Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Timing Management in 5G and Its Implications for Location Privacy

Alexander Schacht, James Long, and John Roth
Electrical and Computer Engineering Department
Naval Postgraduate School
Monterey, United States of America
alexander.schacht@nps.edu jglong@nps.edu jdroth@nps.edu

***Abstract*—The fifth generation (5G) technological leap has arrived, bringing with it promises of incredible data rates and never before seen precision in location accuracy. However this self-same precision carries with it the significant question: how will it be protected? These questions form the underlying motivation for this article where we examine 5G architecture which employs a radio access part commonly termed a cloud or centralized radio access network (C-RAN). The C-RAN centralizes higher-level physical layer processes while keeping low-level processes distributed throughout the physical network. We show how this architecture both increases location-based privacy through improved physical-layer security, but creates new privacy concerns via the extension of the radio access network through fronthauls connecting data transfer among low and high-level processing. Concurrently, the proposed 5G variable subcarrier spacing further exacerbates the former point. Through simulation we quantify the decrease in location privacy given the aforementioned considerations. It is shown that location privacy is inversely proportional to subcarrier spacing for user equipment (UE) connected to multiple 5G access points. Specifically, for a (UE) using the widest allowable subcarrier spacing location privacy drops to approximately three meters.**

1. Introduction

Digital-age privacy is a major source of conflicting ideals within society today. Discussions abound in academia, industry, government, pop-culture, etc., going further to postulate whether privacy has lost most of its original meaning [1]–[3]. Within the amalgam of issues that make up privacy, there is none with more polarizing opinions than location privacy. Location-based services (LBS), originally an optional feature in cellular networks [4], have arguably become an essential part of daily life, from easing travel and deconflicting schedules, to personalization of marketing, sales, and habit formulation. However, with increased precision, and access to a user's location, comes a proportional decline of the user's privacy [5].

5G has become the next fundamental milestone in wireless communications, which will redefine the way we interact with the world around us [6]. Intelligent highways and traffic systems, self-driving vehicles, Internet of Things (IoT), Internet of Skills (IoS); all will require highly efficient, accurate, and, in some cases, continuous positioning information to be complemented by exceedingly location-aware devices. The shift from Long Term Evolution (LTE) to 5G promises to bring millions more connected devices online with location accuracy predicted down to less than a meter [7] resulting in a significant loss in the end user's privacy. To explain, we define privacy generally as the condition of being free from observation by others, where, in this case, the observation of concern is the user's location. As the precision with which location aware devices and network-based localization increases, the user's level of privacy around their location proportionally decreases, thus a loss in privacy. The common trend in society is that this loss of privacy in exchange for the utility provided by LBS, is generally not concerning [8]. We argue the contrary. The exactness of the data, combined with the number of authorized 3rd party groups that will have access to it via applications utilizing LBS already carries the inherent risk of interception by unknown and unauthorized parties. We will show that this risk is exacerbated by the current conceptual design of the 5G network.

The main contribution of this paper is to show to what degree the 5G ultra-dense centralized/cloud radio access network (C-RAN) architectural design is vulnerable to a location-based attack through geometric analysis.

The remainder of this paper is organized as follows. Section 2 compares and contrasts work related to this investigation. Section 3 presents an overview of the C-RAN 5G architecture and reasons for use in this paper. In Section 4, the timing advance (TA) is introduced along with its utility within the 5G network protocol. Section 5 presents our attack model. Section 6 states the structure of our simulation environment. Section 7 reports the numerical results of our simulated statistical studies along with our interpretations. In Section 8, we present strategies for mitigating location vulnerabilities within the aforementioned constraints. Finally, we will make our concluding remarks in Section 9.

2. Previous Work

Methods for localization of user equipment (UE) within the network environment have been a paramount objective for network operators following the 1996 Federal Com-

URI: https://hdl.handle.net/10125/64515
978-0-9981331-3-3

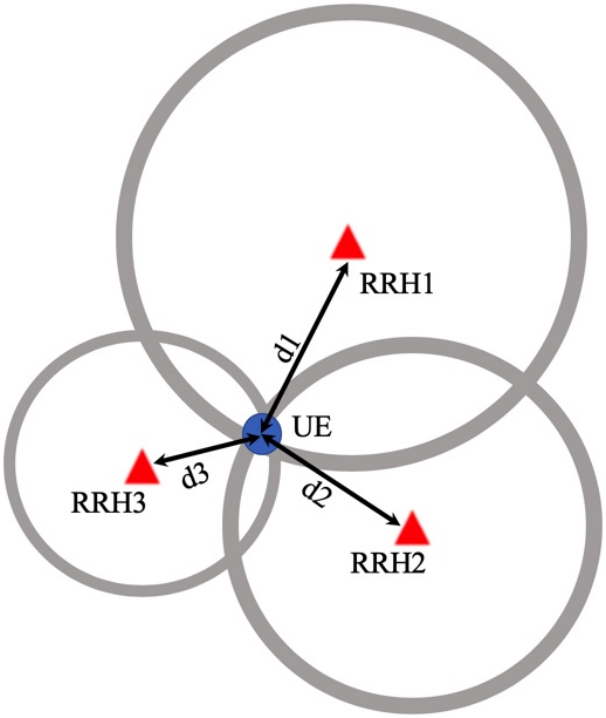

Figure 1: Example of trilateration in a standard LTE architecture.

munications Commission (FCC) mandate for standardized accuracy requirements during enhanced 911 calls [9]. These mandates were revised multiple times and now call for 50 meter or 100 meter location accuracy for 67% of calls and 150 meter or 300 meter accuracy for 90% of calls in an outdoor environment utilizing mobile or network-based solutions, respectively [9]. By 2015, 50 meter horizontal and 3 meter vertical three-dimensional (3D) accuracy requirements are named for calls made indoor [10]. Localization mandates have had far reaching effects on the scope and use of an individual's location data, and continue to set the pace for industry standards.

Five fundamental positioning techniques using radio signals are trilateration, triangulation, proximity, scene-analysis, and hybrid [4]. For this investigation we will focus entirely on the scope of work surrounding trilateration. Trilateration or, more generally, multilateration computes a position solution based on the intersection between common geometric structures created by distance measurements (Time of Arrival (ToA), Received Signal Strength (RSS), etc.) between the UE and the reference transmitter/receiver, as shown in Figure 1. To meet regulatory requirements, operators have done extensive research on both mobile and network-based trilateration techniques. Focusing on network-based solutions, trilateration has been shown in a real deployment as a valid method for achieving previously dictated positioning accuracy [11].

3. C-RAN Architecture

5G promises ultra-low latency (ULL), high capacity, cost effective, and more environmentally friendly communications. In order to realize these demanding aspirations, the way in which the network is structured must be overhauled. To this ideal, the C-RAN architecture was born. The differences between the legacy radio access network (RAN) and this next-generation framework reside in two categories: network re-structuring, and fronthaul/backhaul interface updates.

3.1. Network Re-structuring

The 5G C-RAN, as depicted in Figure 2 scheme is comprised of Baseband Unit (BBU) pools, which consist of numerous, centrally located BBUs. Each pool is distributed across different geographical regions and connected via the fronthaul network to potentially thousands of Remote Radio Heads (RRHs) that are densely aggregated close to UEs. These BBU pools are then connected through the midhaul and backhaul network to the next stage of aggregation and the mobile core network. Network connections have had multiple physical layer proposals [12], however for this we will assume a standard fiber deployment.

This centralized structuring of the network, differs greatly from the traditional RAN where both the BBU and RRH are deployed together as the base station. The C-RAN framework results in greater resource efficiency and sharing, and a decrease in capital expenditures (CapEx) and operational expenditures (OpEx) [13]. It also paves the way for the end game realization of the 5G virtualized network functions (VNF), or cloud architecture, which will allow for advanced network management techniques like network slicing or on demand functionality for updated or novel deployments.

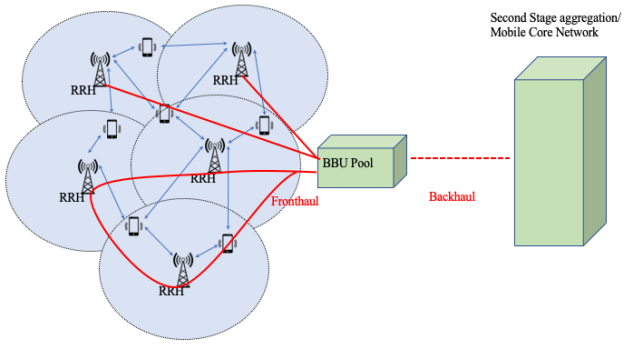

Figure 2: Example of C-RAN Architecture

3.2. Interface Update and Replacement

The fronthaul network of the C-RAN as characterized by LTE, uses common public radio interface (CPRI), an industry cooperation. CPRI establishes the key, physically

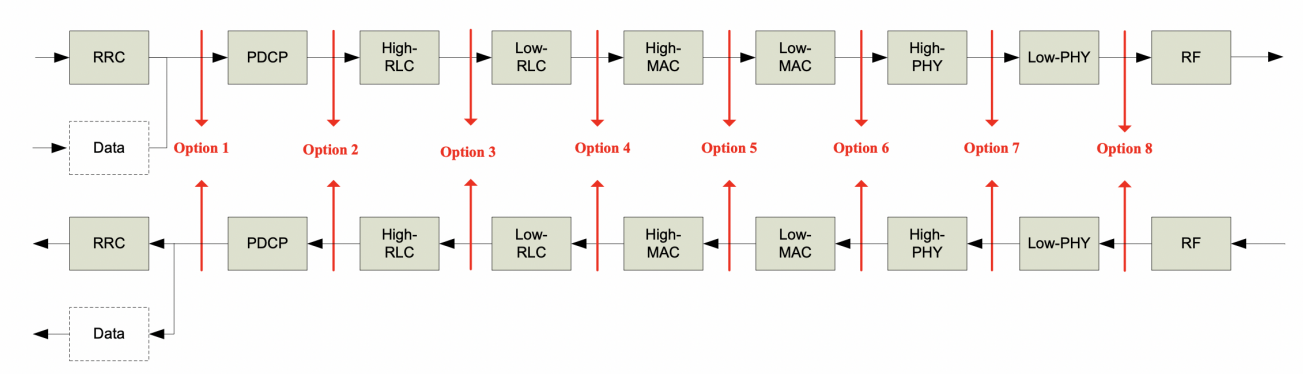

Figure 3: Proposed Physical Layer Splits [14]

separate portions of the traditional base station, defined as the radio equipment control (REC) and radio equipment (RE), which correspond to and are referred to throughout as BBU and RRH, respectively [15]. The BBU encompasses the digital baseband radio functions, while the RRH carries out analog radio frequency tasks. This allows for the spatial separation as defined previously. CPRI links, which make-up the fronthaul, are fiber connections that transport the digitized radio frequency signals between the RRH and BBU [16]. Though this legacy interface offers savings in cost per RRH, it would also require a dramatic increase in capacity required primarily due to the targeted data rate and massive multiple-input multiple-output (MIMO) configuration. The interested reader will find the calculation of the required fiber capacity detailed in [17], which reports 147.5 Gbps for a particular network scheme, while [18] reports 236 Gbps for another. Along with these values being difficult to attain in real-world deployments, another disadvantage is that these capacity requirements are fixed regardless of the actual network traffic volume, which belies the promised efficiency of the network. To find the balance between capacity, latency, and network customizability, the concept of functionally splitting the layer protocols was introduced. Figure 3 depicts the physical layer split (PLS) architecture as defined by 3rd Generation Partnership Project (3GPP) [14]. All functions to the left of a split lie with the BBU, while those to the right lie with the RRH.

Currently, the Institute of Electrical and Electronics Engineers (IEEE), 5G Infrastructure Public-Private Partnership (5GPPP), 3GPP, and the CPRI group are all working to develop a novel fronthaul, based on this PLS architecture. The CPRI group's answer to this call is the enhanced CPRI (eCPRI). This interface bases its PLS off of an option 7/2 fronthaul/backhaul, in which all radio link control (RLC) and media access control (MAC) layer functions are held at the BBU, lower physical layer functions, such as modulation, fast Fourier transform, and resource-mapping are delegated to the RRH [19]. The BBU then sends data to the remainder of the backhaul utilizing UDP, IP, and Ethernet protocols.

We assume for our network an option 7 split in accordance with the eCPRI structure and current industry opinion [20], [21].

4. Timing Management in 5G

The 4G and 5G TA command is used to ensure time-domain synchronization between the UE and the RRHs. Additionally, the TA command is unencrypted and therefore does not guarantee confidentiality. Previously, in LTE, each incremental TA, N_{TA}, had a pre-determined time value that depends on LTE's base unit of time, T_s. Furthermore, T_s depends on the static subcarrier spacing (SCS) LTE employs (15 kHz) [22]. The T_s value is defined as

$$T_s = \frac{1}{\Delta f_{ref} \times N_{f,ref}} = \frac{1}{15 \times 10^3 \times 2048} \approx 32.6 \text{ nsec.}$$

Each incremental TA accounts for 16 of these base units of time such that

$$N_{TA} = 16T_s.$$

This time unit earns its relevance as companies and users continue to leverage LTE infrastructure during the slow offramp towards 5G [23]. Finally, the legacy one-way distance resolution, r, is

$$r = \frac{cN_{TA}}{2} = 78.125 \text{ meters}$$

where c is the speed of light in meters per second [24]. Finally, the distance resolution represented by each TA in LTE is 78.125 m, corresponding to 5G's smallest SCS. However, 5G New Radio is expected to employ new, dynamic SCS values termed "numerologies" [23], [25]. Therefore, a new base unit of time, Tc, has been introduced in [25] which 5G new radio will employ, such that

$$T_c = \frac{1}{\Delta f_{max} \times N_f} = \frac{1}{480 \times 10^3 \times 4096} \approx .51 \text{ nsec.}$$

Thus, relating the two base time units between the standards, [26] introduces κ defined as

$$\kappa = \frac{T_s}{T_c} = 64.$$

TABLE 1: μ and it's corresponding one-way TA distance resolution.

μ	Distance Resolution (meters)	Subcarrier Spacing (kHz)
0	78.125	15
1	39.06	30
2	19.53	60
3	9.77	120
4	4.88	240

Therefore, in 5G's new scheme, each incremental TA value represents an uplink (UL) transmission time delay or transmission time advance equivalent to

$$N_{TA} = \frac{16\kappa T_c}{2^{\mu}}.$$

Where the 2^{μ} factor accounts for the subcarrier spacing. In other words, N_{TA} is conditional upon SCS designated by the value of μ. The new SCS are multiples of the LTE SCS where the new SCS = $2^{\mu} \times 15$ kHz for $\mu \in [0, 4]$ [26].

Thus, the new distance resolutions are determined similarly as before, however they change depending on the SCS such that

$$r = \frac{cN_{TA}}{2} = \frac{\frac{c16\kappa T_c}{2^{\mu}}}{2} = \frac{78.125}{2^{\mu}} \text{ meters.}$$

In 5G, the TA distance resolution is variable and conditional upon μ. Table 1 summarizes the new distance resolutions.

4.1. Timing Advance Group

The Timing Advance Group (TAG) [27] is a 2-bit field that uniquely associates each TA command with a different RRH, up to 4. The mechanism's usefulness stems from that fact when the UE communicates with multiple RRHs, it is very unlikely that the UE will be equidistant from all the servicing RRHs simultaneously. The benefit of communicating with multiple RRHs is that it increases bandwidth and data rates to and from the UE. Carrier aggregation enables the UE to transmit using multiple component carriers simultaneously [28]. Therefore, in order to maintain timing synchronization with each of the RRHs, the TAG associates when the UE should correctly transmit its uplink to the RRH in order to maintain time synchronization with each RRH [29].

Despite the foregone conclusion for multilaterations apt use as a localization technique, utilizing TAs within the traditional LTE framework as a valid method for localization is sparse within the literature. Only in the last few years have researchers shown through simulations and analysis of real-world data, the efficacy of this type of attack, employing the same multilateration method [30]. Our analysis of the effectiveness of the TA within the 5G ultra-dense C-RAN environment complements these previous endeavors, as well as supports the need for further scrutiny of and regard for the user's location privacy.

5. Attack Framework

As stated above, this exploit uses multilateration through the TA units associated with the victim, to perform what is known as a localization attack [14]. In a legacy LTE network, the adversary could position themselves in a way to collect the most amount of information on a target of interest through the open-air interface. Due to the ultra-densification, tight beamforming, large antenna arrays, and use of massive MIMO that makes up the 5G network, this paradigm is made ineffective. However, the aforementioned layer 2 information still undesirably travels unencrypted through the wired fronthaul, only shifting the location of the vulnerability in the network. This framework carries multiple inherent assumptions on adversarial capabilities that are as follows:

1) general knowledge of which BBU pool is servicing the victim,
2) the ability to tap into the fronthaul fiber, and
3) knowledge of the cell-radio network temporary identifier (C-RNTI).

With these assumptions established our adversary has everything required to run our algorithm and be supplied with a most likely estimate of the victim's current position, as demonstrated in the following section.

6. Simulation Environment

Initially, we used a Poisson point process to distribute the RRHs around the target UE. However, since location accuracy is solely a function of the relative angular geometry between the RRHs, we then decided that an arbitrary field density is more appropriate. Therefore, we uniformly distributed either 2, 3, or 4 RRHs in a two dimensional space surrounding the target UE. Generating a larger subset of the infinite process was unnecessary to only then sort them by distance to the UE and finally choose the closest RRHs. Therefore, two main parameters are considered through this investigation. They are the number of RRHs the UE is communicating with and the numerology (i.e., SCS or symbol duration). We have chosen to limit the number of RRHs communicating with the UE to either 2, 3, or 4, which can be supported by the use of the TAGs. According to [23] the numerology varies between 15kHz and 240kHz depending on the BW allocation.

Then, we send each of the 10 possible combinations of supporting RRHs and numerology through our simulation. First, we create a 100,000 km^2 area in which to place our RRHs. Then, we modelled the locations of the RRHs as a uniform random variable and placed them within our simulated testing area. Next, we calculated the TA value that was assigned to the UE from each RRH. For example, if the UE were communicating with 3 RRHs then there would be 3 separate TA values, each associated with its own RRH.

Because the TA value is unique for range of distances, there is an aspect of uncertainty that is introduced. The RRH does not know whether the UE is on the fringe of a TA range, or in the center of a TA ring. In LTE, each TA corresponds to a distance of 78.125 meters from one TA to the next. However, with the largest numerology in 5G, the TA values have shrunk the area of uncertainty (i.e., TA ring width) to 4.88 meters. Thus the TA resolution will be much more accurate and the ability for a RRH to localize a UE has increased significantly.

Now that we have the associated TA with each of the supporting RRHs, we are effectively able to draw rings with a width equal to the distance resolution around each of the RRHs. These rings are the area of uncertainty and account for all of the possible locations of the UE. Clearly, the UE would be contained within, or on the boundary of, the intersection of all the TA rings. In order to estimate the position of the UE p we employed the Non-Linear Least Squares (NLS) method presented in [31] and [32]. Briefly, that involves us minimizing the value of x in the following

$$p = \arg\min_{x} \sum_{i=1}^{N} \left[d_i - \|x - x_i\| \right]^2$$

where d_i is the distance from each RRH to the middle of its respective TA ring. The variable i is an integer value from 1 to N, which is representative of the total number of RRHs supporting the target UE. Lastly, x_i are the locations of the RRHs themselves.

We normalize the position of the UE to be in the center of the plane of possible RRHs locations. We know that this same center point must be contained within the area that represents the points containing all the possible locations of the UE, so that is where we had the NLS algorithm start looking for the UE. In other words, we had the NLS algorithm beginning at the position of the UE, and then measure how far the algorithm diverges from that point, once it stabilizes.

Then, once the NLS algorithm converged on a location, we computed the distance error (i.e. the distance between the UE and the NLS solution.) After simulating one million trials for each of the 15 aforementioned combinations, we generated their respective cumulative distribution functions (CDFs) to better compare the performance results. The respective CDFs are a graphical representation of the likelihood that the position of the targeted user is within a specific distance of the position estimate. For example, using the CDF, one could make a statement that there is an 90% chance that the user is located within 5 meters of a certain position.

Lastly, for simplicity in presenting the argument, this model assumes perfect noise conditions. In real-world scenarios the results would likely be less accurate. Noise conditions are ignored here in order to highlight the specific effect of SCS on distance resolution and localization.

TABLE 2: Location Error Probabilities using 2 RRHs across all numerologies.

μ	**Subcarrier Spacing (kHz)**	**90% Confidence Location Error (m)**	**95% Confidence Location Error (m)**
0	15	168.72	317.46
1	30	85.41	165.71
2	60	42.98	84.42
3	120	21.50	42.48
4	240	10.75	21.36

TABLE 3: Location Error Probabilities using 3 RRHs across all numerologies.

μ	**Subcarrier Spacing (kHz)**	**90% Confidence Location Error (m)**	**95% Confidence Location Error (m)**
0	15	56.29	78.57
1	30	28.21	39.33
2	60	14.14	19.71
3	120	7.06	9.85
4	240	3.53	4.92

TABLE 4: Location Error Probabilities using 4 RRHs across all numerologies.

μ	**Subcarrier Spacing (kHz)**	**90% Confidence Location Error (m)**	**95% Confidence Location Error (m)**
0	15	41.18	49.12
1	30	20.57	24.61
2	60	10.29	12.27
3	120	5.14	6.14
4	240	2.57	3.08

7. Results

As one might expect the scenarios where there are more RRHs yielded better results. In this case, there is more information to use regarding the location of the UE. Additionally, as the numerology increases, so too did the accuracy of the location estimate. We have tabulated the 90% and 95% location error (i.e., circular error probability (CEP)) values for each of the RRH scenarios in Tables 1, 2 and 3. Of note, in the case with 3 RRH, the 95% CEP coincide with the TA distance resolutions for each numerology. This could simply be because it includes the majority of position estimates while discarding outliers, however further research is ongoing.

When comparing the values between Tables 4 and 5, we have an average performance increase from 3RRHs to 4RRHs of 27.1% at the 90% confidence level and a 37.5% increase in performance at the 95% confidence level, regardless of numerology. That is because as the numerology increases, it effectively halves the area of uncertainty. Therefore, the effect is the same across all numerologies.

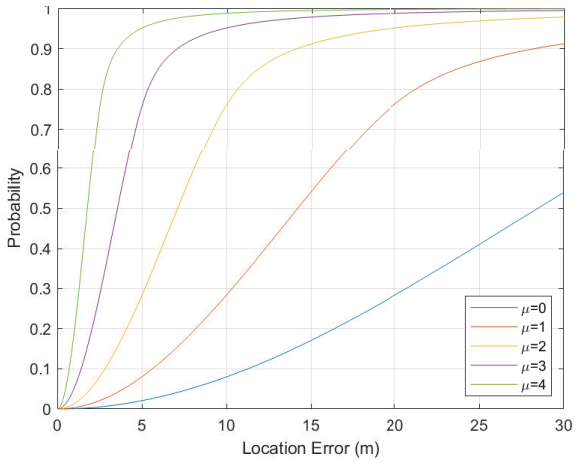

Figure 4: 3 RRH CDFs across all numerologies. (n=1 million).

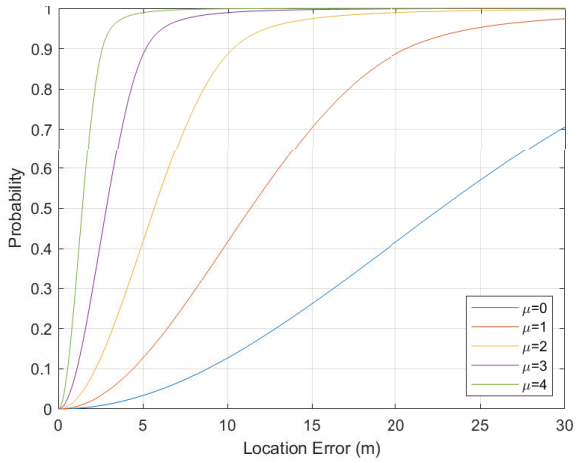

Figure 5: 4 RRH CDFs across all numerologies. (n=1 million).

Additionally, we can see that the incremental trend from one numerology to next is akin to halving the location error. This outcome is likely due to the same reasons that there is constant performance increase from 2 to 3 RRHs, and 3 to 4 RRHs. This observation holds for all cases of the number of RRHs at both confidence levels.

The most accurate location estimation scenario occurs in the situation with 4 RRHs supporting the UE, all of which are transmitting with the largest numerology. Here, one could localize the UE to within 2.57 meters with 90% confidence and to within 3.1 meters with 95% confidence.

However, if you lose one RRH, the 90% confidence error expands to 3.53 m and the 95% confidence error grows to 4.92 m. Therefore, we must take a closer look at the less-than-favorable scenarios where we have fewer RRHs and a lower numerology. Using the LTE numerology (i.e. $\mu = 0$) and just 3 RRHs increases the 95% confidence error to 78.5 meters.

There is a significant performance increase when going from 2 RRHs to either 3 or 4 RRHs. Consider a TA circle defined by the midpoint between the TA rings, and centered at the location of the RRH. Then, in the 2 RRH case, the NLS algorithm will always find the TA circles' intersection point closest to the target UE, when it exists. Thus, the accuracy is mostly a function of the relative position of the two RRHs. At the 90% confidence level, we have an average performance increase of 67% when using 3 RRHs instead of 2, and a 75.95% increase when using 4 RRHs instead of 2. And at the 95% confidence level, we have performance increases of 76.4% and 85.3%, respectively. In other words, using 4 RRHs vice 2, reduces the 95% confidence area of uncertainty by 85.3%. Therefore, in either case, we have dramatic performance increases just by adding even a single extra RRH. Again, we observe the halving of the confidence location error with each incremental increase in μ.

In Figures 6, 7, and 8, we depict the CEP [33] for six

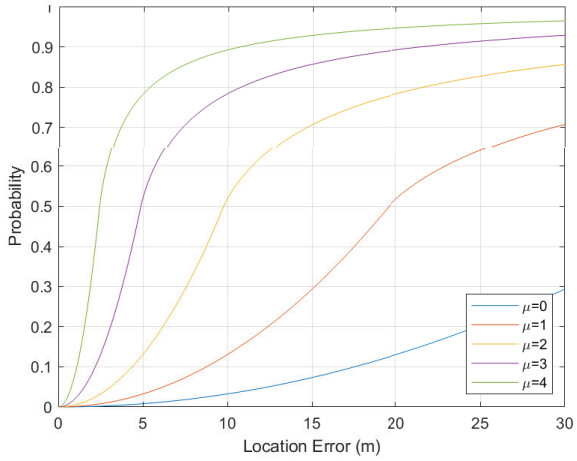

Figure 6: 2 RRH CDFs across all numerologies. (n=1 million).

different cases. The CEP[1] is a tool used for showing the use of location distance error and the confidence location error [34]. The six different cases are the combinations between 2, 3, or 4 RRHs used and the lowest and highest numerologies. Thus, in each case of the number of RRHs, we shows the highest and lowest fidelity of distance error. The blue markers in each image are the estimated position of the targeted UE over 1,000 trials. 1,000 was chosen arbitrarily to be used for demonstration purposes. In fact, the authors used one million trials to generate the previously described CDFs. The targeted users actual position is normalized to the centered of the graph and is depicted as a red asterisk. Finally, the red rings indicate the area with which we can confidently say that the target UE is within. In each of the presented examples, roughly 90% of all the estimates points

[1]CEP 70%: $\Pr[\|\hat{p} - p\|_2 < C] = 0.7$

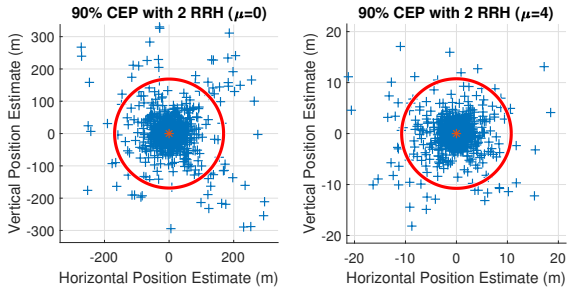

Figure 7: 90% Circular Error Probability (CEP) using 2 RRH with numerologies $\mu = 0$ and $\mu = 4$.

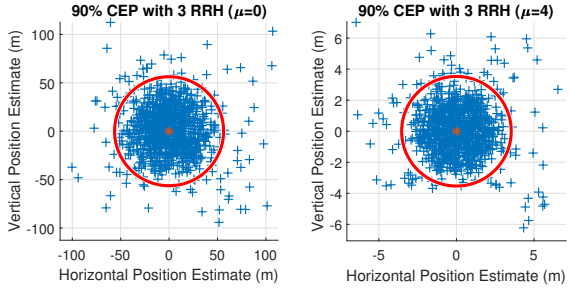

Figure 8: 90% Circular Error Probability (CEP) using 3 RRH with numerologies $\mu = 0$ and $\mu = 4$.

fall withing the CEP. Therefore, the smaller the circle, the more accurate of a location estimate. The radius of the rings can be extracted from the corresponding rows and columns Tables 2, 3, and 4 above. For example, the radius of the circle in the right graph of Figure 8 is 2.57 meters, which corresponds to $\mu = 4$ and 90% confidence in Table 4. At first glance, it may appear that all of the scenarios generate the same results. However, the distinction between them manifests itself in the horizontal and vertical axes. In order to avoid overcrowding of points within the graphs, the authors chose to separate the instances by numerology, as well as the number of RRHs. Additionally, we felt it necessary to rescale the graphs. Otherwise, the distinction between points within, and outside of, the circles may be lost.

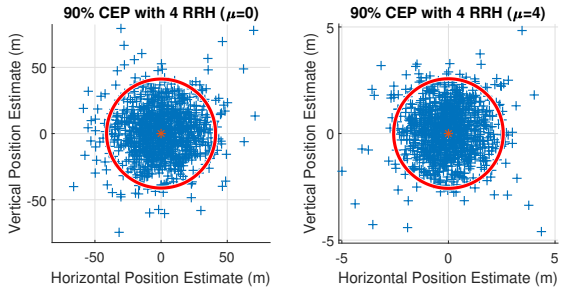

Figure 9: 90% Circular Error Probability (CEP) using 3 RRH with numerologies $\mu = 0$ and $\mu = 4$.

8. Recommended Mitigation Techniques

This attack is entirely reliant on two basic ideas:

1) Data being transferred from RRH to BBU is not encrypted in the form of in-phase and quadrature (I/Q) data.
2) C-RAN fronthaul fiber network

This is where we will focus our mitigation efforts. The first requirement has a seemingly easy solution. If the PLS option is altered to include Layer 2 functionality at the RRH, then eCPRI's built in security measures already associated with IP, IPsec, and Ethernet, MACsec, could be implemented when sending the data across the fiber fronthaul. This measure carries an added benefit in that it further reduces the capacity requirement of the fiber fronthaul. However, this added complexity at the RRH will have an adverse affect on cost and complexity of network deployments, which will in turn increase cost for the end user, dispelling support for this option.

5G's lauded physical layer security potential through heterogenous networks, massive MIMO, directionality through beamforming, and larger antenna arrays, are made inefective by the overall C-RAN structure. The layer of security provided by these methods, no longer matter if all the data from thousands of RRHs in an area are being routed to a single centralized source. There would be no need to attempt the rigors of overcoming these security methods, if the fiber fronthaul can be collected on. This is to say that without the first mitigation in place, or a verifiable way to stop adversaries from collecting the data within the fiber fronthaul, the C-RAN architecture itself presents a security concern.

9. Conclusion

Aggregating TA information, as is the case using a C-RAN architecture, could present a possible location privacy

vulnerability. Here, we've shown that it is possible to localize a user should an actor compromise the 5G infrastructure and gain access to that user's metadata. Moreover, the more information a user has, as in the cases with more RRHs, combined with the increased SCS, allows for ever greater localization resolution. Therefore, as 5G networks slowly start to come online, the technologies it employs could lead to ever more accurate user location data. Finally, we presented some mitigation methods to prevent against such an attack.

References

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

[2] J. Shaw, "Exposed: The erosion of privacy in the internet era," *Harvard Mag.*, 2009.

[3] Reporter of Decisions, "Syllabus: United States v. Jones," *Supreme Court*, Oct. 2011.

[4] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," in *IEEE Communications Surveys Tutorials*, 2018, pp. 1124–1148.

[5] J. D. Roth, M. Tummala, J. C. McEachen and J. W. Scrofani, "On location privacy in LTE networks," in *IEEE Transactions on Information Forensics and Security*, 2017, pp. 1358–1368.

[6] M. Dohler et al., "Internet of skills, where robotics meets AI, 5G and the tactile internet," in *2017 European Conference on Networks and Communications (EuCNC)*, 2017, pp. 1–5.

[7] G. D. G. S.-G. A. Shahmansoori, G. E. Garcia and H. Wymeersch, "Position and orientation estimation through millimeter-wave MIMO in 5G systems," in *IEEE Transactions on Wireless Communications*, 2018, pp. 1822–1835.

[8] L. Barkuus and A. Dey, "Location-based services for mobile telephony: a study of users privacy concerns," in *Proc. of INTERACT, 9th IFIP TC13 Int. Conf. on Human-Computer Interaction*, 2003.

[9] Federal Commun. Commission, "Report and order and further notice of proposed rulemaking on revision of the FCC rules to ensure compatibility with enhanced 911 emergency calling systems," pp. 96–264, 1996.

[10] Federal Commun. Commission, "Second report and order on wireless E911 location accuracy requirements," pp. 10–176, Sep. 2010.

[11] "Fourth report and order on wireless E911 location accuracy requirements," pp. 15–9, Jan. 2015.

[12] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "Location privacy in LTE: A case study on exploiting the cellular signaling planes timing advance," in *IEEE Communications Surveys Tutorials*, 2017.

[13] "Evolving to an open C-RAN architecture for 5G, author=S. Perrin, booktitle=Heavy Reading, year=2017."

[14] 3GPP TR 38.801 (V14.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on new radio access technology; Radio access architecture and interfaces (Release 14)," Mar. 2017.

[15] "C-RAN: the road towards green RAN," China Mobile Research Institute, Tech. Rep., 2013.

[16] CPRI Specification V7.0, "Common Public Radio Interface (CPRI); Interface Specification," Oct. 2015.

[17] "Common public radio interface." [Online]. Available: http://www.cpri.info/

[18] C. Ranaweera, E. Wong, A. Nirmalathas, C. Jayasundara and C. Lim, "5G C-RAN architecture: A comparison of multiple optical fronthaul networks," in *2017 International Conference on Optical Network Design and Modeling (ONDM)*, 2017, pp. 1–6.

[19] eCPRI Specification V1.2, "Common Public Radio Interface; eCPRI Interface Specification," Jun. 2018.

[20] A. M. Corporation. (2018, Feb.) Cloud RAN and eCPRI fronthaul in 5G networks. [Online]. Available: https://medium.com/5g-nr/cloud-ran-and-ecpri-fronthaul-in-5g-networks-a1f63d13df67

[21] Xilinx. Xilinx discusses fronthaul challenges for the 5G optical network. [Online]. Available: https://www.youtube.com/watch?v=UPucJcDAfSk

[22] 3GPP TS 36.211, release 15, (v15.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 15)," Mar. 2019.

[23] N. Instruments. (2018) 5G new radio: Introduction to the physical layer. [Online]. Available: http://www.ni.com/en-us/innovations/wireless/5g/new-radio.htmlwhitepaper

[24] R. Kreher and K. Gaenger, *LTE signaling: Troubleshooting and Performance Measurement*. John Wiley Sons, Inc., 2016.

[25] 3GPP TS 38.211, release 15, (v15.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Physical channels and modulation," Mar. 2019.

[26] 3GPP TS 38.213, release 15, (v15.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Physical layer procedures for control," Mar. 2019.

[27] 3GPP TS 36.321, release 15, (v15.5.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification," Mar. 2019.

[28] E. Dahlman, S. Parkvall, and J. Skold, *4G LTE-Advanced Pro and the Road to 5G*. Elsevier Ltd., 2016.

[29] S. P. E. Dahlman and J. Skold, *5G NR the next generation wireless access technology*. Elsevier Ltd., 2018.

[30] TechnoCom, "TruePosition indoor test report," Jun. 2014.

[31] I. Guvenc and C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," in *IEEE Communications Surveys Tutorials*, 2009.

[32] J. J. Caffery and G. L. Stuber, "Overview of radiolocation in CDMA cellular systems," in *IEEE Commun. Mag.*, 1998, pp. 38–45.

[33] D. J. Torrieri, "Statistical theory of passive location systems," in *IEEE Trans. Aerosp. Electron. Syst.*, 1984, pp. 183–197.

[34] K.W. Cheung, H.C. So, W.-K. Ma, and Y.T. Chan, "Least squares algorithms for time-of-arrival-based mobile location," in *IEEE Transactions on Signal Processing*, 2004, pp. 1121–1128.