Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks

John D. Roth*, Murali Tummala†, and James W. Scrofani†
*Department of Electrical and Computer Engineering
United States Naval Academy
Annapolis, MD, USA
Email: jroth@usna.edu
†Department of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA, USA

***Abstract*—The vulnerability of cellular networks to location-based attacks via uplink timing management commands has been studied since the advent of GSM. However, the introduction of heterogenous networks as the answer to increasing demand for data throughput has resulted in a new vulnerability to such attacks. In this work, we propose Cellular Synchronization Assisted Refinement (CeSAR), an entirely passive method of leveraging available LTE-A downlink synchronization messaging to refine uplink timing advance commands issued by the network. Our results suggest that CeSAR is capable of providing positioning improvement, not only in LTE-A networks but also in legacy deployments, of up to 254 meters.**

1. Introduction

Over the past decade the cellular market has seen a dramatic paradigm shift away from voice telephony to demands for data network traffic support driven by smart phones and an ever increasingly "connected" society. Some estimates project an increase in cellular network capacity of 1000x over the next decade [1]. The family of releases commonly referred to as LTE-Advanced (LTE-A), is poised to address this growing and non-trival demand for data traffic. To this end, industry has looked to cell densification as the mechanism for delivering in the growing LTE standard. LTE release 11 is set to be the first release actually employing these heterogenous networks containing cost efficient pico and femto cells. However, while in a rush to meet market demands, cellular developers have failed to recognize key second order effects of such network deployments that may have serious consequences on user privacy.

The vulnerability of cellular systems to location-based attacks via uplink timing management commands has been studied since the advent of the Global System for Mobile Communications (GSM) [2]. During normal cellular mobility management an uplink timing command called a timing advance (TA) is sent from the base station to the user equipment (UE) in order to ensure the UE uplink frames are properly synchronized thus avoiding intersymbol interference from multiple connected users. This timing information can easily be mapped to a distance thus defining a radius around the base station where the UE may lie. The TA is sent in the clear allowing anyone access to this information.

LTE has inherited the same vulnerabilities developed in GSM; however, the risk of location information leakage has remained low enough that the problem was ignored in the name of data throughput. However, the arrival of heterogenous networks changes the environment sufficiently to reopen the topic.

In this paper we will analyze the LTE-A standard and show how the current trend of cell densification results in new location-based attack vectors. We will then propose and develop a novel method of exploiting these attack vectors, called Cellular Synchronization Assisted Refinement (CeSAR), to obtain accurate location-based information. CeSAR will capitalize primarily on readily available cell downlink information to affect position estimates that provide increases in accuracy as high as 254 meters in some cases.

The rest of this paper is organized as follows. First, we present an evaluation of the location-based security of the LTE-A standard in Section 2. Next, we present CeSAR and define a framework for exploitation of the LTE-A standard in Section 3. We then validate CeSAR through monte carlo network simulation in Section 4.

2. Location Security Aspects of LTE-A

To begin, we turn our attention to an analysis of the LTE-Advanced standard. Here we intend to discuss the salient aspects of 4G that pertain to the security of the UE location. In other words, we intend to show several ways in which the standard can be exploited in order to glean information about the UE location. As previously discussed, in the context of legacy deployments, this is not a new area of research. Rather, deducing the UE location through

1530-1605 2016

DOI 10.1109/HICSS.2016.723

protocol exploitation has been studied since the 1990's [2]. The intent of this work is not to re-evaluate work already done, instead we intend to show how new advances in cellular technology, and their subsequent execution in the LTE-A standards, offers new opportunities for side-channel positioning.

2.1. LTE Positioning Protocol

It is first worth noting how the network currently provides positioning services to the UE in LTE. This is done via the LTE Positioning Protocol (LPP) [3]. LPP allows for several methods of position location: Observed Time Difference of Arrival (OTDOA), Assisted Global Navigation Satellite System (A-GNSS), and finally Enhanced Cell ID (E-CID).

A-GNSS is well studied and provides very reasonable accuracy. With the integration of the required hardware in many modern mobile devices, A-GNSS arises as a adept solution to the mobile location problem. Despite this, there still exists a legacy population without the required hardware that must be serviced. Additionally, A-GNSS usually comes at a high power cost which, given the mobile platform, is undesirable. Finally, the emerging requirement for accurate positioning indoors and in metropolitan canyons requires an alternative solution [4].

OTDOA is a positioning method where a UE will measure the time difference of arrival of the LTE Positioning Reference Signal (PRS) from multiple base stations, or enhanced Node-Bs (eNBs). This information is then sent to a network-based Enhanced Serving Mobile Location Center (E-SMLC). With three or more eNBs, the resulting non-linear system of equations can be solved to provide a position estimate to the UE. However, like A-GNSS, OTDOA suffers in urban and indoor environments where non-line of sight (NLOS) and multipath channels dominate. Release-11 will compliment OTDOA with Uplink Time Difference of Arrival (UTDOA). The main difference being that UTDOA is determined by the eNBs after a signal is sent from the UE [4].

The third method available to LPP for UE positioning is E-CID. Here multiple signal characteristics are obtained at specified physical locations *a priori*. Real time measurements are then taken by the UE to try to match to the *a priori* measurements. This method is sometimes referred to as radio frequency pattern matching (RFPM), database correlation, or fingerprinting in the literature. When a UE initiates an LPP session, and the E-CID is the chosen method from which to derive a position, the network and UE will negotiate which measurements the UE will send to the E-SMLC to determine the position. This measurement set is reliant on the composition of the *a priori* database and the UE capabilities. Measurements specified in the LPP standard include: cell-ID, reference signal received power (RSRP), reference-signal received quality (RSRQ), and TA [3]. The best measurement set useful for positioning is currently an open topic (e.g., [5]); however, RFPM via data fusion has been suggested by the Third Generation Partnership Project (3GPP) [6] via

$$\min_{i} \frac{\parallel h_{RPRP} - \chi_{RSRP,i} \parallel}{\sigma_{\chi^2_{RSRP,i}}} + \frac{\parallel h_{TA} - \chi_{TA,i} \parallel}{\sigma^2_{\chi_{TA,i}}} \qquad (1)$$

where h_{RSRP} is the UE measured RSRP, $\chi_{RSRP,i}$ is the ith pre-recorded RSRP measurement, h_{TA} is the current UE TA, $\chi_{TA,i}$ is the ith pre-recorded TA measurement, and σ_x is the respective database variances.

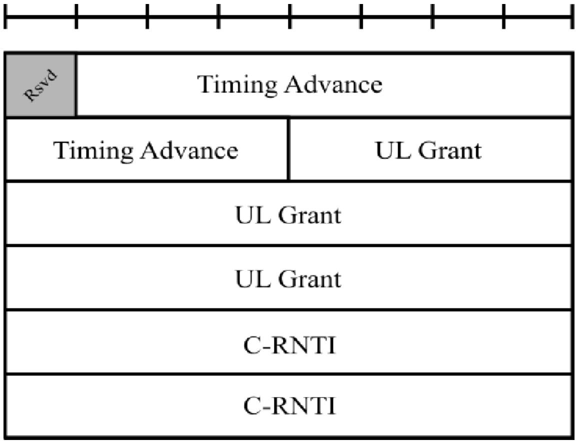

Figure 1: The random access response (RAR) message found in the media access control (MAC) header. After [8].

Finally, it should be noted that LPP sessions are ciphered and, as such, effectively protected data. This study assumes this data to be unreadable and thus not available for exploitation.

2.2. Anatomy of the LTE Timing Advance

Ever since GSM, the TA quantity has been recognized as useful for positioning cellular devices [2], [7]. In this section we aim to develop context for TA inside LTE-A networks.

The TA takes two forms during normal cellular operation. The first is the TA that is negotiated during the initial network random access. After the UE has obtained downlink synchronization via the primary and secondary search signals (PSS/SSS) and the corresponding system information from the master and system information block (MIB/SIB) the UE requests network access from the eNB via a random access preamble. If the request is successful the eNB continues network access negotiation with a random access response (RAR) message. As seen in Figure 1, inside this message is the cell radio network temporary identifier (C-RNTI), an uplink resource grant, and an 11 bit TA quantity where, $T_A \in \{0, 1, \cdots, 1282\}$ [8]. This quantity directs the UE to begin transmission of its uplink frame $16 \times T_A \times T_s$ seconds *before* the beginning of the corresponding downlink frame, where T_s is the sampling frequency [9], [10].

The second form the TA takes is during normal maintenance of the UE connection. Unlike the TA during initial network access, this TA only adjusts the UE's uplink timing

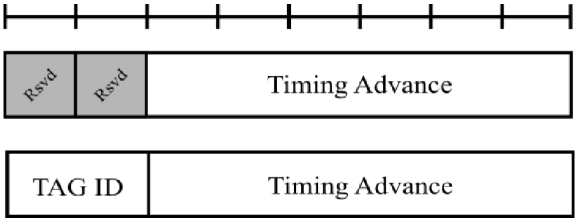

Figure 2: The legacy timing advance command (top) and the release 10+ timing advance command (bottom). From [8].

based on its current timing and is thus relative. As the mobile device moves throughout the vicinity of the eNB its distance to the eNB will likely change. In order to maintain the uplink timing alignment, the eNB will periodically issue TA commands to the UE. These six bit TA commands come in the form of a medium access control (MAC) control element (CE) as seen in Figure 2 [8]. Because only six bits are used $T_A \in \{0, 1, \cdots, 63\}$. Each command moves the UE's current uplink timing by $16 \times (T_A - 31) \times T_s$ seconds. The possibility of a negative value allows for the uplink timing to be advanced or retarded depending on which direction the UE is moving relative to the eNB [9], [10].

The frequency of the maintenance TA is of particular importance as we would like to know how often this information is transmitted and thus how vulnerable it is. This frequency is lower bounded by an LTE-A parameter `timeAlignmentTimer` [11]. This timer is reset each time a TA is received from the eNB; however, if the timer expires the radio connection is considered out of synchronization and the UE must renegotiate with the network to reestablish uplink timing. Because of this, the TA frequency must ensure a TA within the `timeAlignmentTimer` time frame. This parameter has configurable finite durations $\{500, 750, 1280, 1920, 2560, 5120, 10240\}$. The configured duration is common for all serving cells per UE. The duration corresponds to the maximum number of subframes sent in between TAs. Because subframes are continuous in LTE-A and because each subframe is stipulated as 1 ms long by the standard, the available durations can also be interpreted as number of milliseconds [9]. Therefore, when configured for finite[1] duration we can expect a TA to be sent no less frequently than anywhere from one half second to ten seconds. In practice the TA frequency will be higher usually resulting in a TA several times per second [12]. The relative frequency of the TA will be more than appropriate for the purpose of semi-continuous positioning and tracking.

Additionally, as of Release 9, type 1 and type 2 TAs are introduced [13]. A type 2 TA is determined by the eNB via the UE generated random access preamble and calculated as

$$TA_2 = \hat{t}_{eNB,Rx} - \hat{t}_{eNB,Tx} \tag{2}$$

where $\hat{t}_{eNB,Rx}$ is the time instance where the eNB receives the UE random access preamble as determined by the first path and $\hat{t}_{eNB,Tx}$ is the standard eNB frame timing. A type 1 TA is calculated during the maintenance phase via

$$TA_1 = (t_{eNB,Rx} - t_{eNB,Tx}) + (t_{UE,Rx} - t_{UE,Tx}) \tag{3}$$

where the first difference is the time separation between a received uplink frame and its transmit timing and the second difference is the time separation of those same frames only this time at the UE. The second difference is always positive, while the first may be positive or negative. The type 1 TA allows the eNB to determine the round trip time (RTT) with theoretically arbitrarily small error and use this to advance or retard the served UE's uplink timing. It should be noted that this information is never sent over the radio link and is thus not available for exploitation; however, we will later discuss how a passive listener can use this principle to refine a captured TA command via CeSAR.

Both the initial and maintenance TA are sent in the clear. The first, which is found in the RAR, is sent before a security key is negotiated and thus must necessarily not be ciphered. The maintenance TA is sent as a MAC CE. Since the CEs are sent as part of the MAC header, which is below the Packet Data Convergence Protocol (PDCP) sublayer, it is also sent in the clear. This enables anyone within range to observe this traffic. However, if the attacker does not initialize their surveillance during the initial TA they will be unable to effectively use the maintenance TA for ranging as each one is relative to the previous TA.

2.3. Linking Timing Advance to a Specific User

Because a multiplicity of users will be simultaneously connected to a given eNB and because each user may be at different distances from the eNB an attacker must be able to identify which TA is associated with which UE. Each TA has a C-RNTI which is effectively a temporary software address issued by the network to each UE analogous to an Internet Protocol address. The C-RNTI is initially leased to a UE during network access negotiation and issued via the RAR. Maintenance TAs are associated with a specific C-RNTI via downlink scheduling assignments made via the Physical Downlink Control Channel (PDCCH) found in the L1/L2 control region of each subframe [12]. Because the L1/L2 control region of each subframe needs to be decoded by every UE, it is sent in the clear. Therefore, an attacker could use the information in the PDCCH to find the resource on which a transport block for a particular UE is located. The corresponding transport block could then be searched for a TA CE. Of particular importance here is that an attacker must observe a UE access the network in order to initially associate the C-RNTI with the UE.

2.4. Uncertainty in the Timing Advance

Largely because of the discrete nature of the TA, a single measurement from an eNB will reduce the possible location of the UE to an annulus of fixed width with the eNB as its center. This discrete error is also exacerbated by error associated with the eNB antenna height, multipath propagation,

[1] The standard also allows for a configurable inifinite duration of `timeAlignmentTimer`.

and clock bias [14]. By analyzing the quantization error we can determine a lower bound on the area of uncertainty.

As stated in the previous section, a TA will change a UE's uplink timing in increments of $16 \times T_s$. The parameter T_s is the LTE basic unit of time and is given by

$$T_s = \frac{1}{15000 \times 2048} \text{ seconds} \tag{4}$$

where 15000 corresponds to the subcarrier spacing of 15kHz and 2048 corresponds to the maximum Fast Fourier Transform (FFT) size [7], [9]. Assuming speed of light propagation the range of uncertainty, ϵ_{TA}, can then be calculated by

$$\epsilon_{TA} = 16 \times \frac{1}{2} \times \frac{c}{15000 \times 2048} = 78.125 \text{ meters} \tag{5}$$

where c is the speed of light and the extra factor of $1/2$ is included because the eNB must consider the downlink propagation time for the command to reach the UE when issuing a TA.

This line of analysis can also be used to determine the maximum eNB-UE range supportable by LTE. Since the maximum initial TA value is 1282, the formula in (5) can be used to determine a maximum supportable distance of approximately 100km.

2.5. Timing Advance in Handover Scenarios

In order to facilitate inter-cell mobility UEs must usually monitor and evaluate the received signal quality of neighboring cells. The type and frequency of measurements are configurable and are dictated by the network. Measurements normally involve acquisition of the cell PSS and SSS. After this is complete the eNB will have determined the cell-ID and the downlink synchronization giving it access to the cell-specific reference signal. This signal is then used to determine the reference signal received power (RSRP) and/or the reference signal received quality (RSRQ). If the RSRP or RSRQ is larger than a configurable quantity then the network will select that cell for a handover. The network may also handover a UE for various other reasons such as network load [11].

The UE is notified of a handover event by the serving eNB via an `RRCConnectionReconfiguration` message that is generated by the target eNB. This message may include mobility information such as the target cell-ID, physical layer parameters, and the new C-RNTI to assist the UE in establishing its new connection. Notably, the handover is asynchronous, meaning the UE will begin the random access procedure with the target eNB which will involve the negotiation of a new initial TA concurrently while still receiving a TA from the source eNB [11].

The presence of two TAs from spatially disparate beacons presents a unique opportunity for gleaning location estimation. By processing this information at the E-SMLC with TDOA methods a hyperbola can be described around the loci of the source and target eNBs. The advantage of this type of scenario lies in no requirement for the UE to be tightly synchronized with the network effectively removing the error from clock bias. Alternatively, the TOA method may be used which will result in two annuli from the two TAs. The two annuli reduces the target locus to the their area of intersection. Finally, if ciphering is not enabled, the target eNB will issue a new C-RNTI to the UE in the clear allowing a passive listener to map the previous C-RNTI to the new.

2.6. Timing Advance in Heterogeneous Networks and Coordinated Multipoint

Heterogenous network deployments were introduced in LTE Release 10 which allowed for increasing the data capacity of a network through cell densification. When used in conjunction with carrier aggregation (also introduced in Release 10), a primary cell (PCell) and one or more secondaries (SCell) may be configured. The Radio Resource Control (RRC) sublayer is responsible for selecting an PCell and then configuring appropriate SCells [11]. Release 11 further provides support for PCells and SCells that are not co-located. In order to maintain uplink synchronization among all serving cells it was necessary to establish the concept of the timing advance group (TAG). Serving cells that are co-located are assigned to the same TAG, thus removing the need for separate TAs for each individual cell. As seen in Figure 2, TAGs are associated with TA updates in the two bit TAG ID field. The size of the TAG ID field indicates the specification is designed to eventually support up to three additional SCells.

Coordinated Multipoint (CoMP), potentially part of Release 11, is a related technique that aims to improve quality of service at cell boundaries by coordinating the reception of a UE signal at multiple eNBs [15]. Uplink timing alignment becomes difficult in such a scenario as the UE cannot transmit the same signal at different times to ensure each cell receives a time-aligned signal. Solutions to this problem generally involve synchronizing the uplink timing to the nearest serving cell [16] and then selecting other appropriate cells such that the other received signal arrive within the duration of the cyclic prefix [17]. Thus, while it is still an open area of research, the general consensus is for the UE to be uplink synchronized to the closest serving cell [15], [17]. Since CoMP provides no additional location-based information (i.e., the network still only issues one TA) it is not considered further in this study.

3. Passive Exploitation Framework

Our ability to exploit the TA parameter to estimate location information is now explored in several potential scenarios. In each of the scenarios we assume the target is a cellular subscriber who is connected, or is in the process of connecting, to a frequency division duplex (FDD) configured LTE-A network. The attacker is a passive listener who is in the vicinity of the eNB(s) that is(are) interacting with the target. We also assume that the attacker is in the

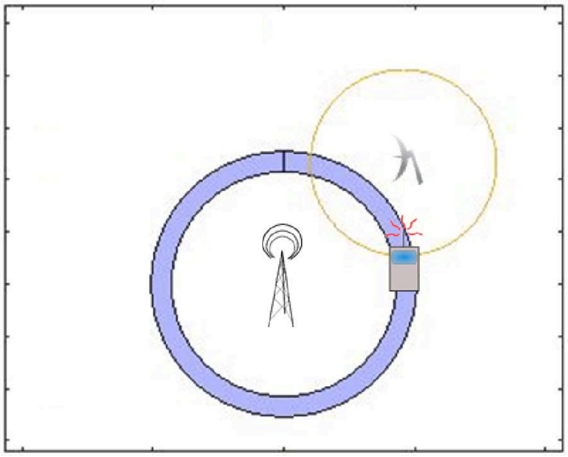

Figure 3: A depiction of a possible environment corresponding to Scenario 1. The serving eNB is shown at the center of the thick TA annulus. The sensor is also shown at the center of the circle computed by CeSAR.

same antenna sector as the target, knows its position, and knows the location of the network infrastructure.

3.1. Scenario 1: CeSAR in Legacy Networks

CeSAR involves the attacker using downlink synchronization to refine an area within the initial TA annulus where the target may be located. First the attacker establishes downlink synchronization with the network by observing the eNB PSS/SSS. Once the attacker has synchronized to the network, she then estimates the downlink frame timing at the eNB by calculating the propagation delay between her and the local eNB. It should be noted that downlink synchronization can be achieved entirely passively, thus the attacker does not need to let her presence be known. Next the attacker listens for TAs sent from the eNB to the target UE. With this knowledge the attacker knows exactly when the target will transmit its uplink frames. Finally, because the attacker has cell synchronization it can calculate the propagation time from the target to the attacker thus creating a circle of negligible width around the attacker on which, somewhere, the target lies.

In this way, CeSAR applies the principle behind the type 1 TA at the attacker location to reduce the original TA annulus from the PCell, $\mathcal{T}_{TA}^{P}$, to its intersection with a circle, $\mathcal{T}_{CeSAR}$, (centered on the attacker) via

$$\mathcal{T}_{\ell} = \mathcal{T}_{TA}^{P} \cap \mathcal{T}_{CeSAR} \tag{6}$$

if we neglect the other error terms enumerated in Section 2.4. The estimated location is the center of the resulting line segment $\mathcal{T}_{\ell}$. A potential realization of Scenario 1 is shown in Figure 3. Overall, this attack never goes beyond observation of layer 2 and can be performed entirely passively.

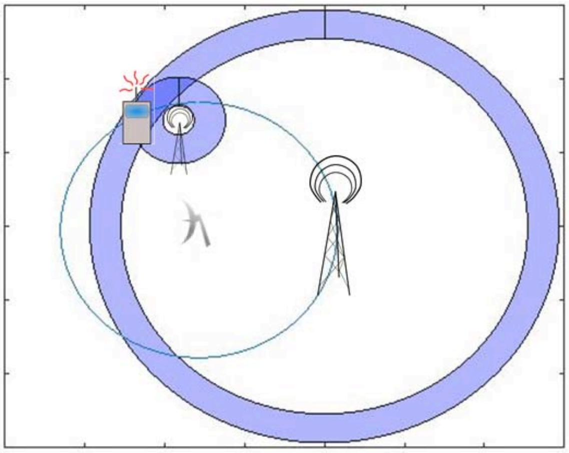

Figure 4: A depiction of a possible environment corresponding to Scenario 2. The serving PCell is shown at the center of the thick TA annulus along with one configured SCell and the annulus corresponding to the SCell TAG. The sensor is also shown at the center of the circle computed by CeSAR.

3.2. Scenario 2: CeSAR and Multiple Timing Advances in Heterogenous Deployments

This scenario considers the CeSAR location-based attack in LTE-A Release 11+ HetNet deployments in which there are at least two serving cells in physically separate locations. While physically disperse SCells (also called pico cells) are not a general requirement for heterogenous networks, SCells are not collocated for the purposes of this study. This scenario will only be available for advanced UE targets enabled for carrier aggregation. Here, multiple TAGs are used for the PCell and SCell(s) representing future network deployments which the structure of the TA CE, shown in Figure 2, has been designed for. We also consider the effect of the current release 11 protocol where only two TAGs are used. In this case when an SCell consists of infrastructure that is grouped into a TAG, but not exactly co-located, then, as described in section 2.6, the TAG is configured to use the pico-cell nearest the target as the reference point.

When each SCell is configured with its own TAG, the attacker listens for all TAGs, $\mathcal{T}_{TA}^{S_i}$, associated with the target's C-RNTI and then calculates the intersection of the resulting annuli as the area within which the target is located, given by

$$\mathcal{T}_{\ell} = \bigcap_{i} \mathcal{T}_{TA}^{S_i} \cap \mathcal{T}_{TA}^{P}. \tag{7}$$

Here i spans the set of SCells configured for the target UE and S^i is the ith SCell.

CeSAR can be used in the same manner as in Section 3.1 to further minimize the locus of possible target locations via

$$\mathcal{T}_{\ell} = \bigcap_{i} \mathcal{T}_{TA}^{S_i} \cap \mathcal{T}_{TA}^{P} \cap \mathcal{T}_{CeSAR}. \tag{8}$$

An example realization of Scenario 2 when only one SCell is configured is presented in Figure 4.

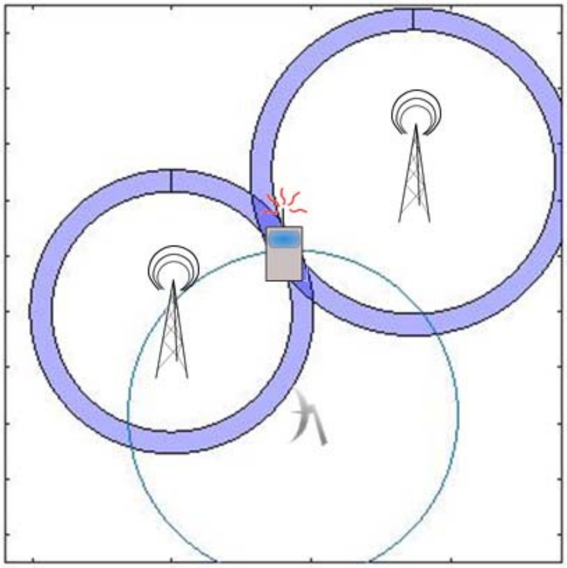

Figure 5: A depiction of a possible environment corresponding to Scenario 3. The originating eNB is shown at the center of the TA annulus along with the target eNB and its corresponding annulus. The sensor is also shown at the center of the circle computed by CeSAR.

When all SCells are configured to used a common TAG the locus of possible location, $\mathcal{T}_\ell$, becomes

$$\mathcal{T}_\ell = \bigcup_i \mathcal{T}_{TA}^{S_i} \cap \mathcal{T}_{TA}^{P} \cap \mathcal{T}_{CeSAR}. \tag{9}$$

The implications of this subtle difference will be explored in Section 4.

In the case where only one TAG is used for all of the SCells, the shape of $\cup_i \mathcal{T}_{TA}^{S_i}$ from the attacker perspective is non-circular. As the attacker does not know which of the pico cells is closest to the target she must calculate an annulus assuming each of the pico cells is closest. This results in the observed TA being placed around each serving pico-cell with each being just as likely to contain the UE.

3.3. Scenario 3: CeSAR in Handover Scenarios

This scenario considers the location-based attack as a PCell handover is initiated. During normal operation the target constantly performs a cell search as outlined in Section 2.5. Here, two annuli from TAs sent from the target cell and the cell of origin intersect to form the locus of possible target locations. This technique may then be refined using CeSAR as outlined in the previous scenarios. An example realization of Scenario 3 is presented in Figure 5.

Besides the advantages already enumerated in Section 2.5, this scenario also gives the attacker access to the initial TA upon which all further relative TAs depend. Thus, this scenario must be observed or the UE must be observed joining the network in order to make Scenarios 1 or 2 practically useful.

TABLE 1: Parameters for the network simulation.

Parameter	Value
Cell Size	500m
Trials per Simulation	1000
Sensor Distribution	Uniform
Target Distribution	Uniform
TA Uncertainty (ϵ_{TA})	78.125m
Target-Sensor Distance	$\geq \epsilon_{TA}/2$
eNB Height Error [14]	0m
NLOS Propagation Error	0m
Network Synchronization Error	0m
Clock Bias Error	0m
Handover Event Location	$\mathcal{N}(\mu = p_{cb}, \sigma = 70\text{m})$ p_{cb} = Cell boundary
Pico Cell Distribution	$\mathcal{N}(\mu = p_T, \sigma = 200\text{m})$ p_T = Target location

4. Results

All results are obtained via monte carlo simulation over the course of 1000 trials per curve. In all cases error is defined as the distance from the estimated target location to the true target location in the euclidean sense. Parameters for the simulations are presented in Table 1.

4.1. Scenario 1

The performance of attempts to locate a target with only one observed TA from the PCell with and without CeSAR are presented via a cumulative distribution function (CDF) in Figure 6. When only one TA is available and CeSAR is not used the estimated target location is selected from a set of guesses uniformly distributed throughout the annulus.

The low performance in this technique can be explained by the high degree of uncertainty offered by a large locus. Small errors are representative of scenarios when the TA quantity is small (i.e., the UE is physically close to the eNB) or in the unlikely scenario that the estimated position is chosen very near to the actual target location.

Large errors are accounted for by large TA values (i.e., the UE is near or on the cell boundary) and when the estimated position is chosen on the opposite side of the annulus as the true target location.

Of special note is this curve's near uniform appearance with the slight non-uniformity accounted for by the irregular shape of the locus.

The second curve presented in Figure 6 contrasts the performance improvements that can be realized through CeSAR. This curve presents in much more of an exponential distribution, shifting the preponderance of errors to much lower values. Here, CeSAR results in 254m improvement in the circular error probable (CEP) 70% metric[2].

Despite significant improvement from the former method, notable large errors are still present. These large

[2] CEP 70% means that 70% of the time the estimated target location will be within some distance of the true target location. For example, the CeSAR curve shown in Figure 6 has a CEP 70% of 71 meters, meaning that 70% of the time the estimate will be within 71m (or less) of the true location.

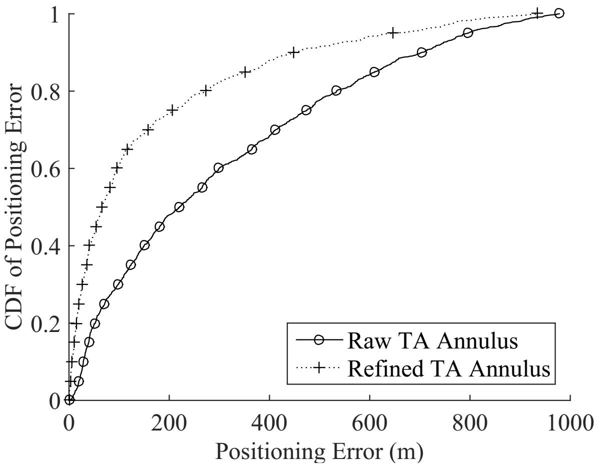

Figure 6: The performance of locating a target with only the observed TA and also the observed TA refined by CeSAR.

errors are realized when the intersection between the circle and annulus results in two separate line segments and the estimated target location is on the opposite segment from the actual target location. Again, larger TAs result in the potential for larger errors, thus cell size can be linked to accuracy.

4.2. Scenario 2

Here we present the results of locating a UE configured for carrier aggregation in release 11+ heterogenous deployments. We first examine the case where each SCell is configured with a unique TAG in Figure 7. The estimated solution is obtained by finding the center of mass of $\mathcal{T}_\ell$ resulting from (7) via an established error residual method outlined in Section 5.A of [18]. The results appear Rayleigh, and we see that the more SCells that are configured the better the accuracy. The CEP 70% ranges from 39.7 meters with one SCell configured to 23.5 meters with four SCells configured. The increase in accuracy as more SCells are configured is due to the larger amount of information about the target location being included in the problem. This phenomenon highlights the potential for more location-based information leakage in hetergenous deployments. Overall, location accuracy is much better than in Scenario 1.

Next, we incorporate the refinement presented in Section 3.1 to the case of heterogenous deployments with unique TAGs. The characterization of preformance in this scenario is presented in Figure 8. Here the estimated location is the center of the line segment $\mathcal{T}_\ell$ resulting from (8).

The introduction of CeSAR gives the error distribution a more exponential form thus providing an improvement over the unrefined case. Here, CEP 70% ranges from 32 meters with one SCell configured to 14 meters with four SCells configured. Similar to the previous case, more configured SCells lead to better accuracy.

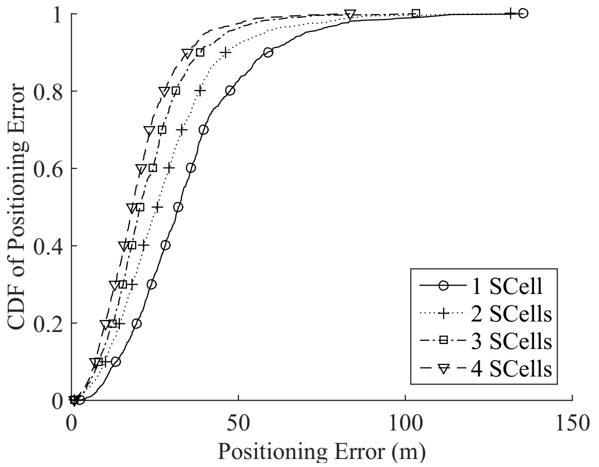

Figure 7: The performance of locating a target in heterogenous network deployments where each SCell is assigned a unique TAG. A comparison of performance when a variable number of SCells are configured is shown.

Next, we examine the effect of using a common TAG for all configured SCells, as per Section 2.6, in conjuction with CeSAR. The effects on performance are presented in Figure 9. While the shape remains exponential it can be seen that more configured cells do not improve positioning accuracy. Because the attacker cannot be sure which of the SCells is the closest to the target, the locus of possible target location becomes the union of the TAG centered around each SCell location, $\underset{i}{\cup}\mathcal{T}_{TA}^{S_i}$. The intersection of the PCell TAG annulus with this set will not necessarily change size which contrasts the case where individual TAGs are configured for each SCell. Additionally, as more SCells are configured $\underset{i}{\cup}\mathcal{T}_{TA}^{S_i}$ remains relatively constant, thus no change in $\mathcal{T}_\ell$ resulting from (9) is noted. In this environment a CEP 70% of 47.8 meters is noted regardless of the number of SCells configured.

4.3. Scenario 3

In this section we present the results of the proposed algorithm in a handover scenario. This type of scenario can be realized in legacy networks with legacy UEs lending it ubiquitous importance. In addition to initial cell association, the handover provides the unique link between the arbitrary C-RNTI and the UE which a passive listener will need in order to identify the correct TA. Second, the initial TA is issued to the UE from the target cell thus establishing a baseline upon which all further TAs are given. Finally, the intersecting rings from both eNBs provide additional location based information not normally available. Here, the locus of possible target locations is defined as the intersection of TAs from the target eNB and the source eNB.

The performance with and without CeSAR are presented in Figure 10. In both cases, the position estimate is achieved

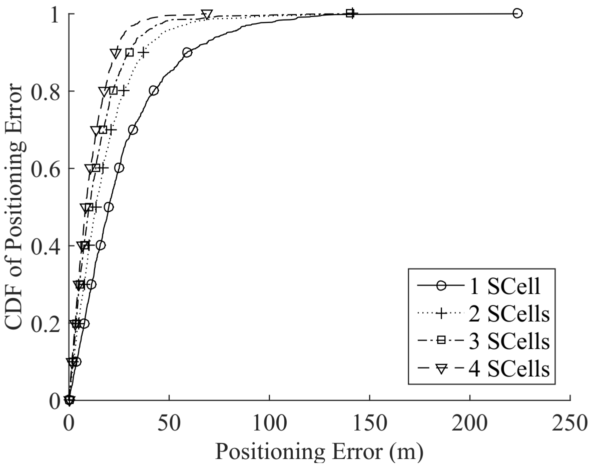

Figure 8: The performance of locating a target in heterogenous network deployments where each SCell is assigned a unique TAG and CeSAR is incorporated. A comparison of performance when a variable number of SCells are configured is shown.

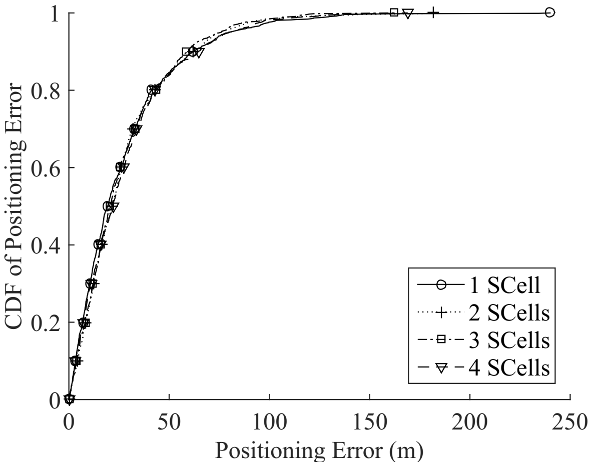

Figure 9: The performance of locating a target in heterogenous network deployments where each SCell shares a common TAG and CeSAR is incorporated. A comparison of performance when a variable number of SCells are configured is shown.

via the same method presented in the Section 4.2. The CEP 70% is 200 meters without CeSAR and 41 meters with CeSAR. Small and large errors can be explained as in Section 4.1 along with the rationale for the significant improvement.

5. Conclusions

In this paper we have evaluated the changing LTE-A standard and demonstrated how it is becoming more vulnerable to location-based attacks. In an effort to continually meet consumer demand for ever increasing throughput. Advanced heterogeneous deployments are widely regarded as the savior of cellular throughput, but place the user at a significant disadvantage for location privacy protection.

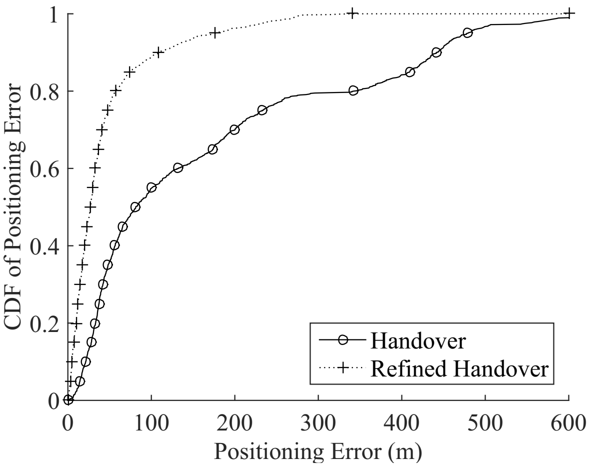

Figure 10: The performance of locating a target a macro cell handover with and without the TA refined as with CeSAR.

In order to exploit this new position-based information we proposed and developed an entirely passive method, CeSAR, where a single sensor may combine network downlink synchronization with its position information to refine a UE location. We have shown how CeSAR integrates readily accessible timing advance information and can provide accurate position estimates of a target in legacy and modern LTE-A networks under various circumstances.

With CeSAR, we have demonstrated that a user could be reliably located during normal legacy intra-cell mobility management to within 158 meters, an improvement of 254 meters. Inter-cell mobility management showed improvements around 159 meters but on a more infrequent basis. In advanced heterogenous LTE deployments the network experiences severe information leakage. Here CeSAR can deliver excellent performance on the order of 14 meters.

Our simple and effective method of refinement demonstrates the relative vulnerability of the LTE-A standard. Further research should be conducted on methods to preserve users' location-based privacy concurrent with throughput improvements.

References

[1] Nokia Siemens Networks, "2020: Beyond 4G," *White Paper*, 2011.

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

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

[4] Ericsson, "Positioning with LTE," *White Paper*, 2011.

[5] T. Wigren, "Adaptive enhanced cell-ID fingerprinting localization by clustering of precise position measurements," *IEEE Trans. Veh. Tech.*, vol. 56, no. 5, pp. 3199–3209, 2007.

[6] 3GPP TR 36.809, (v1.0.0), “Radio Frequency (RF) pattern matching method in LTE,” Aug. 2013.

[7] L. Jarvis, J. McEachen, and H. Loomis, “Geolocation of LTE subscriber stations based on the timing advance ranging parameter,” in *Proc. Military Commun. Conf.*, 2011, pp. 180–187.

[8] 3GPP TS 36.321, release 10, (v10.10.0), “Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification,” Dec. 2012.

[9] 3GPP TS 36.211, release 10, (v10.7.0), “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation,” Feb. 2013.

[10] 3GPP TS 36.213, release 10, (v10.12.0), “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures,” Mar. 2014.

[11] 3GPP TS 36.331, release 10, (v10.16.0), “Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification,” Mar. 2015.

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

[13] 3GPP TS 36.214, release 9, (v9.2.0), “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer; Measurements,” Jun. 2010.

[14] 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.

[15] P. Bhat, S. Nagata, L. Campoy, I. Berberana, T. Derham, G. Liu, X. Shen, P. Zong, and J. Yang, “Lte-advanced: an operator perspective,” *IEEE Commun. Mag.*, vol. 50, no. 2, pp. 104–114, 2012.

[16] M. Zhou and L. Wan, “Analysis into timing advance issue in comp systems,” in *Proc. 70th IEEE Veh. Tech. Conf.*, 2009, pp. 1–5.

[17] Y. Moon, S. Bahng, J. Kim, Y. Park, and W. Kim, “RRH selection and ue transmission timing adjustment for LTE-Advanced uplink MU-MIMO in distributed antenna system environment,” in *Proc. Int. Conf. Inform. Commun. Tech. Convergence*, 2014, pp. 301–305.

[18] I. Guvenc 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.