from data. Moreover, according to the specific subset of parameters subject to this discontinuity, we can model either a Noise-Like Jammer (NLJ) or a spoofing/meaconing attack.

Finally, the considered hypothesis testing problems are solved by means of GLRT-based design procedures and *ad hoc* modifications that incorporate the latent variable model (LVM) [22].

3.2.1 Sensor model and problem formulations

Consider a slowly moving UE that is under tracking by the network infrastructure. Let us denote by $\boldsymbol{Z} = [\boldsymbol{z}_1, \boldsymbol{z}_2, \dots, \boldsymbol{z}_K] \in \mathbb{R}^{N \times K}$ the entire data matrix whose kth column, $k = 1,\dots, K$, contains a set of measurements acquired at the kth time instant. For instance, such measurements can be DoAs, ToAs, OTDoAs, the RSRP, or others provided by the network. In what follows, we assume that the measurement errors are independent over the time and Gaussian distributed with zero mean and covariance matrix depending upon the specific operating scenario (a point better explained below). Thus, in a scenario unaffected by malicious platform actions, all the measurement are IID, namely

$$\boldsymbol{z}_k \sim \mathcal{N}_N(\boldsymbol{m}, \boldsymbol{\Sigma}), k = 1, \dots, K,$$

where $\boldsymbol{m} \in \mathbb{R}^{N\times 1}$ contains the actual values of the UE position parameters and $\boldsymbol{\Sigma} \in \mathbb{R}^{N\times N}$ is the positive definite error covariance matrix, which can exhibit either a generic symmetric structure or can be diagonal. The former case allows us to account for a possible correlation among the measurements at the design stage, whereas the latter case corresponds to independent measurements. Now, if at a certain time index, K_0 say, within the observation interval, a malicious platform performs an attack aimed at disrupting the receiver functionalities by transmitting noise-like signals, the quality of the estimates provided by the sensors would impair due to an increased uncertainty. As a consequence, data matrix can be partitioned into the following two submatrices $\boldsymbol{Z}_{1:K_0} \sim \mathcal{N}_N(\boldsymbol{m}, \boldsymbol{\Sigma}_1, \boldsymbol{I})$ and $\boldsymbol{Z}_{K_0+1:K} \sim \mathcal{N}_N(\boldsymbol{m}, \boldsymbol{\Sigma}_2, \boldsymbol{I})$, where $\boldsymbol{Z}_{1:K_0} = [\boldsymbol{z}_1, \dots, \boldsymbol{z}_{K_0}] \in \mathbb{R}^{N\times K_0}$, $\boldsymbol{Z}_{K_0+1:K} = [\boldsymbol{z}_{K_0+1}, \dots, \boldsymbol{z}_K] \in \mathbb{R}^{N\times(K-K_0)}$, $\boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_1 \succ 0$, and $K_0 \in \Omega_0 \subseteq \Omega = 1, \dots, K$. Under the above assumptions, the detection problem at hand can be formulated in terms of the following hypothesis test

(1)

$$\begin{cases} \boldsymbol{H_0}: \boldsymbol{Z} \sim \boldsymbol{\mathcal{N}}_N(\boldsymbol{m_0}, \boldsymbol{\Sigma_0}, \boldsymbol{I}), \\ \boldsymbol{H_1}: \begin{cases} \boldsymbol{Z_{1:K_0}} \sim \boldsymbol{\mathcal{N}}_N(\boldsymbol{m_1}, \boldsymbol{\Sigma_1}, \boldsymbol{I}), \\ \boldsymbol{Z_{K_0+1:K}} \sim \boldsymbol{\mathcal{N}}_N(\boldsymbol{m_2}, \boldsymbol{\Sigma_2}, \boldsymbol{I}), \end{cases} \end{cases}$$

where $\boldsymbol{m}, \boldsymbol{\Sigma}_0, \boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2$, and K_0 are unknown.

On the other hand, if the hostile platform is aimed at injecting false information into the network receivers, then, starting from the time instant K_0, the mean vector no longer contains the true position of the UE, but its entries are related to the false position information created by the attacker. Therefore, in this case, the considered detection problem becomes:

(2)

$$\begin{cases} \boldsymbol{H_0}: \boldsymbol{Z} \sim \boldsymbol{\mathcal{N}}_N(\boldsymbol{m_0}, \boldsymbol{\Sigma_0}, \boldsymbol{I}), \\ \boldsymbol{H_1}: \begin{cases} \boldsymbol{Z_{1:K_0}} \sim \boldsymbol{\mathcal{N}}_N(\boldsymbol{m_1}, \boldsymbol{\Sigma_1}, \boldsymbol{I}), \\ \boldsymbol{Z_{K_0+1:K}} \sim \boldsymbol{\mathcal{N}}_N(\boldsymbol{m_2}, \boldsymbol{\Sigma_1}, \boldsymbol{I}), \end{cases} \end{cases}$$

where $\boldsymbol{m}_1 \in \mathbb{R}^{N\times 1}$ is an unknown vector containing the location information before that spoofing takes place, $\boldsymbol{m}_2 \in \mathbb{R}^{N\times 1}$ is an unknown vector representing the modified position due to the attack, $\boldsymbol{\Sigma}_1$ and K_0 are unknown.

3.2.2 Noise-like jammer detectors

In this subsection, we focus on problem (1) and develop the GLRT (or approximations of it) whose general expression is given by

(3)

$$\frac{\max\limits_{\mathrm{K}_0}\max\limits_{\boldsymbol{m}_1}\max\limits_{\boldsymbol{\Sigma}_1}\max\limits_{\boldsymbol{\Sigma}_2} f_1(\boldsymbol{Z};\boldsymbol{m}_1,\boldsymbol{\Sigma}_1,\boldsymbol{\Sigma}_2,K_0)}{\max\limits_{\mathbf{m}_0}\max\limits_{\boldsymbol{\Sigma}_0} f_0(\boldsymbol{Z};\boldsymbol{m}_0,\boldsymbol{\Sigma}_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta,$$

where[1] $f_1(\boldsymbol{Z};\boldsymbol{m}_1,\boldsymbol{\Sigma}_1,\boldsymbol{\Sigma}_2,K_0)$ is the PDF (Probability Density Function) of $\boldsymbol{Z}$ under H_1, $f_0(\boldsymbol{Z};\boldsymbol{m}_0,\boldsymbol{\Sigma}_0)$ is the PDF of $\boldsymbol{Z}$ under H_0, and η is the detection threshold[2] to be set in order to ensure a preassigned Probability of False Alarm (P_{fa}), and consider two cases

- the available measurements are uncorrelated leading to diagonal covariance matrices;
- there exists a correlation among the measurements, i.e., the covariance matrices are generally symmetric.

In what follows, we provide the definitions required to implement the detectors along with a sketch of the derivations. The reader is referred to Annex 1 for further details about the mathematical derivations of the NLJ detectors.

3.2.2.1 GLRT for uncorrelated measurements

In this case we assume that

$$\boldsymbol{\Sigma}_0 = diag\left(\sigma_{0,1}^2,\dots,\sigma_{0,N}^2\right),$$
$$\boldsymbol{\Sigma}_1 = diag\left(\sigma_{1,1}^2,\dots,\sigma_{1,N}^2\right),$$
$$\boldsymbol{\Sigma}_0 = diag\left(\sigma_{2,1}^2,\dots,\sigma_{2,N}^2\right) = diag\left(\sigma_{1,1}^2+\Delta\sigma_1^2,\dots,\sigma_{1,N}^2+\Delta\sigma_N^2\right).$$

The maximization of the logarithm[3] of the likelihood function of $\boldsymbol{Z}$ under H_0 (denominator of the left-hand side of (3)) leads to

$$-\frac{K}{2}\sum_{n=1}^{N}\log\hat{\sigma}_{0,n}^2-\frac{1}{2}\sum_{k=1}^{K}\sum_{n=1}^{N}\frac{\left(z_{k,n}-\hat{m}_{0,n}\right)^2}{\hat{\sigma}_{0,n}^2},$$

where we have neglected the constants that do not enter the decision procedure and

(4)

$$\hat{\sigma}_{0,n}^2=\sum_{k=1}^{K}\frac{\left(z_{k,n}-\hat{m}_{0,n}\right)^2}{K},$$
$$\hat{m}_{0,n}=\frac{1}{K}\sum_{k=1}^{K}z_{k,n}.$$

[1] The inequality of equation (3) means that H_0 is rejected when the left-hand side is greater than the threshold.
[2] Hereafter, we denote by η generic detection threshold.
[3] We use the logarithm of the PDF for computational convenience.

As for the numerator of the left-hand side of (3), setting to zero the first derivative of the log-likelihood with respect to $\Delta\sigma_n^2, n = 1, \dots, N$, we obtain

(5)

$$\widehat{\Delta\sigma_n^2} = \begin{cases} \dfrac{1}{K_1}\displaystyle\sum_{k=K_0+1}^{K}\left(z_{k,n} - m_{1,n}\right)^2 - \sigma_{1,n}^2, & \text{if } \widehat{\Delta\sigma_n^2} > 0, \\ 0, \quad \text{otherwise.} \end{cases}$$

Let us define the following sets

$$\Gamma_N = \{1, \dots, N\},$$
$$\Gamma(K_0) = \left\{n \in \Gamma_N : \widehat{\Delta\sigma_n^2} > 0\right\},$$
$$\bar{\Gamma}(K_0) = \left\{n \in \Gamma_N : \widehat{\Delta\sigma_n^2} > 0\right\}.$$

Thus, replacing the above estimates into the log-likelihood and setting to zero the first derivative with respect to $\sigma_{1,n}^2$ yields

$$\hat{\sigma}_{1,n}^2 = \frac{1}{K_0}\sum_{k=1}^{K_0}\left(z_{k,n} - m_{1,n}\right)^2, \quad n \in \Gamma(K_0),$$

$$\hat{\sigma}_{1,n}^2 = \frac{1}{K}\sum_{k=1}^{K}\left(z_{k,n} - m_{1,n}\right)^2, \quad n \in \bar{\Gamma}(K_0).$$

When $n \in \bar{\Gamma}(K_0)$, the maximum likelihood estimate of $m_{1,n}$ is given by $\hat{m}_{0,n}$, whereas if $n \in \Gamma(K_0)$, the estimate is given by the solution of the following equation

$$\frac{1}{K_1}\sum_{k=K_0+1}^{K}\left(z_{k,n} - m_{1,n}\right)^2\left[\sum_{k=1}^{K_0} z_{k,n} - K_0 m_{1,n}\right]$$
$$+\frac{1}{K_0}\sum_{k=1}^{K_0}\left(z_{k,n} - m_{1,n}\right)^2\left[\sum_{k=K_0+1}^{K} z_{k,n} - K_1 m_{1,n}\right] = 0,$$

that maximizes the log-likelihood.

Finally, $\Gamma(K_0)$ and $\bar{\Gamma}(K_0)$ can be estimated verifying for each $n = 1, \dots, N$, and K_0 condition (5). Thus, the resulting decision scheme has the following expression

$$\max_{K_0}\left\{-\frac{K_0}{2}\sum_{n\in\Gamma(K_0)}\log\left[\frac{1}{K_0}\sum_{k=1}^{K_0}\left(z_{k,n} - \hat{m}_{1,n}\right)^2\right] - \frac{K_1}{2}\sum_{n\in\Gamma(K_0)}\log\left[\frac{1}{K_1}\sum_{k=K_0+1}^{K}\left(z_{k,n} - \hat{m}_{1,n}\right)^2\right]\right.$$
$$\left.+\frac{K}{2}\sum_{n\in\Gamma(K_0)}\log\left[\frac{1}{K}\sum_{k=1}^{K}\left(z_{k,n} - \hat{m}_{0,n}\right)^2\right]\right\}\underset{H_0}{\overset{H_1}{\gtrless}}\eta,$$

where with a little abuse of notation, we have maintained symbol $\Gamma(K_0)$ to denote an estimate of $\Gamma(K_0)$. In the following, we refer to these decision rule as NLJ Detector for Uncorrelated Measurements (NLJ-D-UM).

3.2.2.2 GLRT for correlated measurements

In the presence of correlated measurements, the covariance matrices $\boldsymbol{\Sigma}_i, i = 0,1,2$, are no longer diagonal but positive definite symmetric. Moreover, we assume that $K_1 \geq N$ and $K_0 \geq N$. These constraints ensure that the sample covariance matrices based upon $\boldsymbol{Z}_{1:K_0}$ and $\boldsymbol{Z}_{K_0+1:K}$ are nonsingular with probability 1 [23]. As a consequence, in this case $\Omega_0 = N, N+1, \dots, K-N$. It is important to highlight that from an operating point of view and for a sufficiently wide sliding window moving along the temporal dimension, the above requirements may be fulfilled.
Under these design assumptions, the denominator of the left-hand side of (3) can be easily simplified replacing $\boldsymbol{m}_0$ and $\boldsymbol{\Sigma}_0$ with their respective MLE, given by

(6)

$$\bar{\boldsymbol{m}}_0 = \frac{1}{K}\sum_{k=1}^{K} \boldsymbol{z}_k, \quad \bar{\boldsymbol{\Sigma}}_0 = \frac{1}{K}\sum_{k=1}^{K} (\boldsymbol{z}_k - \bar{\boldsymbol{m}}_0)(\boldsymbol{z}_k - \bar{\boldsymbol{m}}_0)^T.$$

As for the numerator of the left-hand side of (3), given K_0 denoting by $\boldsymbol{R} = \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_1$, it is possible to show that maximizing the log-likelihood of $\boldsymbol{Z}$ under H_1 leads to

$$\bar{\boldsymbol{\Sigma}}_2 = \frac{1}{K_1}\sum_{k=K_0+1}^{K} (\boldsymbol{z}_k - \boldsymbol{m}_1)(\boldsymbol{z}_k - \boldsymbol{m}_1)^T,$$

$$\bar{\boldsymbol{R}} = \begin{cases} \bar{\boldsymbol{\Sigma}}_2 - \boldsymbol{\Sigma}_1, & \text{if } \bar{\boldsymbol{R}} \succ \boldsymbol{0}, \\ \boldsymbol{0}, & \text{otherwise.} \end{cases}$$

In the case $\bar{\boldsymbol{R}} = \boldsymbol{0}$, the remaining unknown parameters are estimated as under H_0 and the final decision statistic becomes a constant equal to zero. In the opposite case, we proceed by optimizing the resulting compressed log-likelihood function with respect to $\boldsymbol{\Sigma}_1$ to come up with the following expression

$$\bar{\boldsymbol{\Sigma}}_1 = \frac{1}{K_0}\sum_{k=1}^{K_0} (\boldsymbol{z}_k - \boldsymbol{m}_1)(\boldsymbol{z}_k - \boldsymbol{m}_1)^T.$$

The final problem to be solved is the maximization over $\boldsymbol{m}_1$ that does not admit closed-form solutions in its original form. For this reason, we first recast the partially compressed log-likelihood function as follows

$$-\frac{K_0}{2}\log\det \boldsymbol{M}_0 - \frac{K_1}{2}\log\det \boldsymbol{M}_1 - \frac{K_0}{2}\log(1 + \boldsymbol{u}_0^T \boldsymbol{M}_0^{-1}\ \boldsymbol{u}_0) - \frac{K_1}{2}\log(1 + \boldsymbol{u}_1^T \boldsymbol{M}_1^{-1}\ \boldsymbol{u}_1),$$

where

(7)

$$\boldsymbol{M}_0 = \boldsymbol{S}_0 - \frac{1}{K_0}\boldsymbol{s}_0\boldsymbol{s}_0^T, \quad \boldsymbol{M}_1 = \boldsymbol{S}_1 - \frac{1}{K_1}\boldsymbol{s}_1\boldsymbol{s}_1^T,$$
$$\boldsymbol{S}_0 = \sum_{k=1}^{K_0}\boldsymbol{z}_k\boldsymbol{z}_k^T, \quad \boldsymbol{S}_1 = \sum_{k=K_0+1}^{K}\boldsymbol{z}_k\boldsymbol{z}_k^T, \quad \boldsymbol{s}_0 = \sum_{k=1}^{K_0}\boldsymbol{z}_k, \quad \boldsymbol{s}_1 = \sum_{k=K_0+1}^{K_1}\boldsymbol{z}_k,$$
$$\boldsymbol{u}_0 = \frac{1}{\sqrt{K_0}}\boldsymbol{s}_0 - \sqrt{K_0}\boldsymbol{m}_1, \quad \boldsymbol{u}_0 = \frac{1}{\sqrt{K_1}}\boldsymbol{s}_1 - \sqrt{K_1}\boldsymbol{m}_1.$$

The above equation has been obtained using the following identity

$$\det(\boldsymbol{I} + \boldsymbol{AB}) = \det(\boldsymbol{I} + \boldsymbol{BA})$$

with $\boldsymbol{A}$ and $\boldsymbol{B}$ suitable matrices. Then, we approximate (7) as ($\log(1+x) \approx x$)

$$-\frac{K_0}{2}\log\det\boldsymbol{M}_0 - \frac{K_1}{2}\log\det\boldsymbol{M}_1 - \frac{K_0}{2}\boldsymbol{u}_0^T\boldsymbol{M}_0^{-1}\boldsymbol{u}_0 - \frac{K_1}{2}\boldsymbol{u}_1^T\boldsymbol{M}_0^{-1}\boldsymbol{u}_1$$

and compute the first derivative with respect to $\boldsymbol{m}_1$ to obtain

$$\bar{\boldsymbol{m}}_1 = (K_0\boldsymbol{M}_0^{-1} - K_1\boldsymbol{M}_1^{-1})^{-1}(\boldsymbol{M}_0^{-1}\boldsymbol{s}_0 - \boldsymbol{M}_1^{-1}\boldsymbol{s}_1).$$

Gathering the above results, the final expression of the approximated GLRT is

$$\max_{K_0}\left\{-\frac{K_0}{2}\log\det\left[\frac{1}{K_0}\sum_{k=1}^{K_0}(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)^T\right] - \frac{K_1}{2}\log\det\left[\frac{1}{K_1}\sum_{k=K_0+1}^{K}(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)^T\right] + \frac{K}{2}\log\det\left[\frac{1}{K}\sum_{k=1}^{K}(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_0)(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_0)^T\right]\right\} \underset{H_0}{\overset{H_1}{\gtrless}} \eta,$$

if

$$\frac{1}{K_1}\sum_{k=K_0+1}^{K}(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)^T - \frac{1}{K_0}\sum_{k=1}^{K_0}(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)(\boldsymbol{z}_k-\bar{\boldsymbol{m}}_1)^T \succ \boldsymbol{0},$$

In the case where the above inequality is not true, the approximated GLRT is set to zero. In what follows, we refer to these decision rule as NLJ Detector for Correlated Measurements (NLJ-D-CM).

3.2.2.3 LVM for correlated measurements

Let us assume that the error covariance matrix exhibits a generic symmetric structure and, under H_1, introduce K IID discrete random variables, ω_k say, whose alphabet and unknown PMF are

$$\mathcal{A} = \{1,2\} \text{ and } P(\omega_k = a) = \pi_a, a \in \mathcal{A}, k \in \Omega,$$

respectively. Moreover, the ω_ks are such that when $\omega_k = a$, then $\boldsymbol{z}_k \sim \mathcal{N}_N(\boldsymbol{m}_1, \boldsymbol{\Sigma}_a)$. Therefore, the PDF of $\boldsymbol{z}_k$ can be written exploiting the Total Probability Theorem as

$$f(\boldsymbol{z}_k; \boldsymbol{\pi}, \boldsymbol{m}_1, \boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2) = \sum_{a \in \mathcal{A}} \pi_a f_1(\boldsymbol{z}_k; \boldsymbol{m}_1, \boldsymbol{\Sigma}_a)$$

where $\boldsymbol{\pi} = [\pi_1 \ \ \pi_2]^T$ and $f_1(\boldsymbol{z}_k; \boldsymbol{m}_1, \boldsymbol{\Sigma}_a)$ is the PDF of a Gaussian random vector with mean $\boldsymbol{m}_1$ and covariance matrix $\boldsymbol{\Sigma}_a$. It is important to observe that the PDF of $\boldsymbol{Z}$ no longer depends on K_0. Now, applying the maximum likelihood approach to obtain closed-form expressions for the estimates of the unknown parameters leads to mathematically difficult optimization problems. For this reason, we resort to the Expectation Maximization (EM) [24] algorithm that provides closed-form updates for the parameter estimates at each step and reaches at least a local stationary point.

Therefore, assuming that at the $(h-1)$th step the estimates $\tilde{\boldsymbol{\pi}}^{(h-1)}$, $\tilde{\boldsymbol{m}}_1^{(h-1)}$, $\tilde{\boldsymbol{\Sigma}}_1^{(h-1)}$, and $\tilde{\boldsymbol{\Sigma}}_2^{(h-1)}$ are available, the updates related to the E-step are given by

$$\tilde{q}_k^{(h-1)}(a) = \frac{\tilde{\pi}_a^{(h-1)} f_1\left(\boldsymbol{z}_k; \tilde{\boldsymbol{m}}_1^{(h-1)}, \tilde{\boldsymbol{\Sigma}}_a^{(h-1)}\right)}{\sum_{m \in \mathcal{A}} \tilde{\pi}_m^{(h-1)} f_1\left(\boldsymbol{z}_k; \tilde{\boldsymbol{m}}_1^{(h-1)}, \tilde{\boldsymbol{\Sigma}}_m^{(h-1)}\right)}.$$

The M-step gives rise to the following updates

$$\tilde{\pi}_a^{(h)} = \frac{1}{K} \sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(a),$$

$$\tilde{\boldsymbol{\Sigma}}_a^{(h)} = \frac{1}{\tilde{q}_k^{(h-1)}(a)} \boldsymbol{S}_a\left(\tilde{\boldsymbol{m}}_1^{(h)}\right),$$

$$\tilde{\boldsymbol{m}}_1^{(h)} = \left(\tilde{q}_k^{(h-1)}(1)\boldsymbol{M}_{0,1}^{-1} - \tilde{q}_k^{(h-1)}(2)\boldsymbol{M}_{1,2}^{-1}\right)^{-1}\left(\boldsymbol{M}_{0,1}^{-1}\boldsymbol{s}_{0,1} - \boldsymbol{M}_{1,2}^{-1}\boldsymbol{s}_{1,2}\right),$$

where the update for $\boldsymbol{m}_1$ is obtained through the approximation $\log(1+x) \approx x$ and

$$\boldsymbol{M}_{0,1} = \sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(1)\boldsymbol{z}_k\boldsymbol{z}_k^T - \frac{1}{\tilde{q}^{(h-1)}(1)}\boldsymbol{s}_{0,1}\boldsymbol{s}_{0,1}^T,$$

$$\boldsymbol{M}_{1,2} = \sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(2)\boldsymbol{z}_k\boldsymbol{z}_k^T - \frac{1}{\tilde{q}^{(h-1)}(2)}\boldsymbol{s}_{1,2}\boldsymbol{s}_{1,2}^T,$$

$$\boldsymbol{s}_{0,1} = \sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(1)\boldsymbol{z}_k, \quad \boldsymbol{s}_{1,2} = \sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(2)\boldsymbol{z}_k,$$

with

$$\tilde{q}^{(h-1)}(a) = \sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(a).$$

The iterations of the EM algorithm terminate when a stopping criterion is satisfied. The latter can be related to the maximum number of iterations (dictated by computational power) and/or the variation of the likelihood function at each iteration.

As for the maximization under H_0, since the PDF under the null hypothesis remains unaltered with respect to the previous case, we can clearly use the MLE $\bar{\boldsymbol{m}}_0$ and $\bar{\boldsymbol{\Sigma}}_0$ and the final decision rule can be written as

$$\frac{\prod_{k=1}^{K}\sum_{a\in\mathcal{A}}\tilde{\pi}_a^{(h)} f_1\left(\boldsymbol{z}_k;\tilde{\boldsymbol{m}}_1^{(h)},\tilde{\boldsymbol{\Sigma}}_a^{(h)}\right)}{f_0(\boldsymbol{Z};\bar{\boldsymbol{m}}_0,\bar{\boldsymbol{\Sigma}}_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta.$$

The above decision rule will be referred to as LVM-based NLJ Detector (LVM-NLJ-D).

3.2.3 Spoofing detection architectures

Recall that in the presence of a spoofing attack, the decision problem to be solved is given by (2) and, hence, the GLRT has the following form

(8)

$$\frac{\max\limits_{K_0}\max\limits_{\boldsymbol{m}_1}\max\limits_{\boldsymbol{m}_1}\max\limits_{\boldsymbol{\Sigma}_1} f_1(\boldsymbol{Z};\boldsymbol{m}_1,\boldsymbol{m}_2,\boldsymbol{\Sigma}_1,K_0)}{\max\limits_{\boldsymbol{m}_0}\max\limits_{\boldsymbol{\Sigma}_0} f_0(\boldsymbol{Z};\boldsymbol{m}_0,\boldsymbol{\Sigma}_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta,$$

In the next subsections, we derive the GLRT for both correlated as well as uncorrelated measurements. Finally, we suitably modify it by incorporating the LVM for the case of correlated measurements.

3.2.3.1 GLRT for uncorrelated measurements

As in Subsection 3.2.2.1, we assume here that covariance matrices are diagonal. Thus, the result of the maximization under H_0 is the same as in Subsection 3.2.2.1 and is given by (4), whereas under H_1 it is possible to obtain closed-form expressions for the MLEs of the unknown , namely, $\forall n = 1, \dots, N$,

$$\hat{m}_{1,n} = \frac{1}{K_0}\sum_{k=1}^{K_0} z_{k,n}\,, \qquad \hat{m}_{2,n} = \frac{1}{K_1}\sum_{k=K_0+1}^{K} z_{k,n},$$

$$\hat{\sigma}^2_{1,n} = \frac{1}{K}\left[\sum_{k=1}^{K_0}\left(z_{k,n}-\hat{m}_{1,n}\right)^2 + \sum_{k=K_0+1}^{K}\left(z_{k,n}-\hat{m}_{2,n}\right)^2\right].$$

The final decision rule is given by

$$\max_{K_0}\left\{\frac{K}{2}\sum_{n=1}^{N}\log\left[\frac{1}{K}\sum_{k=1}^{K}\left(z_{k,n}-\hat{m}_{0,n}\right)^2\right] - \frac{K}{2}\sum_{n=1}^{N}\log\left[\frac{1}{K}\left(\sum_{k=1}^{K_0}\left(z_{k,n}-\hat{m}_{1,n}\right)^2 + \sum_{k=K_0+1}^{K}\left(z_{k,n}-\hat{m}_{2,n}\right)^2\right)\right]\right\} \underset{H_0}{\overset{H_1}{\gtrless}} \eta.$$

In the next sections, we will refer to this architecture as Spoofing Detector for Uncorrelated Measurements (SP-DUM).

3.2.3.2 GLRT for correlated measurements

In this case, the estimates under H_0 are given by (6), whereas under H_1 they have the following expressions

$$\bar{\boldsymbol{m}}_1 = \frac{1}{K_0}\sum_{k=1}^{K_0} \boldsymbol{z}_k\,, \qquad \bar{\boldsymbol{m}}_2 = \frac{1}{K_1}\sum_{k=K_0+1}^{K} \boldsymbol{z}_k\,,$$

$$\bar{\boldsymbol{\Sigma}}_0 = \frac{1}{K}\left[\sum_{k=1}^{K_0}(\boldsymbol{z}_k - \bar{\boldsymbol{m}}_1)(\boldsymbol{z}_k - \bar{\boldsymbol{m}}_1)^T + \sum_{k=K_0+1}^{K}(\boldsymbol{z}_k - \bar{\boldsymbol{m}}_2)(\boldsymbol{z}_k - \bar{\boldsymbol{m}}_2)^T\right].$$

It follows that the GLRT (8) becomes

(9)

$$\max_{K_0}\left\{\log\det\left[\sum_{k=1}^{K}\left(\boldsymbol{z}_{k,n} - \bar{\boldsymbol{m}}_0\right)\left(\boldsymbol{z}_{k,n} - \bar{\boldsymbol{m}}_0\right)^T\right] - \log\det\left[\sum_{k=1}^{K_0}\left(\boldsymbol{z}_{k,n} - \bar{\boldsymbol{m}}_1\right)\left(\boldsymbol{z}_{k,n} - \bar{\boldsymbol{m}}_1\right)^T + \sum_{k=K_0+1}^{K}\left(\boldsymbol{z}_{k,n} - \bar{\boldsymbol{m}}_2\right)\left(\boldsymbol{z}_{k,n} - \bar{\boldsymbol{m}}_2\right)^T\right]\right\} \underset{H_0}{\overset{H_1}{\gtrless}} \eta.$$

The above decision scheme is referred to in the following as Spoofing Detector for Correlated Measurements (SP-D-CM).

3.2.3.3 LVM for correlated measurements

Let us consider again K IID discrete random variables ω_k such that when $\omega_k = a$, then $\boldsymbol{z}_k \sim \mathcal{N}_N(\boldsymbol{m}_a, \boldsymbol{\Sigma}_1)$. Therefore, the PDF of $\boldsymbol{z}_k$ can be written exploiting the Total Probability Theorem as

$$f(\boldsymbol{z}_k; \boldsymbol{\pi}, \boldsymbol{m}_1, \boldsymbol{m}_1, \boldsymbol{\Sigma}_1) = \sum_{a\in\mathcal{A}} \pi_a f_1(\boldsymbol{z}_k; \boldsymbol{m}_a, \boldsymbol{\Sigma}_1).$$

Applying the EM algorithm we obtain that the E-step is

$$\tilde{q}_k^{(h-1)}(a) = \frac{\tilde{\pi}_a^{(h-1)} f_1\left(\boldsymbol{z}_k; \tilde{\boldsymbol{m}}_a^{(h-1)}, \tilde{\boldsymbol{\Sigma}}_1^{(h-1)}\right)}{\sum_{m\in\mathcal{A}} \tilde{\pi}_m^{(h-1)} f_1\left(\boldsymbol{z}_k; \tilde{\boldsymbol{m}}_m^{(h-1)}, \tilde{\boldsymbol{\Sigma}}_1^{(h-1)}\right)},$$

where $\tilde{\boldsymbol{m}}_a^{(h-1)}, a \in \mathcal{A}, \tilde{\boldsymbol{\Sigma}}_1^{(h-1)}$, and $\tilde{\pi}_a^{(h-1)}, a \in \mathcal{A}$, are the available estimates at the hth step. On the other hand, the M-step yields

$$\tilde{\pi}_a^{(h)} = \frac{1}{K}\sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(a)$$

$$\tilde{\boldsymbol{m}}_a^{(h)} = \frac{1}{\tilde{q}^{(h-1)}(a)}\sum_{k=1}^{K} \tilde{q}_k^{(h-1)}(a)\boldsymbol{z}_k, a \in \mathcal{A},$$

$$\tilde{\boldsymbol{\Sigma}}_1^{(h)} = \frac{1}{K}\sum_{k=1}^{K}\sum_{a\in\mathcal{A}} \tilde{q}_k^{(h-1)}(a)\left(\boldsymbol{z}_k - \tilde{\boldsymbol{m}}_a^{(h)}\right)\left(\boldsymbol{z}_k - \tilde{\boldsymbol{m}}_a^{(h)}\right)^T.$$

Gathering the above results, we obtain the following decision rule

$$\frac{\prod_{k=1}^{K}\sum_{a\in\mathcal{A}} \tilde{\pi}_a^{(h)} f_1\left(\boldsymbol{z}_k; \tilde{\boldsymbol{m}}_a^{(h)}, \tilde{\boldsymbol{\Sigma}}_1^{(h)}\right)}{f_0(\boldsymbol{Z}; \bar{\boldsymbol{m}}_0, \bar{\boldsymbol{\Sigma}}_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta.$$

Finally, we will refer to this decision rule as LVM-based Spoofing Detector (LVM-SP-D).

3.2.4 Performance assessment on simulated data

In this section, we present a case study to evaluate the performance of the previously devised detectors assuming that the localization function is based on ranging, DOA estimation, and RSRP measurements. As for the performance metrics, we adopt the probability of detection (P_d) as a function of the parameter variation forced by the attacks and for a preassigned value of the P_{fa}.

Consider a scenario with a UE that is localized based upon range and DOA estimates (azimuth and elevation angles) from a single Access Node (AN). As a consequence, the vector size is N = 3. The nominal distance between the AN and the UE is 200 m with an SNR equal to -20 dB. We model the range error as resulted in [25] where ranging is performed through downlink (DL)-TDOA measurements of 5G positioning reference signal in an urban macro environment

with line-of-sight conditions. The DOA measurements are characterized as in [26] where the angle estimates are obtained through a beam-RSRP of DL with 16 UE beams.

We resort to standard Monte Carlo counting techniques where the P_d and the detection thresholds are estimated over 1000 and $100/P_{fa}$ independent trials, respectively, with $P_{fa} = 10^{-2}$. The NLJ attack is simulated by varying the variance of the noise affecting the measurements. We set the number of iterations for the EM-based architectures to 10.

3.2.4.1 Performance of the NLJ detection architectures

The detection performances for the NLJ-D-UM, NLJ-DCM, and LVM-NLJ-D are shown in Figure 3 and Figure 4, where we plot the P_d curves against the measurement variance variation represented by γ. Figure 3(a) shows the performance of the NLJ-D-UM assuming K = 24 and different values for the SNR (corresponding to different line types). As expected, while the SNR does not have a remarkable impact on the performance, the value of K_0 influences the P_d. As a matter of fact, the latter does not increase monotonically with K_0 and the best performance is obtained for K_0 = K/2. The performances of NLJ-D-CM are reported in Figure 3(b) which shares the same parameter values as in the previous subfigure. The results confirm the insensitivity of the performance to the SNR and the value of K_0. From the comparison between Figure 3(a) and Figure 3(b), it turns out that NLJ-D-UM exhibits better performance than the NLJ-D-CM since the former exploits the information related to the actual structure of the error covariance matrix, whereas the latter is designed without assuming any special structure for the covariance matrix. Finally, in Figure 3(c), we show the P_d curves associated with the LVM-NLJ-D for K = 24. The figure points out that this architecture experiences a very poor performance for the case $K_0 = K/4$ and, generally speaking, its performance is worse than those of the other detectors. In Figure 4, we analyse the effect of the sliding window size on the detection performance. In fact, these figures are analogous to the previous three figures except for *K = 32*. As expected, in this case, since the number of available data increases, the estimation quality improves leading to better detection performance for all the proposed architectures.

As final remark, it is important to underline that despite the fact that the NLJ-D-CM is designed assuming the most general structure for the covariance matrix, the detection loss with respect to the NLJ-D-UM, whose performance is estimated under perfectly matched design conditions, becomes negligible as K increases.

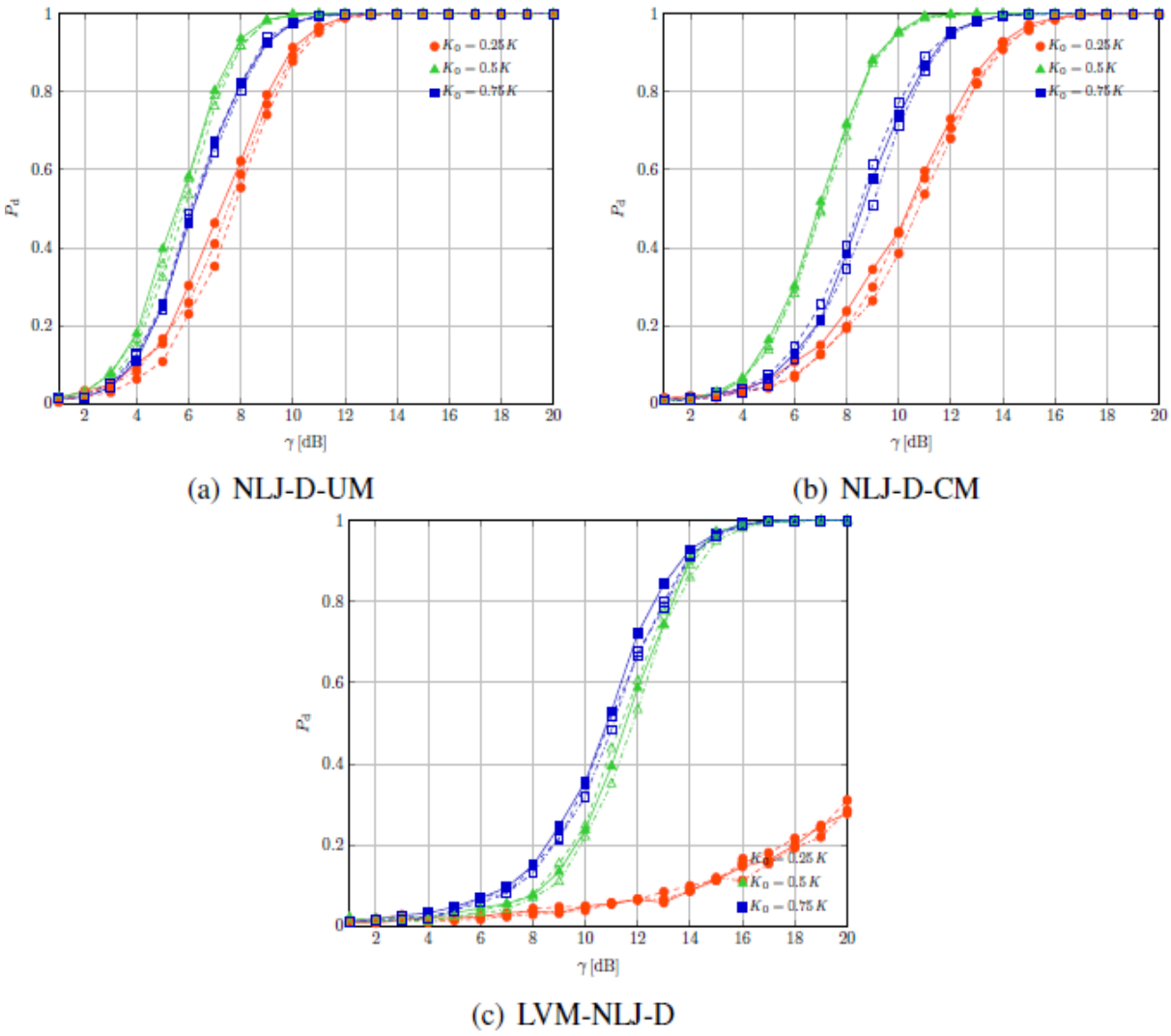

Figure 3. Performance of NLJ detectors assuming K=24.

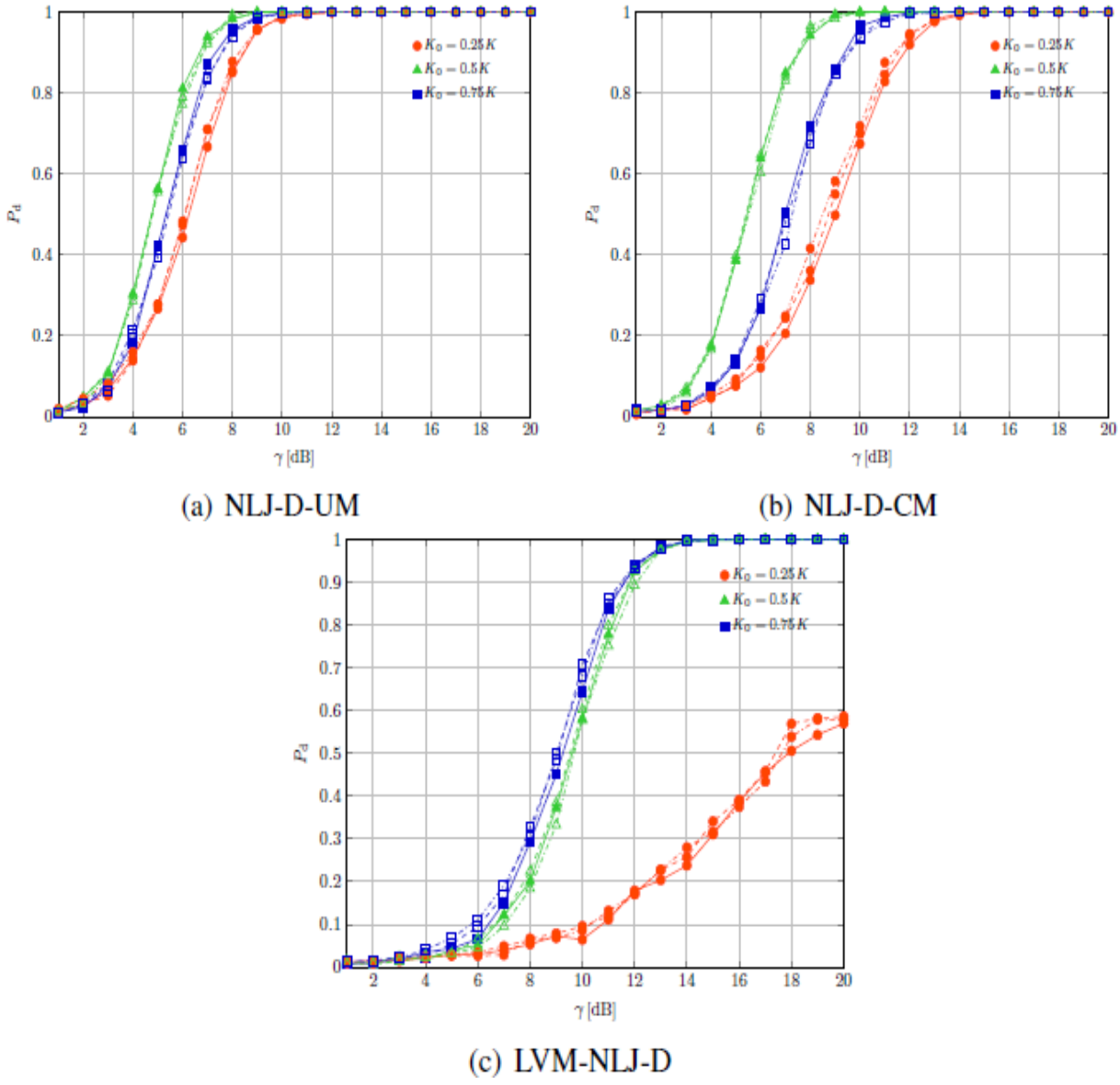

Figure 4. Performance of NLJ detectors assuming K=32.

3.2.5 Performance of the spoofing detection architectures

The performance assessment of the SP-D-UM, SP-D-CM, and LVM-SP-D in terms of probability of spoofing detection is provided in Figure 5 assuming $K = 24$ and in Figure 6 assuming $K = 32$. Unlike NLJ detectors, in this case, the SNR variations significantly affects the P_d that, in this case, increases with the SNR. This behavior can be observed for all the proposed spoofing detectors. As for the loss of SP-D-CM with respect to the SP-D-UM due to the more general design assumptions of the former with respect to the latter, in this case, it is less important than that observed in Figure 3 and Figure 4. Moreover, notice that, differently from the LVM-NLJ-D, the LVM-SP-D can achieve a P_d values greater than 0.9 for each considered value of K_0.

Another important aspect to be underlined is that for high K values, the P_d variation induced by K_0 reduces. Summarizing, also in the presence of a spoofing attacks, the SP-D-CM guarantees good trade-off between performance and application fields.

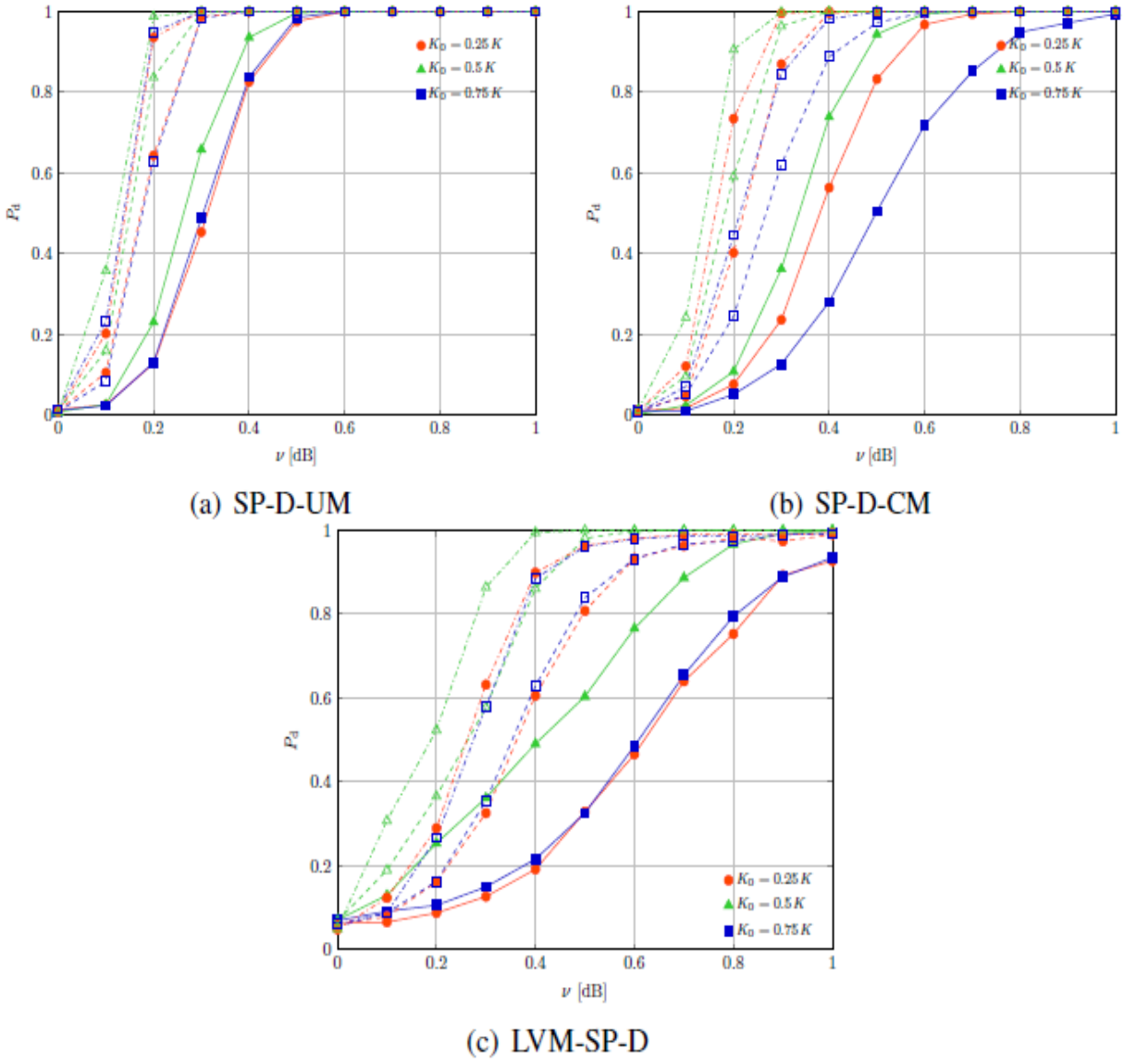

Figure 5. Performance of spoofer detectors assuming K=24.

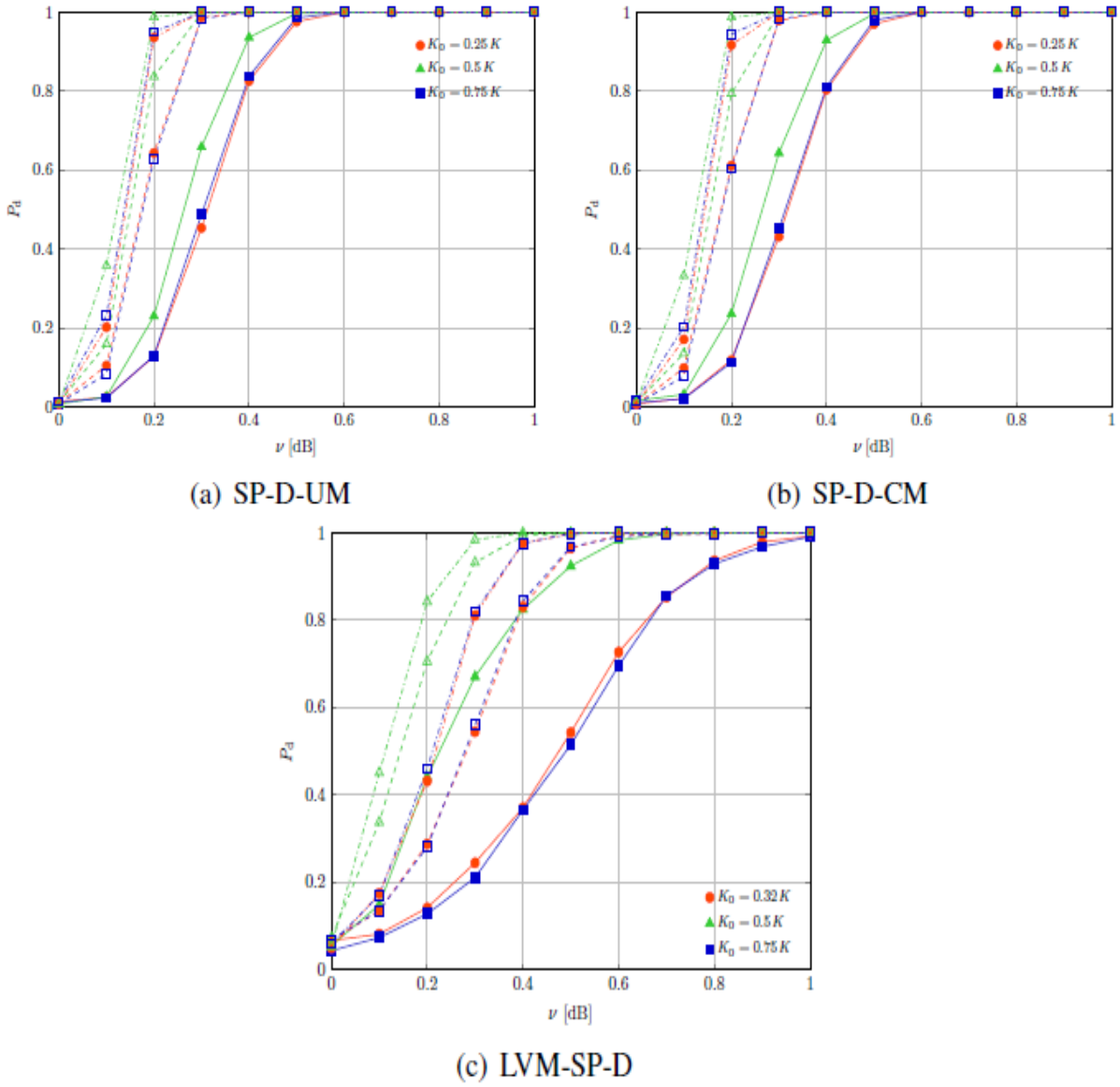

Figure 6. Performance of spoofer detectors assuming K=32.

3.3 UE-Centric jammer detection using power measurements: experimental results

As stated at the beginning of this section, although the evolving 3GPP standards have devised solutions to thwart several kinds of attacks, the attackers can leverage practical concerns that force operators to slowly and incrementally deploy next-generation cellular technologies. Therefore, an attacker can convince the UE to believe that the only base station available in a coverage area is a fake one implementing a past generation standard, thereby circumventing the new protections.

For this reason, in this subsection we propose some solutions aimed at making the UE aware that an attack is in course. To this end, we tailor previous designs to the problem of detecting (possibly) smart jammers and RBS signals by means of power measurements that can be easily collected by the UE using common applications such as Netmonster ©, Network Signal Guru ©, or Network Cell Info ©. Such applications provide instantaneous and average measurements related to the noise power and SNR. More importantly, the information collected by UEs (including the results of detection and other side information) can be transmitted to the network infrastructure in order to undertake further actions against hostile actors.

As in the previous subsection, we adaptively monitor, within a preassigned temporal sliding window, a number of physically observable quantities that can be gathered from commodity receivers. We formulate the following decision problems, which differ in the set of data distribution parameters subject to possible variations caused by the malicious actions and lead to three different designs:

1. the first problem assumes that only the covariance matrix changes after the instant K_0 while the means are generally different due to possible environment interference

$$\begin{cases} \mathrm{H}_0: \begin{cases} \boldsymbol{Z}_{1:K_0} \sim \mathcal{N}_N(\boldsymbol{m_1}, \boldsymbol{\Sigma}, \boldsymbol{I}), \\ \boldsymbol{Z}_{K_0+1:K} \sim \mathcal{N}_N(\boldsymbol{m_2}, \boldsymbol{\Sigma}, \boldsymbol{I}), \end{cases} \\ \mathrm{H}_1: \begin{cases} \boldsymbol{Z}_{1:K_0} \sim \mathcal{N}_N(\boldsymbol{m_1}, \boldsymbol{\Sigma_1}, \boldsymbol{I}), \\ \boldsymbol{Z}_{K_0+1:K} \sim \mathcal{N}_N(\boldsymbol{m_2}, \boldsymbol{\Sigma_2}, \boldsymbol{I}). \end{cases} \end{cases}$$

   Applying the GLRT, we obtain the following decision scheme

$$\max_{K_0}\left\{-\frac{K_0}{2}\log\det\left(\frac{\boldsymbol{A}_1}{K_0}\right)-\frac{K_1}{2}\log\det\left(\frac{\boldsymbol{A}_2}{K_1}\right)\right\}+\max_{K_0}\left\{-\frac{K}{2}\log\det\left(\frac{\boldsymbol{A}_1+\boldsymbol{A}_2}{K}\right)\right\}\underset{H_0}{\overset{H_1}{\gtrless}}\eta,$$

   where

$$\boldsymbol{A}_i = \boldsymbol{Z}_{K_0 i+1:K_0 i+K_i}\boldsymbol{Z}^T_{K_0 i+1:K_0 i+K_i} - K_{i-1}\bar{\boldsymbol{m}}_i\bar{\boldsymbol{m}}_i^T, \quad i = 0,1$$

$$\boldsymbol{Z}_i = \left[\boldsymbol{z}_{K_0 i+1}, \dots, \boldsymbol{z}_{K_0 i+K_i}\right].$$

   This detector will be referred to in the following as Naive Change Detector (NCD).

2. The second problem is a modification of the previous one assuming that under H_0 both the mean and the covariance matrix of the $\boldsymbol{z}_k$s are constant with *k*, namely, we neglect possible changes due to other interference sources

$$\begin{cases} \mathrm{H}_0: \boldsymbol{Z}_{1:K_0} \sim \mathcal{N}_N(\boldsymbol{m}_1, \boldsymbol{\Sigma}, \boldsymbol{I}), \\ \mathrm{H}_1: \begin{cases} \boldsymbol{Z}_{1:K_0} \sim \mathcal{N}_N(\boldsymbol{m}_1, \boldsymbol{\Sigma}_1, \boldsymbol{I}), \\ \boldsymbol{Z}_{K_0+1:K} \sim \mathcal{N}_N(\boldsymbol{m}_2, \boldsymbol{\Sigma}_2, \boldsymbol{I}). \end{cases} \end{cases}$$

As a consequence, the GLRT is

$$\max_{K_0}\left\{-\frac{K_0}{2}\log\det\left(\frac{\boldsymbol{A}_1}{K_0}\right)-\frac{K_1}{2}\log\det\left(\frac{\boldsymbol{A}_2}{K_1}\right)\right\}+\max_{K_0}\left\{-\frac{K}{2}\log\det\left(\frac{\boldsymbol{A}_0}{K}\right)\right\}\underset{H_0}{\overset{H_1}{\gtrless}}\eta,$$

where

$$\boldsymbol{A}_0=\sum_{i=0}^{1}\boldsymbol{Z}_{K_0 i+1:K_0 i+K_i}\boldsymbol{Z}_{K_0 i+1:K_0 i+K_i}^T-K\bar{\boldsymbol{m}}_0\bar{\boldsymbol{m}}_0^T.$$

We will refer to it as Modified NCD (MNCD).

3. The last problem that is worth to be investigated moves the effects of the attacks on the mean only and is given by (2). Thus, the resulting detector is defined by (9) and for brevity we refer to it as SpD.

3.3.1 Performance analysis and comparisons on real recorded data

The above decision rules are assessed through a real-world experimental playground setup relying upon the Open Air Interface project and Software-Defined Radios respectively, instrumented as a jamming device, as a 4G RBS, and as a 4G receiver. Notice that since the processed measurements can be obtained through common mobile applications, they are technology agnostic and, hence, for simplicity, we have built up a scenario using 4G devices. Moreover, as stated before, the attacker forces the UE to connect to a past-generation base station. The performance metric is the P_d.

3.3.1.1 Open Air Interface (OAI) project

Open Air Interface is an open source SDR prototyping platform created by the Mobile Communications Department at EURECOM which includes: OAI Radio Access Network (OAI-RAN), which implements 4G and 5G Radio Access Network 3GPP stack (eNB, gNB and 4G, 5G UE), and OAI Core Network (OAI-CN), which currently implements 4G Evolved Packet Core and some 5G Core functions of 3GPP stack (MME, HSS, S-GW, P-GW, AMF, SMF, UPF and NRF).

The OAI targets a reference implementation of 'Release 14 LTE' based on the current 4G implementation and to progressively add enhancements from 3GPP study items defining the future 5G standard.

The software runs on general purpose computing platform (for ex. Intel/ARM) and interfaces with wide variety of SDR platforms (EXMIMO, USRP, BladeRF, LimeSDR).

3.3.1.2 Experimental Setup

The experimental setup comprises three Ettus USRP B210 devices that can be tuned over a wide radio frequency range, from 70 MHz to 6 GHz, and, hence, can cover all the LTE frequency bands. The three radio transceivers are used to emulate a legitimate base station, the UE, and the attacker (see Figure 7). On the software side, we exploit the OAI project that provides a full real-time indoor/outdoor experimental 3GPP-compliant LTE implementation [27]. More importantly, it is a reference platform in the context of 5G research and includes: OAI Radio Access Network (OAI-RAN), which implements a 4G and 5G (eNB, gNB and 4G, 5G UE) radio access network, and OAI Core Network (OAI-CN), which implements the Evolved Packet Core 4G and 5G Core Network. We assume $P_{fa} = 10^{-2}$, whereas K (namely, the number of data) depends on the specific scenario.

We have used a modified version of the code that allows us to extrapolate some UE-side features that characterise the connection with the base station. More specifically, from the UE we extrapolate the following features:

- SINR (sum of all TX/RX antennas, time average, in dB);
- estimated received signal power (sum of all TX/RX antennas, time average);
- average estimated noise power and instantaneous estimated noise power.

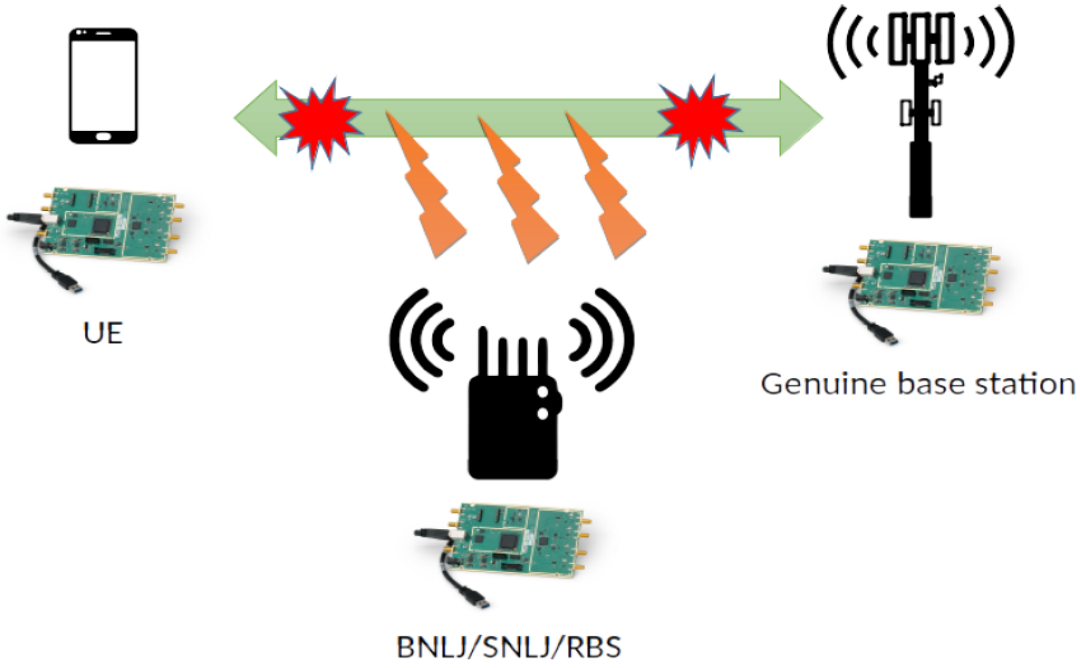

Figure 7. Experimental setup.

3.3.1.3 Experimental results: NLJ attack

We consider here two kinds of NLJ: a Barrage NLJ, which transmits wideband noise, and a Smart NLJ, which performs frequency hopping and uses a narrow band noise.

In the first operating scenario, the threat is represented by a BNLJ illuminating the UE in order to saturate its receiver forcing the disconnection from the genuine base station. In Figure 8, we show the effects of the implemented BNLJ on the collected measurements. As expected, the noisy signals injected into the UE receiver lead to an abrupt variation of both the measured noise level and the SINR. The detection performance of the proposed architectures in the presence of the BNLJ attack with JNR = 25 dB is shown in Figure 9 using 2-dimensional vectors containing the SINR and the average noise power. This analysis highlights that NCD, MNCD, and SpD share good detection performance and can declare the presence of a BNLJ when the latter begins its transmission. It is clear that once the BNLJ has modified the measurement values, the P_d curves drop close to zero due to the stationarity of the modified values.

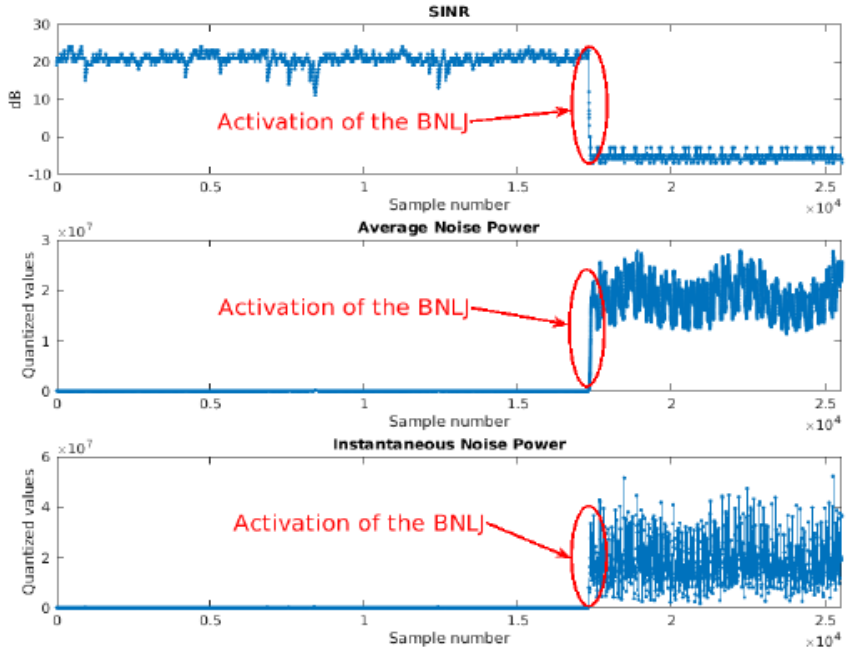

Figure 8. SINR, average noise power, and instantaneous noise power versus sample number for the scenario that includes a BNLJ with JNR = 25 dB.

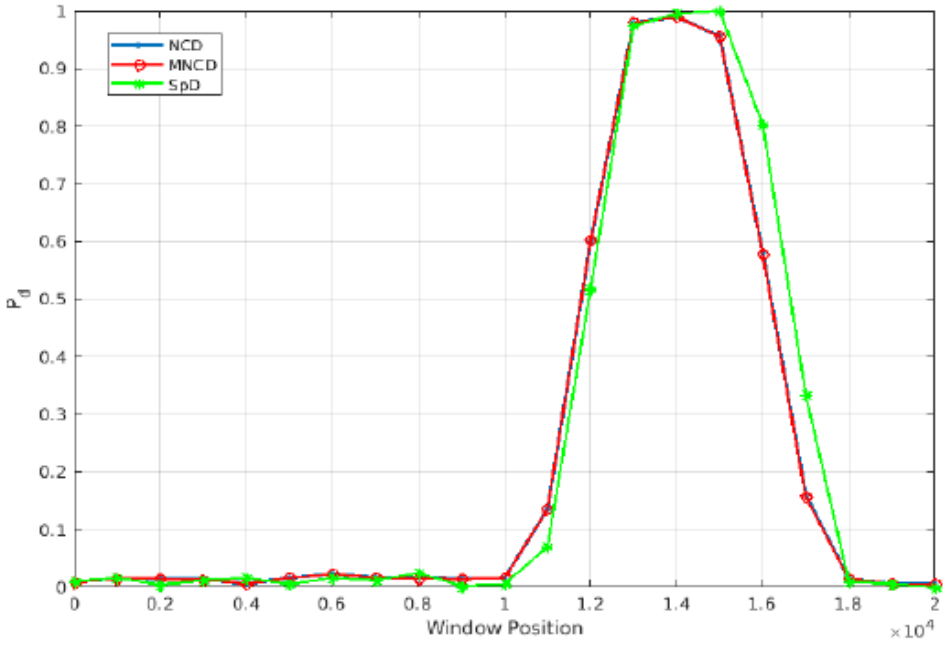

Figure 9. P_d versus sliding window position for the scenario that includes a BNLJ with JNR = 25 dB.

The next scenario replaces the BNLJ with a SNLJ maintaining unaltered the JNR (of 25 dB), whose effects on data can be observed in Figure 10. The SNLJ does not jam the entire spectrum of the LTE channel but acts as a frequency hopping jammer. Therefore, the jamming signals cover a small window of 60 contiguous sub-carriers (corresponding to 450 KHz of jammed

spectrum), and these sub-carriers move rapidly within the LTE channel every 0.1 seconds. In order to increase the jamming efficiency, the generated interference signal carries an LTE structure with randomly generated LTE pseudo-subframes. Finally, it uses the two transmission chains of the Ettus USRP B210 board to maximize its effect by sending two independent interference signals, tuned on the same LTE channel but covering different spectral windows.

The effects of this action consist of a series of spikes in the noise power data and notches in the SINR data. Figure 11 contains the P_d curves obtained by processing average and/or instantaneous noise power measurements. Inspection of the figure points out that the NCD and the MNCD share the same performance and can achieve P_d values close to 1. On the other hand, the curves related to the SpD are below $P_d = 0.5$. Moreover, the figure unveils that an integration rule of the "contacts" is also required in order to introduce a hysteresis that mitigates the P_d variations induced by the SNLJ behavior. This need is corroborated by Figure 12, where we plot a binary curve that is 1 if a detection occurs and 0 otherwise.

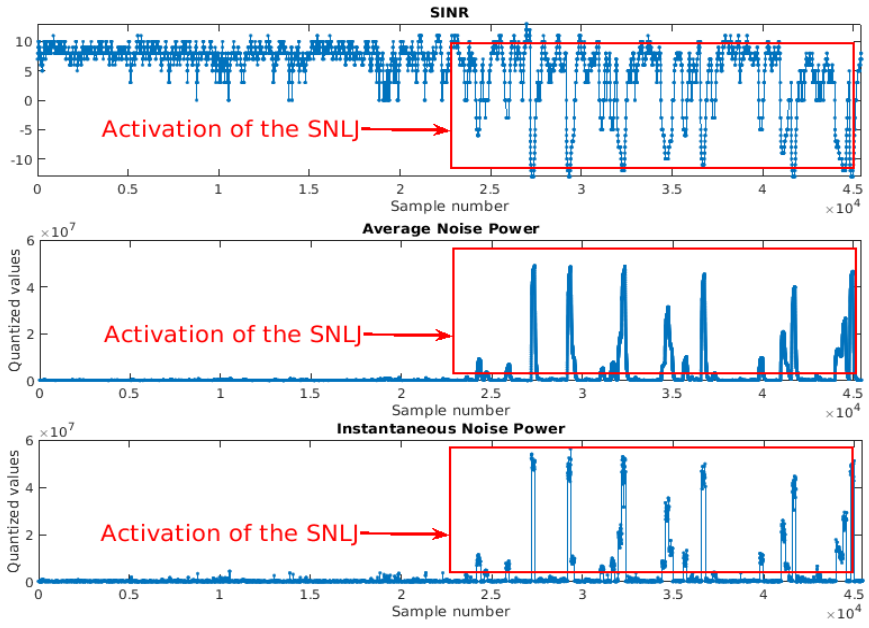

Figure 10. SINR, average noise power, and instantaneous noise power versus sample number for the scenario that includes a SNLJ with JNR = 25 dB.

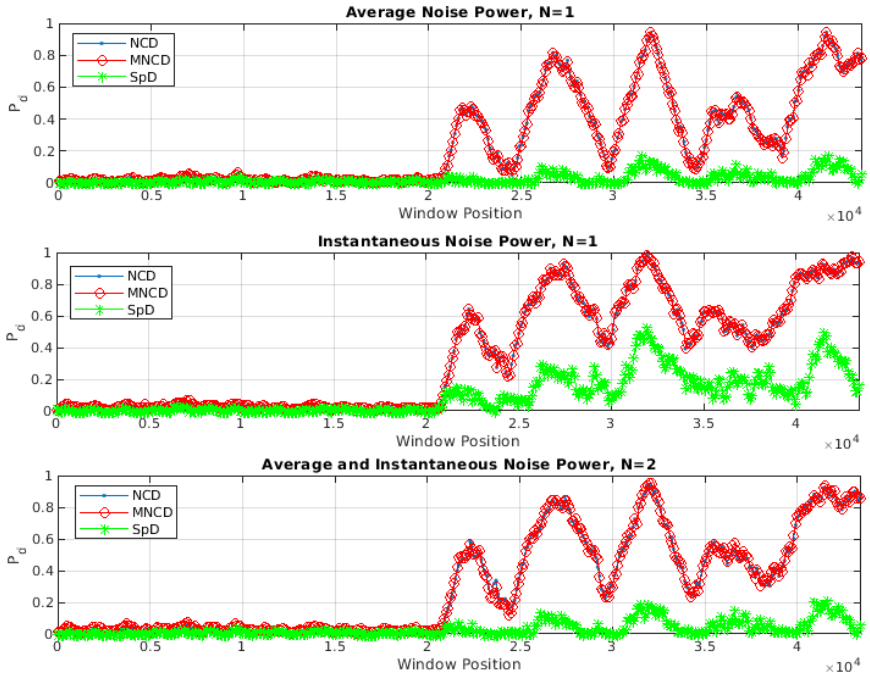

Figure 11. P_d versus sliding window position for the scenario that includes a SNLJ with JNR = 25 dB.

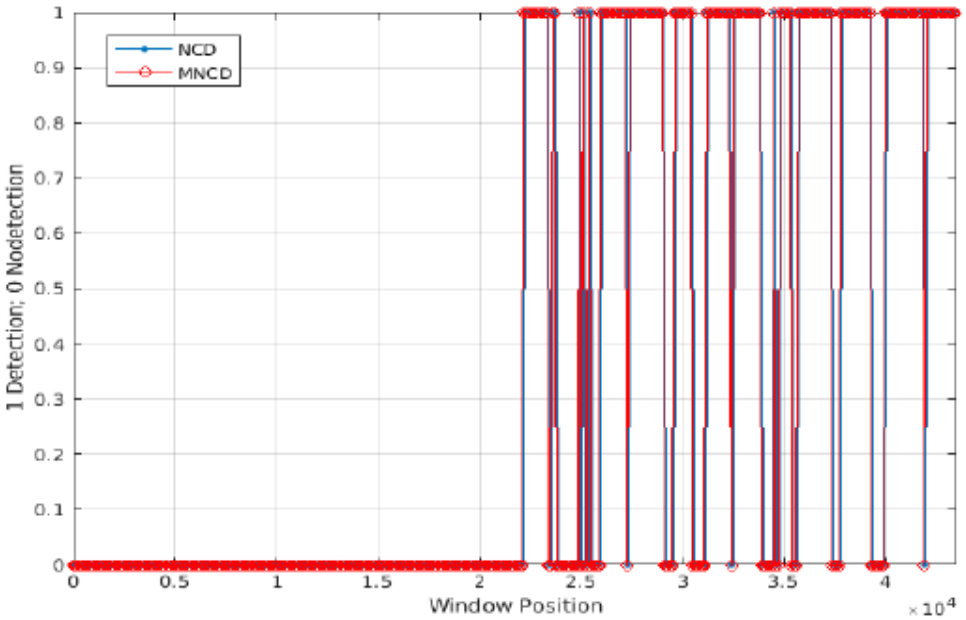

Figure 12. Binary function indicating that a detection occurs versus sliding window position for the scenario that includes a SNLJ with JNR = 25 dB.

3.3.1.4 Experimental results: RBS activation

In this last subsection, we consider a scenario where the RBS comes into play and transmits interfering signals. Specifically, RBS signals interfere with those of the genuine base station as shown in Figure 13, where the measurement behaviour is similar to that observed in the

presence of the BNLJ. The P_d curves are shown in Figure 14, where all the considered detection architectures are capable of achieving $P_d = 1$ when the position of the sliding window is such that it contains the time instant at which the RBS activates. In addition, the curves are very close to each other.

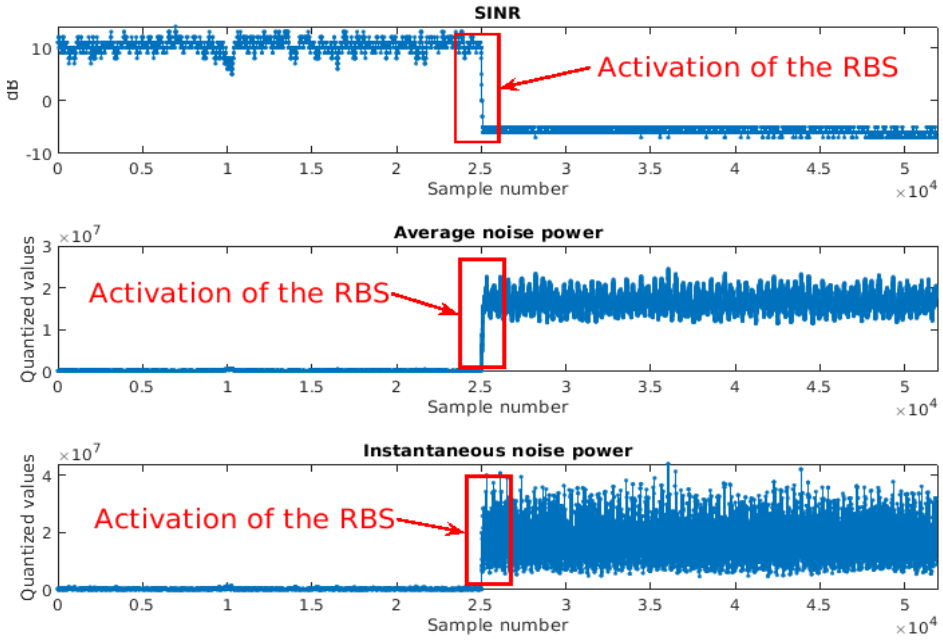

Figure 13. SINR, average noise power, and instantaneous noise power versus sample number for the scenario that includes the RBS.

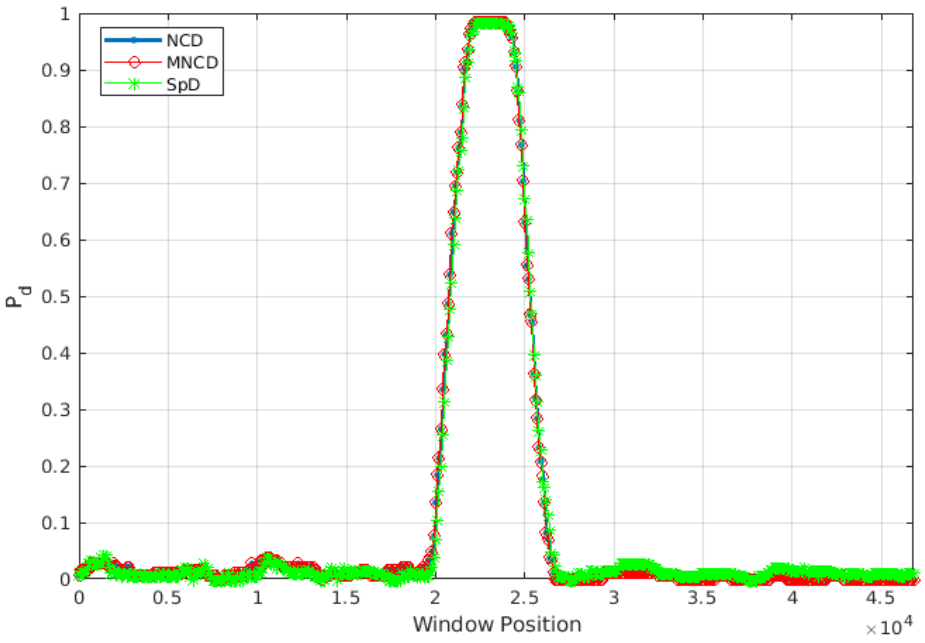

Figure 14. Pd versus sliding window position for the scenario that includes the RBS.

4 Location Security Algorithms: Threat Model and Bounds

In terms of non-adversarial localization, the analysis of localization accuracy of wireless networks has been extensively studied in the literature. Fisher information has been used extensively in the literature to derive the user localization information in the presence of multiple impairments due to signal propagation, and uncertainties about the position of the reference nodes. In [28], a performance measure called the squared position error bound has been derived using Fisher information, and it was derived for network localization in multipath environments. Nevertheless, a formal threat model for the localization error in the presence of adversarial localization is still missing while it is important for the design and comparison of countermeasures. In LOCUS, we are investigating localization tampering attacks, focusing on the case where the information of anchor nodes (e.g., base stations or access points) are tampered, hence undermining the user's localization accuracy.

First, we provide a mathematical model for the description of such spoofing attacks. Then, we derive the SPEB (squared position error bound) in the presence of tampering attacks and compare it with the case in the absence of the attack. While the model is technology-agnostic, we use RSSI-based localization, with the well-known trilateration algorithm to exemplify their derivation. Numerical results show the effect of system parameters on the localization error. We believe that the proposed model and bound can give insights into the impact of such attacks on the accuracy of user localization and provide a benchmark for the design and analysis of detection and mitigation solutions.

4.1 Threat Model

We consider a very classical scenario: an end-device infers its own position by means of suitable measurements taken from a set of reference anchor stations whose position is assumed known. A location spoofing attack can be technically performed by several different means: by altering the measurement process so that the reference anchor station is perceived as closer (or farther, or shifted) from its real place, or by deploying a rogue station claiming to be a legitimate one but placed in a different position, or by corrupting the control system which provides the legitimate anchors' positions.

Our proposed threat model aims to abstract from the specific details of each attack, and rather has the ambition to provide a reference formal model common to all the above specific cases. The intuitive idea is that a location attack occurs when the attacker is capable to associate an anchor's position to an observable not representative of the claimed position, being irrelevant whether this is obtained by tampering the measurements or by spoofing the claimed position. In what follows we formalize this notion.

4.1.1 Formal model

Consider a localization network as consisting of N_b anchors for inferring the location of an agent at $\boldsymbol{p}$. The i-th anchor is at position $\boldsymbol{p}_i$, and $\boldsymbol{p}_b = [\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_{N_b}]$. The agent location is inferred based on measurements of signals communicated between each anchor and agent. In particular, the measurement vector is $\boldsymbol{z} = [z_1, z_2, \ldots, z_{N_b}]$, where z_i is measured between the i-th anchor and the agent. An example illustration is given in Figure 15. The localization algorithm exploits $\boldsymbol{z}$ together with the information about the anchors' positions. Each measurement depends on the true anchor and agent positions according to a measurement model and the measurements from different anchors are independent. Example cases are when the measurement is a timing, angle, or power measurement and we know the signal speed and the anchors' position.

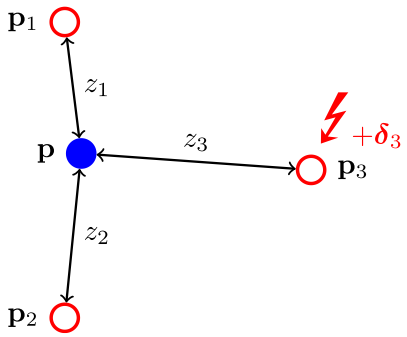

Figure 15 Example scenario with Nb = 3 anchors and one agent in the presence of a spoofing attack against the third anchor.

If we model the agent position as a deterministic but unknown parameter and the anchor positions as a deterministic and known parameter, the likelihood function for the vector $\boldsymbol{p}$ is:

$$f(\boldsymbol{z}, \boldsymbol{p}, \boldsymbol{p}_\mathbf{b}) = \prod_{i=1}^{N_\mathrm{b}} f(z_i, \boldsymbol{p}, \boldsymbol{p}_i)$$

where each $f(z_i, \boldsymbol{p}, \boldsymbol{p}_i)$ is obtained according to the measurement model. If the likelihood function is known, the maximum likelihood (ML) estimator is the optimal solution, as it achieves the Cramer–Rao bound (CRB) asymptotically in the high signal-to-noise ratio (SNR) regimes. The ML estimator is unbiased, i.e. $E\{\hat{\boldsymbol{p}}_{sp}\} \neq \boldsymbol{p}$, where E represents the expected value. In most cases, the likelihood function is unknown in general, as it is unknown the exact distribution of the measurements or some of its parameters. In such practical cases, sub-optimal estimators are considered, e.g. using the well-known trilateration or the least square algorithms.

4.1.2 Error Model for the Spoofing Attack

In the presence of a spoofing attack, where the anchor positions are tampered, the main effect is that measurements are taken with respect to the true anchor, and therefore they follow the true measurement model. Nevertheless, as the information about the anchor position is tampered, if there is no detection or awareness of such a tampering attack, the localization algorithm will estimate the agent position according to an incorrect measurement model, i.e. considers the anchor in a wrong position. The effect of such an incorrect measurement model on the accuracy of localization depends on several system parameters and on the estimator itself. In general, different estimators will be less or more robust to this type of attack. In the case of a ML estimator, the position estimate under attack will be

$$\hat{\boldsymbol{p}}_{sp} = \text{argmax}_{\{\tilde{\boldsymbol{p}}\}} \prod_i f(\boldsymbol{z}_i, \tilde{\boldsymbol{p}}, \boldsymbol{p}_i + \boldsymbol{\delta_i}).$$

Note that for $\boldsymbol{\delta_i} \neq \boldsymbol{0}$ for some i, the ML estimator is biased, i.e. $E\{\hat{\boldsymbol{p}}_{sp}\} \neq \boldsymbol{p}$. We define the spoofing error as $\boldsymbol{e}_{sp} = \hat{\boldsymbol{p}}_{sp} - \boldsymbol{p}$. Let us now consider the following system of N_b equations with respect to $\breve{\boldsymbol{p}}$

$$z_0(\breve{\boldsymbol{p}}, \boldsymbol{p_i} + \boldsymbol{\delta_i}) = z_0(\boldsymbol{p}, \boldsymbol{p_i}) \quad \forall i = 1,2, \dots, N_\text{b}.$$

If there exists a solution to such system, the solution $\breve{\boldsymbol{p}}$ would be the position of the agent in the case the true position of the i-th anchor would be $\boldsymbol{p}_i + \boldsymbol{\delta_i}$ for each $i = 1,2, \dots, N_\text{b}$ and the measurement between the anchor and the i-th anchor would have the expected value z_i . In such a case, i.e. in the absence of any spoofing, a ML estimator for the case with an agent at $\breve{\boldsymbol{p}}$ and the anchors $\boldsymbol{p}_i + \boldsymbol{\delta_i}$ would solve the equivalent problem as in Sec. 4.1.1 as an unbiased estimator. Then, $E\{\hat{\boldsymbol{p}}_{sp}\} \neq \breve{\boldsymbol{p}}$. It follows that, being this the identical problem as in Sec. 4.1.1 we have $E\{\boldsymbol{e}_{sp}\} \neq \breve{\boldsymbol{p}} - \boldsymbol{p}$. Note that this is valid for any estimator that is unbiased in the absence of an attack, i.e. $E\{\hat{\boldsymbol{p}}_{sp} \mid \boldsymbol{\delta_i} \neq \boldsymbol{0}\ \forall i\} = \boldsymbol{p}$ and that is based on a measurement model. If $\breve{\boldsymbol{p}}$ does not exists, i.e. the system of N_b equations has no solution, then the error will depend on the specific localization algorithm and the measurement model.

4.1.3 Example Case Study: range-based Localization using RSSI

As an example, we here focus on the range-based localization using received signal strength indicator (RSSI). In this case, each anchor transmits with power P_T. The signal propagates in fading channel where the fading is modelled as a lognormal random variable. Thus, the power received at the agent from the ith anchor depends on the true distance between the ith anchor and the agent, the path-loss exponent, and the fading is independent from anchor to anchor. Then, the received power is considered as the measurement for each anchor-agent

link, and the measurement model as a function of the positions is given by the power-distance law through the path-loss exponent.

4.2 Error Bound under Spoofing Attack

Consider the measurement model $f(z_i, \boldsymbol{p}, \boldsymbol{p_i})$ for the observation z_i and unknown deterministic parameter vector $\boldsymbol{p}$. Let $\hat{p}$ be any unbiased estimate of $\boldsymbol{p}$ given $\boldsymbol{p_i}$. Based on the information inequality, which gives a lower bound on the mean squared error (MSE) of estimators, we have

$$E\{||\boldsymbol{p} - \hat{\boldsymbol{p}}||^2\} \geq \text{trace}\{\mathbf{J}_p^{-1}\}$$

where $\mathbf{J}_p$ is the Fisher information matrix for the parameter vector $\boldsymbol{p}$ and $trace\{\mathbf{J}_p^{-1}\}$is called the SPEB [28].

As we have discussed in Sec. 4.1.2, an estimator $\hat{\boldsymbol{p}}$ that is unbiased in the absence of a tampering attack, becomes biased when $\boldsymbol{\delta_i} \neq \mathbf{0}$ for any i due to the incorrect measurement model. In such a case, the expected value of the estimated position is affected by a bias due to the tampering attack. The information inequality on the mean squared error of such a biased estimator should take into account the biases. In particular, we define

$$\boldsymbol{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}} = \frac{\partial E\{\hat{\boldsymbol{p}}|\boldsymbol{\delta_i} \neq \mathbf{0}\}}{\partial \boldsymbol{p}}$$

and we derive the SPEB for a biased estimator $\hat{\boldsymbol{p}}$ as

$$E\{||\boldsymbol{p} - \hat{\boldsymbol{p}}||^2|\boldsymbol{\delta_i} \neq \mathbf{0}\} = \text{trace}\{\boldsymbol{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}} \mathbf{J}_p^{-1} \boldsymbol{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}}{}^T\}$$

4.3 Case Study

In this section, we evaluate the effects of tampering with location estimates using simulation results. We consider a network on $N_b = 3$ anchors uniformly distributed on a circumference of radius $r = 1$ km. We consider the agent as uniformly distributed within a squared area of 1 by 1 km. RSSI-based localization is considered with σ varying from 0.1 to 10, and σ = 2. The spoofing is simulated considering a constant value δ_i = $[\delta, \delta]$ for all the spoofed anchors. We consider the case with a single spoofed anchor and two spoofed anchors. Location estimation is performed with a least square algorithm, which is equivalent to the MLE when σ is constant and the underlying distribution is Gaussian.

Figure 16 shows the SPEB and MSE varying δ when a single or two anchors are spoofed. The second spoofed anchor increases both the MSE and the SPEB. Note that the value of the MSE with two spoofed anchors and δ = 270 m is comparable to the MSE with a single spoofed anchor with δ = 350 m.

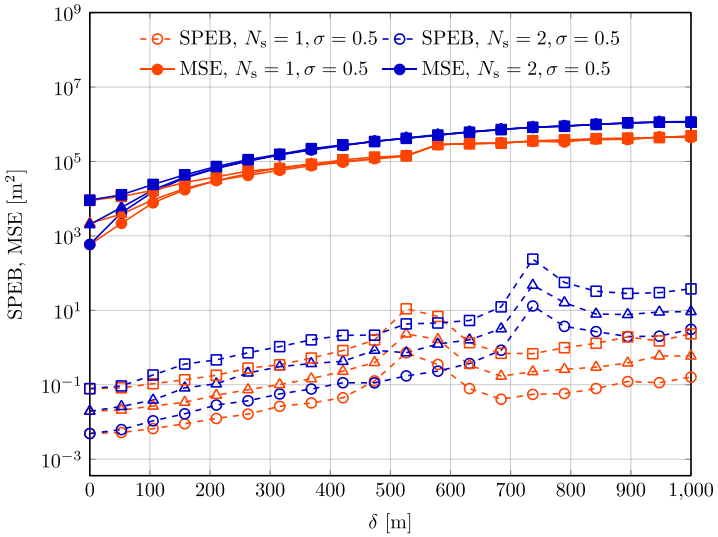

Figure 16 SPEB (dashed) and MSE (solid) varying δ, with σ = 0.5 (circles), σ = 1 (triangles), and σ = 2 (squares); single spoofed anchor (red) and two spoofed anchors (blue)

Figure 17 shows the SPEB and the MSE as a function of σ for δ = 100, 400, and 800 m with a single or two spoofed anchors. When the value of δ is above 100 m, the effect of sigma is negligible for any value of σ in the interval considered. Also, when δ = 100 m, the effect of the number of spoofed anchors is much smaller than when δ > 100 m.

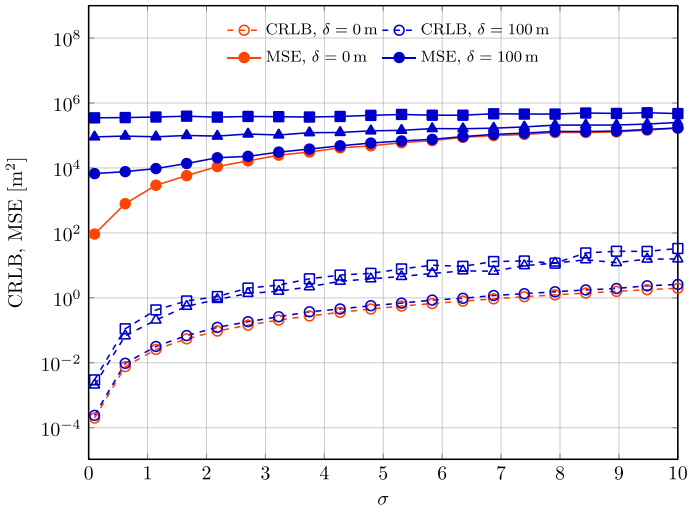

Figure 17 SPEB (dashed) and MSE (solid) varying σ with δ = 100m (circles), δ = 400m (triangles), and δ = 800m (squares); a single spoofed anchor (red) and two spoofed anchors (blue)

Figure 18 shows the MSE varying the number of anchors N_b for the case with a single or two spoofed anchors. As it could be expected, the MSE decreases with the number of anchors that are not affected by spoofing. In particular, with $N_b = 8$, the case with a single spoofed anchor is very close to the case without spoofing, meaning that the effect of the spoofing has been

mitigated with a greater number of anchors. On the other side, when two anchors are spoofed, even $N_b = 8$ anchors are not sufficient to mitigate completely the effect of the spoofing.

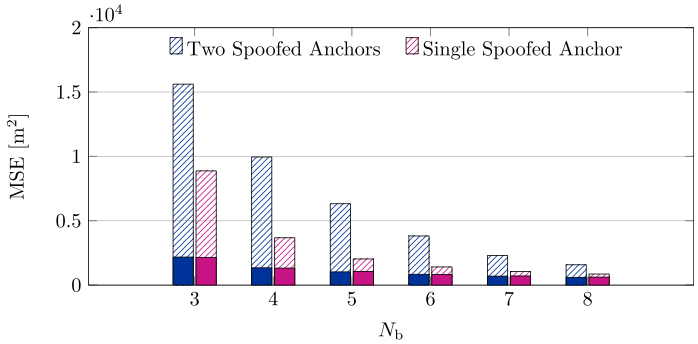

Figure 18 MSE for different numbers of anchors in the case of two spoofed anchors (blue) and a single spoofed anchor (magenta), with spoofing (dashed) and without spoofing (full).

5 LOCUS privacy algorithms

The Deliverable D2.2 has provided an overview on the privacy implication for LBSs and cellular networks, and D2.4 has presented the functions that have been considered to include the privacy concerns into the complete lifecycle of the LOCUS platform, especially in the design part. In this deliverable we consider the study of specific functionalities that reduce the risk to produce privacy threats in user data management.

Indeed, one of the challenges of the LOCUS project is to keep data simply usable by third-party stakeholders, that can provide LBSs to the LOCUS domain. As a consequence, different services and opportunities can become available for the users.

On the other side, LBS rises several privacy issues. This happens when an attacker, especially an untrusted LBS, can create an association between identity, request content and location of a user [29]. This information can be possibly obtained from location-based requests to LBS, specifically when the background knowledge is available.

5.1 LOCUS privacy functions

As presented in D2.4, the LOCUS architecture includes a specific functional block dedicated to location security and privacy. These functionalities are applied to different parts of the LOCUS architecture through the function interfaces, enabled by the LOCUS APIs. In order to achieve this goal, LOCUS supports all the security requirements related to mobile devices, network, and third-party entities. In fact, the interface is acting as a connection between the Security & Privacy Layer and the appropriate APIs exposing functionalities, 3rd party applications for network management, as well as other vertical applications that shall exploit localization analytics as a service provided by LOCUS platform.

During the study and the design of the LOCUS platform architecture, the following privacy functions have been defined (they are detailed in D2.4):

- **Sanitization**: this function implements the process of removing user sensitive information from stored location data;
- **k-anonymity**: this function implements a data process to produce data output where a user cannot be distinguished from at least the other k - 1 individuals;
- **Obfuscation**: this function implements techniques that aim at blurring or perturbing the location information contained in LOCUS persistence entity because of its potential sensitivity;
- **Policy definition**: this function implements the setting of the privacy policy. It describes a fine-grained sanitization policy developed for private data, to facilitate their release to the public, and a sanitization tool that applies the policy;
- **Result Aggregation**: the privacy of a user/device is further protected by using a “hiding in a crowd” approach; 3rd party can query on any features which interest them but they only receive aggregate responses (counts, histograms, etc.) to address data query correlations.

From the previous list, two functions will be implemented and made available in the LOCUS Proof of Concept. They are k-anonymity and Result Aggregation. The study of the algorithms to implement the two functions in LOCUS is addressed in the task 2.3. Specifically, this deliverable shows the descriptions and the performances of the designed algorithms, while the implementation process, including the APIs, will be presented in D5.3 of the WP5.

5.2 LOCUS privacy model

We consider the model with an untrusted LBS server, that starting from the users queries with position and content request, can track users or release their personal data to third parties. Consider, for example, a service request originating from the house of a user. The request contains sufficient information to identify the requester, even though any other identification data are not present in the request content. Indeed, the untrusted LBS can map the exact coordinates that are part of the user request to a publicly available house owner registry. Moreover, if a series of requests for LBSs are matched to the same individual then it is possible for the service provider to identify places that this user frequently visits, reveal his/her personal information or alternative lifestyles, as well as build up a complete profile of the user based on the history of his/her movement in the system.

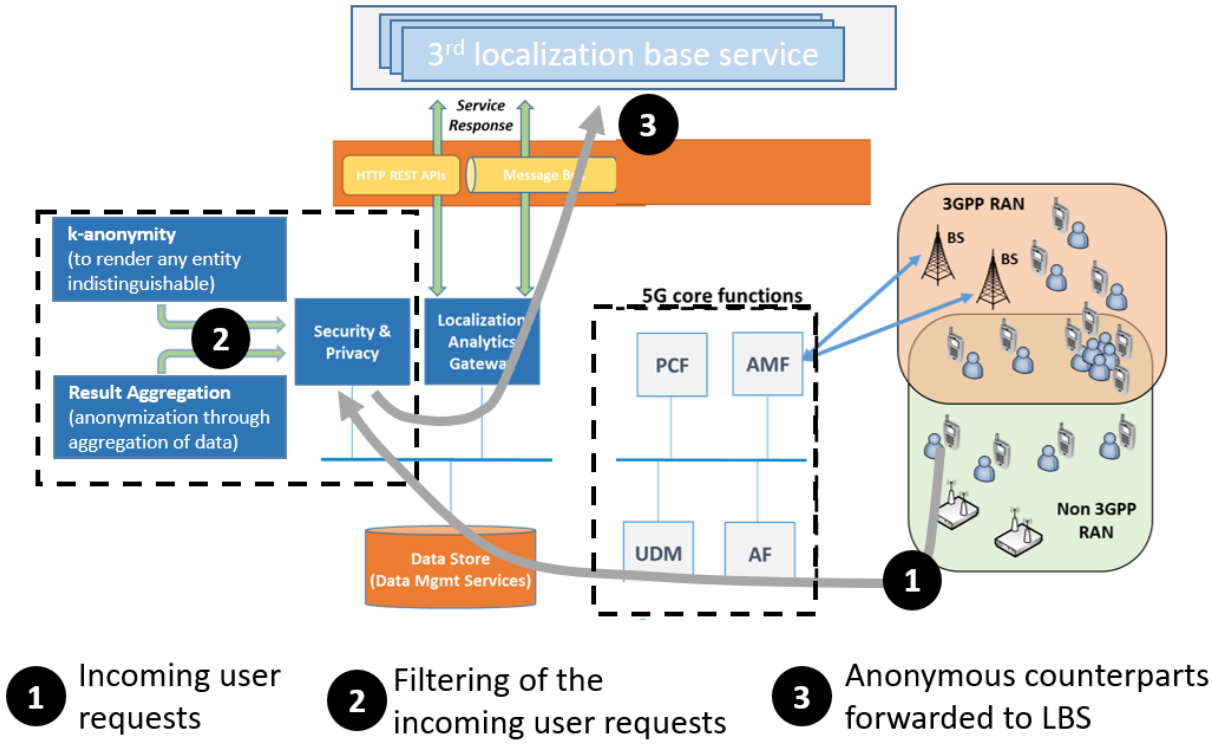

Figure 19 - LOCUS LBS privacy model

Figure 19 presents the considered model for privacy in LBSs in LOCUS with three different phases. We consider a population of users who are supported by LOCUS infrastructure. For

each user, the system performs a location update to the platform data storage. A set of 3rd party LBSs are subscribed to the LOCUS domain. In the figure, phase 1 indicates the incoming request from the users. The role of the privacy module is to filter the incoming user requests (phase 2) and to produce anonymous counterparts that can be safely forwarded to the LBS (phase 3). To produce the anonymous counterpart, the privacy module has to incorporate algorithms that works towards two main directions:

1. removing any obvious identifiers that are part of the user request (e.g., ID, name)
2. effectively transforming the exact location of request into a spatiotemporal area (the area of anonymity). This area must include a sufficient number of nearby users so as to prevent the attacker from locating the requester. These users formulate the anonymity set of the requester.

Same consideration can be done for the result aggregation function, different from the previous description, the request is provided from the LBS and contains any interesting features. In this case the privacy module only responds through aggregate data using statistical functions and extracted features.

5.3 Related work

This subsection will report the literature related to the algorithms to execute privacy preserved LBS content requests. The main body of research includes approaches that are based on the notion of k–anonymity, which has been originally proposed by Samarati and Sweeney [30] [31] in the context of relational data. To satisfy k–anonymity in LBSs, the most widely adopted anonymization strategies are:

- Dummy location approach [32] [33]
- Data/spatial cloaking technology [34] [35] [36]
- Historical/trajectory approaches [37] [38]

Dummy location approach. The dummy location approach generates multiple dummy locations and integrates the users' real locations into the dummy ones and sends them to the service provider for privacy protection. The dummy approach is mainly useful when k-anonymity is applied in regions with few users or sparse regions. However, many techniques do not fully consider the context when generating data. For example, the generated dummy location points may be located in sparsely populated regions such as lakes, rivers, and swamps. If the attacker has mastered certain background knowledge (such as maps and historical query records), the dummy location can be easily filtered out by the adversaries, which cannot satisfy the user's anonymity requirement. Finally, if the attacker retrieves the protected algorithm, it can filter dummy locations and extract the real user position.

Data/spatial cloaking technology. Data dependent cloaking strategies formulate the region of anonymity based on the actual location of each user in the system and his/her distance from the location of request [39]. Specifically, these strategies retrieve the k–1 nearest neighbours

of the requester and generate a region that includes all the k users. Space dependent cloaking strategies take into consideration the total area that is covered by the anonymizer to formulate the regions of anonymity. Specifically, these strategies partition the area in a grid fashion. An example is to generate the region of anonymity by retrieving the users in each cell of the grid (starting from the cell of the requester and moving to neighbouring cells) until at least k users are found. Casper [35] is one of the most popular grid–based approaches to location k–anonymity. In Casper the entire area is divided in a grid–fashion and organized in a pyramid data structure of layers that is similar to a Quad–tree [40]. Since the Casper algorithm uses quad-tree to partition the spatial region and fails to consider the distribution of the target user's adjacent users, when it merges the quadrants, it also considers redundant regions. Casper is secure only for uniform data distributions. Hilbert Cloak [36] does not suffer from this shortcoming as it generates the same Anonymity Spatial Region (ASR). The approach is based on k–bucket cloaking; it dynamically arranges the users into groups of k and computes the ASR as the Minimum Bounding Rectangle (MBR) enclosure that contains the k users in the group of the requester.

Historical/trajectory approaches. Previous approaches do not consider the story of the user requests, while in historical K–anonymity approaches the participants of the anonymity set are selected based on their history of movement in the system, with the requirement that at some time in their history of movement these users were close to the point of request. This means that if an LBS can successfully track the requests of a user through all the requests, then there would be at least k - 1 other users whose personal history of locations is consistent with these requests; in other words, from the LBS perspective, there would be at least k users who may have issued those requests.

Finally, trajectory k–anonymity approaches consider the analysis of future requests, this approach is appropriate for service in which the current position of the user has to be communicated to the service provider for as long as the user travels.

In [41] an anonymous region constructing algorithm based on kd-trees [42] is proposed. It works in densely and sparsely populated regions. The proposed scheme is compared with other literature algorithms, they show how the kd-tree algorithm can improve the search efficiency. Moreover, the request content among users is considered. A weight is assigned to the request content in the user group based on the number of request types and the distribution in the user group.

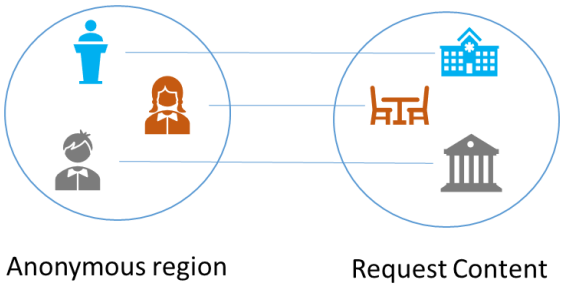

Figure 20 - Location privacy protected

To better understand the contribution of the content, the Figure 20 represents a perfect scenario where the location privacy of the user is protected because both the area of the anonymous region and the difference of the request content are all larger.

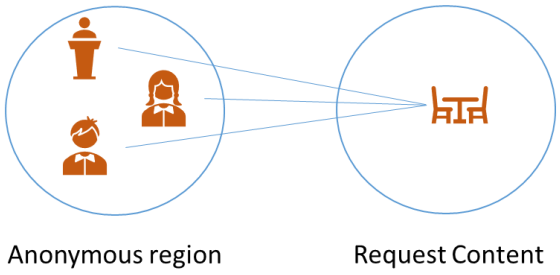

Figure 21 - Content privacy inferred

Differently, Figure 21 shows that the user's content privacy information can be inferred. In this case, the request contents are the same with different users, there exists risk of privacy leakage.

We consider this last approach for the privacy preserving functions supported from LOCUS platform. In this deliverable we report the study of the algorithm and the performance results in comparison with traditional approaches that do not consider content requests and kd-tree data structure. We evaluate these algorithms on a real dataset provided from a network operator.

5.4 Data from real scenario

To evaluate the proposed privacy functions, we use real-world mobility traces. Data is provided from the network operator; users are tracked through GPS coordinates with a resolution time of 15 minutes.

The type of data required for LOCUS algorithms' training includes measurement of network infrastructures, with the focus being on location data inside the network itself. The Dataset is provided after an anonymization process and the dataset covered an interval time of 24 hours in September 2020.

Since the data originate from real persons, particular care has been taken in the anonymization procedures before distributing the data to the partners inside LOCUS. Mobile device and subscriber data (call details, duration, IMSI, IMEI, location, signal performance) are collected and transferred temporarily to the Big Data system, where they are anonymised with a salt-key generation every 15 minutes from bash-script and Hive table so as to be made available for the LOCUS project. The anonymization function uses as input: a) data for anonymisation and b) salt key. The personal identifiers in the data (IMEI, IMSI) are encrypted with a SHA-2 cryptographic hash function. The location data records GPS coordinates together to other network information. GPS coordinates are retrieved from network estimation algorithms.

The dataset used has over 20 000 000 location traces splitting in 3 different subsets, related to three different location areas in Greece.

Dataset	Location area	Rows number	Users number
1	Attica road	19 093 907	414 108
2	Athens	1 032 253	49 968
3	Domokos	408 538	7 287

Table 2 – Rows number and unique users for subset

Table 2 shows the details for each subset in terms of rows number and unique users' number. The table also includes the name of the location area where data are collected. In the figures below the areas where the datasets have been extracted are depicted.

Attica road (Figure 22) is the ring road of the greater metropolitan area of Athens and the backbone of the road network of the whole Attica prefecture. It is extended along 70km and has two separate directional carriageways. In the central reservation of Attica road, the suburban railway of Athens has been constructed. The datasets extracted from this area contain different types of mobility users.

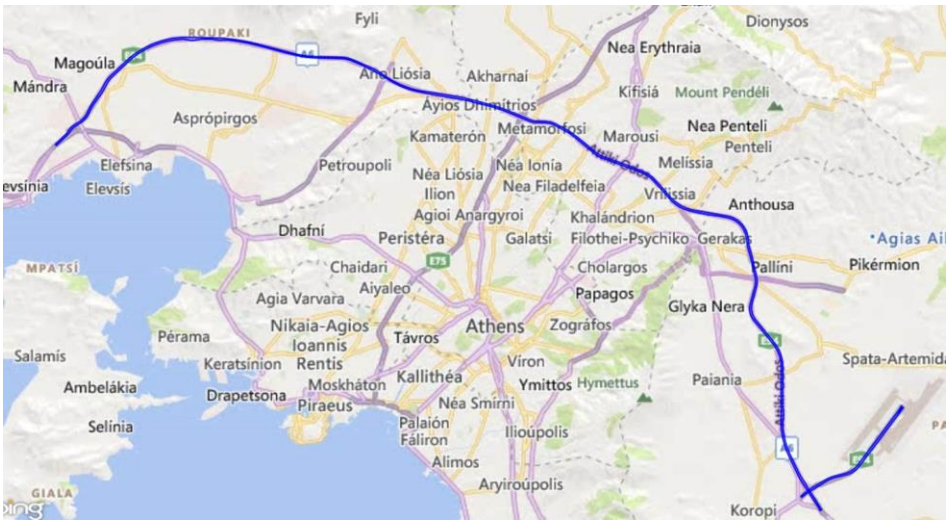

Figure 22 – Attica Road

Athens centre (Figure 23) is a dense urban area. The Centre of Athens is a very populous area with an increased population due to many visitors on a daily basis. It has been chosen due to its high density for the dense urban dataset extraction.

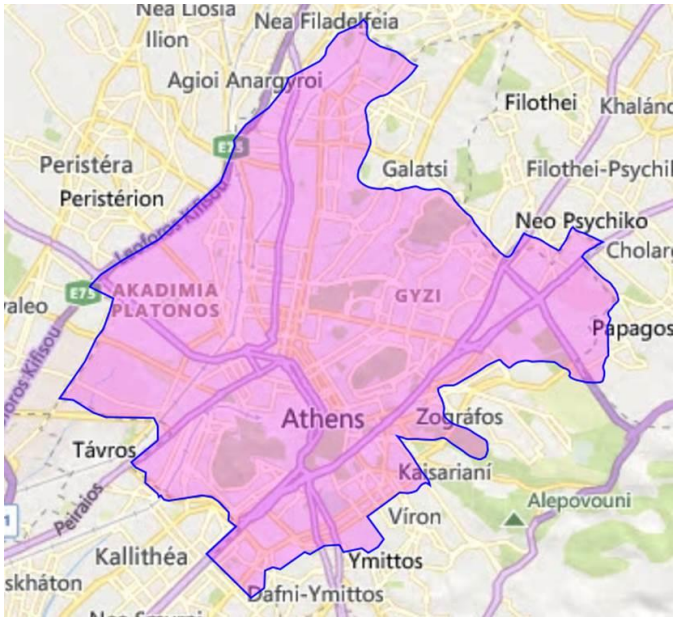

Figure 23 – Athens Centre Area (Pink Polygon)

Domokos municipality (Figure 24) is located in the north of Athens in Central Greece. It has been selected as a rural area for dataset extraction since it combines different terrains as well as part of the Athens Thessaloniki national Road.

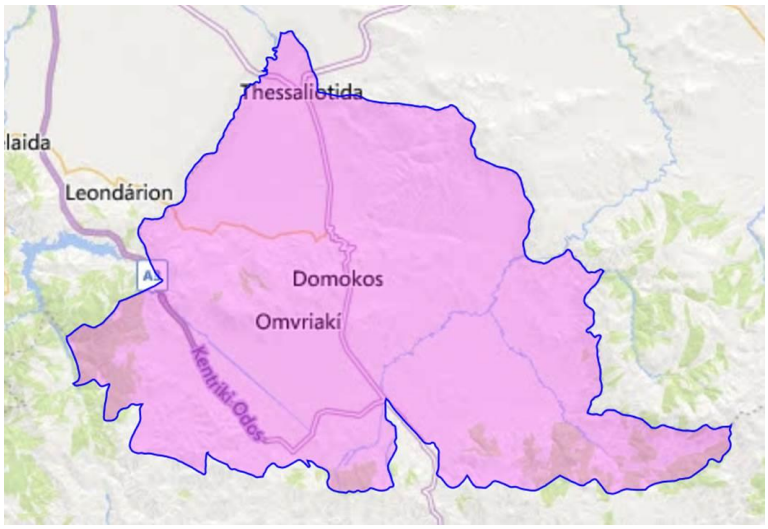

Figure 24 – Municipality of Domokos

A detail for a subset of the users' position is reported in Figure 25, where different colours represent different users.

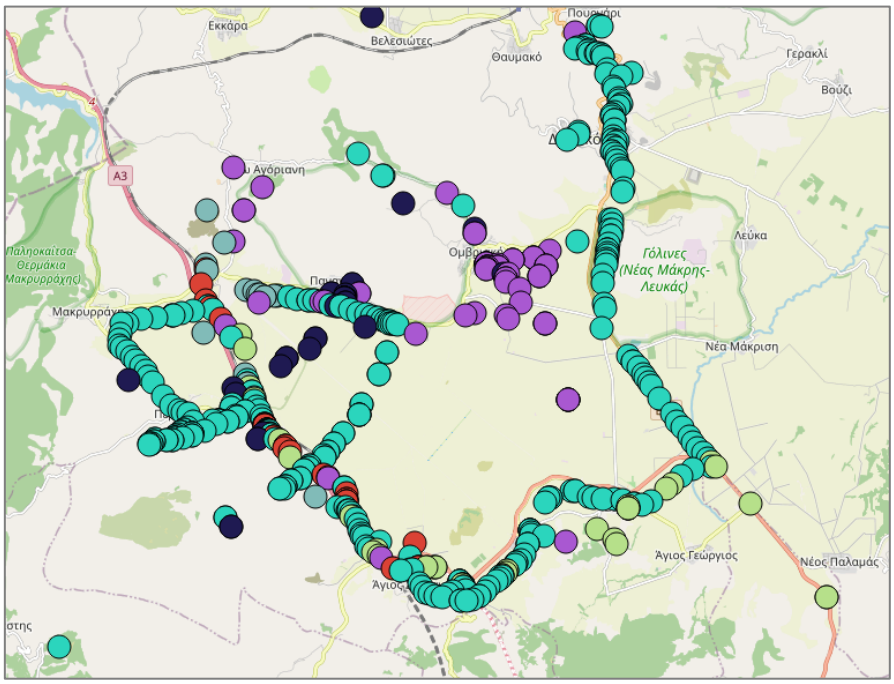

Figure 25 – Example of subset users positions for the Domokous area

We extend the dataset information in order to consider different user contents requests. We add 15types of points of interests (POIs) randomly and uniformly deployed in the considered area.

5.5 LBS privacy algorithm considered in LOCUS

In this subsection, we first present some concepts related to the entropy evaluation for a group of *k* neighbour users and then introduce the procedure of the proposed algorithm. Anonymous entropy method is considered to select users who are evenly distributed with real users, including the request content. The goal of the anonymous entropy method on distance is as follows: if the sum of distances between *k*−1 users and the real user among m user groups are equal, the user group which is evenly distributed is selected. Otherwise, if the total distances are not equal, the user group with a larger distance is selected. In order to achieve the above goal, the entropy is used to select a user group on distance. Here, the weight of the neighbour user u_i in the *n*th user group is denoted as α_{ni}, that is,

$$\alpha_{ni} = \frac{\mathrm{dist}(u_{real}, u_i)}{\sum_{j=1}^{2k} \mathrm{dist}(u_{real}, u_j)} (\mathrm{i} = 1, \cdots, \mathrm{k} - 1)$$

Where $\mathrm{dist}(u_i, u_j)$ denotes the Euclidean distance between u_i and u_j. Additionally, the request content among users is considered. A weight is assigned to the request content in the user group based on the number of request types and the distribution in the user group, that is

$$\beta_n = \frac{2 booleanu\left(u_i^c, u_j^c\right)}{k(k-1)} (\mathrm{i}, \mathrm{j} = 1, \cdots, \mathrm{k}, \mathrm{i} \neq \mathrm{j})$$

Taking into account the distance between users in the user group and the distribution of the request content jointly, the anonymous entropy for the nth user group is defined as the sum of the entropy in terms of distance and the difference on request content in the *n*th user group, denoted by,

$$H_n = \sum_{i=1}^{k-1} \alpha_{ni} \, log_{10} \, \alpha_{ni} + \beta_n$$

Finally, the entropy is used to measure the uncertainty of a group of users, the bigger the value of the entropy the more uncertain the group. Formally, it is defined as where the probability that the user is identified. In many cases, the entropy is used to evaluate the anonymity of anonymous regions. Here, we adopt the same evaluation criteria as well.

The proposed method works similarly to [41], after collecting the LBS requests sent by users, the module anonymously processes the location privacy, identity, request content, and other information according to the requirements of the users. The procedure is as follows:

1. Construct the kd-tree based on the region where the requesting user is located.

2. The nearest neighbour users are searched on the kd-tree, and the anonymity is processed according to the algorithm.

The selected algorithm works in this mode. Suppose that there are 2k users in a region, k−1 users are selected randomly to form a user group Ui with real users. The process is repeated m times, and m user groups are formed, where m is defined by the user according to his privacy requirements. In sparsely populated regions, considering the historical records and geographical distribution, the algorithm achieves k-anonymity by selecting dummy users with high historical query probability, relatively uniform geographical distribution, and large difference in request contents.

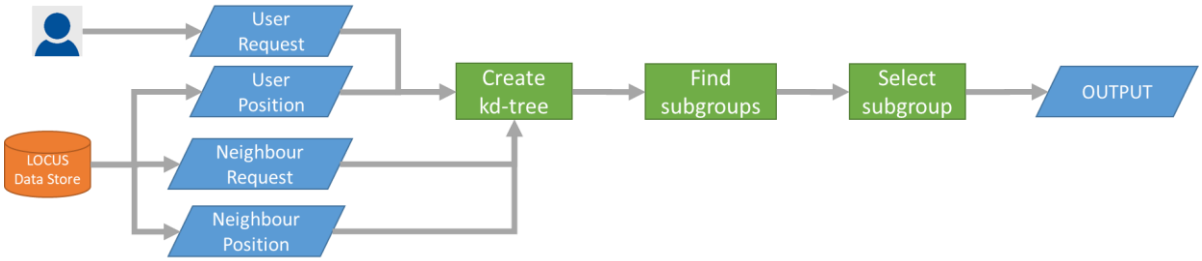

Figure 26 - Flow diagram of the selected algorithm

The flow diagram of the selected algorithm is shown in Figure 26. We use the LOCUS data store to collect users' data, we use this data together with the user request to feed the kd-tree module. After the successful construction of kd-tree, we find the nearest 2k users of real users according to the kd-tree search algorithm. The next module finds all the possible subgroups containing 2k-1 nodes. Each user group includes real users and the randomly selected k−1 users among 2k neighbour users. In the last module, according to our anonymous entropy method, the uncertainty of the user groups is evaluated. Then, the user group with the largest entropy is selected and provided the output. The same method is considered for the result aggregation function, it has been executed before to enforce the aggregate operation and apply the statistical functions.

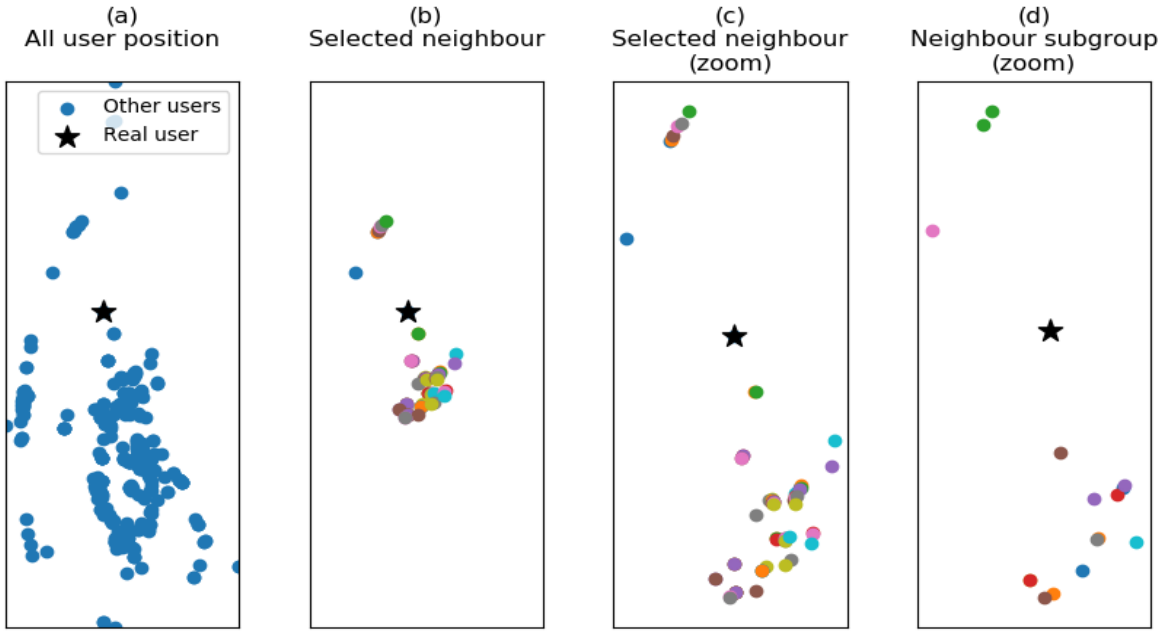

Figure 27 - Example of selected algorithm on the real dataset

Finally, Figure 27 represents an example of operation of the algorithm. We use dataset 1 and only 1000 users are selected. Subfigure (a) shows the whole area where the users are placed, where the star marker is employed to represent the real user. Subfigure (b) and (c) show the nearest 2k users of real users (users are plotted with different colours), in subfigure (c) the area is zoomed to better show the user placement. Finally, subfigure (d) shows the selected user group with the largest entropy.

5.6 Evaluation result

In this subsection, we evaluate the performance of our scheme via extensive experiments. For this experiment we use the real dataset presented before and we generate up to 1000 queries originating at random users; we consider 15 different types of request content. We use these users to generate the Minimum Bounding Rectangle (MBR) and compare the proposed algorithm with the quad-tree algorithm used in Casper [35]. For the proposed method, we also show the performance when the user content request is or is not considered. To evaluate the performance we use entropy results and the area of the anonymous region at different k-value and number of users.

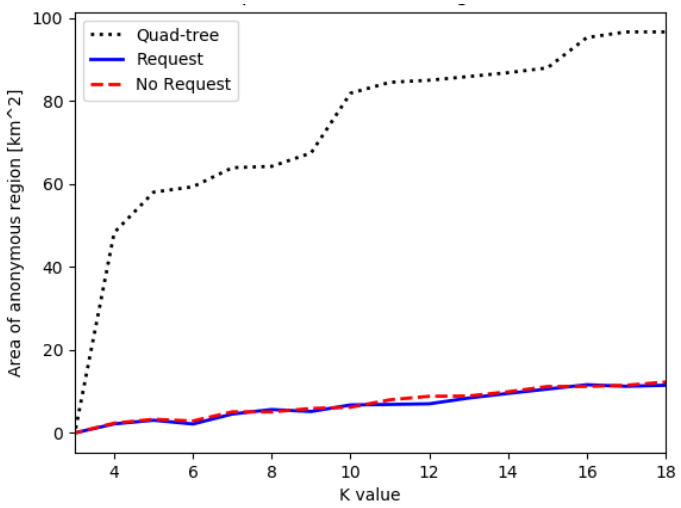

Figure 28 - Relationship between the area of anonymous region and k value.

Figure 28 shows that the area of the anonymous region formed by quad-tree algorithm, and proposed algorithm gradually increases with the rise of the k value. Assume that the number of people in the region is 1000 here. Differently from the proposed method, in quad-tree with the increase of *k*, the area of anonymous regions becomes increasingly large. The Quad-tree algorithm does not take into full account the location relationships of the neighbouring users. In particular, when it extends to a high level, each expansion leads to a larger area increase, generating redundant space.

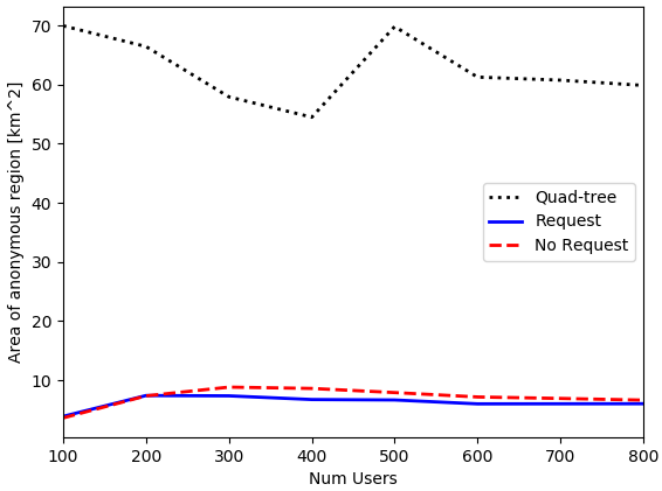

Figure 29 - Relationship between the number of users and the area of the anonymous region.

Figure 29 shows the relationship between the area of the anonymous region and the number of users under the condition of k = 15; again we consider the quad-tree algorithm and the proposed algorithm. It can be seen from the curves that the area of the anonymous region gradually decreases with the increase of user number. After the user density reaches 700, it

tends to be stable. Also in this case, in quad-tree the area of the anonymous regions is large in comparison with the proposed method.

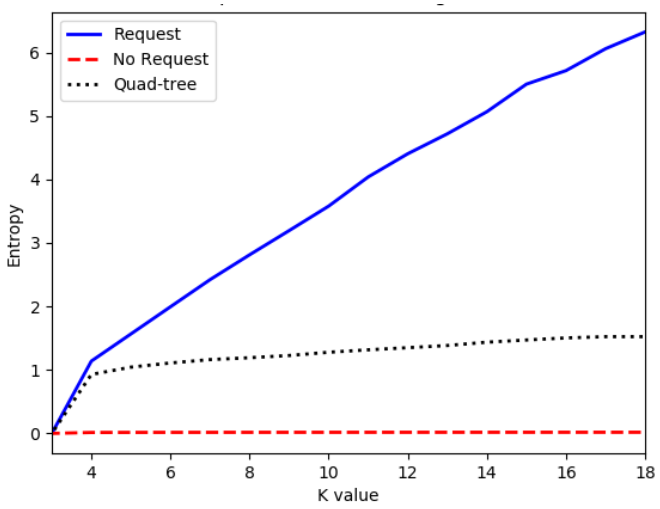

Figure 30 - Comparison of anonymity between the proposed algorithm and the quad-tree algorithm under different k values.

Figure 30 indicates the privacy level in terms of entropy of the different schemes; we can see that the anonymity of the proposed algorithm and quad-tree algorithm gradually increases with the raise of the k value. The performance of the proposed algorithm, when we consider the content of the user request, is better than that of the quad-tree algorithm.

From the analysis of the two metrics, the area of the anonymous region and the entropy, we notice that quad-tree presents a large area and low entropy, consequently the anonymous region contains a large number of redundant regions which mean that there is no user there. Differently, the proposed scheme provides a small area and high entropy, especially if we consider the content of the user request.

An attacker can exclude a number of users based on the background information, so the anonymity of the quad-tree algorithm cannot reach 1/k.

5.7 Security analysis and conclusion

For the considered model, an attacker can only collude with an LBS server provider. LBS service provider owns both the history queries and current queries which include the user's identifier, the region, and the request content. In the proposed algorithm, 2k neighbour query users are first selected, and then the anonymous entropy method is used to select k−1 query users to construct an anonymous region based on the requested content and distance.

The LBS service provider cannot speculate the real location of the query user based on the information already available. In the sparse algorithm, 2k locations with the similar query probability to the real location are first selected, and then the user group is stochastically

constructed according to the distance relationship among 2k locations. On this basis, the anonymous entropy method is utilized to select the anonymous region to ensure the uncertainty. Therefore, even if the LBS service provider hold global information, it cannot infer the real location of the user. If the attacker knows all the positions of the k-1 users in the anonymous region, based on the background information, the attacker can only randomly deduce the location of the requesting user, and the probability of successful deducing is 1/k.

In order to improve the performance of the proposed scheme, in the final version of the implemented functions, we will also consider the story of the request and the trajectory to the user to perform the evaluation of the anonymous region. Finally, the proposed method will be also robust from an attacker that has knowledge about the user story or tracks the movement of each user in the system.

In conclusion, in this section we dealt with the privacy aspects for users served by the LOCUS platform. In this context, an attacker may collude with an LBS service provider to utilize the information obtained by the LBS service provider to infer other sensitive information of legitimate users for profit. We propose a scheme that can protect the user's location privacy by the interference of other neighbours when the real user is located in densely populated regions. In sparsely populated regions, our scheme also can protect the user's location privacy by generating dummy locations.

6 Integrity in the evolving 3GPP standards

The ability to safely navigate means that users must trust their estimated position with a high degree of confidence. Positioning integrity adapted from 3GPP TR 22.872, is the trustworthiness of position estimates.

Positioning Integrity *is a measure of the trust in the accuracy of the position-related data provided by the positioning system and the ability to provide timely and valid warnings to the LCS client when the positioning system does not fulfil the condition for intended operation.*

The study item in 3GPP considers investigating on new integrity assistance data and procedures to be considered in LPP (LTE Positioning Protocol) and associated specifications, to assist in quantifying positioning integrity for the positioning system. At the time of our previous deliverable on this topic (D2.2), the integrity topic was newly kicked-off in the Rel-17 NR positioning enhancement study item (SI), and in D2.2 we already mentioned the use-cases from LOCUS point of view that benefit from positioning integrity, and the positioning integrity KPIs in which were already available from satellite navigation industry. At this point in time, the Rel-17 SI has been finalized and all the agreements are summarized in the 3GPP TR 38.857 (i.e. [43]). In the continuation of the SI, a work-item has been recently approved and started on NR Positioning Enhancements [44] to go through the outcome of the SI. In this section, we briefly go through the background behind the study in 3GPP and also bring up the positioning integrity error categories.

6.1 Brief overview of positioning integrity in 3GPP Rel-17

To address the higher accuracy, lower latency location, high integrity and reliability requirements resulting from new applications and industry verticals for 5G, a Rel-17 Study Item of “Study on NR Positioning Enhancements” has been carried out by 3GPP, which covers the enhancements and solutions necessary to support the high accuracy (horizontal and vertical), low latency, network efficiency (scalability, overhead, etc.), and device efficiency (power consumption, complexity, etc.) requirements for commercial uses cases (incl. general commercial use cases and specifically Industrial IoT (IIoT) use cases) and GNSS positioning integrity requirements. The accomplishments of the study for positioning enhancements are documented in [43].

The following KPIs for positioning integrity are defined and standardized for the study:

Target Integrity Risk (TIR): The probability that the positioning error exceeds the Alert Limit (AL) without warning the user within the required Time-to-Alert (TTA). The TIR is usually defined as a probability rate per some time unit (e.g., per hour, per second or per independent sample).

Alert Limit (AL): The maximum allowable positioning error such that the positioning system is available for the intended application. If the positioning error is beyond the AL, the positioning system should be declared unavailable for the intended application to prevent loss of positioning integrity. When the AL bounds the positioning error in the horizontal plane or on the vertical axis then it is called Horizontal Alert Limit (HAL) or Vertical Alert Limit (VAL), respectively.

Time-to-Alert (TTA): The maximum allowable elapsed time from when the positioning error exceeds the Alert Limit (AL) until the function providing positioning integrity annunciates a corresponding alert.

Integrity Availability: The integrity availability is the percentage of time that the PL is below the required AL.

The relationship between the KPIs and the Protection Level (PL), and their impacts on the positioning solution are further examined below.

The TIR is a design constraint for a positioning system and represents the probability that a positioning error exceeds the AL, but the positioning system fails to alert the user within the required period of time (i.e., TTA). In practice, the TIR is very small. For example, <10-7/hr TIR translates to one failure permitted every 10 million hours (equivalent to 1142 years approximately).

Positioning integrity system failures are known as Integrity Events and integrity events occur when the positioning system outputs Hazardous Misleading Information (HMI).

Misleading Information (MI) is an integrity event occurring when, being the system declared available, the position error exceeds the protection level but not the alert limit.

Hazardously Misleading Information (HMI) is an integrity event occurring when, being the system declared available, the position error exceeds the alert limit.

A useful representation for interpreting the relationship between the positioning integrity KPIs and PL is the so-called Stanford Diagram [45] in Figure 31. It should be noted that the Positioning Error (PE) in this diagram is the difference between the true position and the estimated position, computed by the positioning device. In practice, the true position is not known.

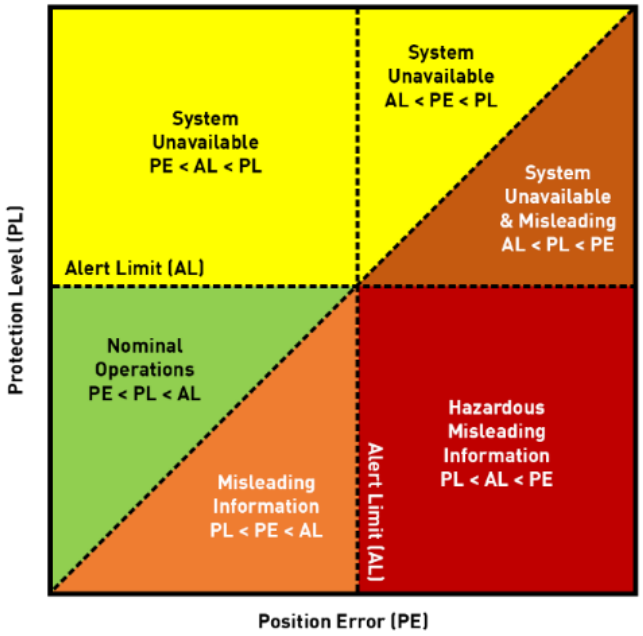

Figure 31 Stanford Diagram for integrity events, adapted from [33].

Nominal Operation is when PE < PL < AL

System unavailable is when AL < PL

Misleading Operation is when PL < PE

Hazardously Operation is when PL < AL < PE

6.2 Positioning integrity error categories

The 3GPP focus in the Rel-17 SI has been down-scoped to only cover RAT-independent GNSS positioning integrity, therefore the error categories which have been identified are all limited to this positioning method only. It is very likely that when the RAT-based positioning integrity will eventually be included in further 3GPP releases, then more error category sources would be also explored in 3GPP. Here we list the error categories already acknowledged by 3GPP in Rel-17 SI.

The positioning integrity assistance is under discussion in the Rel-17 work item. The UE or LMF are responsible for mitigating potential error sources, namely feared events, locally. Example feared events are described below

1. Feared events in the GNSS assistance data
    a. Incorrect computation of the GNSS Assistance Data
    b. External feared event impacting the GNSS Assistance Data

2. Feared events during positioning data transmission
    a. Data integrity faults, which include data corruption check, data authentication and signature

3. GNSS feared events
    a. Satellite feared events, e.g., bad signal-in-space or bad broadcast
    b. Atmospheric feared events, including Ionospheric and Tropospheric indicators
    c. Local Environment feared events, e.g., Multipath, Interference, Spoofing

4. UE feared events
    a. GNSS receiver measurement error
    b. Hardware faults
    c. Software faults

5. LMF feared events
    a. Hardware faults
    b. Software faults

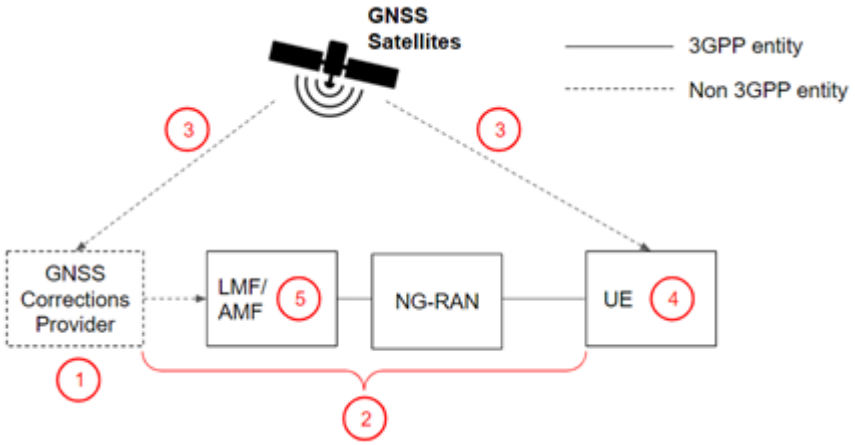

Figure 32 Illustration of simplified relationship between the positioning integrity feared event categories and the 3GPP positioning architecture [42]

The detection of feared events is necessary to support the implementation of positioning integrity. Assistance information and associated IEs can be optionally sent between the LMF and the UE to mitigate the feared events. To ensure that the system meets the integrity goals and requirements, it must be systematically validated, possibly including compliance to relevant industry functional safety specifications such as ISO-26262 for automotive. Integrity validation is considered outside the scope of the 3GPP specifications as it concerns a specific integrity system implementation [43].

The GNSS and UE feared events both reflect local and receiver-centric errors. The GNSS signal multipath is affecting the GNSS receiver measurement errors, in addition to other receiver-specific measurement errors. These errors concern environmental aspects, which means that it is not possible to process and interpolate observations from a network of reference stations alone in order to assess such errors. In addition, there is a need for crowd-sourced UE observations of the measurement errors. If UEs in a region can be selected and configured to provide observations relevant for the region, then this information can be provided to the location server, which can provide crowd-sourced information to other UEs when entering the region.

The UE could identify GNSS signals subject to multipath using a technique such as RAIM (receiver autonomous integrity monitoring) [46] or RANSAC (random sample consensus) [47] to identify GNSS signals associated to a significant positive estimation bias, which can be seen as an indication of multipath.

In order to be helpful, the UE needs to provide a positioning estimate and time stamp together with the GNSS signals determined to be subject of significant multipath. Since satellites move, the multipath indication may only be relevant for certain satellite positions along the orbit. However, it is also an indication of the environment as such – to what extent it is subject to multipath, blocking etc. In a similar manner, the UE can report about high interference levels, suspected jamming or spoofing etc.

Given crowd-sourced UE information about GNSS and local UE feared events, the location server can provide regionalized information to a UE that enters a region about feared events in terms of the local environment and UE measurement errors. The information can be very crude such as indicators/flags or more elaborate and specific with quantified assessments of the errors.

LOCUS continuously monitors this topic in 3GPP standardization and provides input and contributions to RAN2 WG from Ericsson [48]. Integrity KPI standardization would impact the signalling support between the Location Management Function (LMF) and the UEs. Currently, this support would only impact the GNSS RAT-independent positioning method and can benefit use-cases such as vehicular and public safety where an outdoor positioning is sufficient. However, there are many other use-cases such as Industrial IoT, which is also among the LOCUS use-cases and is being studied in WP3, that can definitely benefit from the integrity support for RAT-dependent positioning methods such as DL-TDOA, etc.

7 Annex 1: Derivations of NLJ Decision Schemes

In the annex, provided as a separate file, we provide further details about the derivations of the decision rules described in Section 3.2.

8 Conclusion

This document has presented the results of the activities related to the location security and privacy issues in LOCUS.

The activities focused on location security are manifold. First, we have devised a family of countermeasure algorithms against (possibly smart) noise-like jammer and spoofer attacks. Such algorithms are fed by location data provided by the infrastructure and rely on well-established design criteria as the GLRT. The preliminary performance analysis has been carried out on simulated data showing the effectiveness of the proposed strategies. Second, we have focused on the UE side and modified the previously devised decision rules in order to work on power measurements collected by the UE. Remarkably, we have assessed the performance of these decision schemes in a real-world scenario where the UE, the smart jammer, and the RBS were instrumented by software defined radios (SDRs). Finally, a threat model has been presented for location security algorithms and the position error bound in the presence of a spoofing attack has been derived. The error bound have been investigated through an example case study using RSSI measurements.

For what concerns location privacy, a model has been defined along with an overview of the related work. Moreover, an LBS privacy algorithm developed in LOCUS has been described and a security analysis has been conducted through real data provided by OTE.

The document concludes with an overview of the main positioning integrity techniques in 3GPP and a taxonomy of the main positioning integrity errors.

9 References

[1] *Study on NR positioning support,* 2019.

[2] *NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN,* 2020.

[3] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020.

[4] *Study on 5G security enhancements against false base stations,* 2020.

[5] R. Ma, J. Cao, D. Feng, H. Li, B. Niu, F. Li and L. Yin, "A Secure Authentication Scheme for Remote Diagnosis and Maintenance in Internet of Vehicles," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, 2020.

[6] B. Li, Z. Fei and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," *IEEE Internet of Things Journal,* vol. 6, pp. 2241-2263, 2019.

[7] F. Raissi, S. Yangui and F. Camps, "Autonomous Cars, 5G Mobile Networks and Smart Cities: Beyond the Hype," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 2019.

[8] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine,* vol. 54, pp. 54-61, 2016.

[9] F. M. Aziz, J. S. Shamma and G. L. Stüber, "Resilience of LTE networks against smart jamming attacks: Wideband model," in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2015.

[10] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2013.

[11] D. Rupprecht, K. Kohls, T. Holz and C. Pöpper, "Breaking LTE on Layer Two," in *IEEE Symposium on Security & Privacy (SP)*, 2019.

[12] S. F. Mjølsnes and R. F. Olimid, *Easy 4G/LTE IMSI Catchers for Non-Programmers,* 2017.

[13] R. M. Rao, S. Ha, V. Marojevic and J. H. Reed, *LTE PHY Layer Vulnerability Analysis and Testing Using Open-Source SDR Tools,* 2017.

[14] R. Borgaonkar, L. Hirschi, S. Park and A. Shaik, “New privacy threat on 3G, 4G, and upcoming 5G AKA protocols,” *Proceedings on Privacy Enhancing Technologies,* vol. 2019, p. 108–127, 2019.

[15] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi and J.-P. Seifert, “Practical attacks against privacy and availability in 4G/LTE mobile communication systems,” *arXiv preprint arXiv:1510.07563,* 2015.

[16] A. Shaik, R. Borgaonkar, S. Park and J.-P. Seifert, “New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities,” in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, New York, NY, USA, 2019.

[17] I. Palamà, F. Gringoli, G. Bianchi and N. B. Melazzi, “The Diverse and Variegated Reactions of Different Cellular Devices to IMSI Catching Attacks,” in *Proceedings of the 14th International Workshop on Wireless Network Testbeds, Experimental Evaluation & amp; Characterization*, New York, NY, USA, 2020.

[18] A. Shaik and R. Borgaonkar, “New vulnerabilities in 5G networks,” in *Black Hat USA Conference*, 2019.

[19] A. Shaik, R. Borgaonkar, S. Park and J.-P. Seifert, “On the impact of rogue base stations in 4G/LTE self organizing networks,” in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2018.

[20] A. Lilly, “IMSI catchers: hacking mobile communications,” *Network Security,* vol. 2017, p. 5–7, 2017.

[21] H. Khan, B. Dowling and K. M. Martin, “Identity confidentiality in 5G mobile telephony systems,” in *International Conference on Research in Security Standardisation*, 2018.

[22] K. P. Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012.

[23] R. J. Muirhead, “Aspects of multivariate statistical theory,” vol. 197, 2009.

[24] A. P. Dempster, N. M. Laird and D. B. Rubin, “Maximum Likelihood from Incomplete Data via the EM Algorithm,” *Journal of the Royal Statistical Society (Series B - Methodological),* vol. 39, pp. 1-38, 1977.

[25] J. A. del Peral-Rosado, O. Renaudin, C. Gentner, R. Raulefs, E. Dominguez-Tijero, A. Fernandez-Cabezas, F. Blazquez-Luengo, G. Cueto-Felgueroso, A. Chassaigne, D. Bartlett, F. Grec, L. Ries, R. Prieto-Cerdeira, J. A. Lopez-Salcedo and G. Seco-Granados, “Physical-

Layer Abstraction for Hybrid GNSS and 5G Positioning Evaluations," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019.

[26] E. Rastorgueva-Foi, M. Costa, M. Koivisto, K. Lepp_nen and M. Valkama, "User Positioning in mmW 5G Networks Using Beam-RSRP Measurements and Kalman Filtering," in *2018 21st International Conference on Information Fusion (FUSION)*, 2018.

[27] N. Nikaein, R. Knopp, F. Kaltenberger, L. Gauthier, C. Bonnet, D. Nussbaum and R. Ghaddab, "Demo: OpenAirInterface: An Open LTE Network in a PC," New York, NY, USA, 2014.

[28] M. Z. Win, Y. Shen and W. Dai, "A Theoretical Foundation of Network Localization and Navigation," *Proceedings of the IEEE,* vol. 106, no. 7, p. 1136–1165, 2018.

[29] C. Bettini, S. Mascetti, D. Freni, X. Wang, and S. Jajodia, "Privacy and Anonymity in Location Data Management," *Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques.,* no. 10.1201/b10373-13, 2010.

[30] P. Samarati and L. Sweeney., "Protecting privacy when disclosing information: K–anonymity and its enforcement through generalization and suppresion.," *In Proceedings of the IEEE Symposium on Research in Security and Privacy (SRSP),* p. 384–393, 1998.

[31] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Transactions on Knowledge and Data Engineering,* vol. 13, no. 6, p. 1010–1027, 2001.

[32] B. Niu, Q. Li, X. Zhu, G. Cao and H. Li, "Achieving k-anonymity in privacy-aware location-based services," Toronto, 2014.

[33] D. Wu, Y. Zhang and Y. Liu, "Dummy Location Selection Scheme for K-Anonymity in Location Based Services," Sydney, 2017.

[34] O. Abul, F. Bonchi and M. Nanni, "Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases," Cancun, 2008.

[35] M. F. Mokbel, C.-Y. Chow and W. G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Istanbul, 2007.

[36] P. Kalnis, G. Ghinita, K. Mouratidis and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," *IEEE Transactions on Knowledge and Data Engineering,* vol. 19, no. 12, p. 1719–1733, 2007.

[37] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Phoenix, 2008.

[38] B. Gedik and L. Liu, “Location Privacy in Mobile Systems: A Personalized Anonymization Model,” Columbus, 2005.

[39] C. Bettini, X. S. Wang and S. Jajodia, “Protecting Privacy against Location-Based Personal Identification,” in *Proceedings of the Second VDLB International Conference on Secure Data Management*, Berlin, 2005.

[40] R. Finkel and J. Bentley, “Quad Trees: A Data Structure for Retrieval on Composite Keys.,” *Acta Inf.,* vol. 4, pp. 1-9, 3 1974.

[41] L. Ni, F. Tian, Q. Ni, Y. Yan and J. Zhang, “An anonymous entropy-based location privacy protection scheme in mobile social networks,” *Eurasip Journal on Wireless Communications and Networking,* vol. 2019, 4 2019.

[42] H. Samet., “The Design and Analysis of Spatial DataStructures. ,,” *Addison–Wesley Longman Publishing Co.,Inc.,* 1990.

[43] 3GPP, “TR 38.857 Study on NR positioning enhancements,” Release 17, 2021.

[44] 3GPP, “RP-210903, Revised WID on NR Positioning Enhancements,” Release 17, 2021.

[45] E. S. Agency, “Integrity,” *Navipedia,* no. <https://gssc.esa.int/navipedia/index.php/Integrity>, 2018.

[46] S. H. a. J. Wang, “GNSS receiver autonomous integrity monitoring (RAIM) performance analysis,” *GPS Solutions,* vol. 10, pp. 155-170, 2006.

[47] A. A. S. G. S. T. G. Castaldo, “P-RANSAC: An Integrity Monitoring Approach for GNSS Signal Degraded Scenario,” *International Journal of Navigation and Observation,* 2014.

[48] Ericsson, “R2-2103917 GNSS Integrity aspects of GNSS local environment and UE feared events,” 2021.

[49] A. Gkoulalas-Divanis, P. Kalnis and V. Verykios, “Providing K–Anonymity in Location Based Services,” *SIGKDD Explorations,* vol. 12, pp. 3-10, 11 2010.