High-Band Related Threats in 5G Network

Giorgi Akhalaia [1] and Maksim Iavich [2]

[1] *Georgian Technical University, Tbilisi, Georgia, akhalaia.g@gtu.ge*
[2] *Caucasus University, Scientific Cyber Security Association. Tbilisi, Georgia. miavich@cu.edu.ge*

Abstract

The deployment of 5G networks, which has been prompted by the development of IoT, mobile devices, and AI, is expected to create a new ecosystem that incorporates various industries, including emergency services, security, and healthcare. Introduction of a new standard always brings new threats. As mobile devices are frequently used by end-users for everyday activities, the risk of sensitive data and personally identifiable information (PII) leakage is significantly increased. In this context, the research focuses on evaluating the privacy of end-users in relation to location-based services (LBS) threats in 5G networks. The study involved conducting various experimental works to determine the best method of locating a device without requiring additional permissions from the end-user. The results showed that using cell-towers for device location was more effective than the standard approach using the Global Navigation Satellite System (GNSS) method. The study also found that high-band operating spectrum could be used to determine device location with just one cell tower, rather than relying on information from a minimum of three visible cell-towers. The only limitation to this process is the switch function, which is responsible for ensuring smooth roaming between towers. The research aimed to determine how 5G network architecture affects end-user location privacy, identify which operating spectrum of 5G network is more vulnerable, and assess the extent of this vulnerability.

Keywords

LBS threats, 5G Network Threats, Device Tracking, User Privacy in 5G

1. Introduction

The world top tech manufacturers are facing challenges in making their products more portable and mobile to increase their usage. This trend is being driven by the extensive development of portable devices such as smartphones, IoT, and microcomputers like the Raspberry Pi and Arduino, which have become increasingly important in our daily lives. The development of these mobile devices has served as a catalyst for the improvement of telecom standards, prompting engineers to work on the 5th generation network (5G). The upcoming 5th generation network is a new telecom standard that will be more diverse by integrating various industries into a single network, which also increases the risk of cyber threats to the network. The focus of our research is to evaluate the location-based vulnerabilities of User Equipment (UE) within the 5G ecosystem. The 5G standard is designed to meet three key performance indicators: enhanced mobile broadband, massive machine type communications, and ultra-reliable low latency communication, which will surpass the limitations of traditional telecom communication and usher in a new era in mobile communication. However, this will require network engineers to make some software and technical changes to meet the requirements set forth by 3GPP. Therefore, our study aims to examine these modifications and assess how software/technical improvements affect the security level of devices in terms of location tracking. Our research objectives are:

28th Conference on Information Society and University Studies (IVUS'2023), May 12, 2023, Kaunas, Lithuania
EMAIL: gakhalaia@cu.edu.ge (G. Akhalaia); miavich@cu.edu.ge (M. Iavich);

- Dows a new architecture of 5G network effect on UE LBS privacy?
- Which of the 3 operating spectrum represents more vulnerable?
- To assess scale of this vulnerability.

2. Literature Overview

This paper presents ideas that have been thoroughly researched and developed, drawing on the latest scientific literature, technical documents, official reports, standard analyses, and overviews from world-leading companies and mobile network operators[1]. Experts were consulted to discuss major improvements, technical and design changes in 5G networks, as well as the various threats associated with them. To conduct experimental work during the research, the authors used a combination of various self-written tools and open-source projects that were readily available online[9]. Our research methodology combined both theoretical analysis and practical experiments to ensure its validity. While most similar research focuses on the standard methods of device tracking, such as triangulation or trilateration, our study aimed to enhance the efficiency of these methods. In this article, the authors are exploring the signal strength parameter as a means of approximating the location of a device. While some researchers believe that this method can achieve high levels of accuracy, others argue that the complexity of the system makes it difficult to determine whether signal strength is diminished by distance or other limiting factors. The key difference between our study and other articles is that we locate devices by predicting the frequencies they are operating on and intercepting their attachment requests to cell towers. Manipulating frequencies has been successfully demonstrated by other researchers, but the use of operating spectrum for device tracking has not yet been documented in scientific or practical journals. The concept of manipulating radio frequencies is related to research on mitigating RF pollution, which explores ways to reduce RF exposure indoors by employing various building materials. Our study builds upon this research by demonstrating that high frequencies can be utilized to track devices, a notion that was validated through our experimental work.

3. Methods of Locating Devices

There are various techniques of tracking the devices. Tracking involves determining the precise location of a device and its variations during a specific time frame. The fundamental concept for determining the location of a device using various methods is the same: a reference system is required, against which the User Equipment (UE) can calculate its coordinates. GNSS satellites or cell-towers are frequently used as reference systems. UE calculates its coordinates by processing data and measuring signals obtained from GNSS satellites or cell-towers. Arrival time, frequencies, signal strength, and angle are commonly used to determine device location. The accuracy of the mobile cell-towers depends mainly on the accuracy with which the telecom service providers configure them. In some regions, for emergency services like 9-1-1 or 1-1-2, the government regulates and mandates a specific level of cell-tower accuracy. [2]

Mobile positioning is a commonly utilized technology that serves a variety of purposes in daily life, such as checking in on social media, navigation, emergency and critical services, and advertising. Unfortunately, there are instances where hackers or unauthorized individuals attempt to track devices and end-users without permission. Our analysis focused on examining the GNSS techniques and cell-tower method for locating and tracking devices.

The Geodetic technique, which involves utilizing the Global Navigation Satellite System (GNSS), is the most precise and accurate method for determining a device's location on the earth. GNSS satellites emit signals from space, which GPS-enabled devices receive and process to ascertain their actual location (as shown in Figure 1). Only scientific, geodetic-level GNSS systems are capable of achieving millimeter-level accuracy and high precision, as they can use multiple signal types to overcome ionospheric effects and various types of noise. User-friendly devices, on the other hand, are generally

only compatible with the L1 band, which provides accuracy within a range of 3-5 meters, but is still adequate for tracking purposes. However, GNSS has some limitations, particularly for indoor use, where devices must have direct line of sight with satellites, which must also be in good geometric positions. The GNSS method is also commonly referred to as Global Positioning System (GPS) in some articles, with GPS being operated by the United States as the first satellite provider. Assisted-GPS (A-GPS) is a method where cell-towers are used for locating device. That is the best solution for in-door use, like in building or for underground use. But it has a lower accuracy than standard GPS method. (Figure 1, 2)

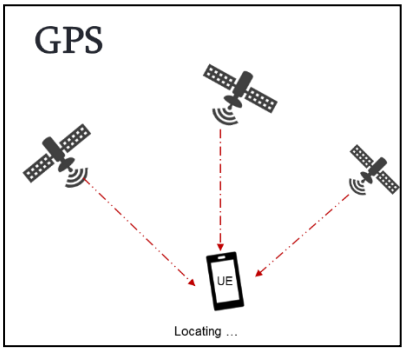

Figure 1: GPS Method

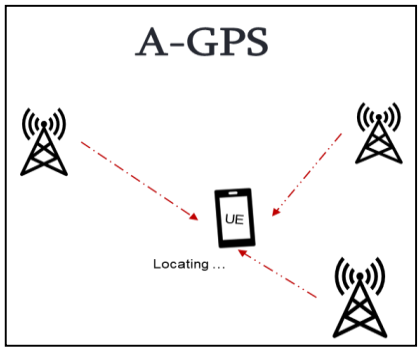

Figure 2: A-GPS Method

GSM network operators aim to establish a strong network coverage by strategically installing cell-towers with specific geometries. By determining the x and y coordinates of these cell-towers, a device can calculate its own location by relying on the coordinates of at least three visible cell-towers. Two commonly used techniques are triangulation and trilateration. In triangulation, two lines from the cell-towers to the UE and a third line between the cell-towers are used to create a triangle (as shown in Figure 4). The sides of the cell-towers and angles, such as Alfa and Beta, are already known. On the other hand, in trilateration, the distances are recalculated from each tower and the common area between them represents the estimated coordinates of the device (as shown in Figure 3). Some papers may refer to trilateration as distance measuring.

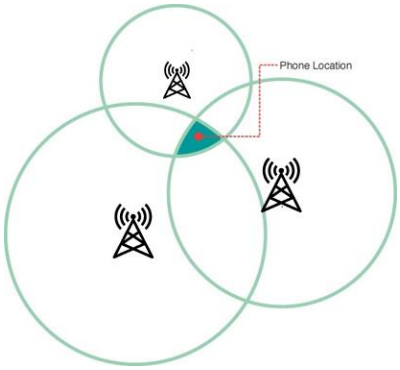

Figure 3: Trilateration Method

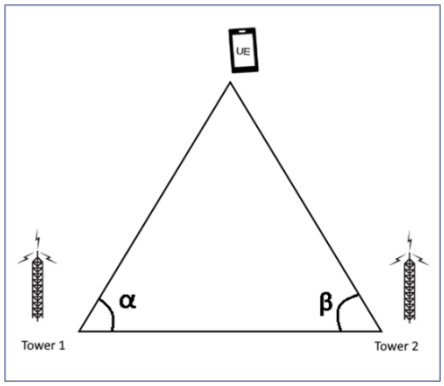

Figure 4: Triangulation Method

techniques. [2]. In the trilateration method (as illustrated in Figure 3), the possible locations of the device are represented by green circles, which denote the maximum coverage area of the tower for a specific radius. To determine the device's location, we must compute the intersection of these circles. This involves solving equations that take into account the distance between the device and each tower,

which enables the calculation of the device's estimated location within the overlapping area of the circles.

1. By using a 2D model, the equations for determining the device's location can be simplified and the calculations can be performed more efficiently.
   equations per circle:

$$(x - x_1)^2 + (y - y_1)^2 = r_1^2$$

$$(x - x_2)^2 + (y - y_2)^2 = r_2^2$$

$$(x - x_3)^2 + (y - y_3)^2 = r_3^2$$

2. Open parentheses for each eq.:

$$x^2 - 2x_1x + x_1^2 + y^2 - 2y_1y + y_1^2 = r_1^2$$

$$x^2 - 2x_2x + x_2^2 + y^2 - 2y_2y + y_2^2 = r_2^2$$

$$x^2 - 2x_3x + x_3^2 + y^2 - 2y_3y + y_3^2 = r_3^2$$

3. Rewrite the system using A,B,C,D,E,F

$$A_x + B_y = C$$
$$D_x + E_y = F$$

4. Solution for the system will be:

$$x = \frac{CE - FB}{EA - BD}$$

$$y = \frac{CD - AF}{BD - AE}$$

This is the simplified two-dimensional version of the trilateration [3]

4. Experimental Work

4.1. Collect GNSS data from the devices

We have conducted simulations for different scenarios to determine the most efficient method of tracking devices. With the abundance of software designed to steal data from devices on the market, we utilized storm-braker in our study. [4] Storm-Braker is a Linux-based open-source software that produces a malicious link to obtain the latitude and longitude coordinates of the targeted device. Nevertheless, this method has its limitations as it requires the GPS module to be enabled and the user's

permission. When attempting to extract GNSS data, end-users are repeatedly prompted with alerts such as "software/Link/Webpage wants to use device's location" (as shown in figure 9). It's worth noting that activating the GPS module is not obligatory for all devices, and many users disable the GNSS module to conserve battery life.

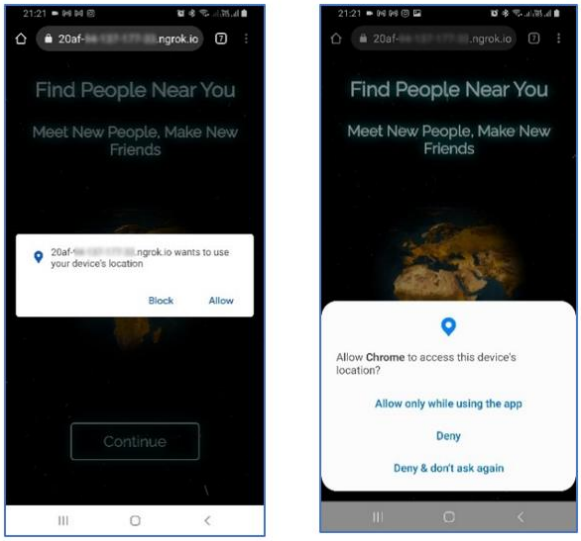

Figure 9: experimental study (GNSS)

Second important note is that, usually device does not track GNSS signals in background. Hence, when we need to track them using satellites, we have to enable GPS module and startup measurements process on device. Because of the security aspects, operating systems (like Android, Windows, iOS) automatically draws sign of "location", alerting user that GNSS measurement has been started. Therefor this method is very noisy. Also, because of the GNSS method limitations, if the victim is in building or at any other location, where they do not have "open sky", hacker cannot locate using satellites. Hence, according to the research this method is not the best solution for device tracking without user permission.

4.2 Gathering Cell-Towers using Smartphones

We leveraged the default transmission of information by cell-towers, which includes their Lat/Long coordinates and IDs, to gather and map the locations of all towers within the city.

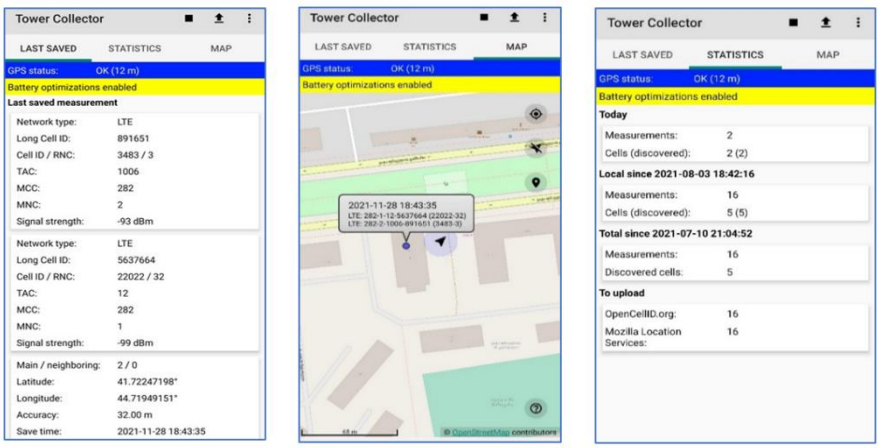

Figure 10: collecting cell tower information.

During our experimental work, we utilized an application called "Tower Collector", which can be found on the "Play Store" market. Figure 10 provides details on a particular tower, including its network type, which indicates that it is an LTE network tower. The RNC (Radio Network Controller) manages and controls the connected NODE BS and is responsible for encryption at this level. The LAC/TAC (for UMTS/LTE networks) serves as a unique identifier for the current location area, while the Mobile Network Code (MNC) identifies the network operator and the Mobile Country Code (MCC) identifies the country. Lastly, the Cell-ID represents a unique identification for the Base Transceiver Station (BTS) or sector for the specific LAC. [5]

The signal strength parameter is highly debated as a factor in determining device location due to its complexity. Various articles have explored its value in solving device location, but it can be influenced by a multitude of factors, making it difficult to interpret. Low signal strength may not always represent a long distance from towers and could be caused by external factors such as buildings interfering with radio waves. Figure 10 displays the results of our mapping of device location and towers, while Figure 10 presents the corresponding statistical information. Attackers can exploit the detailed information provided by telecom towers to map the entire network and attempt to track devices by collecting visible tower data from victims. It is worth noting that devices constantly search for cell-towers and switch to the tower with the strongest signal, and attackers can calculate approximate coordinates of the device by intercepting that information. The process of tracking cell-towers occurs in the background on devices, meaning that hackers do not need to initiate any additional software or hardware module (as required for the GNSS method) to track the device.

4.3 Locating device using mmWave (High-band)

The 5G standard requires significant changes to fulfill the requirements of 3GPP. with one of the most important changes being to the operating spectrum. The spectrum is divided into three categories, including the Low-Band, which operates below 1 GHz and is less affected by buildings, making it ideal for use in urban areas. However, this range has a bandwidth limitation of up to 100 Mbps. The Mid-Band, which operates from 1 GHz to 6 GHz, offers better bandwidth of up to 1 Gbps, but the signal from this range is more susceptible to interference from buildings. Lastly, the High-Band/mmWave operates between 6 GHz to 100 GHz and provides the best bandwidth in the 5G network at 10Gbps. However, this range is highly susceptible to interference from buildings. [1]

Based on our research, we have found that the limitations of the High-Band in the 5G network can be leveraged to locate devices using only one visible tower, as opposed to three visible towers. By combining two factors - firstly, that the High-Band range is greatly impacted by buildings and secondly, that devices constantly scan for cell-towers to find the strongest signal - we can assume that a device must be in close proximity to a mmWave tower to connect to it. Otherwise, the device will connect to a tower from a different category. As such, by extracting information from a device when it is connected or in range of a mmWave tower, we can estimate its location without needing data from three visible towers or a minimum of three visible GNSS satellites.

Our research team assumed that devices will generally not be connected to high-band due to their limitation with buildings and building materials. So, to test our assumption we simulated different cases when attacker controls victim’s device Switch Function, which manages smooth roaming between cell-towers. We forced devices to keep them connected on mmWave towers. We created a simulated map of cell-towers and found that when the device could not connect to a high-band tower, it was likely outside the coverage area and not in a populated area. With further processing, this information could be used to estimate possible device locations. We used Raspberry PIs with GPS and 5G antennas, Kali OS, and simulation software for their experiments. (Table 1).

Device	Quantity	Usage

Raspberry Pi with LTE and GPS Modules	10	5-For Base Station 3 - For Fake Base Station 2 - For User Equipment
Smartphone with GPS support	5	For User Equipment
Laptop	2	Manage and Monitor Experimental Work
Results		
Algorithm Type	**Success/Fail**	**Comment**
GPS (Catch data from UE)	Success	Success with noise if GPS module was enabled. User interaction was needed. As they were alerted by the system
A-GPS (Catch data from UE)	Success	10/10
MITM by Fake towers	Success	10/10
Stealing Frequency Info	Success	8/10

Table 1: Technical Details of experimental work

Figure 11: Raspberry Pis, with GPS and 5G Modules

It should be mentioned the LBS in 5G Network is not safe from MITM type of attack. [6] [18] This means that the possibility of fake towers exists, as discussed earlier. During emergency situations, telecom towers are used to determine the location of user equipment (UE), and the accuracy of the results depends on the quality of input data. The latitude and longitude coordinates of towers are a crucial factor in this equation. Therefore, if the network is compromised by fake towers that transmit falsified coordinates, the calculated location for the device will not be precise.

As experimental studies, we have conducted cyber-attack with the following conditions/case studies:

- We conducted an analysis of High-Band, mmWave frequencies and how they are impacted by various obstacles, including buildings and building materials
- Our analysis involved intercepting the attach request that the user device sent, which provided us with all the critical parameters for both the device and the cell-towers.
- Our actions resulted in the device being forced to always connect to High-Band frequencies in the 5G network
- Through our understanding of the tower locations, which cell-tower was serving the target device, and the limitations imposed by high-frequency radio waves, we managed to track the user using only a single tower.

5. Conclusion

The 5G Network's advancement is critical for the progression of existing services and future innovations. Successfully implementing secure networks will overcome existing limitations and unlock new opportunities. With the vast target market for 5G, hackers are bound to take an interest, making it crucial to prioritize working on security protocols, policies, and network design. Our analysis, both theoretical and practical, highlighted the vulnerabilities associated with location-based identification in 5G networks. Consequently, we conducted an experimental cyber-attack to supplement our theoretical findings.

According to our studies, the most accurate method of locating a device, the GNSS technique, is also the noisiest, as operating systems alert users when third parties attempt to steal GPS data. Moreover, this technique is ineffective when the GPS module is disabled. The second experiment revealed that stealing A-GPS information from the device is less noisy but requires information from at least three visible towers to solve the trilateration equation. The most fascinating experiment involved using the limitations of the 5G network's third category of operating spectrum to determine the device's location using only one tower instead of three. However, this approach may be disrupted by the Switch Function of the device, which connects to the tower with the strongest signal. To overcome this issue, we manually controlled the switching function and left the device on the third operating spectrum despite signal strength. Our experimental, successful cyber-attack confirmed the location-based vulnerabilities in 5G networks that must be addressed before widespread deployment.

6. Recommendations

As the recommendations, according to our studies, user devices should not connect to high-band 5G network the very first time. It should be redirected from middle or low-band operating spectrum. Which has coverage in longer distances, that will harden determining the device location. Security solution can be deployed in software of high-band network. They should not broadcast their lat/long in high precision, it should be done in a way to be protected from wardriving or any other techniques that are used to plot cell-towers.

7. Acknowledgment

The work was conducted as a part of PHDF-21-088 financed by Shota Rustaveli National Science Foundation of Georgia.

8. References

1. Huawei Technologies CO,. LTD in “5G Network Architecture – A high Level Perspective”, 2016
2. S. Asad Hussain, S. Ahmed, M. Emran, “Positioning a Mobile Subscriber in a Cellular Network System based on Signal Strength”, IAENG International Journal of Computer Science, 34:2, IJCS_34_2_13,2007. https://www.researchgate.net/publication/26492533
3. Cell Phone Trilateration Algorithm, Online Journal “Computer Science”, 2019. (Last access: 10.12.2021) https://www.101computing.net/cell-phone-trilateration-algorithm/
4. Ultrasecurity, “Strom-Breaked” (Software Package), (Last access: 8.12.2021) https://github.com/ultrasecurity/Storm-Breaker
5. Johhny, “How to find the Cell Id location with MCC, MNC, LAC and CellID (CID)”, 2015 https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid
6. M. Iavich, G. Akhalaia, S.Gnatyuk. Method of Improving the Security of 5G Network Architecture Concept for Energy and Other Sectors of the Critical Infrastructure, In: Zaporozhets A. (eds) Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control, vol 399. Springer, Cham. https://doi.org/10.1007/978-3-030-87675-3_14,
7. M. K. Maheshwari, M.Agiwal, N. Saxena, R. Abhishek. "Flexible Beamforming in 5G Wireless for Internet of Things”, in IETE Technical Review, 36:1, 3-16, DOI: 10.1080/02564602.2017.1381048, 2017. https://doi.org/10.1080/02564602.2017.1381048
8. M. Ivezic, L. Ivezic, “5G Security & Privacy Challenges” in 5G.Security Personal Blog, 2019. https://5g.security/cyber-kinetic/5g-security-privacy-challenges/
9. A. Shaik, R.Borgaonkar, S. Park, J.P. Selfert. ” New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities” in WiSec ’19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, DOI: 10.1145/3317549, ISBN: 9781450367264, 2019.
10. A. Purdy, “Why 5G Can Be More Secure Than 4G” in Forbes online journal, 2019.

https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/?sh=2ffcdf1657b2
11. Qualcomm Technologies inc. “What is 5G”, in online article. https://www.qualcomm.com/5g/what-is-5g
12. SK Telecom, in “5G architecture design and implementation guideline”, 2015.
13. M. Hanif, “5G Phones Will Drain Your Battery Faster Than You Think”, in online journal, 2020. https://www.rumblerum.com/5g-phones-drain-battery-life/
14. Samsung in online report “Samsung Phone Battery Drains Quickly on 5G Service” https://www.samsung.com/us/support/troubleshooting/TSG01201462/
15. Yusof, R., Khairuddin, U., and Khalid, M., ‘A New Mutation Operation for Faster Convergence in Genetic Algorithm Feature Selection’,In International Journal of Innovative Computing, Information and Control, Vol. 18, No. 10, 2012, pp 7363-7380.
16. The EU Space Programme (Last Access: 10.12.2021) https://www.euspa.europa.eu/european-space/eu-space-programme
18. Akhalaia, G., Iavich, M., Gnatyuk, S. (2022). “Location-Based Threats for User Equipment in 5G Network”. *Advances in Computer Science for Engineering and Education*. ICCSEEA 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 134. Springer, Cham. https://doi.org/10.1007/978-3-031-04812-8_11