Positioning in 5G Networks - Overview and Security Threats

Lukas Wittmer, Leander Seidlitz, Jonas Andre*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: lukas.wittmer@tum.de, seidlitz@net.in.tum.de, andre@net.in.tum.de

Abstract—**Determining your position is something humans always wanted to do. In present times many different technologies, like GPS, assist this process. As Satellite-based positioning struggles in environments where the sky is obstructed, like forests or indoors, new technology has to cover these areas. This technology is positioning via the 5G mobile communications network as the 5G coverage grows better and better. This paper will provide an overview of positioning metrics, like Time-of-Arrival measurements, and the approaches to determine an exact location from these measurements. Furthermore this paper gives an overview of the security aspects of the 5G positioning ecosystem. This overview includes possible attack targets, like the Location-Information-Service-Provider, and possible threats to the system and their consequences. These threats range from interferences to Man-in-the-Middle-Attacks by an active attacker, which can steal or alter the location information of a user.**

Index Terms—**5G networks, positioning, security**

1. Introduction

With 5G rising in popularity and its coverage growing dense, other features than communication are becoming much more viable. One of these features is the increased usability for positioning a device located in the 5G network. This is especially useful in indoor environments where traditional positioning techniques like the Global Navigation Satellite System (GNSS), better known as one of its subsystems GPS, fail to provide sufficient coverage. This paper aims to explain the basics of 5G-based positioning by covering the most relevant metrics and approaches to archieve an accurate position estimate. Furthermore, as security is and always will be a relevant topic in mobile communications, this paper will explore the different threats and attack targets a 5G positioning system offers.

1.1. Related Work

With 5G positioning being a topic of current research, an increasing number of papers have been published dealing with different aspects of position estimation using the 5G infrastructure. Some of these papers deal with similar topics to this paper and are referenced in the following section.

A paper that is similar to this paper is "Positioning in 5G and 6G networks—A Survey" by Mogyorósi, Revisnyei et al. [1]. It provides an overview of positioning methods while focusing on machine learning assisted approaches. It also provides an outlook on the influence of the introduction of 6G on the presented approaches.

Another paper with a similar topic is "A Look at the Recent Wireless Positioning Techniques With a Focus on Algorithms for Moving Receivers" by Tahat, Kaddoum et al. [2]. This paper deals with the general use of wireless networks for positioning. The wireless networks that are referenced in this paper include Bluetooth, WLAN and RFID.

The book " A comprehensive guide to 5G security" by Liyanage, Madhusanka et al. [3] deals with the security aspect of 5G positioning. After giving an overview of positioning mechanisms in 5G, it deals with threats to security in the 5G positioning network. It also provides an overview of the security mechanisms of 5G that help to mitigate the mentioned threats.

2. Measurement Modes

Positioning in mobile environments can be done in different ways. These ways differ in the active communicators, like the base stations, the device whose position is to be estimated and possible other devices helping with the positioning. They also differ in the devices calculating the distance.

The first measurement mode to be presented, is network-centric positioning. In network-centric positioning the network is doing the computation, while the device to be located is sending signals needed for measuring and receiving its estimated position. For the user device to use the estimated position in e. g. a navigation application, the position data has to be sent to the device via the network. A graphic representation of this approach can be seen in Figure 1 (a).

In device-centric positioning, the roles of the network and the device are reversed. While the network sends measuring signals, the device receives them and does the position computation on its own. Therefore, no position estimates need to be sent over the network, which is beneficial to privacy (more on that in Section 5). An example of a device-centric architecture can be seen in Figure 1 (b).

While device- and network-centric positioning are two opposed approaches, both can be supplemented by cooperative positioning. In Figure 1 (c) one can see that while doing cooperative positioning, other devices, that are not base-stations of the network can also send measurement signals or their position estimates to the device to be located. This additional data increases the accuracy of the estimated position.

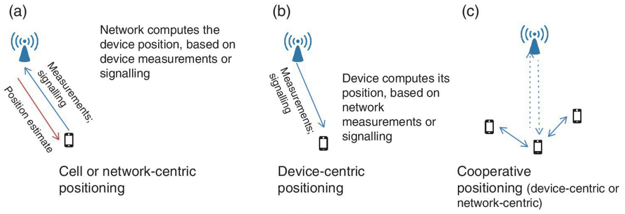
(a)
Network computes the device position, based on device measurements or signalling
Measurements; signalling
Position estimate
Cell or network-centric positioning
(b)
Measurements; signalling
Device computes its position, based on network measurements or signalling
Device-centric positioning
(c)
Cooperative positioning (device-centric or network-centric)

Figure 1: Different measurement modes [3]

In the rest of this paper network centric positioning will be used as the default measurement mode, but the metrics and approaches presented, work with other modes. The explanations in this chapter are based on [3, Chapter 13].

3. Position Metrics

The metric that takes the least computational effort that can be used to estimate the position of a device is whether its present within a certain base station's range. This metric is known as Cell-ID and can be used to give a rough position estimation of the device as described by Larsson in [4].

A metric for accurate positioning is the Time of Arrival (ToA). When the sending time of a signal is known, the time in flight of the signal can be calculated. From this, the distance between the origin of the signal to the receiver can be computed. This metric needs the sender and receiver to sync their clocks, in order to provide accurate measurements. The modus operandi for such a measurement is described by Van Haute, Verbeke et al. in [5].

When synchronisation of receiver and sender is not feasible, ToA measurements are not possible. If the distance measurement should still use time as its primary measurement, the time difference between the arrival of multiple signals, known as Time Difference of Arrival (TDoA), can be used. In this approach, the receivers still have to be synchronised, but no synchronization between the sender and receiver is necessary. A brief overview of TDoA measurement is given by Tahat et al. in [2].

Another metric for positioning is the Angle of Arrival (AoA) or Direction of Arrival (DoA). This metric uses the fact that base stations receive the same signal on multiple antennas. The angles at which the signal arrives at the receiver can be computed by measuring the time difference with which it arrives at the different antennas of the receiver. When this measurement is combined with the knowledge of the distance between the antennas at the receiver, the angle of Arrival can be computed, using trigonometric functions. A more in-depth analysis of this metric is provided by Tuncer and Friedlander in [6]. This metric is supported by 5G in particular, as 5G base-stations are equipped with up to thousands of antennas, providing a good basis for AoA measurements [1].

The Received Signal Strength (RSS) is one of the oldest metrics used in positioning. This metric dates back to 1969, as it was developed as a method to locate moving vehicles, e. g. police cars as stated by Figel, Sheperd and Trammell in [7]. This metric uses the fact that the signal strength scales with the distance it has to traverse. The method to derive a distance from the strength of the received signal is described by So and Lin in [8]. A problem with RSS as a metric is that it is susceptible to environment interference, as described in [2].

4. Approaches to Positioning

As the different metrics explained in the previous chapter, except for the Cell-ID approach, compute only a distance or an angle but no location, these measurements need to be processed further. This processing can happen differently based on the chosen approach.

4.1. Cell-ID-based Positioning

Cell-ID-based positioning is a basic form of positioning in mobile networks. In this approach the location of the connected base station is assumed as its location, as described by del Peral-Rosado, Raulefs et al. in [9]. However, this technique is imprecise in regions with low population density and sparse cell coverage as a single base station covers a large area in these regions. Better accuracy can be archieved by this method, if multiple base-stations are combined [1]. If a device is or was recently present in more than one base-stations cell the area in which the device is probably located can be narrowed down to the area that is covered by both base-stations.

4.2. Angle-based Positioning

Angle-based positioning is one of two approaches that use geometric properties. It uses the AoA metric to determine the position of a device. With the position of the base station and the angle at which the signal arrived, a Line of Bearing (LOB) can be computed. If the LOBs of multiple base stations are combined, the device can be positioned at the intersection of the lines. As the intersection of lines only requires two LOBs, two base stations are sufficient for an angle-based positioning approach [2]. More base-stations can help to improve the accuracy by eliminating outliers or false measurements. This approach is also known as triangulation. A challenge to the angle based approaches are the non line of sight (NLOS) conditions. The NLOS conditions are that without a line of sight between the device and a base station the accuracy of the corresponding measurement drops dramatically, which can lead to a wrong position estimation due to multipath propagation of the signal. Multipath propagation describes the reflection of a radio signal from surfaces and can therefore existence of multiple paths from the sender to the receiver. This results in different angles from which the signal can arrive. Approaches using ToA or TDoA (see Section 4.3 and 4.4) also struggle with NLOS conditions but not to the extent of angle based approaches, as there are methods to mitigate their effects in timing based systems.

4.3. Range-based Positioning

Another approach that uses geometric properties is range-based positioning. This approach uses the distance

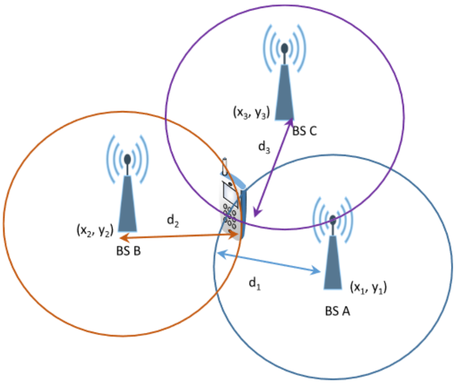

Figure 2: Range-based positioning with RSS or ToA [2]

from the device to multiple base stations. This distance can be derived from time measurements (ToA or TDoA metric) or signal strength (RSS metric). Range-based positioning needs at least three involved base-stations, instead of the two needed by angle-based positioning. While the geometric representation for the position estimation involving RSS and ToA is using the intersection of three circles around the base stations, with the respective distances as radii, also known as trilateration (as seen in Figure 2) the TDoA approach instead uses the intersection of hyperbolas around the base stations as no ranges but only range differences are know [2].

4.4. Fingerprinting-based Positioning

While the previously mentioned approaches use ad hoc measurements, fingerprinting-based positioning uses another method to estimate positions. The typical procedure for this approach consists of two phases: the offline or training phase and the online phase. During the training phase, the observed area is divided into a grid of measurement points. Multiple measurements of the chosen metric are then acquired at each measurement point. These metrics can be any metric from Cell ID to RSS, but some, like RSS, are more suitable to be used by a fingerprinting approach. These metrics are combined in a fingerprint that is identifying each measurement point. These fingerprints are inserted into a database that is used during the online phase. In the online phase the same measurements are repeated and combined into another fingerprint. This fingerprint is matched against the fingerprints within the database generated in the offline phase. As these measurements are influenced by NLOS conditions (Section) 4.2), the measurements are extended to minimize the effect of these conditions. As the grid divides the measurement area into discrete intervals, but the position is on a continuous scale, the coordinates of the nearest points are averaged to find the position. This procedure is described using RSS measurements by Yu, Jiang et al. in [10].

4.5. AGNSS Positioning

Assisted Global Navigation Satellite System (AGNSS) positioning is an approach that uses the mobile network differently than others. Its primary use is for indoor positioning, while still using a Global Navigation Satellite System (GNSS) like GPS. As these systems struggle to lock onto their positioning satellites while indoors due to effects like NLOS conditions (Section 4.2), additional data transmitted via a 5G network can help the devices to lock onto the satellites. The functionality of AGNSS is described by Mautz in [11].

5. Security

As a device's location is sensitive information, it attracts the attention of parties that want to abuse it. This abuse can range from location-specific advertisements without the users' permission, to attackers altering the reported location of a device to steal it. To better understand the vulnerability of the 5G positioning system, the attack targets and security threats are shown in the following sections.

5.1. Attack Targets

In the 5G positioning network, every participant can be an attack target, but not every target is equally susceptible to every threat. The three main categories of targets in attacks on 5G positioning are the Location Information Service Provider (LISP), the Location Based Service Provider (LBSP) and the User Equipment (UE). The UE can be divided further into the end-user equipment and the Location Information Collaborators (LIC).

The LISP is the provider of the positioning infrastructure, e. g. the base stations that either send out the measurement signals in device-centric positioning or receive the measurement signals in network-centric positioning. They also provide the LBSP access to their positioning database, if the positioning is network-centric. In a device-centric environment the location is provided by the device itself.

The LBSP, on the other hand, is the provider of the service the UE needs its location for. This service can be a navigation app, a running app or even the tracking of autonomous robots in, e.g. a factory.

The end-user device is by far the most commonly known participant in the system. This device can be any device with access to the 5G network, like a mobile phone, a car with a built-in SIM-Card or a mobile robot in a factory.

The LIC is an optional participant in the system as its only present in a cooperative positioning environment. LICs can be from the same device spectrum as the end-user device and help the end-user device estimating its position, as 5G allows device-to-device communication. While using an LIC can improve the accuracy of position estimation, it is also the device type with the greatest potential to be malicious.

Figure 3 shows important traffic that for position estimation, like position or service data, is transported via the UE. This fact makes the UE a prime target for attacks on location privacy.

5.2. Security Threats

The threats to security in the 5G positioning system can be categorized by the participants they affect. These

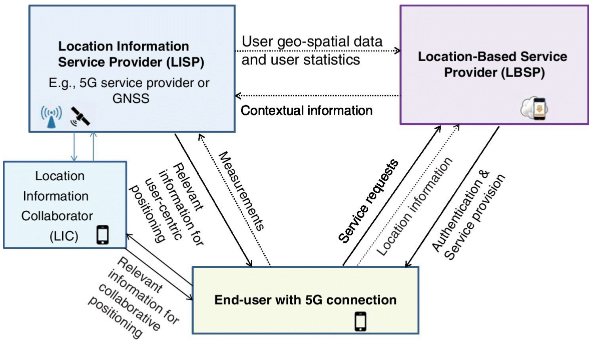
Location Information Service Provider (LISP)
E.g., 5G service provider or GNSS
User geo-spatial data and user statistics
Contextual information
Location-Based Service Provider (LBSP)
Location Information Collaborator (LIC)
Relevant information for user-centric positioning
Measurements
Service requests
Location information
Authentication & Service provision
Relevant information for collaborative positioning
End-user with 5G connection

Figure 3: 5G positioning targets [3]

threats can have different effects on the system, ranging from a financial loss at an LBSP, e. g. if a user can use the service without paying for it, up to position information theft, e. g. if a location database gets compromised.

The first category of threats are threats affecting multiple participants or every participant of the system. This category includes Denial-of-Service- or Distributed-Denial-of-service-attacks that saturate any participant, therefore making it unavailable for the whole system. Depending on the attacked participant, this can either decrease the estimations accuracy, e. g. if only a single base station is unavailable, or render the whole system inoperable, e. g. if the UE is saturated. Also in this category is the Man-in-the-Middle (MiM)-attack. In this context, the main target for a MiM-attack would be the communication between the UE and the LBSP, as this communication will include information about the location and authentication. An eavesdropping attack is also possible in a network-centric system. If an attacker has multiple nodes positioned in the area covered by the target UE it can record the measurement signals emitted by the UE and perform a TDoA, AoA or RSS measurement by itself. A ToA measurement is impossible in this scenario as the attacker is purely passive and therefore can not synchronize its clocks with the UE.

The next category includes threats that affect the LISP. One of these threats is the presence of malicious nodes in the system that send fake signals to the base stations, to create errors in the position estimate. Another threat to the LISP, that does not require an attacker, is interference. As 5G is using radio signals to send messages, these signals can be jammed either intentionally by an attacker, or unintentionally by other participants or natural causes, like a storm. The jamming of signals can alter or prevent measurements, making the positioning system unusable.

Threats that affect the LBSP are also a category of threats that the 5G positioning system has to deal with. This category includes the unauthorized use of the LBSPs service, either being unpaid use, in case of a paid service, by hijacking the signals or the misuse of the service, e.g. an employer tracking the phones of his employees to detect if they are working or not. Another threat to the LBSP is the leakage or theft of information from the LBSP database. This threat is a concern for privacy reasons, as the location of any user using an LBSPs service e. g. Google Maps, could be obtained if the location database is breached.

As stated in the closing paragraph of Section 5.1, the UE may be the prime target for an attack as it is the central part of the positioning calculation. It also is the weakest part of the system, from a security perspective, as the users of the UE tend to be careless about restricting how their data is used, as described by Gašparović, Nicolau and Marques in [12]. A threat that comes from this category is location-tracking malware that is installed directly on the UE. This malware can report the location of the UE without the user knowing. Another threat to the UE is the loss of accuracy when using a fingerprinting approach that can come from errors in the communication between the measuring UE and the LISP while building the database in the training phase. These errors, if not corrected, can lead to inaccuracies in the position estimation during the online phase of the positioning. Another threat for the UE, that is also a threat to the LISP, is interference, as they prevent both the LISP and the UE from communicating. Another threat that was mentioned above is location theft. When location theft is mentioned in the context of the UE, it is not about the location of a device becoming public but rather about a device reporting a fake location. This can result in e. g. identity theft if a user is authenticated via his location. A deeper explanation of these threats and others, as well as some methods for protection against them, can be found in [3, Chapter 13].

6. Conclusion and future work

We gave an overview of the current positioning metrics and approaches using the 5G mobile communications network. Additionally, we presented an overview of attack targets and threats to security in the 5G positioning ecosystem. The 5G system provides several metrics for position estimation, including Time-of-Arrival, Angle-of-Arrival and Received-Signal-Strength. Multiple measurements of these metrics have to be combined to result in an exact position. The approach and the metrics that are used for estimating the position determine the minimum of required base stations to determine an exact location. Range-based approaches, that use trilateration as their theoretical foundation, need three base-stations while angle based approaches, using the AoA metric and triangulation as their theoretical foundation, need only two base stations. Additional base stations can increase the accuracy by providing additional information or by elimination outliers, caused by interferences or NLOS conditions. From the security point of view, the system provides three main attack targets. The LISP, the LBSP and the UE, are susceptible to several threats, that are either unintentional, like interferences caused by storms, or intentional, like DoS-Attacks or MiM-Attacks by an adversary.

As the newer generation of mobile communications is rising on the horizon with 6G, it will be interesting to see what additional features for positioning come with it and how current metrics and approaches will be improved. Furthermore, it will be interesting to dive deeper into the security topic and analyse different concrete attacks on the mobile positioning architecture. Methods to prevent these attacks could be learned and the security of the infrastructure and location privacy could be improved. These two topics provide a first basis for possible future research and papers.

References

[1] F. Mogyorósi, P. Revisnyei, A. Pašić, Z. Papp, I. Törös, P. Varga, and A. Pašić, “Positioning in 5g and 6g networks—a survey,” *Sensors*, vol. 22, no. 13, p. 4757, 2022.

[2] A. Tahat, G. Kaddoum, S. Yousefi, S. Valaee, and F. Gagnon, “A look at the recent wireless positioning techniques with a focus on algorithms for moving receivers,” *IEEE Access*, vol. 4, pp. 6652–6680, 2016.

[3] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[4] J. Larsson, “Distance estimation and positioning based on bluetooth low energy technology,” 2015.

[5] T. Van Haute, B. Verbeke, E. De Poorter, and I. Moerman, “Optimizing time-of-arrival localization solutions for challenging industrial environments,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1430–1439, 2016.

[6] E. Tuncer and B. Friedlander, *Classical and modern direction-of-arrival estimation*. Academic Press, 2009.

[7] W. Figel, N. Shepherd, and W. Trammell, “Vehicle location by a signal attenuation method,” *IEEE Transactions on Vehicular Technology*, vol. 18, no. 3, pp. 105–109, 1969.

[8] H. C. So and L. Lin, “Linear least squares approach for accurate received signal strength based source localization,” *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 4035–4040, 2011.

[9] 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,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1124–1148, 2017.

[10] F. Yu, M. Jiang, J. Liang, X. Qin, M. Hu, T. Peng, and X. Hu, “Expansion rss-based indoor localization using 5g wifi signal,” in *2014 International Conference on Computational Intelligence and Communication Networks*. IEEE, 2014, pp. 510–514.

[11] R. Mautz, “Overview of current indoor positioning systems,” *Geodezija ir kartografija*, vol. 35, no. 1, pp. 18–22, 2009.

[12] M. Gašparović, P. Nicolau, A. Marques, C. Silva, and L. Marcelino, “On privacy in user tracking mobile applications,” in *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2016, pp. 1–6.