Location Security under Reference Signals' Spoofing Attacks: Threat Model and Bounds

Stefania Bartoletti*
stefania.bartoletti@ieiit.cnr.it
webmaster@marysville-ohio.com
National Research Council of Italy, IEIIT-CNR / CNIT
Bologna, Italy

Giuseppe Bianchi
Università degli Studi di Roma "Tor Vergata" / CNIT
Rome, Italy

Danilo Orlando
Università degli Studi "Niccolò Cusano"
Rome, Italy

Ivan Palamà
Università degli Studi di Roma "Tor Vergata" / CNIT
Rome, Italy

Nicola Blefari-Melazzi
Università degli Studi di Roma "Tor Vergata" / CNIT
Rome, Italy

ABSTRACT

Most localization systems rely on measurements gathered from signals emitted by stations whose position is assumed known as ground truth, namely anchors. As demonstrated by a significant bulk of experimental research, location security is threatened when an attacker becomes able to tamper either the signals emitted by the stations, or convince the user that the anchor station is in a different position than the true one. With this paper, we first propose a formal threat model which captures the above-mentioned wide class of attacks, and permits to quantitatively evaluate how tampering of one or more anchor locations undermines the user's localization accuracy. We specifically derive a Cramér Rao Bound for the localization error, and we assess a number of example scenarios. We believe that our study may provide a useful formal benchmark for the design and analysis of detection and mitigation solutions.

KEYWORDS

Location security, spoofing, tampering, localization, Cramér Rao bound

ACM Reference Format:
Stefania Bartoletti, Giuseppe Bianchi, Danilo Orlando, Ivan Palamà, and Nicola Blefari-Melazzi. 2021. Location Security under Reference Signals' Spoofing Attacks: Threat Model and Bounds. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3465481.3470098

This work was supported by the European Union's Horizon 2020 research and innovation programme under Grant no. 871249 and under Grant no. 830892.

ARES 2021, August 17–20, 2021, Vienna, Austria
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3470098

1 INTRODUCTION

Location information is enabling a plethora of new services beyond classic navigation, including smart network management and location-based analytics, which leverage the accurate estimation of users' location. However, while the social and economic value of localization information grows in mobile networks[4, 7, 10], and while the cellular networks are in the process of including localization facilities in the incoming 3GPP standardization [1, 2], a multiplicity of adversaries may find threatening value in attacking localization technologies and services so as to alter the end-user's belief of being in a given position - imagine for instance the potentially dramatic consequences of a location deception attack that diverts a driver-less car out of its path.

The networking community has broadly explored localization threats in several domains[11–13], and also with specific focus on the experimental proof-of-concept of attacks [3, 14, 17]. A striking recent example is reference [15] which demonstrates how to divert an aircraft out of its landing track by exploiting the lack of authentication of ILS (Instrument Landing System) radio communications.

In terms of nonadversarial localization, the analysis of localization accuracy of wireless networks has been widely studied in the literature. The Fisher information is used to examine the accuracy of maximum likelihood estimators of an unknown parameter vector. Specifically, Fisher information has been used extensively to derive the user's localization information in the presence of multiple impairments to signal propagation, leading to the minimum achievable localization error, namely squared position error bound (SPEB) [5, 9, 16, 18].

Nevertheless, in terms of adversarial localization, a formal threat model for the localization error is still missing. Such threat model would be pivotal for the design and comparison of countermeasures. In this paper, we investigate 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 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 localization

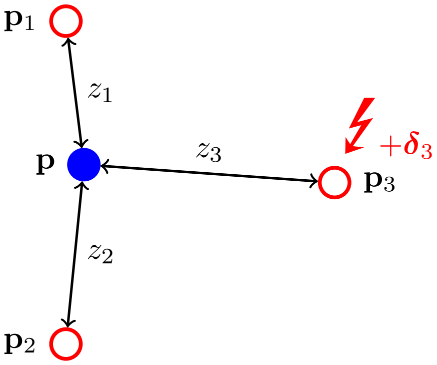

Figure 1: Example scenario with $N_\mathrm{b} = 3$ anchors and one agent in the presence of a spoofing attack against the third anchor.

on received signal strength indicator (RSSI) to exemplify its 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's localization and provide a benchmark for the design and analysis of detection and mitigation solutions. Table 1 describes the notation used for the model derivation.

2 THREAT MODEL

The scenario considered in this paper is a very classical one: 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.

2.1 Formal model

Consider a localization network as consisting of N_b anchors for inferring the location of an agent, which is at $\mathbf{p}$.[1] The ith anchor is at position $\mathbf{p}_i$, and $\mathbf{p}_\mathrm{b} = [\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_{N_\mathrm{b}}]$. The agent location is inferred based on measurements of signals communicated between each anchor and agent. In particular, the measurement vector is $\mathbf{z} = [z_1, z_2, \dots, z_{N_\mathrm{b}}]$, where z_i is measured between the ith anchor and the agent.

An example illustration is given in Fig. 1. The localization algorithm exploits $\mathbf{z}$ together with the information about the anchors' positions [6]. Each measurement depends on the true anchor and agent positions according to a measurement model, e.g.

$$z_i = z_0(\mathbf{p}, \mathbf{p}_i) + n_i \tag{1}$$

where $n_i \sim \mathcal{N}(0, \sigma_i^2)$ 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.

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 $\mathbf{p}$ is

$$f(\mathbf{z}, \mathbf{p}, \mathbf{p}_\mathrm{b}) = \prod_{i=1}^{N_\mathrm{b}} f(z_i, \mathbf{p}, \mathbf{p}_i) \tag{2}$$

where each $f(z_i, \mathbf{p}, \mathbf{p}_i)$ is obtained according to the measurement model in (1).

If the likelihood function is known, the maximum likelihood (ML) estimator is the optimal solution, as it achieves the Cramér–Rao bound (CRB) asymptotically in the high signal-to-noise ratio (SNR) regimes, as we will discuss in Sec. 3. The ML estimator is unbiased, i.e. $\mathbb{E}\{\hat{\mathbf{p}}\} = \mathbf{p}$, where $\hat{\mathbf{p}}$ is the estimate of $\mathbf{p}$. In most cases, the likelihood function is unknown in general, as the parameters of the measurement distribution can be unknown (or, at most, partially known). In such practical cases, sub-optimal estimators are considered, e.g. using the well known trilateration algorithm or the least square algorithm.

2.2 Error Model for the Spoofing Attack

In the presence of a spoofing attack, where the anchor positions are tampered, the main effect is that the measurement z_i is taken with respect to the true anchor at $\mathbf{p}_i$, and therefore follows the true measurement model $z_0(\mathbf{p}, \mathbf{p}_i) + n_i$. Nevertheless, as the information about the anchor position is tampered, i.e. the information on $\mathbf{p}_i$ is biased as $\mathbf{p}_i + \boldsymbol{\delta}_i$, where $\boldsymbol{\delta}_i$ the bias, 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. $z_0(\mathbf{p}, \mathbf{p}_i + \boldsymbol{\delta}_i) + n_i$. 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

$$\hat{\mathbf{p}}_\mathrm{sp} = \operatorname*{argmax}_{\tilde{\mathbf{p}}} f(\mathbf{z}, \tilde{\mathbf{p}}, \mathbf{p}_i + \boldsymbol{\delta}_i)\,. \tag{3}$$

Note that for $\boldsymbol{\delta}_i \neq \mathbf{0}$ for some i, the ML estimator is biased, i.e. $\mathbb{E}\{\hat{\mathbf{p}}_\mathrm{sp}\} \neq \mathbf{p}$. We define the spoofing error as $\mathbf{e}_\mathrm{sp} = \hat{\mathbf{p}}_\mathrm{sp} - \mathbf{p}$.

Let us now consider the following system of N_b equations with respect to $\check{\mathbf{p}}$

$$z_0(\check{\mathbf{p}}, \mathbf{p}_i + \boldsymbol{\delta}_i) = z_0(\mathbf{p}, \mathbf{p}_i) \quad \forall i = 1, 2, \dots, N_\mathrm{b}\,. \tag{4}$$

If there exists a solution to (4), such vector $\check{\mathbf{p}}$ would be the position of the agent in the case the true position of the ith anchor would be $\mathbf{p}_i + \boldsymbol{\delta}_i$ for each $i = 1, 2, \dots, N_\mathrm{b}$ and the measurement between the anchor and the ith anchor would have the expected value z_i. In

[1] In this paper, we consider $\mathbf{p} \in \mathbb{R}^2$.

Table 1: Notation.

Symbol	Description
$\mathbf{x}$	boldface and lowercase letter denotes a vector
$\mathbf{X}$	boldface and uppercase letter denotes a matrix
$(\cdot)^{\mathrm{T}}$	denotes the transpose of the multivariate argument
$(\cdot)^{-1}$	denotes the inverse of the matrix argument
$\mathbb{E}\{\cdot\}$	denotes the expected value of the random argument
$\|\cdot\|$	denotes the Euclidean norm
$\mathrm{tr}\{\cdot\}$	denotes the trace of the matrix argument
$\mathbf{0}$	denotes the null vector of suitable size
$\sim$	means is distributed as
$\mathcal{N}(\mu, \sigma^2)$	denotes the univariate Gaussian distribution with mean μ and variance σ^2
$\frac{\boldsymbol{\partial}\mathbf{f(x)}}{\boldsymbol{\partial}\mathbf{x}}$ with $\mathbf{f}(\mathbf{x}) = [f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_N(\mathbf{x})]^{\mathrm{T}}$	denotes $[\nabla f_1(\mathbf{x}), \nabla f_2(\mathbf{x}), \ldots, \nabla f_N(\mathbf{x})]^{\mathrm{T}}$ with $\nabla f(x)$ the gradient of $f(x)$.

such a case, i.e. in the absence of any spoofing, a ML estimator for the case with an agent at $\check{\mathbf{p}}$ and the anchors $\mathbf{p}_i + \boldsymbol{\delta}_i$ would solve the equivalent problem as in (3) as an unbiased estimator. Then, $\mathbb{E}\{\hat{\mathbf{p}}\} = \check{\mathbf{p}}$. It follows that, being this the identical problem as (3) we have

$$\mathbb{E}\{\hat{\mathbf{e}}_{\mathrm{sp}}\} = \check{\mathbf{p}} - \mathbf{p}\,. \tag{5}$$

Note that (5) is valid for any estimator that is unbiased in the absence of an attack, i.e. $\mathbb{E}\{\hat{\mathbf{p}}\,|\boldsymbol{\delta} = \mathbf{0}\} = \mathbf{p}$ and that is based on a measurement model as in (1). If $\check{\mathbf{p}}$ does not exists, i.e. the system of N_{b} equations in (4) has no solution, then the error will depend on the specific localization algorithm and the measurement model.

2.3 Example Case Study: Range-based Localization using RSSI

As an example, we here focus on the range-based localization using RSSI. In this case, each anchor transmits with power P_{T}. The signal propagates in fading channel where the fading is modeled as a lognormal random variable $n_i \sim \mathcal{N}(0, \sigma^2)$. Thus, the power received at the agent from the ith anchor is

$$z_i = 10 \log_{10} \frac{P_{\mathrm{T}}}{d_i^{\eta}} + n_i \tag{6}$$

where $d_i = \|\mathbf{p} - \mathbf{p}_i\|$ is the true distance between the ith anchor and the agent, η is the path-loss exponent, and $n_i \sim \mathcal{N}(0, \sigma^2)$ are statistically independent.

In this case, given the anchors' spoofed positions $\mathbf{p}_i + \boldsymbol{\delta}_i$ with $i = 1, 2, \ldots, N_{\mathrm{b}}$, and following (4), we have

$$\check{\mathbf{p}} : \|\check{\mathbf{p}} - \mathbf{p}_i - \boldsymbol{\delta}_i\| = \|\mathbf{p} - \mathbf{p}_i\| \quad \forall i = 1, 2, \ldots, N_{\mathrm{b}}\,. \tag{7}$$

When $N_{\mathrm{b}} = 3$, we have $\mathbf{p} = \mathbf{A}^{-1}\mathbf{c}$, where

$$\mathbf{A} = 2\begin{bmatrix}(x_2 - x_1), (y_2 - y_1)\\(x_3 - x_2), (y_3 - y_2)\end{bmatrix}$$
$$\mathbf{c} = \begin{bmatrix}r_2^2 - r_1^2 + (d_1^2 - d_2^2)\\r_3^2 - r_2^2 + (d_2^2 - d_3^2)\end{bmatrix} \tag{8}$$

and $r_i = \|\mathbf{p}_i\|$. In such a case, if there exists a solution to the system of equations in (7), such solution is $\check{\mathbf{p}} = \check{\mathbf{A}}^{-1}\check{\mathbf{c}}$, where

$$\check{\mathbf{A}} = \mathbf{A} + 2\begin{bmatrix}(\delta_{x,2} - \delta_{x,1}) & (\delta_{y,2} - \delta_{y,1})\\(\delta_{x,3} - \delta_{x,2}) & (\delta_{y,3} - \delta_{y,2})\end{bmatrix}$$
$$\check{\mathbf{c}} = \begin{bmatrix}\check{r}_2^2 - \check{r}_1^2 + (d_1^2 - d_2^2)\\\check{r}_3^2 - \check{r}_2^2 + (d_2^2 - d_3^2)\end{bmatrix} \tag{9}$$

where $\check{r}_i = \|\mathbf{p}_i + \boldsymbol{\delta}_i\|$, and $\boldsymbol{\delta}_i = [\delta_{x,i}, \delta_{y,i}]$. Note that we can also write $\check{\mathbf{p}} = \mathbf{G}\mathbf{p}$ with $\mathbf{G} = \check{\mathbf{A}}^{-1}\mathbf{Q}_{\mathrm{c}}\mathbf{A}$ and $\mathbf{Q}_{\mathrm{c}}$ being a transformation matrix such that $\check{\mathbf{c}} = \mathbf{Q}_{\mathrm{c}}\mathbf{c}$.

3 ERROR BOUND UNDER SPOOFING ATTACK

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

$$\mathbb{E}\{\|\hat{\mathbf{p}} - \mathbf{p})\|^2\} \geq \mathrm{tr}\{\mathbf{J}_{\mathbf{p}}^{-1}\} \tag{10}$$

where $\mathbf{J}_{\mathbf{p}}$ is the Fisher information matrix for the parameter vector $\mathbf{p}$ and $\mathrm{tr}\{\mathbf{J}_{\mathbf{p}}^{-1}\}$ is called the SPEB [16].

As we have discussed in Sec. 2, an estimator $\hat{\mathbf{p}}$ that is unbiased in the absence of a tampering attack, i.e., $\mathbb{E}\{\hat{\mathbf{p}}\,|\boldsymbol{\delta} = \mathbf{0}\}$, becomes biased when $\boldsymbol{\delta} \neq \mathbf{0}$ due to the incorrect measurement model. In such a case, $\mathbb{E}\{\hat{\mathbf{p}}\,|\boldsymbol{\delta} \neq \mathbf{0}\} = \mathbf{p} + \mathbf{e}_{\mathrm{sp}}$, where $\mathbf{e}_{\mathrm{sp}}$ is the bias due to the tampering attack.

The information inequality on the mean squared error of such a biased estimators should take into account the bias $\mathbf{e}_{\mathrm{sp}}$. In particular, we define

$$\boldsymbol{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}} = \frac{\partial\,\mathbb{E}\{\hat{\mathbf{p}}\,|\boldsymbol{\delta} \neq \mathbf{0}\}}{\partial\mathbf{p}} \tag{11}$$

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

$$\mathbb{E}\{\|\hat{\mathbf{p}} - \mathbf{p}\|^2|\boldsymbol{\delta} \neq \mathbf{0}\} = \mathrm{tr}\left\{\boldsymbol{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}}\mathbf{J}_{\mathbf{p}}^{-1}\boldsymbol{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}}^{\mathrm{T}}\right\}. \tag{12}$$

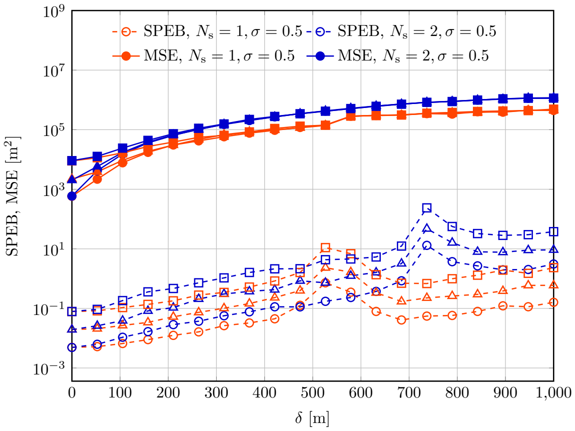

Figure 2: SPEB (dashed) and MSE (solid) varying δ, with σ = 0.5 (circles), σ = 1 (triangles), and σ = 2 (squares); single spoofed anchor (red) and two spoofed anchors (blue).

3.1 Example Case Study: range-based Localization using RSSI

The (12) is general for any biased position estimator. For range-based localization with RSSI, $\mathbf{J_p}$ is well known from the literature [8] and given by

$$\mathbf{J_p} = \left(\frac{10\eta}{\ln(10)\,\sigma}\right)^2 \sum_{i=1}^{N_b} \frac{(\mathbf{p}_i - \mathbf{p})^{\mathrm{T}}(\mathbf{p}_i - \mathbf{p})}{\|\mathbf{p}_i - \mathbf{p}\|^4}\,. \tag{13}$$

From (9), it follows that $\mathbf{\Psi}_{\hat{\mathbf{p}},\boldsymbol{\delta}} = \check{\mathbf{A}}^{-1}\mathbf{Q}_c\mathbf{A}$, where $\mathbf{Q}_c$ is a transformation matrix such that $\check{\mathbf{c}} = \mathbf{Q}_c\mathbf{c}$.

4 NUMERICAL RESULTS

In this section, we evaluate the effects of tampering on location estimation 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 following the measurement model in (6) with σ varying from 0.1 to 10, and $\eta = 2$. The spoofing is simulated considering a constant value $\boldsymbol{\delta}_i = [\delta, \delta]$ equal 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.

Fig. 2 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. As a matter of fact, the value of the bias is the leading parameter and therefore even a single spoofed anchor can impact dramatically the localization performance.

Fig. 3 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. This fact corroborates what observed in Fig. 2 and shows that the measurement noise has a little impact in the presence of spoofing attacks.

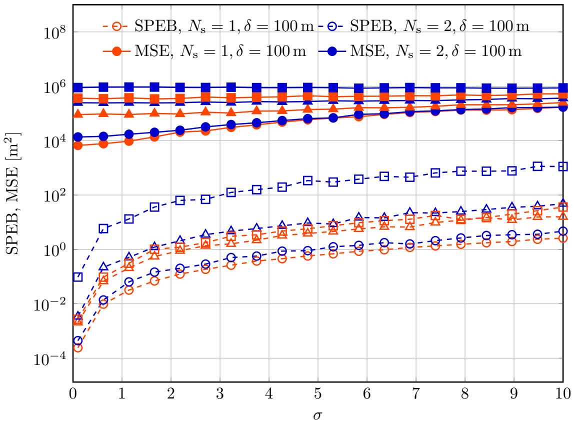

Figure 3: SPEB (dashed) and MSE (solid) varying σ with δ = 100 m (circles), δ = 400 m (triangles), and δ = 800 m (squares); a single spoofed anchor (red) and two spoofed anchors (blue).

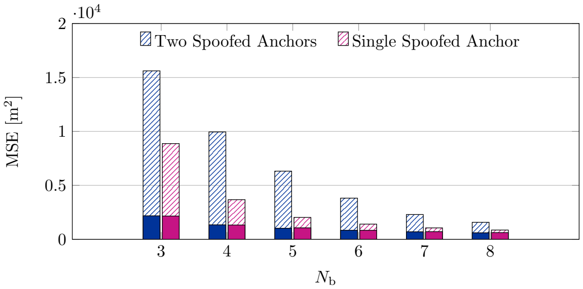

Figure 4: MSE for different numbers of anchors in the case of two spoofed anchors (blue) and a single spoofed anchor (magenta), with spoofing (dashed) and without spoofing (full).

Fig. 4 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. These results provides a quantitative indications of the number of non-spoofed anchors required to compensate the bias introduced by the spoofed anchors.

5 CONCLUSION

The main contribution of this paper is the proposal of a formal reference model designed to abstract a variety of location spoofing attacks. We present a mathematical model for describing spoofing assaults. The relevant Cramér-Rao bound is then derived in the presence of tampering attacks and compared to the case in which the assault is not present. While the model is technology agnostic, we demonstrate its derivation using RSSI-based localization. The effect of system parameters on the localization error is demonstrated numerically. Owing to its generality, our model may become a convenient formal benchmark for location security assessment, an area which appears to attract a growing interest, also considering the ongoing native integration of positioning technologies in the evolving 5G network. Future works will focus on the development of techniques for the detection and mitigation of the location spoofing attacks.

REFERENCES

[1] 3GPP. 2018. *Study on positioning use cases.* Technical Report (TR) 22.872. 3rd Generation Partnership Project (3GPP). Version 16.1.0.

[2] 3GPP. 2019. *Study on NR positioning support.* Technical Report (TR) 38.855. 3rd Generation Partnership Project (3GPP). Version 16.0.0.

[3] Fadel Adib and Dina Katabi. 2013. See through Walls with WiFi! *SIGCOMM Comput. Commun. Rev.* 43, 4 (Aug. 2013), 75–86. https://doi.org/10.1145/2534169.2486039

[4] P. Asuquo, H. Cruickshank, J. Morley, C. P. A. Ogah, A. Lei, W. Hathal, S. Bao, and Z. Sun. 2018. Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures. *IEEE Internet of Things Journal* 5, 6 (2018), 4778–4802. https://doi.org/10.1109/JIOT.2018.2820039

[5] Sandro Bellini and Guido Tartara. 1974. Bounds on Error in Signal Parameter Estimation. 22, 3 (March 1974), 340–342.

[6] Andrea Conti, Santiago Mazuelas, Stefania Bartoletti, William C. Lindsey, and Moe Z. Win. 2019. Soft Information for Localization-of-Things. *Proc. IEEE* 107, 11 (Nov. 2019), 2240–2264. https://doi.org/10.1109/JPROC.2019.2905854

[7] Vishwa Gaul. 2020. Location-based Services Market by Component, Technology, Application and Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2020-2027.

[8] Sinan Gezici, Zhi Tian, Georgios B. Giannakis, Hisashi Kobayashi, Andreas F. Molisch, H. Vincent Poor, and Zafer Sahinoglu. 2005. Localization via Ultra-wideband Radios: A Look at Positioning Aspects for Future Sensor Networks. 22, 4 (July 2005), 70–84.

[9] F. Gustafsson and F. Gunnarsson. 2005. Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements. 22, 4 (July 2005), 41–53.

[10] Haosheng Huang and Georg Gartner. 2018. Current Trends and Challenges in Location-Based Services. *ISPRS International Journal of Geo-Information* 7, 6 (2018). https://doi.org/10.3390/ijgi7060199

[11] Elena Simona Lohan, Anette Alén-Savikko, Liang Chen, Kimmo Järvinen, Helena Leppäkoski, Heidi Kuusniemi, and Päivi Korpisaari. 2018. 5G positioning: security and privacy aspects. *A Comprehensive Guide to 5G Security* (2018), 281–320.

[12] Qian Luo, Yurui Cao, Jiajia Liu, and Abderrahim Benslimane. 2019. Localization and navigation in autonomous driving: Threats and countermeasures. *IEEE Wireless Communications* 26, 4 (2019), 38–45.

[13] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi Sensing with Channel State Information: A Survey. *ACM Comput. Surv.* 52, 3, Article 46 (June 2019), 36 pages. https://doi.org/10.1145/3310194

[14] S. Roth, S. Tomasin, M. Maso, and A. Sezgin. 2021. Localization Attack by Precoder Feedback Overhearing in 5G Networks and Countermeasures. *IEEE Transactions on Wireless Communications* (2021), 1–1. https://doi.org/10.1109/TWC.2021.3055851

[15] Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. 2019. Wireless Attacks on Aircraft Instrument Landing Systems. In *28th USENIX Security Symposium.*

[16] Moe Z. Win, Yuan Shen, and Wenhan Dai. 2018. A Theoretical Foundation of Network Localization and Navigation. *Proc. IEEE* 106, 7 (July 2018), 1136–1165. https://doi.org/10.1109/JPROC.2018.2844553 special issue on *Foundations and Trends in Localization Technologies.*

[17] Kexiong Curtis Zeng, Yuanchao Shu, Shinan Liu, Yanzhi Dou, and Yaling Yang. 2017. A practical GPS location spoofing attack in road navigation scenario. In *Proc. 18th Int. Workshop on Mobile Computing Systems and Applications.*

[18] J. Ziv and M. Zakai. 1969. Some Lower Bounds on Signal Parameter Estimation. 15, 3 (May 1969), 386–391.