Quantifying Location Privacy in Urban Next-Generation Cellular Networks

John D. Roth, Murali Tummala, John C. McEachen, and James W. Scrofani
Department of Electrical and Computer Engineering
Naval Postgraduate School
jdroth, mtummala, mceachen, jwscrofa@nps.edu

Abstract

With urbanization and cellular subscribership rising sharply, cellular use in urban locales has become a normative behavior for the majority of the world's population. As the research community pushes the limits of what is possible in the next generation cellular arena, it is prudent to simultaneously hold in tension the responsibility to provide appropriate protections to the ultimate end users of such technology. To this end, this research illustrates a location-based attack in modern cellular networks. This attack leverages control information sent over the radio access network without the benefit of encryption. We show how this attack is particularly potent in urban localization where it is important to infer location in three dimensions. We quantify the efficacy of such an attack, and therefore the associated location privacy, through simulation both in a generic cellular environment and in an environment modeled after downtown Honolulu. Our results show that accuracy on the order of 15 meters is possible.

1. Introduction

Urbanization is a fact of modern demography. Indeed, most of the world's population currently lives in urban areas and population shift rates to urban centers of up to 80% have been seen in recent years. With a projected worldwide urban population of three billion, 60% of the projected five billion strong global population, city centers become an increasingly important area for researchers to consider [1].

Additionally, the areas which saw the most growth in cellular subscribership in the last quarter of 2016 were China and India [2], the two countries also expected to contribute the most to global urbanization between now and 2050 [1]. This fact, and the fact that global subscribership penetration has risen above 100% [2] highlight the need for an awareness in the cellular research community of the impact and effects of this burgeoning technology on our global society. With the first deployment of 5G looming on the horizon of the upcoming winter Olympics in one of the worlds most populous urban centers [3], consideration of the effect that 4G has had when designing the future evolution of interconnectivity is prudent.

The privacy and security of cellular networks has long been considered [4]. Indeed, Chief Justice John Roberts of the United States Supreme Court wrote in an opinion that "The fact that technology [cell phone] now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought" [5]. While the privacy of the *content* of our digital communications is generally held as axiomatic, the privacy associated with the location of the user equipment (UE) is less often regarded. Consider over the last decade the normalization of mobile device ownership as evidenced by the aforementioned statistics. Previous to this paradigm shift, it was well-known that a cyber-persona existed in the digital world as an expression of our identity rooted in the physical. Now, the mobile device, or UE, provides a connection between that digital cyber-persona and the physical world. Thus, the nascence of location-privacy, while not often touted, is an emerging threat to the increasingly digital fabric of society.

To this end, this research serves to raise awareness of location-privacy concerns in next generation cellular networks, which we define as Long Term Evolution (LTE) and emerging 5G trends as well as parallel standards such as Worldwide Interoperability for Microwave Access (WiMAX). Because of the popularity of the 3G Partnership Project (3GPP) standards, we frame the manuscript in the context of the associated protocols, however we acknowledge the applicability of this research also to peer cellular standards. Specifically, we present a generalization of a previously re-

URI: http://hdl.handle.net/10125/50620
ISBN: 978-0-9981331-1-9

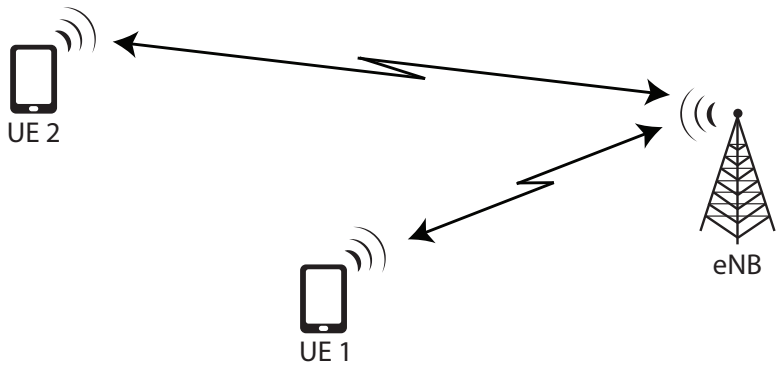

Figure 1: The challenge of mobility management in OFDMA-enabled cellular networks is shown in this figure. Because UE 1 is closer than UE 2, its variable propagation delay must be compensated for by adjusting their uplink burst time via the TA such that their frames will arrive at the serving eNB relative to an absolute schedule maintained at the eNB.

ported vulnerability to the LTE standard [6], [7] which examines the vulnerability in the context of urban city centers where the majority of cellular subscribership is growing. In this environment, high-rise buildings are manifold thus making the requirement for positioning in three dimensions $\mathbb{R}^3$ a necessity.

The remainder of this paper is organized as follows. Section 2 discusses the relevant background to cellular positioning. The subsequent section describes the theoretical framework necessary to evaluate cellular positioning in $\mathbb{R}^3$. Next, Section 4 provides a summary background of the relevant vulnerability in LTE which underscores modern cellular location-privacy concerns. We then propose an extension to the previously introduced exploit highlighting its relevance to positioning in three dimensions. This exploit, and implication for location privacy in $\mathbb{R}^3$, is then quantified in Section 6 via simulation. Finally, a summary discussion is provided in Section 7.

2. Location-Based Exploitation in Cellular Networks

Location-based services (LBS) are now a presumed component of cellular service. The prevalence of popular mobile applications allowing users to voluntarily "check in" to geographic locations as well as the necessity for emergency first responders to locate those requesting such services are exemplar cases for legitimate cellular localization. Indeed, LBS are enabled specifically in the LTE standard via a dedicated LTE Positioning Protocol (LPP) [8]. Despite the requirement for this service, it does not negate the need for standard architecture to be designed to protect against its unauthorized use. In fact, LPP does just this by making use of encrypted sessions to transport data to and from the LBS client. However, less obvious portions of the standard unwittingly provide a would-be attacker information as to a the location of a potential victim in the form of a timing advance (TA).

The TA is a necessary artifact of wide-area cellular networks operating under an orthogonal frequency-division multiple access (OFDMA) scheme [9]. The necessity of the TA comes from the need to manage UE mobility throughout the serving area. OFDMA requires that UE uplink bursts arrive in strictly scheduled time slots at the base station, also known as the enhanced-Node B (eNB). In order to meet this requirement, the network must be able to compensate for a varying propagation delay from a mobile UE to the serving eNB, as shown in Figure 1. In LTE this is accomplished with the TA.

Because the TA provides a link between distance and time, its use as a positioning tool has been studied ever since its inception in the Global System for Mobile Communications (GSM) [10], [11]. However, it never gained much traction due to its limited ability to provide UE-eNB distance information. In GSM, timing requirements were lax enough that the TA would only provide information accurate to 550 m at most, hardly enough to spur interest [11]. These limitations notwithstanding, the tighter timing requirements in LTE provide a level of accuracy up to 78.125 m [12], which bring the TA back under consideration as a viable method for cellular localization. Unfortunately, the security architecture of LTE does not afford for

the confidentiality of the TA and other signaling plane information critical for the protection of user privacy as it is not encrypted [7], [13]. As this information is sent in the clear, it provides the vehicle for location exploitation in LTE. This exploit can be further enhanced with the previously introduced Cellular Synchronization Assisted Refinement (CeSAR) method [6], [7], which is summarized in a subsequent section.

The TA has been previously considered formally as a location privacy preserving mechanism (LPPM) [13], [14] with both a user anonymization component (the cell-radio network temporary identifier (C-RNTI) [9]) and an information obscurity component (the discretization of distance via the TA [15]). The obscurity component of the LPPM is described with the model

$$\hat{d}_i = \| \mathbf{p} - \mathbf{x}_i \|_2 + U_{\mathrm{TA}}, \tag{1}$$

where $\hat{d}_i$ is the perceived distance from the i^{th} eNB and the UE, $\mathbf{x}_i = [x_i, y_i]^T$ is the location of the i^{th} eNB, $\mathbf{p} = [x, y]^T$ is the location of the UE, and U_{TA} is a uniform random variable (RV) which represents the quantization noise introduced by the binary nature of the TA [15]. The efficacy, however, of the information obscurity is inversely proportional to data rate [7]. Thus, as data rates increase towards 5G levels, location privacy will decline as long as the aforementioned signaling data remains unencrypted. Although not the focus of this paper, similar concerns have been raised about the quality of anonymity provided the user via the C-RNTI [4], [16], making the legitimacy of the overall 3GPP model for user privacy suspect.

Exploration of this vulnerability has only been undertaken in the context of approximately flat tracking areas where $\mathbb{R}^2$ is a suitable model. On the other hand, urban locales constitute a decidedly three-dimensional tracking area where $\mathbb{R}^3$ is a more appropriate model. The result of a localization model in $\mathbb{R}^2$ when the infrastructure lies in $\mathbb{R}^3$ has been previously studied and revealed that consideration of the third orthogonal dimension provided the information necessary to provide significant gains in localization accuracy [17]. We add to these past contributions, by showing how the CeSAR method can be used to exploit the LTE signaling plane to continue to improve localization accuracy in $\mathbb{R}^3$ under the assumption of a target UE which is not at ground level.

3. A Localization Bound in $\mathbb{R}^3$

In this section, we introduce and utilize the Cramér-Rao Lower Bound (CRLB) as an appropriate metric through which to understanding the positioning scenario. We first develop the bound as classically used in $\mathbb{R}^2$ and then generalize it to $\mathbb{R}^3$.

3.1. The Cramér-Rao Lower Bound

The CRLB is a statistical lower bound on the accuracy of an unbiased estimator [18]. In our application, that estimator $\hat{\mathbf{p}} = [\hat{x}, \hat{y}]^T$ is attempting to infer an actual UE position $\mathbf{p} = [x, y]^T$. The CRLB is an ergodic bound defined by the trace of the inverse of the Fisher information matrix [19]

$$\mathrm{CRLB} = \sqrt{\mathrm{Tr}\left(\mathbf{I}^{-1}\right)}, \tag{2}$$

where the Fisher information matrix $\mathbf{I}$ is given by [19]

$$\mathbf{I} = -\mathrm{E}\left\{ \frac{\partial^2}{\partial \mathbf{p}^2} \log \mathrm{p}(\mathbf{d}|\hat{\mathbf{d}}) \right\}. \tag{3}$$

When the parameter to be estimated is $\mathbf{p} = [x, y]^T$, the expectation in (3) can be evaluated to [19]

$$\mathbf{I} = \begin{bmatrix} \sum_i \frac{(x-x_i)^2}{\sigma_i^2 d_i^2} & \sum_i \frac{(x-x_i)(y-y_i)}{\sigma_i^2 d_i^2} \\ \sum_i \frac{(x-x_i)(y-y_i)}{\sigma_i^2 d_i^2} & \sum_i \frac{(y-y_i)^2}{\sigma_i^2 d_i^2} \end{bmatrix}. \tag{4}$$

When $\mathbf{p} = [x, y, z]^T$, as in $\mathbb{R}^3$, it is trivial to show that (4) generalizes to

$$\mathbf{I} = \begin{bmatrix} \sum_i \frac{(x-x_i)^2}{\sigma_i^2 d_i^2} & \sum_i \frac{(x-x_i)(y-y_i)}{\sigma_i^2 d_i^2} & \sum_i \frac{(x-x_i)(z-z_i)}{\sigma_i^2 d_i^2} \\ \sum_i \frac{(y-y_i)(x-x_i)}{\sigma_i^2 d_i^2} & \sum_i \frac{(y-y_i)^2}{\sigma_i^2 d_i^2} & \sum_i \frac{(y-y_i)(z-z_i)}{\sigma_i^2 d_i^2} \\ \sum_i \frac{(z-z_i)(x-x_i)}{\sigma_i^2 d_i^2} & \sum_i \frac{(z-z_i)(y-y_i)}{\sigma_i^2 d_i^2} & \sum_i \frac{(z-z_i)^2}{\sigma_i^2 d_i^2} \end{bmatrix}. \tag{5}$$

The implication of the definition of the CRLB in (2) is that the conditioning of $\mathbf{I}$ is critical so that the inverse can be found. From (4) it can be seen that $\mathbf{I}$ becomes ill-conditioned as all eNBs and the target UE become approximately collinear. This result is generalized to $\mathbb{R}^3$ as $\mathbf{I}$ becomes ill-conditioned when all eNBs are approximately coplanar. This can be proven by observing that $\mathbf{I}$ becomes singular when the infrastructure is collinear (cf. (4)) or coplaner (cf. (5)) since the determinant goes to zero. It is intuitively satisfying to observe that when the entirety of the infrastructure is in $\mathbb{R}^n$ that information provided in the $n+1^{\text{th}}$ orthogonal dimension will be nil.

3.2. A Case Study in $\mathbb{R}^3$ Localization

To further appreciate the implications in $\mathbb{R}^3$ to positioning, consider a 20 story high-rise building, which lies at the center of a triangle of three eNBs, each 55 m high. It can be shown from (4) that this is

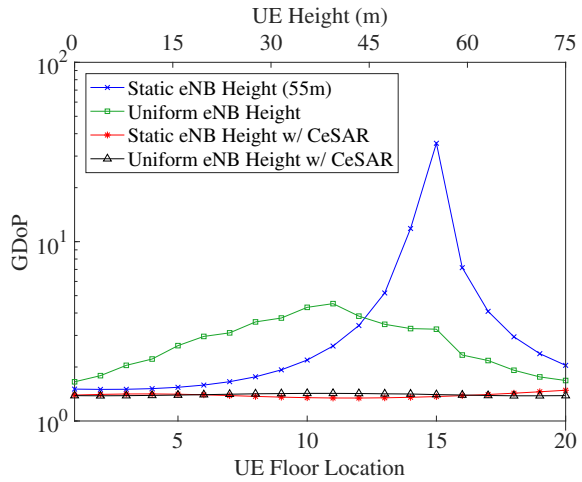

Figure 2: The theoretical positioning performance with three eNBs inside a 20 story building is presented. The performance is shown to degrade when the UE approaches the same height as the supporting infrastructure. Further, the performance is shown to be similarly poor when the infrastructure and target UE have uniformly distributed heights. The effects of poor positioning performance are shown to be abated by establishing a fourth node at the base of the building.

an optimal geometry for information in $\mathbb{R}^2$ when there are three eNBs.

Now, let the geometric dilution of precision (GDoP) be the Fisher information matrix $\mathbf{I}$ when $\sigma = 1$ for all eNBs. Under this condition, the matrix in (4) or (5) is just a function of geometry. GDoP is then a useful lens through which to view positioning accuracy since it can be interpreted as the scale factor, set by the participating infrastructure, that relates the distance measurement accuracy to overall positioning accuracy by [19]

$$\sigma_{\hat{\mathrm{p}}} = \mathrm{GDoP} \times \sigma_{\hat{d}} \ . \tag{6}$$

First, referring to the results presented in Figure 2, consider the GDoP calculated when the target UE is in each floor of the building. In this result, we see that performance exponentially degrades as the target UE approaches the height of the eNBs. In fact, when the UE is at exactly the height of the infrastructure, the positioning performance is infinitely poor due to no information in the z-direction being conveyed (cf. (5)). Therefore, this reveals a difficulty in urban positioning in that the region which is approximately coplanar to the surrounding infrastructure defines a region of very poor theoretical performance.

Practically, cellular infrastructure is not coplanar (although one cannot rule out situations of approximate coplanarity). To understand the effect of positioning performance on infrastructure of varying height we let the height of each eNB be uniformly distributed along with the UE height. The expected positioning performance, as expressed by GDoP is also shown in Figure 2. Although this model virtually guarantees $\mathbf{I}$ will never be singular, this result still shows areas of significant performance degradation, namely around the center of the extrema of the UE heights. Thus, it is not in practical deployment geometries that resolution will be found.

Consider now a scenario where, in addition to the existing eNBs there is an additional node at the base of the building. With this model in mind, we repeat the first experiment where the infrastructure height is left constant at 55 m and the results are presented alongside the previous results in Figure 2. Here we see the local phenomenon of poor performance near the height of the eNBs nullified due to the introduction of information parallel to the previously missing dimension. The results of the second experiment with the new model is also shown in Figure 2. Again we see a reduction of previous poor performance by the information made possible by the new node.

Thus, we find a significant problem in urban positioning performance when only surrounding infrastructure is utilized: there are likely regions of low accuracy at significant heights. However, we find that these regions of concern are removed when a ground level node is introduced. The nature and scope of this terminal will be the subject of the discussion in the next section.

4. Cellular Synchronization Assisted Refinement

CeSAR is a previously introduced [6], [20] method of passive location refinement suitable for protocols which provide wireless access to large area networks via a time-division multiple access (TDMA) scheme, or variant thereof, such as 4G/LTE and also potentially 5G [3], [21]. Previous work has shown CeSAR to be able to mitigate the effects of poor GDoP in $\mathbb{R}^2$ which improves TA-based accuracy to as tight as 40 m [7].

At its core, CeSAR is a TA-based localization method which enables its passive nature. TA-based localization in cellular networks is not a new concept [10], [11], but the tighter timing requirements of LTE relative to legacy standards, such as GSM, make practical levels of accuracy possible. Further, the introduction of a extra-network sensor facilitates a higher level of accuracy through introduction of a new node

and the flexibility to mitigate the dilution of accuracy of potentially poor network infrastructure geometry (which LBS is typically beholden to) [22]. These effects come at no cost of bandwidth to the network due to its passive nature, which simultaneously act as a force multiplier for network operators [22] and a latent signaling plane vulnerability making attribution and detection of unauthorized positioning difficult [13].

A summary of the CeSAR method is as follows.[1] First, an extra-network sensor is required. This sensor need not be complicated or expensive. In fact, due to the introduction of software-defined radio (SDR), the sensor could be implemented by an amateur operator. The sensor first synchronizes to the serving eNB in order to observe unencrypted network traffic sent over the signaling plane. Next, the sensor observes TA commands being issued to the target UE. This not only gives the sensor an idea of the approximate distance the UE is from the eNB, but also the absolute time at which the UE will transmit its next uplink burst. With the latter information, it is possible for the sensor to monitor the time of flight of that burst and thus calculate the sensor-UE distance. These inferred distances are then used to multi-laterate the target position.

5. Two-Step Algorithm for Localization

We propose a two-step (2S) algorithm for $\mathbb{R}^3$ localization of mobile devices in urban environments. The proposed algorithm is low-cost, easy to implement, and passive, thus not requiring already strained network resources. Further, it mitigates the weakness shown in Section 3.

5.1. Step 1: Positioning in $\mathbb{R}^2$

In the first step, the UE position $\mathbf{p}_2$ in $\mathbb{R}^2$ is estimated using (4) [7], [12]. To realize optimal or near-optimal results we utilize the maximum-likelihood estimate (MLE) in $\mathbb{R}^2$ found via [19]

$$\sum_i \frac{(d_i - \hat{d}_i)(x - x_i)}{\sigma_i^2 d_i} = 0 \tag{7}$$

$$\sum_i \frac{(d_i - \hat{d}_i)(y - y_i)}{\sigma_i^2 d_i} = 0. \tag{8}$$

We note here that, in practice, solving (7) and (8) is not realistic as the true location $\mathbf{p} = [x, y]^T$ of the target UE is required. Therefore, alternate pragmatic means for reasonable estimates of location in $\mathbb{R}^2$ exist, such as the residual-error technique [19], [23]

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \sum_i (\hat{d}_i - \| \hat{\mathbf{p}} - \mathbf{p}_i \|_2)^2, \tag{9}$$

where $\mathbf{p}_i$ is the location of the i^{th} eNB. We also note that because the desired estimate lies in $\mathbb{R}^3$, the result of first locating in $\mathbb{R}^2$ will introduce some inevitable error which was studied in [17]. Thus, we provide a second step to not only close the gap on this error, but to improve beyond previous limitations pointed out in [17].

5.2. Step 2: Obtaining Orthogonal Information

In the second step, a CeSAR sensor, as described in Section 4 and [22], is placed at the *refined* $\hat{\mathbf{p}}_2$ location. We qualify the sensor location as refined since pragmatic steps can be used to optimize the estimate beyond simply placing the sensor at $\hat{\mathbf{p}}_2$ when it is known that the UE is located inside a building or not at ground level.

First, the k-nearest neighbor buildings are found to the unrefined $\hat{\mathbf{p}}_2$. Each of the k neighbors are then used to range the UE at each building location. The neighbor with the lowest distance estimate $\hat{d}_s$ is then taken as the most probable building location of the UE and $\hat{\mathbf{p}}_2$ is updated accordingly. We describe this step as "building rounding".

The final position estimate in $\mathbb{R}^3$ is then obtained by combining the available information via

$$\hat{\mathbf{p}}_3 = \left[\hat{\mathbf{p}}_2, \hat{d}_s\right]^T. \tag{10}$$

5.3. Considerations in Implementation

The potential application base of 2S is broad. While we present it as a location-based attack in cellular networks, the application of the algorithm need not hold to such myopia. It is easy to see how 2S could be used by a motivated attacker to locate a target; less trivial is how such a method would be used for legitimate LBS. Specifically, constantly moving cellular infrastructure to iteratively locate a UE of interest may not be realistic in a commercial network deployment. In this case, we propose a change to cellular architecture to support this type of urban positioning. Namely, we propose the installation of many such fixed CeSAR sensors at the base of points of interest. For instance, dominant high-rises in a cityscape may serve as ideal locations for installation. While such adjustments to the status quo of physical cellular architecture are generally economically undesirable, the nascence of

[1] The interested reader is referred to [6], [7], [22], and [20]) for a more detailed treatment of the CeSAR method.

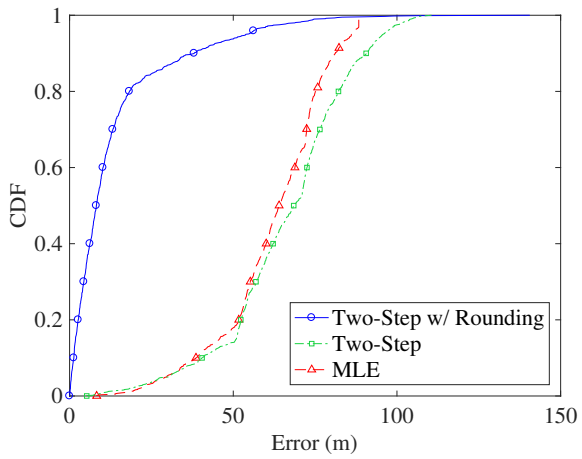

Figure 3: The performance of localization in $\mathbb{R}^3$ via different positioning algorithms is shown. The building rounding technique, used in the 2S algorithm, is shown to be highly significant such that accuracy is improved beyond that of MLE.

5G technology may provide the appropriate segway for such a shift. Because of the proposed high-frequency spectral real estate proposed for 5G [3], maintaining line-of-sight between a UE and its serving infrastructure becomes more important to maintain quality of service. We therefore propose that integration of the CeSAR sensor with next-generation architecture is viable.

6. Experimental Validation

In this section, we show the 2S algorithm to outperform standard MLE localization in $\mathbb{R}^3$. We first demonstrate its efficacy in a generic scenario. We then use a model of downtown Honolulu with measurements taken in an actual off-location LTE network deployment to predict how the method will perform in a real-world environment.

6.1. Generic Results

In this simulation, we consider a 500 m × 500 m notional tracking area. Building positions are modeled as a Poisson point process with intensity $\lambda = 20$. Building heights are modeled as a uniform RV $U \in (10, 400)$ m. The experiment is evaluated via the Monte Carlo method by simulating a new generic urban center with each iteration. During each trial, four buildings are selected at random to be the host for a parasitic cell tower which sits on the roof, as is common practice in actual urban deployments. Finally, the TA is simulated with a Gaussian measurement error where $\sigma = 50$ m which has been shown to be a reasonable error and also as an appropriate surrogate for the otherwise descrete TA measurement [7]. That error is then rounded to the nearest 78.125 m in line with how the TA presents in an actual LTE network deployment. Also in line with the results of [7], the sensor measurement error is modeled as Gaussian where $\sigma = 10$ m.

The results of the first investigation, shown in Figure 3 as a cumulative distribution function (CDF)[2], contrast the 2S algorithm with the MLE. The resulting circular error probable (CEP) 70%[3] accuracy is approximately 76 m, 72 m, and 13 m for 2S without building rounding, MLE, and 2S with building rounding respectively. The improvement in performance of 63 m CEP 70% of the 2S method with the building rounding technique illustrates the potency of this portion of the algorithm. However, even without rounding, 2S performs comparable to MLE, which is practically unrealistic to use (cf. (7) and (8)). Further, it is clear that 2S with building rounding outperforms MLE and 2S without building rounding in all scenarios, even at the tail of the error distribution.

6.2. Downtown Honolulu Results

The goal of this simulation is to demonstrate the efficacy of 2S (with building rounding) in an actual urban environment. To this end, a portion of downtown Honolulu, shown in Figure 4, measuring approximately 400 m × 600 m was selected. The area under consideration is bounded by Bethel, South Beretania, and Alakea Streets on the North, East, and South respectively. The western border of the area under consideration is established by Ala Moana Boulevard. Twenty-seven of the most prominent buildings in this fifteen-block urban center were modeled by latitude, longitude, and approximate building height (which ranged from 16 m to 136 m when height is approximated at 4 m per building story). The location of four buildings which serve as hosts to parasitic eNBs were identified via publicly available antenna registration records and imagery, and used as such in this simulation.

Again, Monte Carlo trials were used to evaluate performance. The target location was chosen randomly, with uniform distribution, inside one of the 27 buildings with random height inside of that building. The

[2]The CDF is defined as the probability that a realization of a RV will be less than some constant value x, (i.e., $F_X(x) = \Pr[X \leq x]$).

[3]CEP 70% is explicitly defined in terms of the CDF as $F_X(0.7) = \Pr[X \leq 0.7]$.

Figure 4: The area under consideration is a five by three block portion of downtown Honolulu measuring approximately 600 m × 400 m in area. Twenty-seven of the largest buildings are modeled in the simulation, four of which have been identified as hosting parasitic cell towers. The border of the area under consideration is established by Bethel St., S. Beretania St., Alakea St., and Ala Moana Blvd. Imagery ©2017 Google, Map Data ©2017 Google.

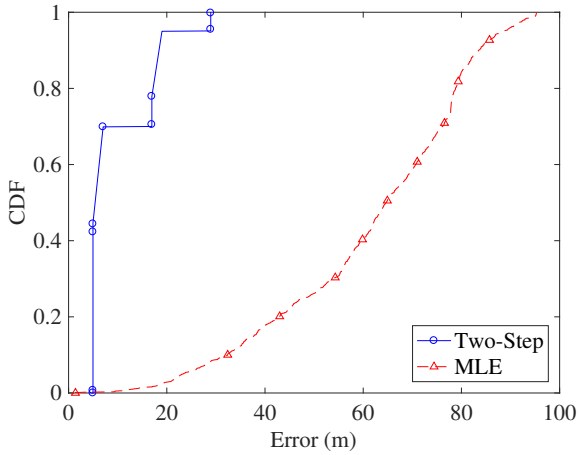

Figure 5: In this figure, the performance of 2S is evaluated against MLE in a simulation environment which models downtown Honolulu. Measurements from an actual off-site network deployment are used in this simulation. Significant improvement is realized through 2S demonstrating the efficacy of the method in a realistic urban environment.

TAs used were recorded from real-world off-site LTE network deployments and applied to the simulated eNBs. For CeSAR sensor data, actual radio frequency ranging measurements taken at 900 MHz, also collected off site, were used [7]. These measurements were obtained by transmitting a pseudo-noise sequence and then using a matched filter at the receiver.

The results of this experiment are presented in Figure 5 again as a CDF. Here we see 2S (with building rounding) providing significant gains over MLE. At the CEP 70% level, MLE provides 76 m of accuracy while 2S provides 17 m of accuracy. The step-wise nature of the curve representing 2S is due to the discrete nature of the radio ranging measurements used as the CeSAR sensor data (set by the maximum sample rate of the equipment). In fact, the correct building is always found during the first step of 2S thus the error realized is only that due to inaccuracies in measuring height. This realistic result demonstrates the power inherent in 2S.

7. Dénouement

In this paper, we have extended previous results which reported on and quantified the vulnerability of LTE to user privacy via signaling plane information. Specifically, we extended these results from $\mathbb{R}^2$ to a model more appropriate to urban deployments in $\mathbb{R}^3$, an undeniably three-dimensional cityscape. Accompanying this extension, a novel algorithm, 2S, for urban positioning was proposed which leveraged the exploitation previously identified in CeSAR. 2S was shown to mitigate poor GDoP which is specific to positioning in $\mathbb{R}^3$. The performance of 2S was examined in two simulation testbeds utilizing the Monte Carlo method. In the first, a generic city center was randomly generated to assess general performance. Next, a model of downtown Honolulu was created to assess the performance in a specific, real-world environment. In both cases, 2S was found to outperform the MLE taken directly on $\mathbb{R}^3$ and provided accuracies on the order of 15 m CEP 70%.

These results highlight the need for a minor, but significant shift in LTE security architecture. By moving the signaling plane under the umbrella of encryption, the potency of this vulnerability would be dramatically reduced. Instead, the confluence of its current plaintext form and nascent SDR technology threatens location privacy in a very real way. Additionally, we put forth that when designing for future generations of cellular deployments, such as 5G, a balance between performance and security should be held in tension. Our relentless pursuit of the Shannon limit must be

tempered with a respect for the privacy and security of those who will ultimately benefit from these emerging technologies.

References

[1] Department of Economic and Social Affairs, United Nations, "World urbanization prospectus," 2014, retrieved: May, 2017. [Online]. Available: https://esa.un.org/unpd/wup/

[2] Ericsson, "Ericsson mobility report," Februrary 2017, retreived: May, 2017. [Online]. Available: www.ericsson.com/mobility-report

[3] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 8, pp. 1617–1655, 2016.

[4] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[5] Riley v. California, U.S. 13-132, 2014.

[6] 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.*, 2016, pp. 5842–5850.

[7] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "On location privacy in LTE networks," *IEEE Trans. Inf. Forens. Security*, vol. 12, pp. 1358–1368, Jun 2017.

[8] 3GPP TS 36.355, release 10, (v10.12.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)," Jul. 2014.

[9] E. Dahlman, S. Parkvall, and J. Sköld, *4G LTE/LTE-Advanced for Mobile Broadband*. Academic Press, 2011.

[10] C. Drane, M. Macnaughtan, and C. Scott, "Positioning GSM telephones," *IEEE Commun. Mag.*, vol. 36, no. 4, pp. 46–54, 1998.

[11] J. Bull, "Wireless geolocation," *IEEE Veh. Tech. Mag.*, vol. 4, pp. 45–53, 2009.

[12] L. Jarvis, J. McEachen, and H. Loomis, "Geolocation of LTE subscriber stations based on the timing advance ranging parameter," in *Proc. Military Commun.*, 2011.

[13] J. D. Roth, M. J. C. Tummala, Murali, and J. W. Scrofani, "Location privacy in LTE: A case study on exploiting the cellular signaling planes timing advance," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017.

[14] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Security Privacy*, 2011, pp. 247–262.

[15] 3GPP TS 36.321, release 10, (v10.10.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification," Dec. 2012.

[16] I. Bilogrevic, M. Jadliwala, and J.-P. Hubaux, "Security and privacy in next generation mobile networks: LTE and femtocells," *Femotcell Workshop*, 2010.

[17] R. Whitty, M. Tummala, and J. McEachen, "Precision geolocation of mobile wimax subscribers using timing adjust measurements," in *Proc. 45th Hawaii Int. Conf. Sys. Sci.*, 2012, pp. 5639–5648.

[18] M. DeGroot and M. Schervish, *Probability and Statistics*, 4th ed. Pearson, 2012.

[19] I. Güvenç and C.-C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 3, pp. 107–124, 2009.

[20] J. D. Roth, M. Tummala, and J. C. McEachen, "Device and method for cellular synchronization assisted location estimation," U.S. Patent 9 655 077.

[21] J. Qiao, X. Shen, J. Mark, Q. Shen, Y. He, and L. Lei, "Enabling device-to-device communications in millimeter-wave 5G cellular networks," *IEEE Commun. Mag.*, vol. 51, pp. 20–27, Jun 2013.

[22] J. D. Roth, M. Tummala, and J. C. McEachen, "Efficient system geolocation architecture in next-generation cellular networks," *IEEE Systems J.*, to be published.

[23] J. Caffery, "A new approach to the geometry of TOA location," in *Proc. IEEE Veh. Technol. Conf.*, vol. 4, sep 2000, pp. 1943–1949.