A Network-Based Positioning Method to Locate False Base Stations

LEYLI KARAÇAY1, ZEKI BILGIN2, AYŞE BILGE GÜNJDÜZ1, PINAR ÇOMAK1, EMRAH TOMUR1, ELIF USTUNDAG SOYKAN1, UTKU GÜLEN1, AND FERHAT KARAKOÇ1

1Ericsson Research, 34367 İstanbul, Turkey
2Arçelik Research, 34950 İstanbul, Turkey

Corresponding author: Leyli Karaçay (leyli.karacay@ericsson.com)

This work was funded by the Scientific and Technological Research Council of Turkey (TUBITAK), through 1515 Frontier RD Laboratories Support Program under project 5169902.

ABSTRACT In recent years False Base Stations (FBSs) have received increased attention. A False Base Station can perform active or passive attacks against mobile devices or user equipment (UE) to steal private information, such as International Mobile Subscriber Identifier (IMSI), to trace users locations, or to prevent users from getting service from operators. Most of the existing solutions related to FBS have focused on the detection aspects of the false station rather than locating its position. However, once an FBS is detected in a network, discovering its exact location precisely and remotely becomes highly crucial to initiate preventive actions. In this work, we propose a network-based localization method for estimating the exact geographical position of an FBS whose existence is already detected in a cellular network. Our method relies on a comparative pairwise analysis of the Reference Signals Received Power (RSRP) values reported as a standard procedure by the UEs in the vicinity of FBS through their measurement reports. Specifically, for each pair of related measurement reports, we identify a half-plane indicating the probable location of the FBS and then predict the exact location based on the intersection of all obtained half-planes. We have implemented and experimentally evaluated our proposed method in the Network Simulator 3 (ns-3) and showed that it accurately estimates FBS location with meter-level precision under different scenarios in a cellular network.

INDEX TERMS False base station, localization, measurement reports, trilateration, cellular network security.

I. INTRODUCTION Mobile networks are regarded as critical infrastructure [1]. Maintaining trustworthiness of mobile networks is crucial as their importance and role in daily life increase. A well-known security threat in this domain is False Base Station (FBS) which exploits the radio interface between mobile phones and base stations. FBS, which is also known as Rogue Base Station (RBS), International Mobile Subscriber Identifier (IMSI) Catcher, or Stingray, can launch active or passive attacks against user equipment (UE).

The attack capability of FBS varies depending on the security features of the mobile network generation. One of their initial attacks is to acquire IMSIs of subscribers; however, they can launch other types of attacks depending on the capabilities of FBS [2], [3]. For example, FBS transmits synchronization signals with sufficient power to attract the UE so that UE attempts to connect to the FBS. Although the connection fails as the authentication is required, this attempt can lead to the leakage of private information in 4G networks. More specifically, at the initial state of a mobile communication, multiple synchronization signals (SSs) from nearby base stations (BSs) are received by UE during the cell selection stage. Since the UE is synchronized with the strongest SS, an FBS might confuse the UE by transmitting an SS with strong power. This can result in serious vulnerabilities for subscribers such as private information leakage, eavesdropping, denial of service [4]–[6].

Since FBS may pose severe threats, many previous works in the literature investigate the FBS issues by focusing mainly on how to detect them in mobile networks [4], [7]–[12]. Alongside the detection, finding the exact geographical location of the detected FBS is also a significant matter when it comes to taking technical or legal actions. Although several
works exist in the literature regarding how to make positioning in mobile networks, none of them deal with locating the FBS specifically, [13], [14]. To the best of our knowledge, this is the first study focusing on localization of FBS, unlike many other detection studies.

Localization of network devices and nodes, in general, can be done using different information and parameters such as timing advance (TA) which corresponds to the length of time a signal takes to reach the base station from a mobile phone, round trip time (RTT) which is the amount of time it takes for a signal to be sent plus the amount of time it takes for acknowledgement of that signal having been received, reference signal received power (RSRP), and angle of arrival (AoA) [13]. For instance, multilateration is a common method for locating the node by the distance measurements with the other nodes using the aforementioned parameters [15]. In mobile networks, the received signal power of the base stations is known by the UE. With the path loss calculation of the received signal power of BS, the distance between a UE and a BS can be estimated. Moreover, when three UE locations and the transmit signal power of a BS are known, the location of the BS can be estimated via trilateration, which is a special case of multilateration. However, for the FBS localization case, transmit signal power of FBS is not known, and trilateration is not applicable. This challenge prevents predicting the distance between the FBS and the UE that sends the measurement reports. This problem also appears in any case when transmitting signal power of the network node to be localized is unknown.

We propose a network-based method for positioning transmitting nodes in a cellular network without requiring the information of transmitting power of the targeted node. Our proposed method relies on a differential analysis of received signal strengths. Among many potential use cases, we particularly demonstrated how this method can be used to localize an FBS in a mobile network. The proposed method makes use of the UEs typical measurement reports (MRs) indicating existence of the FBS. Using other information for localization such as TA, RTT or AoA requires identifying UEs with corresponding measurements. Since typical MRs are collected anonymously, UEs cannot be identified from the reports. Therefore we do not use other information which needs to be associated with UEs, rather we benefit from MRs and related RSRPs. We implemented and experimentally evaluated our method in the packet-level discrete-event network simulator ns-3, and showed that it accurately estimates the location of the FBS.

The main contributions of this study are listed below:

- We propose a novel localization method for FBS, which is not addressed before.
- We implemented and experimentally evaluated our method in the ns-3 mobile network simulator under varying conditions including the presence of blockages in the environment and errors in UE locations.
- We show that our method can estimate the location of an FBS, by narrowing down the potential location of a detected FBS from an area with a radius of several kms to a distance of a few meters.

The rest of the document is organized as follows: Firstly, related works on the area and a short background are given in section II and III, respectively. In section IV, the proposed FBS localization method is described. Implementation details and experiments are elaborated in section V. Finally study is concluded in section VI.

## II. RELATED WORKS

As discussed in the previous section, it is highly critical to locate a malicious network node like FBS, with the aim of taking preventive actions against possible threats, providing network security, and preserving privacy of subscribers. So far, most of the works either focus on detecting an FBS or localization of a legitimate network device/node and the rogue access points (RAP) in Wi-Fi. There are some other studies on FBS, but concentrating on detection rather than localization. Such previous studies have made discovering the location of FBS precisely and remotely highly crucial to initiate preventive actions. Here we provide a comprehensive review, and summarized in the Table 1 about both FBS detection and FBS localization in detail along with their limitations.

IMSI catchers are radio devices that pose as fake cellular base stations and used for intercepting mobile phone traffic and tracking location data of mobile phone users. Snoopsnitch and Android IMSI Catcher are similar Android applications to identify IMSI catchers by capturing and analyzing radio signal [24]. Abodunrin et al. proposed an approach to detect FBS using the information collected from Snoopsnitch and Android IMSI Catcher applications [16]. Authors particularly stated that the proposed approach is considered applicable for 2G and 3G only, yet might be robust deficient since the experiments mentioned above did not run on a real-world network. Another device-based detection approach using cell fingerprint according to the cell identifiers and locations has been proposed in [17]. It was stated that no experiments were performed, so the proposal was only theoretical.

Dabrowski et al. proposed two-headed approaches to detect FBS [4]. The first approach relies on a dedicated stationary device that scanned the positioned area in a passive mode. The other one is an Android UE application that controls baseband information and signals collected from a built-in Global Positioning System (GPS) receiver with no root privileges. Another similar approach is SeaGlass, which was proposed by Ney et al. [8]. The proposed approach is based on the processing of data collected from the sensors installed by the volunteers on their vehicles. Thus, detected FBSs could be regarded to be at a city-wide scale. In [18], researchers focused on a single 3GPP Radio Access Technology and taking into account the measurement reports sent to UEs from the 2G network. The proposed approach scrutinized the measurement report in terms of the Base Station Identity Code (BSIC) and the Absolute
Radio Frequency Channel Number (ARFCN) to identify FBS cells.

Timing Advance (TA) measurement, which is the RTT (Round Trip Time) from mobile phone to BS, is one of the main approaches for finding the locations of legitimate BSs [13]. In [14], Raitoharju et al. estimate a position of legitimate base station using TA measurement in Gaussian Mixture Filter and Point Mass Filter approaches. They collect the actual positions using a UE whose location is assumed known and pinned to the map. Then experiments are done by comparing the actual position from the estimated one. The mobile phone position is assumed to be known since otherwise, measuring TA is not possible when the radio link is in an idle state. Roth et al. propose a different approach to locate a base station in [20]. They proposed an approach to find the shorter distance between UE and legitimate BS compare to prior proposed distance detection. Therefore, they performed a location privacy attack against the UE to illustrate how the TA can be modeled as an obfuscation mechanism. The attacking approach consists of the augmentation of TA measurement with the proposed calculation, named Cellular Synchronization Assisted Refinement (CeSaR) [25]. According to their experimental results, the proposed approach improved the accuracy of distances between the UE and legitimate BS was determined between 95 meters and 157 meters. In contrast, the only TA approach accuracy in distance prediction was between 240 meters and 290 meters. This study differs from our study because it finds the distance, not the location. Since the distance can be thought of as the radius of a circle for an exact location and it refers to any point around that circle. All these studies are motivated to find the position of legitimate BS. The studies related to localizing legitimate BSs mostly attract the attention of researchers with the motivation of using it in future studies to find the position of UEs. However, from the perspective of a telecom operator, the positions of stationary legitimate BSs have already known, and therefore localizing legitimate BSs may not be considered as an issue to be resolved. Our study differs from the studies in this group in that we estimate the location of an FBS using only the standard measurement reports collected from UEs.

Finding the location of the RAP is another popular area of the existing studies. Wang et al. proposed an approach to locate a RAP by exploiting Channel State Information (CSI), which is referred to as known channel properties of a communication link [21]. The main motivation for selecting the CSI is that they are readily available from commercial Wi-Fi devices. In the study [22], the authors proposed an approach to locate the RAP using the Particle Swarm Optimization algorithm. In the approach, at least the location of one legitimate AP is assumed as known. A set of Received Signal Strengths (RSS) information belongs to a known location which has both legitimate AP and the Rogue AP is collected. The collected RSS information is used in the Particle Swarm Optimization Algorithm to estimate the distance of the Rogue AP. The min distance to locate a RAP is obtained around 2 m. Another study to find the location of RAP is conducted by Zhuang et al. [23]. A Trusted Portable Navigator (T-PN) based, autonomous crowd-sourcing model, is proposed to locate the RAP. According to the proposed approach, RSS measurements and T-PN based position information pairs are

### TABLE 1. Comparison table for papers in the related works section.

| The Study          | Data Information                                                                 | Technology | Real World Experiment | Objective                                | Year   |
|--------------------|----------------------------------------------------------------------------------|------------|-----------------------|------------------------------------------|--------|
| Abodunrin et al. [16] | collected radio signals via Snopsnitch                                           | 2G/3G      | No                    | FBS Detection                           | 2015   |
| Alrashede et al. [17] | cell fingerprint according to the cell identifiers and locations                | 4G         | No                    | FBS Detection                           | 2019   |
| Dabrowski et al. [4]  | baseband information and signals collected from a built-in Global Positioning System (GPS) receiver | 2G/3G      | Yes                   | FBS Detection                           | 2014   |
| Ney et al. [8]       | collected from the sensors installed by the volunteers on their vehicles         | 2G         | Yes                   | FBS Detection                           | 2017   |
| Steig et al. [18]    | measurement reports from UE to 2G network                                         | 2G         | No                    | FBS Detection                           | 2016   |
| Nakarmi et al. [19]  | reported cell identifiers in collected measurement reports are compared with the underlying network topology | 2G/3G/4G/5G | Yes                   | FBS Detection                           | 2021   |
| Raitoharju et al. [14] | TA measurements                                                                    | 4G         | Yes                   | Legitimate BS localization              | 2018   |
| Roth et al. [20]     | TA measurements                                                                   | 4G         | No                    | Finding the distance between UE and legitimate BS as a privacy attack | 2017   |
| Wang et al. [21]     | CSI obtained from commercial Wi-Fi device                                         | WiFi       | No                    | Rogue Access Point Localization         | 2016   |
| Awad et al. [22]     | RSS informations belong to both legitimate and rogue AP                           | WiFi       | No                    | Rogue Access Point Localization         | 2017   |
| Zhuang et al. [23]   | RSS measurements and T-PN based position information pairs                        | WiFi       | No                    | Rogue Access Point Localization         | 2014   |
collected by a smartphone in a daily routine. These pairs are used as inputs to the non-linear weighted Least Square method to estimate RAP location. Researchers have shown that RAP location could be estimated efficiently as an indoor solution using T-PN and RSS measurement together. RAP and FBS localization problems are similar in the sense that they both aim to detect unauthorized transmitting nodes in a network. On the other hand, they also have major differences regarding underlying communication technology, industry standards, and threats which leads to develop solutions particular to each problem.

III. BACKGROUND

In a cellular network, UEs can be configured to send measurement reports to the network node they have connected (e.g., eNB in 4G). Typically, these measurement reports contain information about the base stations in the surrounding area of the reporting UEs. This information may comprise physical cell identifiers, carrier frequency, and/or Reference Signals Received Power (RSRP) and Reference Signal Received Quality (RSRQ). The content and reporting frequency of these measurement reports are standardized by 3GPP and can be configured by the network node. In case of an FBS presence, some of the reported measurements by surrounding UEs might contain information about the FBS, such as its advertised cell identifier and measured RSRP/RSRQ values.

In [19], an FBS detection method is proposed based on analysis of UEs measurement reports such that the cell identifiers in the collected measurement reports are extracted and then compared with the legitimate cell identifiers of the underlying network topology to check if there are any inconsistencies among neighborhood relations, which is treated as a potential sign of FBS existence. According to this method, when an FBS is detected, there are supposed to be some UEs whose measurement reports contain information (e.g., RSRP) about the detected FBS. The proposed FBS localization method steps in after this point and deals with only those measurement reports containing information about FBS.

IV. FBS LOCALIZATION

The objective of our localization method is to estimate the geographical position of an FBS, whose presence in a region is already detected by a feasible method such as [19]. Notice that although we explain our method from the context of 4G, it can also be applied in other generations of mobile networks.

Our method relies on pairwise analysis of the measurement reports which contain information about the FBS. Figure 1 shows the main stages of our method. The proposed method steps in after the detection of the existence of an FBS. In the first stage, the MRs which contain information about the FBS are acquired from the network, which may already have obtained from the FBS detection phase. Notice that these MRs comprise information about both the FBS and legitimate evolved Node Bs (eNBs) in the proximity of the reporting UEs, but do not provide any information about the UE location according to existing mobile communication standards.

Since the UEs locations at reporting time are used in our localization method, in the second stage, we estimate them via trilateration based on the RSRP values of the legitimate eNBs reported in the MRs with the assumption that locations of the eNBs are known. In the third stage, we predict the location of the FBS through pairwise analysis of the RSRP values related to the FBS in the selected MRs along with estimated UE locations.

A. STEP-1: GETTING MEASUREMENT REPORTS

In a mobile cellular system, the network nodes such as gNB in 5G and eNB in LTE collect measurement reports from the UEs connected to them mostly in an event-triggered manner as a standard procedure defined by 3GPP. However, in this step, the measurement reports we are interested in are the ones that contain information about the detected FBS. Identification of these measurement reports is described within the scope of FBS detection in [19]. In that paper, the cell identifiers reported in the collected measurement reports are compared with the underlying network topology to check for any inconsistencies. An inconsistent cell identifier is considered a possible sign of the presence of FBS. Adopting the same approach, we are interested in those measurement reports that contain information about the detected FBS.

B. STEP-2: ESTIMATION OF THE UE LOCATIONS

Our FBS localization method requires to know locations of the UEs at the time of sending measurement reports. This can be achieved by performing trilateration technique based on the information embedded in the MRs as follows:

1) TRILATERATION

A measurement report already contains RSRP values of the serving (connected) cell and nearby cells around the UE. Therefore, assuming that the locations and transmitting power of legitimate base stations are known, which is a valid assumption at least for a network operator, location of a UE at the reporting time can be estimated by trilateration using an appropriate radio propagation model based on the RSRP values embedded in the measurement report. As a mere example, Equation 1 may be used according to the Friis
propagation loss model [26]–[28]:

\[ P_r = \frac{P_t G_r G_t \lambda^2}{(4\pi d)^n L} \]  

(1)

where \( P_r \) and \( P_t \) are the received and transmitted signal power respectively, \( G_r \) and \( G_t \) denote the gains of receiver and transmitter antennas respectively when compared to an isotropic radiator with unit gain, \( \lambda \) denotes the wavelength, \( d \) denotes the distance, \( L \) represents the system loss, and the parameter \( n \) is the path-loss exponent that varies between 1.6 to 6 depending on the environment (e.g. \( n = 2 \) for free-space propagation, and \( n = 2.7 \) to 3.5 for urban area cellular radio [28]).

From this equation, the distance \( d \) between the transmitting device and the receiving device can be calculated when all other parameters are known. However, due to lack of direction or angle information, the distance between a single pair of devices is generally not enough by itself to localize the receiving device. Given that wireless signals travel omnidirectionally, the estimated distance may only be indicative of an area in the form of a ring strip in which the receiving device is likely to be located, wherein the transmitting device is taken as the center of such area. Thickness of the strip depends on uncertainty in measurements and propagation model. For localization purposes, trilateration technique relies on the measurements of several different transmitting nodes (at least three), by which multiple circular strip areas can be obtained, each of which indicates the likely location of the targeted device. The intersection of these circular areas then yields the most probable location of the targeted device. Such situation is exemplarily illustrated in Figure 2, where the targeted device is a UE and the transmitting nodes are radio network nodes of a cellular network, such as eNB and gNBs of a 4G and 5G network respectively, for example.

2) RSRP VALUES

RSRP is the average power of Resource Elements (RE) that carry cell specific Reference Signals (RS) over the entire bandwidth, so RSRP is only measured in the symbols carrying RS. Although RSRP is actually measured in dBm (decibel milliwatts), UEs report not the original measured quantity but integer values mapped with the measured quantity according to 3GPP TS 36.133 for LTE and TS 38.133 for NR (new RAR), which defines the reporting range of RSRP from \(-156 \) dBm to \(-44 \) dBm with 1 dB resolution. The mapping of measured RSRP values is as shown in Table 2 [29]. Depending on the implementation, all the measured quantity values below \(-140 \) dBm can be either mapped to 00 without taking 1 dB resolution into consideration, or mapped to corresponding negative integer values given in Table 2 with 1 dB resolution. Thus, we obtain this integer values not the original measured quantity from UEs measurement reports, which introduces uncertainty into estimation of UE locations due to 1 dB resolution in the mapping. For example, the reported RSRP value of 95 may correspond to any measured quantity value between \(-46 \) dBm and \(-45 \) dBm according to the Table 2. Additionally, RSRP measurements can be greatly affected by some factors such as fading and multipath propagation which mainly occurs due to scattering and reflection of radio signals from obstacles [30]–[33]. For these reasons, it is inevitable to see a deviation in RSRP measurements even for the same distances. As pointed out earlier, due to such factors causing uncertainty, it is likely to have some error in the MR-based estimation of UE locations as illustrated in Figure 2, where the strip thickness represents uncertainty.

Although we describe trilateration here as an appropriate way to estimate location of UEs using the reported received signal strengths, any other possible method for UE localization could also work for our FBS localization method.

### TABLE 2. RSRP measurement report mapping [29].

| Reported value | Measured quantity value (dBm) |
|----------------|-------------------------------|
| -17            | RSRP < -156                   |
| -16            | -156 ≤ RSRP < -155           |
| ...            | ...                           |
| -03            | -143 < RSRP < -142           |
| -02            | -142 ≤ RSRP < -141           |
| -01            | -141 < RSRP < -140           |
| 00             | RSRP < -140                   |
| 01             | -140 ≤ RSRP < -139           |
| 02             | -139 ≤ RSRP < -138           |
| ...            | ...                           |
| 95             | -46 ≤ RSRP < -45             |
| 96             | -45 ≤ RSRP < -44             |
| 97             | -44 ≤ RSRP                   |

C. LOCALIZING FBS

1) ANALYSIS OF A SINGLE PAIR OF MEASUREMENT REPORTS

To explain the main idea of our localization method in a simple scenario, consider a case with two measurement reports (MR1 and MR2) containing RSRP values for the FBS as illustrated in Figure 3a. We first seek to answer the question "What one can infer about the exact location of the FBS from such a single pair of measurement reports?".

Notice that these measurement reports may be sent by the same UE at different reporting times or may belong to different UEs. Either case is suitable for our method. In fact, it is not possible to distinguish the reporting UE because...
locations at the time of reporting, which are obtained as line (dashed black) connecting the locations where MR1 and MR2 were sent. This is because every point in the half-plane II is more closer to the reporting location of MR2 with respect to the reporting location of MR1.

2) ANALYSIS OF MULTIPLE PAIR OF MEASUREMENT REPORTS

In the previous part, we analysed what can be deduced about location of a FBS from a single pair of measurement reports containing RSRP values of the FBS, and showed that potential location of the FBS can be identified as a half-plane in this case. In reality, many such measurement reports do usually exist, and each 2-combinations of them can be used for FBS localization as explained in the previous part. For example, if we have \( n \) measurement reports, we can perform \( \binom{n}{2} \) number of pairwise comparisons of the measurement reports, each of which yields a half-plane indicating the potential area of the FBS. After deducing many such half-planes, we overlap all of them and take the most intersected area as the most probably location of the FBS.

Figure 4 illustrates this for a scenario of four measurement reports. As seen in Figure 4(a)-(f), there appear six half-planes in total for six pairwise comparisons of the measurement reports, and when they are overlapped as in Figure 4g, several intersections occur. The area overlapped most indicates the most probably location of the FBS, and the other intersected areas indicates relatively less probably areas of the FBS depending on the degree of overlap. In Figure 4g, the most overlapped area is circumscribed with red line, and the geometric center of this most overlapped area can be considered as the estimated exact location of the FBS.

D. FORMAL MODEL

Let \( R = \{ r_1, r_2, \ldots, r_n \} \) be the set of measurement reports containing information about the detected FBS, one of which is RSRP value. Since we make a pairwise comparison of the RSRP values associated with the FBS in different measurement reports, there can be at most \( \binom{n}{2} \)-many pairwise comparisons for the set \( R \) of \( n \) elements.

Consider \((r_i, r_j)\), one of the pairs of measurement reports. The location where a UE sends a measurement report can be estimated by trilateration, as described earlier in Section IV-B. Suppose that \( l : r_j \rightarrow (x_j, y_j) \) is a function that estimates the location of UE in two-dimensional space when explained in Section IV-B. Then, draw an infinite line (i.e. red line) crossing the middle point of first line segment perpendicularly, which splits whole plane into two half-planes. Now, for this example, the likelihood that the FBS is located in half-plane II is greater than the likelihood of having the FBS in half-plane I. This is because every point in the half-plane II is more closer to the reporting location of MR2 with respect to the reporting location of MR1.
it sends the measurement report $r_i$. For the sake of clarity, we continue to derive our mathematical model in the context of Figure 3b as follows.

Let us denote the reporting locations of $UE_i$ and $UE_j$ by $(x_i, y_i)$ and $(x_j, y_j)$, respectively. Then considering a line $d_{ij}$ (dashed black line in the Figure 3b), which connects these two locations, we can define the line $d_{ij}^\perp$ (red line) which is perpendicular to $d_{ij}$ and passing through the middle point $(x_{ij}, y_{ij})$ of $d_{ij}$, where $x_{ij} = (x_i + x_j)/2$ and $y_{ij} = (y_i + y_j)/2$. Thus the slope of $d_{ij}^\perp$ can be found by

$$m_{d_{ij}^\perp} = -\frac{x_j - x_i}{y_j - y_i}. \tag{2}$$

Since the slope and one point on it are known, we can write the equation of the line $d_{ij}^\perp$ as given in Equation 3

$$y - y_{ij} = m_{d_{ij}^\perp} \cdot (x - x_{ij}) \tag{3}$$

Then, for the pair of measurement reports $(r_i, r_j)$, depending on the RSRP values associated with the FBS in $r_i$ and $r_j$, the area where the FBS is likely to be located can be in one of the two half-spaces ($HS$), which is obtained by separating the whole space by the line $d_{ij}^\perp$. The $HS_{ij}$, which corresponds to $r_i$ and $r_j$, can be found with the following inequalities:

$$\begin{align*}
&y > m_{d_{ij}^\perp} \cdot (x - x_{ij}) + y_{ij} \quad \text{if } |RSRP_i| > |RSRP_j| \\
&y < m_{d_{ij}^\perp} \cdot (x - x_{ij}) + y_{ij} \quad \text{if } |RSRP_i| < |RSRP_j| \\
&y = m_{d_{ij}^\perp} \cdot (x - x_{ij}) + y_{ij} \quad \text{if } |RSRP_i| = |RSRP_j| \tag{4}
\end{align*}$$

We ignore the comparison case of $|RSRP_i| = |RSRP_j|$ since those are rounded integer values as explained before, so not precise enough to make an equality decision. Also, this case yields a line instead of a half-space, which may misguide us. The expected rate of this equality situation that we ignore is around 1% out of all pairwise comparisons of the MRs according to our experimental results given in the following section.

Finally, the location of the FBS can be identified as the area in the intersection of the all half-spaces obtained from the pairwise comparison of the related measurement reports as expressed in Equation 5.

$$\text{Loc}(FBS) = \bigcap_{i \neq j} HS_{ij} \tag{5}$$

for each pair $(r_i, r_j) \in R \times R$.

Notice that there may be inconsistency between the half-spaces identified as mentioned above for each pair of the related measurement reports such that intersection of the all half-spaces would be empty. This may happen due to error.
or noise in RSRP measurements or in location estimations of the UE. To resolve possible such inconsistencies among the identified half-spaces, we use a majority vote scheme such that the intersection area where is overlapped by the greatest number of half-spaces is chosen as the likely FBS location.

V. EXPERIMENTS
We implemented the proposed method to evaluate its performance under different scenarios using discrete-event network simulator ns-3.1 The ns-3 simulator has an LTE module which is composed of the LTE model and the EPC model. The LTE model includes the LTE Radio Protocol stack that resides entirely within the UE and the eNB nodes, whereas the EPC model includes core network interfaces, protocols and entities that reside within the network nodes. In our implementation, we collect a series of standard measurement reports from UEs deployed in an area containing both multiple legitimate eNBs and one malicious device, i.e., FBS. Based only on the collected measurement reports, assuming the locations of legitimate eNBs are known, we first perform trilateration to estimate the location of UEs where the measurement reports are sent, and then predict the location of FBS in a Cartesian coordinate system.

The pseudo code of our implementation for post-processing of the collected measurement reports is given in Algorithm 1. In our implementation, we divide the rectangular deployment area (i.e. the region of interests - ROI) into small grids whose size is determined by the resolution parameter. We represent this area by a two-dimensional array where each element corresponds to a grid in the ROI. We then initialize this array by assigning an arbitrary score (e.g. 100) to each element. For a pair of MRs, we first estimate the reporting locations where these two MRs were sent by applying trilateration on the RSRP values embedded in these MRs. Then we go through each grid in the ROI one by one, and for each grid, we calculate the distance between the grid center and the estimated reporting locations. Based on this information acquired, we evaluate whether it is possible to have the FBS in the examined grids according to our approach by checking the consistency between the reported RSRP values of the FBS in these MRs and the calculated distance between the grid center and the estimated reporting locations. If it is not possible to have the FBS in a grid, then we decrease the score of this grid, otherwise the score is kept. We repeat this process for all possible pairs of MRs. Finally, we select the grids with the highest score (corresponding to the intersection of half-planes) and take the center of them as the FBS location.

The resolution parameter has a significant impact on the computation time of our algorithm because the array size (i.e. the number of grids to be examined in the ROI) depends on this parameter. Our experimental analysis showed that setting the resolution parameter to 5 instead of 1 (corresponds to 5 meter step-size instead of 1 meter in searching the region) shortens the computation time by 25 times without degrading the accuracy significantly, and therefore we set this parameter to 5 in the following experimental analysis. Figure 5 shows the flowchart of our above mentioned implementation.

A. EXPERIMENTAL SETUP
In our experimental setup, we placed 4 legitimate eNBs and one FBS in two different deployment areas: (i) Region-A with the size of 500 m × 500 m and (ii) Region-B with the size of 1000 m × 1000 m. We performed 20 simulation runs for two scenarios: (i) no obstacles (e.g. building) in the radio signal propagation environment and (ii) buildings exist in the radio signal propagation environment. While the positions of legitimate eNBs were manually set and remained same over different trials, the position of the FBS was randomly selected for each trial as depicted in Figure 6. The position of legitimate base stations in Region-B are doubled in x and y coordinates in comparison to Region-A. The UEs were initially placed randomly into the deployment area and attached to the legitimate eNBs. Each UE performed random walk for

---

1 https://www.nsnam.org

---

Algorithm 1 FBS Localization

| Input: | $R = \{r_1, r_2, \ldots, r_n\}$ | $r_i$ | measurement reports |
|---|---|---|---|
| Output: | FBS location |
| 1: | procedure TRILATERATION($r_i$) |
| 2: | return ($x_i, y_i$) | $r_i$ | reporting (UE) location |
| 3: | end procedure |
| 4: | $ROI[k][m] \leftarrow (x_{km}, y_{km}, \text{score}_{km})$ | $r_i$ | define a 2D array keeping the coordinates of grid centers and the score initialized with an arbitrary value |
| 5: | for each $(r_i, r_j) \in (R^2 - (r_i, r_j))$ do |
| 6: | $d_{i} \leftarrow \text{EUCLID}(x_{km}, y_{km}, (x_i, y_i))$ | $r_i$ | distance from grid center to first reporting location |
| 7: | $d_{j} \leftarrow \text{EUCLID}(x_{km}, y_{km}, (x_j, y_j))$ | $r_j$ | distance from grid center to second reporting location |
| 8: | if $\text{rsrp}_i > \text{rsrp}_j$ and $d_i > d_j$ then |
| 9: | decrease the score |
| 10: | else if $\text{rsrp}_i > \text{rsrp}_j$ and $d_i < d_j$ then |
| 11: | keep the score |
| 12: | continue |
| 13: | end if |
| 14: | end for |
| 15: | Intersection $\leftarrow \{ROI[k][m] | \text{score}_{km} == \text{max}\}$ | $r_i$ | the grids with the greatest score yields intersection of the half-spaces |
| 16: | LocationFBS $\leftarrow \text{Center}(\text{Intersection})$ | $r_i$ | geometric center of the intersection area is the estimated location of FBS |
its mobility with a constant speed of 10 m/s and randomly changing its direction at every 2 seconds. Unlike the UEs, the legitimate eNBs and FBS are stationary during each trial.

To make handover mechanism enabled between eNBs, the X2 interface must be configured appropriately in ns-3, where each eNB can be configured whether it admits handover requests or not. Normally, every eNB is set as to admit this request by default. The A2A4RSRQ handover algorithm is used in our simulations which is based on event A2 and event A4 measurements. According to event A2, when the RSRQ of the serving cell becomes worse than threshold (i.e. servingCellThreshold), it starts looking for the neighbour cell with the best RSRQ; then it checks whether the difference between best neighbour RSRQ and serving cell RSRQ is greater than a certain offset threshold (i.e. NeighbourCellOffset). When both event conditions are met, the handover procedure is triggered for the UE to the best neighbour. We simulate the behaviour of FBS by using an eNB with handover feature disabled via setting the boolean attribute LteEnbRrc::AdmitHandoverRequest to False in its X2 interface configuration. Initially all UEs are manually attached to the legitimate base stations; then depending on the movement pattern of the UEs, they can be handed over to another legitimate base stations. Thus, the FBS neither becomes an initial serving cell for the UEs nor it can be the target cell in the handover process, but it can advertise itself to the UEs in the surrounding area.

Simulation parameters which are used in our scenarios are given in Table 3.

For each trial of experiment, we log the following data by using a callback function in ns-3 which is called when an eNB receives a measurement report:

- **Time:** Time of receiving a measurement report of a UE at eNB. This information is used for debugging purposes and not taken into consideration in the algorithm.

### Table 3. Simulation parameters.

| Parameters              | Value                        |
|-------------------------|------------------------------|
| Simulation Duration     | 25 s                         |
| Carrier Frequency       | 1800 MHz                     |
| Number of UEs           | 40                           |
| eNB height              | 40 m                         |
| UE height               | 1.5 m                        |
| eNB Power               | 46 dB                        |
| Path Loss Model         | Friis free space mode (no building) Hybrid Model (with building) |
| Antenna Configuration   | 1x1                          |
| servingCellThreshold    | 30 dB                        |
| NeighbourCellOffset     | 1                            |

![Flowchart](image)
• \( \text{ue}_x, \text{ue}_y, \text{ue}_z \): 3-dimensional position info of the reporting UE at the time of sending the measurement report to eNB. Notice that we use this information only to calculate the error in the estimation of UE location at reporting time while applying trilateration procedure. Our method does not actually need this information.

• \( \text{spCI}, \text{sr} \): Physical Cell ID (PCI) and reported RSRP for the serving cell.

• \( \text{List[pci}, \text{nrs} \): List of neighbor cell PCIs and corresponding RSRP values which are reported by the UE.

In our simulation scenarios, each UE can report up to five RSRP values, one for the serving cell and four for other neighboring cells since there are four legitimate base stations and one FBS. However, the number of reported neighboring cell can be less than four when UE is not in the vicinity of other cells. We extract this information from the measurement reports at eNBs. Note that we use only RSRP values in our algorithm. So, our experiment shows a realistic scenario in a sense that we utilized the measurement reports that are already accessible in real networks easily. After having the measurement reports in a real network, it is straightforward to implement the proposed method.

### B. EXPERIMENTAL RESULTS

After collecting measurement reports from the above-mentioned **ns-3** simulations, for each experimental trial, we estimated FBS location by performing the post-processing stage given in Algorithm 1, and then calculated the estimation error by comparing our result with the ground truth, i.e. accurate location information of the FBS. Finally, we took the average of the estimation errors, found in all trials.

Since our method requires estimating UE locations where the measurement reports are sent, we also present our results for estimation of UE locations via trilateration based on the RSRP values embedded in the measurement reports.

#### 1) EXPERIMENTS WITHOUT BUILDINGS

In this set of experiments, we evaluated performance of our method when there is no obstacles like buildings in the radio signal propagation environment.

In the step of estimating UE locations via trilateration, we need to derive the relationship between RSRP values and corresponding distances based on the signal propagation path loss model of the environment. This is necessary so that we can estimate the distance (i.e. the radius of ring strips in trilateration, see Figure 2) between UEs and eNBs from the RSRP values as accurately as possible. Although **ns-3** provides the RSRP-distance relationship, we intentionally avoid benefiting from this for several reasons. First, even though the RSRP-distance relationship taken directly from **ns-3** code could be useful for the experiments when there is no obstacles, it would be useless for the experiments with buildings because the presence of obstacles invalidates the signal propagation path loss formulas. Second, we would like to proceed in the same way as we would proceed in a real use-case practice. Notice that in real world applications appropriate propagation path loss models may already be available for certain environments such as urban and rural areas.

To extract the RSRP-distance relationship in the simulation environment, we made additional experiments to collect RSRP samples from some randomly chosen UEs whose locations (and indirectly their distance to eNBs) are known under the mentioned simulation conditions in **ns-3**. Figure 7 indicates the RSRP and distance relationship in Region A when there is no obstacles in the radio signal propagation environment. As seen in Figure 7, RSRP takes only integer values for the reason explained in Section IV-B, and as a result of this resolution limitation in RSRP measurements, we see deviations in distance values for the same RSRP values. The relationship between the RSRP values and the corresponding distance values can be mathematically expressed by applying an appropriate regression technique over these measurement data as visually drawn with the red line in Figure 7. We applied exponential regression over this data and obtained the propagation path loss model given in Equation 6. The R-squared value (goodness-of-fit) for the given trend line is 0.9941, meaning strong correlation and very good fit of the trend line to the data.

\[
\text{Distance} = 1995373 \times e^{(-0.12028 \times \text{RSRP})} \tag{6}
\]

| Region          | Error in Estimating UE Locations | Standard Deviation |
|-----------------|----------------------------------|--------------------|
| A (500 m x 500 m) | 12.27 meters                     | 1.44 meters        |
| W (1000 m x 1000 m) | 20.79 meters                     | 2.40 meters        |

We estimated UE locations at reporting time via trilateration based on the RSRP values in the collected measurement reports by using the signal propagation model given in Equation 6. Table 4 shows the average and standard deviation for our MR-based trilateration error in the estimation of UE locations over all trials of the experiments in Region A and B.
As seen in Table 4, we found the average trilateration error for UE locations as around 12 meters and 20 meters for Region A and B respectively which seems pretty acceptable considering the uncertainties mentioned in Section IV-B.

After estimating the UE locations where MRs were sent, we predicted the FBS location for each experimental trial in which FBS location was determined randomly. We calculated the average error in estimating the location of the FBS over 20 trails of experiments. To observe the impact of the number of measurement reports on the estimation error, for each trial, we gradually increased the number of measurement reports from 10 to 150 by increasing the simulation time. Notice that these measurement reports can be either reported by one specific UE in different locations or reported by different UEs. Figure 8 shows the average estimation error in FBS location when considering only the most and the 2nd most overlapped areas of the half-spaces in our method for different number of measurement reports in Region A and B. By the most overlapped area, we mean the region where the highest number of half-spaces overlapped, and by the 2nd most overlapped area we mean the region where the number of intersected half-spaces is the second largest.

As seen in Figure 8, in Region A, FBS localization error is around 21 m when 10 MRs are used in our method, and then gradually decreases as the number of MRs used is increased. FBS localization error becomes around 9 m, 8 m, 8 m, 7 m, 7 m, and 7 m when 25, 50, 75, 100, 125, and 150 MRs are taken into consideration in our method. It seems that increasing the number of MRs from 10 to 25 improves the estimation accuracy considerably (i.e. decreasing the error from 21 m to 9 m), but any further increment in the number of MRs has not significant impact on the estimation accuracy, which means taking into consideration a limited number of MRs in FBS localization would be sufficient to get a good location estimation. The results for the 2nd most overlapped area are similar to the results for the most overlapped area. Notice that this performance has been achieved despite the UE locations obtained by trilateration contain error. It is also interesting to observe that the FBS localization error (around 10 m) is less than the UE localization error (around 12 m), despite the former depends on the latter, which implies our FBS localization method tolerates the error in UE locations. When we have larger deployment area (i.e. Region B), the FBS localization error is increased and becomes about 33 meters on average. The reason behind this increase is that by enlarging the region, the error in estimating the location of UEs is increased, also we obtain larger overlapped areas when comparing half-planes.

Our algorithm also yields heatmap indicating probable locations of FBS on a map. As an example, Figure 9 is the estimation heatmap from a trial based on 10 measurement reports in Region A, indicating the probable location of FBS for the region of interest. The green star in the center of the darkest red area (i.e. the most overlapped) in the heatmap represents our estimation for FBS location. Although we take the center of this identified most overlapped area as our estimation, FBS may indeed be anywhere in this identified region, which is one of the root causes of FBS localization error.

2) EXPERIMENTS WITH BUILDINGS
In this set of experiments, we evaluated performance of our method when some obstacles like buildings exist in the environment, which is a more realistic scenario and expected to affect the propagation pathloss model.
In this case, we created 16 buildings using the Buildings module in ns-3. We set 2 floors in each building where each floor consists of 2 rooms along the x-axis and 4 rooms along the y-axis. Other attributes were left to default, e.g., building type is residential with concrete wall and windows. We set the size of buildings as $20 \times 20 \times 25$ meters on x-axis, y-axis and z-axis respectively, and positioned them in the form of grid separated from each other by 135 meter on the horizontal and vertical axis. We set a building-aware pathloss model, i.e., HybridBuildingsPropagationLossModel, which combines several well-known pathloss models in order to mimic different outdoor and indoor scenarios including indoor-to-outdoor and outdoor-to-indoor scenarios. The settlement information of buildings and legitimate base stations in Region A is illustrated in Figure 6.

As in the previous experimental setup, we derived the relationship between RSRP and distance for the above-mentioned simulation environment by sampling a certain number (around 100) of RSRP measurements at known distances to associated eNBs. Figure 10 shows the distribution of these measurements with the corresponding distance values. Compared with Figure 7, it seems from Figure 10 that the existence of buildings causes a disruptive effect on signal propagation, which is an expected result as pointed out by several studies [34]. When we applied e-exponential regression on these data, we found the regression curve given in Equation 7, with the R-squared value of 0.8917. This R-squared value is less than the R-squared value of the regression line given in Equation 6, which means accurate estimation of the distance from RSRP value is harder in the presence of buildings. Notice that Equation 7 is an approximated mathematical relationship between RSRP and distance for the environment in this experimental setup, and it is fine to use it for the purpose of FBS localization even though it may not be precise enough.

\[
\text{Distance} = 207965 \times e^{(-0.09251 \times \text{RSRP})} \quad (7)
\]

We estimated the UE locations where corresponding MRs were transmitted by performing trilateration based on the RSRP values embedded in the MRs and the approximated path loss model given in Equation 7. We found that the average error in estimation of UE locations is about 47 m and 69 m for Regions A and B respectively as given in Table 5. Compared with the previous case (no buildings), we observe that the average error in the estimation of UE locations is increased which is apparently due to obstacles that distract signal propagation in the environment.

After the step of estimating UE locations as mentioned above, we performed prediction of FBS locations. Figure 11 shows average FBS localization error over 20 different trials for different number of MRs for both regions. As seen in the figure, FBS localization error is about 54 m and 103 m for Regions A and B respectively when 10 MRs are used. The error gradually decreases as the number of MRs used is increased and remains constant at around 32 m and 73 m after 50 MRs for Region A and B respectively.

Table 6 shows our experimental results all together for both FBS and UE localizations under different scenarios.

3) COMPUTATION TIME
We conducted all experiments on a 64-bit Windows-10 PC with an Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz processor and 32.0 GB RAM for the two examined scenarios (i.e. with and without buildings). The computation time includes extracting and reading the MRs from log records,
TABLE 6. Performance comparison of both FBS and UE localizations under different scenarios.

| Experiment         | Scenario               | Average Error in UE localization | Average Error in FBS localization |
|--------------------|------------------------|----------------------------------|-----------------------------------|
| With buildings     | Region A (500 m × 500 m) | 47.75 m                         | 32.51 m                           |
|                    | Region B (1000 m × 1000 m) | 69.23 m                         | 73.15 m                           |
| No buildings       | Region A (500 m × 500 m) | 12.77 m                          | 10.08 m                           |
|                    | Region B (1000 m × 1000 m) | 20.79 m                          | 36.19 m                           |

VI. CONCLUSION

In this study, we presented a network-based method for estimating the exact location of a false base station. To the best of our knowledge, there is no previous study that proposed a solution for locating FBS in a mobile cellular network where almost all of the effort so far focused on detecting false base stations. Our novel localization method utilizes measurement reports regularly sent by UEs in proximity of FBS and performs comparative pairwise analysis of measured RSRP values to find the geographical location of an already detected FBS.

We implemented our method in ns-3 network simulator and showed that it makes accurate estimations for the location of an FBS with meter-level precision. We experimentally verified the performance of our proposed method under different scenarios including blockages and uncertainties in a mobile network. In the experiments, we observed that increasing the number of measurement reports used in location estimation improves the performance up to a certain number of measurement reports, after which there is no significant change. We also found that the computation time of the proposed method is quite acceptable (e.g. about 6 seconds for 10 MRs) given that the FBS localization is performed only if the event of FBS detection occurs.

Our method relies on the data already existent in measurement reports standardized by 3GPP and does not require any additional information about UEs or other network elements to estimate FBS location. These measurement reports contain anonymous data in the sense that privacy-sensitive information like locations cannot be linked to specific UEs. Therefore, our method is not expected to cause any risk with regard to privacy. In contrast, it aims to protect privacy of mobile subscribers against FBS threat.

Another advantage of the presented method is its scalability due to being independent of the size of the network and number of UEs. Besides, since it is network-based, there is no need for installing additional components such as probes to the mobile network, which makes our method easily deployable in real networks. It is sufficient to put the FBS localization algorithm proposed in this paper as an application software running in the same environment with the FBS detection software. Notice that in case there are more than one FBS in the area having different PCI, those FBSs can be located by running our proposed method individually for each one. However, if one FBS chooses an identical PCI in the same frequency band with the other FBS, multiple RSRPs associated with the same PCI will be reported in the measurement reports causing PCI conflict which is a known problem in cellular networks and treated by several methods [35], [36]. Due to this PCI conflict, it will be difficult for our algorithm to distinguish which RSRP to use when estimating one of the FBS, since both FBSs have the same PCI.

As a future work we plan to improve our results for the environments including obstacles. Also, we would like to test our presented method on a real network.
REFERENCES

[1] F. Bisogni et al., “The European perspective of telecommunications as a critical infrastructure,” in Proc. Int. Conf. Crit. Infrastruct. Protection, Berlin, Germany: Springer, 2012.

[2] D. Wehrle, “Open source IMSI-catcher,” M.S. thesis, Dept. Comput. Sci., Albert-Ludwig-Universität Freiburg, Breisgau, Germany, 2009.

[3] C. Paget, “Practical cellphone spying,” Def Con, Las Vegas, NV, USA, Tech. Rep. 18, 2010.

[4] A. Dabrowski, N. Pianta, T. Kiepl, M. Mulazzani, and E. Weippl, “IMSI-catcher if you can: IMSI-catcher-catchers,” in Proc. 30th Annu. Comput. Secur. Appl. Conf. (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, Belgium: ICST, 2014, pp. 246–255.

[5] K. Normann, M. Näslund, and E. Dubrova, “Protecting IMSI and user privacy in 5G networks,” in Proc. 9th EAI Int. Conf. Mobile Multimedia Commun., 2016, pp. 159–166. [Online]. Available: http://dl.acm.org/citation.cfm?id=3021385.3021415

[6] S. Park, A. Shaik, R. Borgaonkar, and J.-P. Seifert, “Anatomy of commercial IMSI catchers and detectors,” in Proc. 18th ACM Workshop Privacy Electron. Soc. (WPES), New York, NY, USA, 2019, pp. 74–86. doi: 10.1145/3338498.3358649.

[7] T. Van Do, H. T. Nguyen, N. Momchil, and V. T. Do, “Detecting IMSI-catcher using soft computing,” in Proc. Int. Conf. Soft Comput. Data Sci. Springer, 2015, pp. 129–140.

[8] P. Ney, I. Smith, G. Cudacaru, and T. Kohno, “SeaGlass: Enabling city-wide IMSI-catcher detection,” Proc. Privacy Enhancing Technol., vol. 2017, no. 3, pp. 39–56, Jul. 2017.

[9] K.-W. Huang and H.-M. Wang, “Identifying the fake base station: A location based approach,” IEEE Commun. Lett., vol. 22, no. 8, pp. 1604–1607, Aug. 2018.

[10] Z. Zhang, X. Ji, T. Zhang, J. Zhang, W. Xu, Z. Li, and Y. Liu, “FBiSleuth: Fake base station forensics via radio frequency fingerprinting,” in Proc. Asia Conf. Comput. Commun. Secur., 2018, pp. 261–272.

[11] A. Ali and G. Fischer, “Symbol based statistical RF fingerprinting for fake base station identification,” in Proc. 29th Int. Conf. Radioelectronika (RADIOELEKTRONIKA), Apr. 2019, pp. 1–5.

[12] A. Ali and G. Fischer, “Enabling fake base station detection through sample-based higher order noise statistics,” in Proc. 42nd Int. Conf. Telecommun. Signal Process. (TSP), Jul. 2019, pp. 695–700.

[13] S. M. Razavi, F. Gunnarsson, H. Ryden, A. Busin, X. Lin, X. Zhang, S. Diwedi, I. Siomiama, and R. Shreevastav, “Positioning in cellular networks: Past, present, future,” in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1–6.

[14] M. Raitoharju, S. Ali-Löytty, and L. Wirola, “Estimation of base station position using timing advance measurements,” Proc. SPIE, vol. 8285, Oct. 2011, Art. no. 82855L.

[15] L. Asmaa, K. A. Hatim, and M. Abdelaziz, “Localization algorithms research in wireless sensor network based on multilateration and trilateration techniques,” in Proc. 3rd IEEE Int. Colloq. Inf. Sci. Technol. (CIST), Oct. 2014, pp. 415–419.

[16] D. S. Abodunrin, “Detection and mitigation methodology for fake base stations detection on 3G/2G cellular networks,” M.S. thesis, Dept. Sci. Technol., School Elect. Eng., Aalto Univ., Jul. 2015.

[17] H. Alrasheide and R. A. Shaikh, “IMSI catcher detection method for cellular networks,” in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), May 2019, pp. 1–6.

[18] S. Steig, A. Aarnes, T. Van Do, and H. T. Nguyen, “A network based IMSI catcher detection,” in Proc. 6th Int. Conf. IT Converg. Secur. (ICITCS), Sep. 2016, pp. 1–6.

[19] P. K. Nakarmi, M. A. Ersoy, E. U. Soykan, and K. Normann, “Murat: Multi-RAT false base station detector,” 2021, arXiv:2102.08780. [Online]. Available: https://arxiv.org/abs/2102.08780

[20] J. Roth, M. Tummala, J. McEachen, and J. Scrofani, “Location privacy in LTE: A case study on exploiting the cellular signaling Plane’s timing advance,” in Proc. 50th Hawaii Int. Conf. Syst. Sci., 2017, pp. 6285–6292.

[21] C. Wang, X. Zheng, Y. Chen, and J. Yang, “Locating rogue access point using fine-grained channel information,” IEEE Trans. Mobile Comput., vol. 16, no. 9, pp. 2560–2573, Sep. 2017.

[22] F. Awad, M. Al-Refaei, and A. Al-Qerem, “Rogue access point localization using particle swarm optimization,” in Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICs), Apr. 2017, pp. 282–286.

[23] Y. Zhuang, B. Wright, Z. Syed, Z. Shen, and N. El-Shemy, “Fast WiFi access point localization and autonomous crowdsourcing,” in Proc. Ubiquitous Positioning Indoor Navigat. Location Based Service (UPINLBS), Nov. 2014, pp. 272–280.

[24] Security Research Labs. (2019). Snoopsnitch. [Online]. Available: https://opensource.srlabs.de/projects/snoopsnitch

[25] J. D. Roth, M. Tummala, and J. W. Scrofani, “Cellular synchronization assisted refinement (CeSAR): A method for accurate geolocation in LTE–A networks,” in Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS), Jan. 2016, pp. 5842–5850.

[26] H. T. Friis, “A note on a simple transmission formula,” Proc. IRE, vol. 34, no. 5, pp. 254–256, May 1946.

[27] C. S. R. Murthy and B. Manoj, Ad Hoc Wireless Networks Architectures and Protocols. Upper Saddle River, NJ, USA: Prentice-Hall, 2005.

[28] M. Vissvanathan, Simulation of Digital Communication Systems Using MATLAB, Los Gatos, CA, USA: Smashwords, 2013.

[29] LTE: Evolved Universal Terrestrial Radio Access (E-UTRA): Requirements for Support of Radio Resource Management, 3rd Generation Partnership Project (3GPP), Technical Specification, document 3GPP (TS) 36.133, Dec. 2020, version 16.7.0.

[30] S. Gullu, “Comparison of reference signal received power measurements between cell phone and scanning receiver in LTE,” M.S. thesis, Dept. Elect. Eng., College Eng. Florida Inst. Technol., Melbourne, FL, USA, Dec. 2017.

[31] R. C. V. Macario, “The multipath propagation problem,” in Cellular Radio: Principles and Design, London, U.K.: Macmillan Education, 1997, pp. 112–127, doi: 10.1007/978-1-349-14433-4_5.

[32] A. Vannelli, D. Micheli, and G. Muratore, “Statistical analysis of smartphone MDT signaling power measurements for radio maritime LTE propagation study,” in Proc. Int. Symp. Electromagn. Comput. (EMC Eur.), Sep. 2020, pp. 1–6.

[33] H. Xian, W. Muqing, M. Jiansong, and Z. Cunyi, “The impact of channel environment on the RSRP and RSRQ measurement of handover performance,” in Proc. Int. Conf. Electron., Commun. Control (ICECC), Sep. 2011, pp. 540–543.

[34] S. E. Carpenter and M. L. Sichitiu, “An obstacle model implementation for evaluating radio shadowing with ns-3,” in Proc. Workshop Ns-3, May 2015, pp. 17–24.

[35] R. Verissimo, P. Vieira, A. Rodrigues, and M. Queiruz, “PCI and RSI conflict detection in a real LTE network using supervised learning,” URSI Radio Sci. Bull., vol. 2018, no. 364, pp. 11–19, 2018.

[36] A. P. Lestari, A. N. Mufti, and U. K. Usman, “Optimization of PCI conflict detection in LTE-advanced using collision and confusion methods considering reuse distance algorithm,” in Proc. Int. Conf. Signals Syst. (ICSigSys), May 2018, pp. 20–24.

LEYLI KARAÇAY received the M.Sc. and Ph.D. degrees in computer science and engineering from Sabanci University, Turkey, in 2012 and 2020, respectively. She had worked as a Teaching Assistant at Sabanci University for seven years. She has some scientific research papers published in journals and conference proceeding in the area of security. She joined Ericsson Research, Turkey, in October 2019, where she works as an Experienced Security Researcher.

ZEKI BILGIN received the B.S. and M.degrees in electrical and electronics engineering from Gazi University, Ankara, and the Ph.D. degree in computer science from the City University of New York, NY, USA. He works as a Senior Specialist at Arcelik Research and previously served as an Experienced Security Researcher for Ericsson Research, Turkey. He involved in many industrial and academic research projects related to telecommunication, the IoT, 5G, cybersecurity, social computing, computer vision, smart grid, and machine learning. He has authored many scientific articles and inventions in these domains.
AYŞE BILGE GÜNDÜZ received the M.Sc. degree in computer engineering from Istanbul Technical University, in 2016. She is currently pursuing the Ph.D. degree with Yildiz Technical University (YTU), Istanbul, Turkey. She worked six years as a Research Assistant at YTU. She currently works as a Security Researcher with Ericsson Research, Turkey.

PINAR ÇOMAK was born in Ankara, Turkey. She received the B.Sc. degree in mathematics, and the M.Sc. and Ph.D. degrees in cryptography from Middle East Technical University (METU), in 2010, 2013, and 2020, respectively. She had worked as a Research Assistant at METU for eight years. She authored some international conference papers related to coding theory, computational algebra, and cryptography. She joined Ericsson, in September 2019, and has been working as an Experienced Security Researcher at Ericsson Research, Istanbul, Turkey.

EMRAH TOMUR received the B.S. and M.Sc. degrees in electronics engineering from Bilkent University, in 1999 and 2001, respectively, and the Ph.D. degree in information systems from Middle East Technical University, in 2008. He has been working as a Master Researcher at Ericsson, since January 2019, where he is leading the research team in the area of security. Before joining Ericsson, he worked as the research and development manager at private sector companies and the technology transfer manager in universities, where he gave courses and served as a graduate thesis advisor. He has several scientific research papers published in journals and conference proceedings in the area of security. He also worked in numerous various national and international research and development projects funded by EU or national agencies. His technical expertise is on security of Internet of Things, M2M, and wireless sensor networks.

ELF İUSTUNDAG SOYKAN received the M.S. and Ph.D. degrees in computational science and engineering from Istanbul Technical University. She had worked at The Scientific and Technological Research Council, National Cryptology Institute, for 13 years in security domain. She joined Ericsson Research as a Senior Security Researcher, in 2018. She has published several papers in international conferences, mostly on information security and privacy. Her research interests include ML/AI security, privacy enhancing technologies, and the IoT security.

UTKU GÜLEN received the B.Sc. degree in electronics and communication engineering from Yildiz Technical University, Istanbul, Turkey, in 2012, and the M.Sc. degree from Bahcesehir University, Istanbul, in 2014, where he is currently pursuing the Ph.D. degree in computer engineering. He joined Ericsson Research, Turkey, as an Experienced Security Researcher, in 2020. His research interests include applied cryptography, network security and public-key cryptography on embedded systems, and the IoT devices.

FERHAT KARAKOÇ received the B.Sc., M.Sc., and Ph.D. degrees in computer engineering from Istanbul Technical University. He has been working as a Security Researcher and a 3GPP SA WG3 Delegate at Ericsson, since 2020. Before joining Ericsson, he worked on information security and cryptography at private sector companies and public institutes. He also taught information security and cryptography related courses at universities. He has several scientific research papers on cryptography, published in journals and conferences.

* * *