Identification of the Location in the 5G Network

Giorgi Akhalaia

Caucasus University
Scientific Cyber Security Association

SCIENTIFIC CYBER SECURITY ASSOCIATION

კავკასიის უნივერსიტეტი
CAUCASUS UNIVERSITY

DEEPSEC.NET

Caucasus Cyber Security Center
Caucasus University

Vienna, Austria 2022

Short Biography

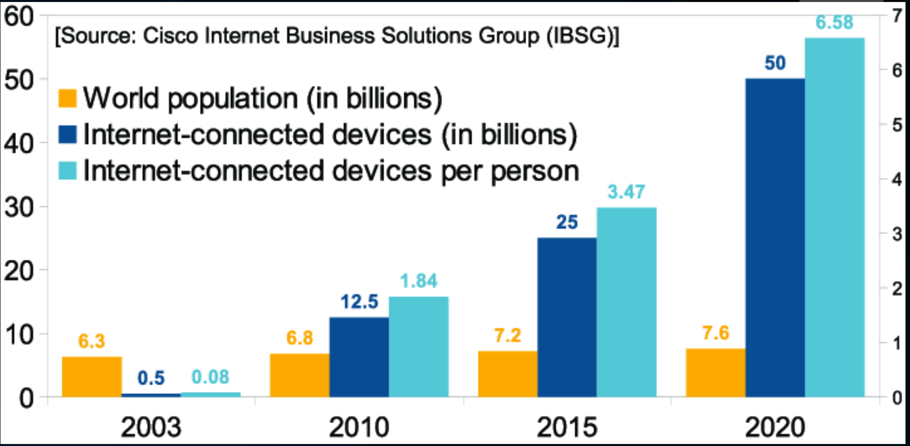
- Technical Director at Scientific Cyber Security Association
- Researcher at Caucasus University
- Cyber Security Main Specialist at Caucasus Cyber Security Center – Regional Representative of BITSENTINEL
- Head of Geodesy **and** Gravimetry Department at Ilia Stat University
  Manage Scientific GNSS Network of Georgia

Introductio n

Over the last decade rate of mobile device development has extremely increased.

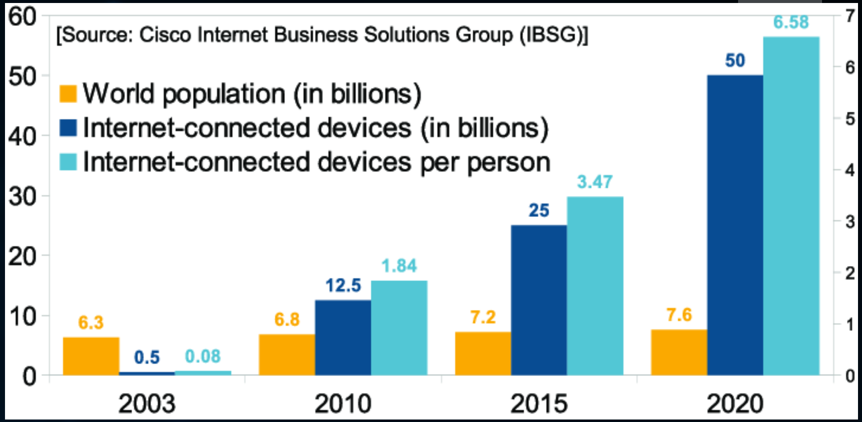
Microcomputers, smartphones, IoT devices can provide majority of everyday services, including emergency, security, healthcare, and education.

Development of mobile devices itself triggered the 5G network deployment. Which will create new ecosystem with variety of industries and will exceed the limit of telecom



Introductio
n

New standards, functionality, services, products always arise new cyber threats. Our research idea was to study location-based vulnerabilities for user equipment in 5G network.



Study objectives were to assess if new standard increased the risk of locating devices without their prior permissions.

We have compared existing location-based threats with newly arisen and assessed which one is more vulnerable.

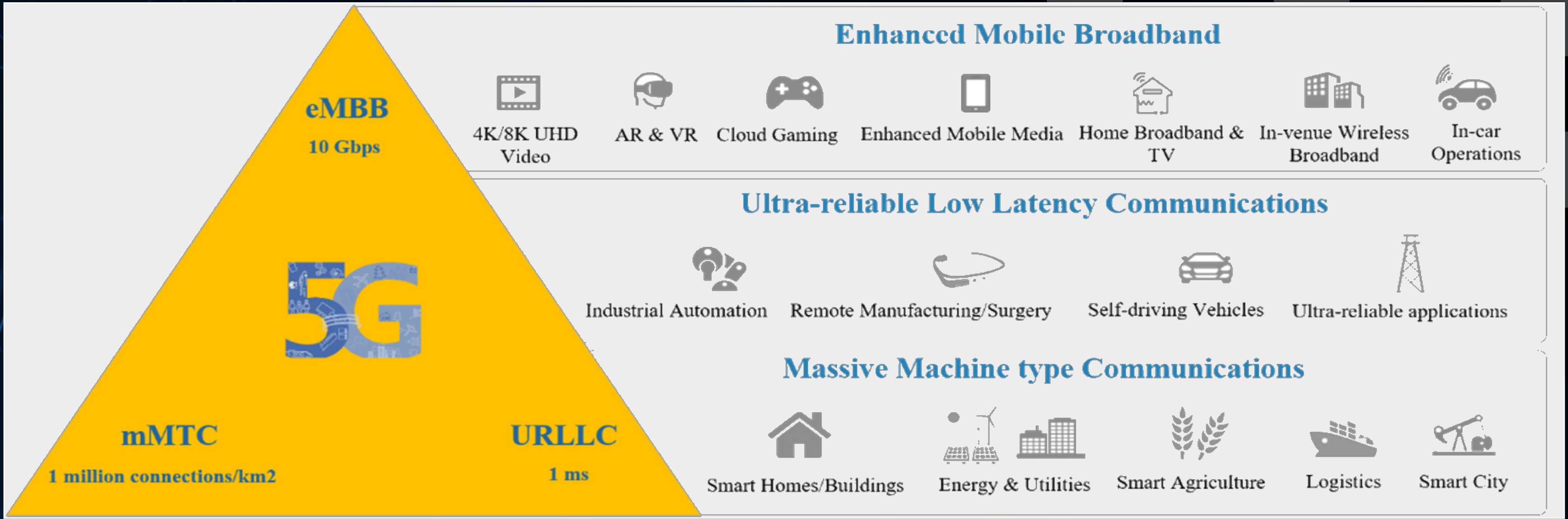
Objectives of Our Study

- Does 5G architecture affect on UE location privacy?

- Which Band is more vulnerable?

- Identify device location in mobile network using 5G vulnerability

5G Objectives and Target Groups



SK Telecom in "5G architecture design and implementation guideline"

- **eMBB - more than 10 Gbps**
- **uRLLC – up to 1 ms Latency**
- **mMTC – more than 1 million connected device for square km**

General Technical Changes

Operating Spectrum

Low-band -- < 1 GHz

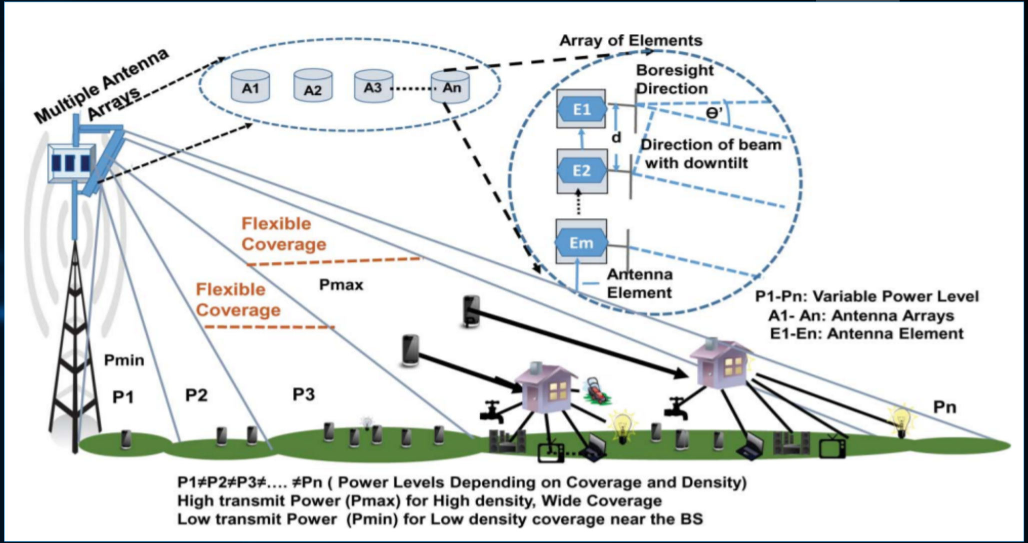
Frequencies from this range are less affected by buildings, so it is used in densely populated areas. However, bandwidth limitation of this band is about 100 Mbps

Mid-band -- 1 GHz – 6 GHz

This category has more bandwidth (about 1 Gbps), but also it is more affected by buildings, than Low-band

High-band -- 6 GHz – 100 GHz (mmWave)

This range will have the highest bandwidth and it is about several 10Gbps.



M.K Maheshwari in “Flexible Beam Forming in 5G Network”

Methods of locating Device

Concept of determining device location for different techniques is the same: reference system should be chosen and after that device calculates its coordinates.

Usually reference systems are GPS satellites or cell-towers.

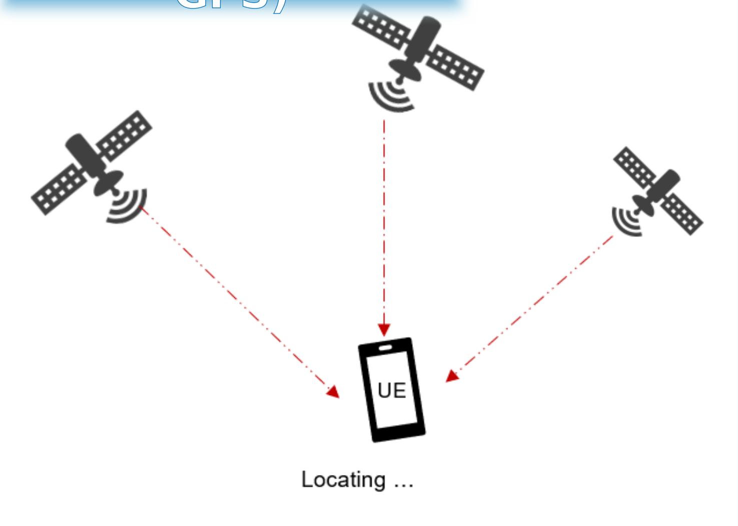
Device determines its location by measuring and processing signals tracked from satellites or cell-towers

Usually, frequencies, arrival time, angle and signal strength are used to locate device.

GNSS - **G**lobal **N**avigation **S**atellite **S**ystem

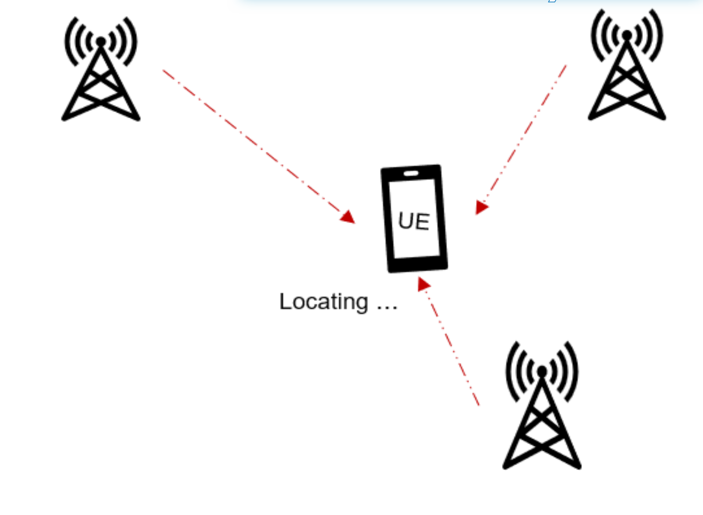
Locating Device

GNSS (also called GPS)



The most precise method, technique for determining device location is GNSS – Global Navigation Satellite System.

A-GPS (Cell-Towers)



A-GPS (Assisted GPS). This method uses cell-towers for locating device.

A-GPS

Trilateration

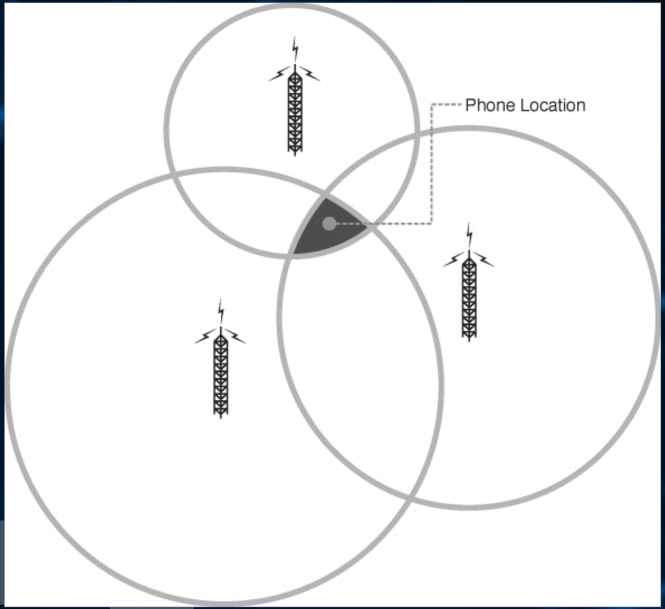


Illustration 1

Triangulation

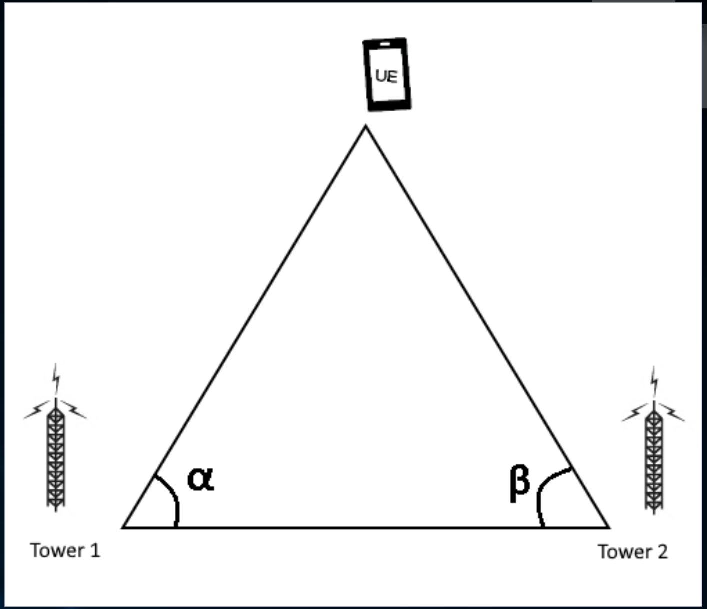
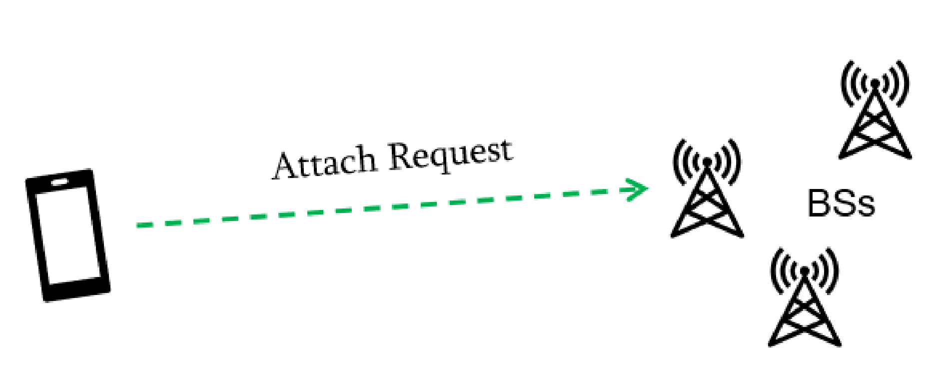


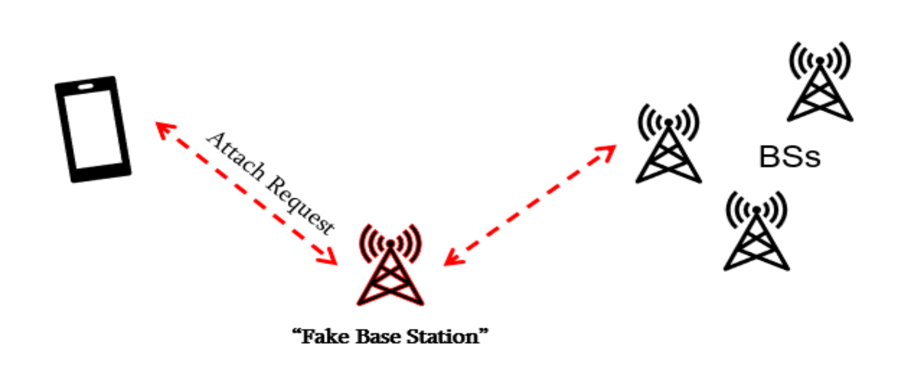
Illustration 2

Fake BS - MITM

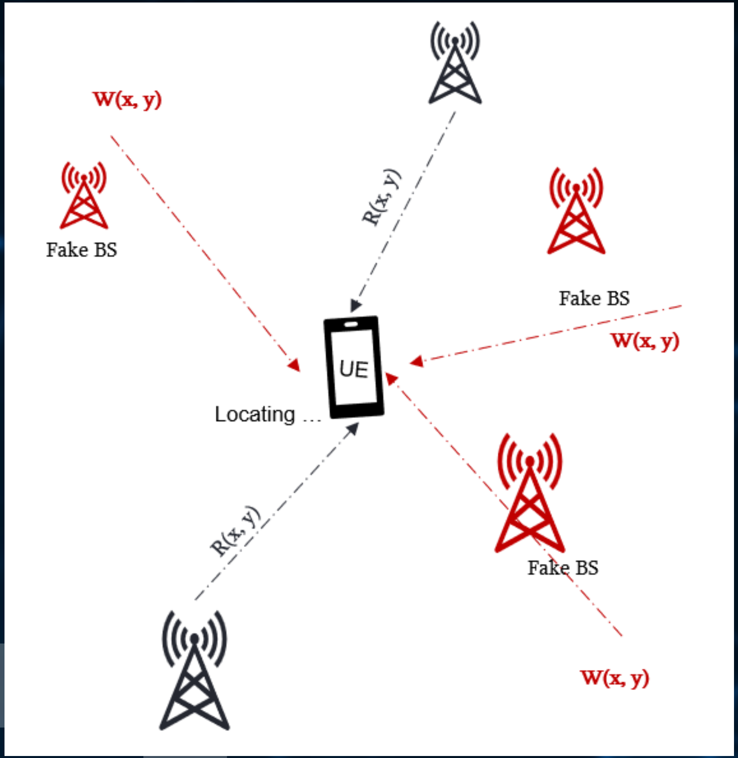
1. Attach Process (Normal Case)



2. Fake BS - MITM – in 5G Network:



Fake Base Stations in Network



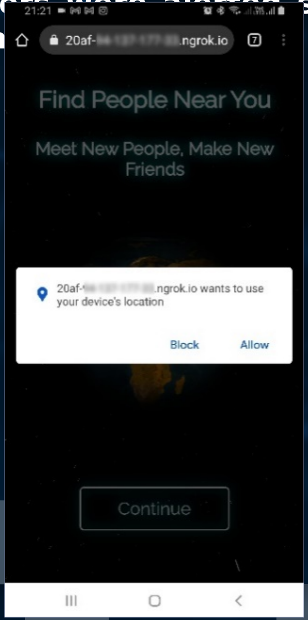
Fake base station cause low precision while locating device. Sometimes impossible to determine location

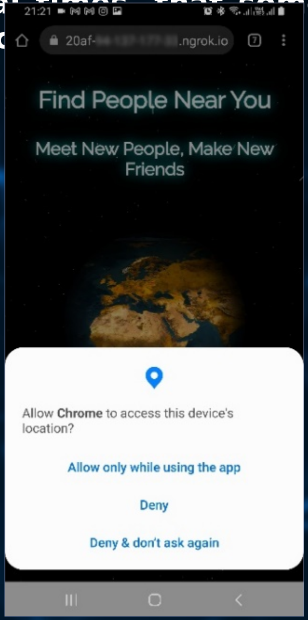
- Because of wrong inputs, device might be relocated or located with very low precision

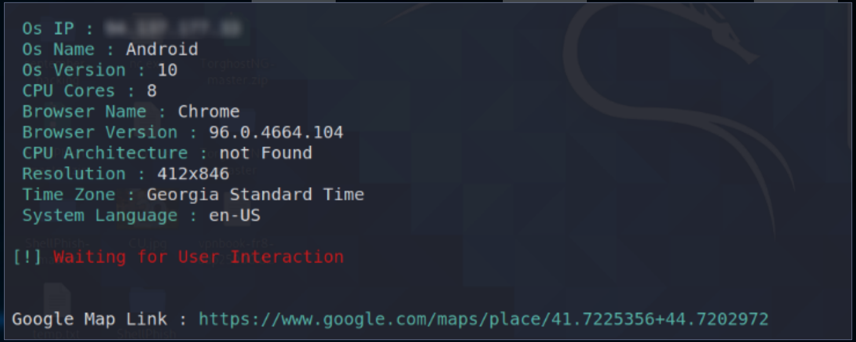
Experimental Work: Case 1: GNSS Method

During the experimental work we simulated different cases to determine, which technique is the easiest way to track the device.

We used Storm-Braker to steal the coordinates smartphone. As it tries to steal GPS information, users were alerted several times, that someone wa on loc

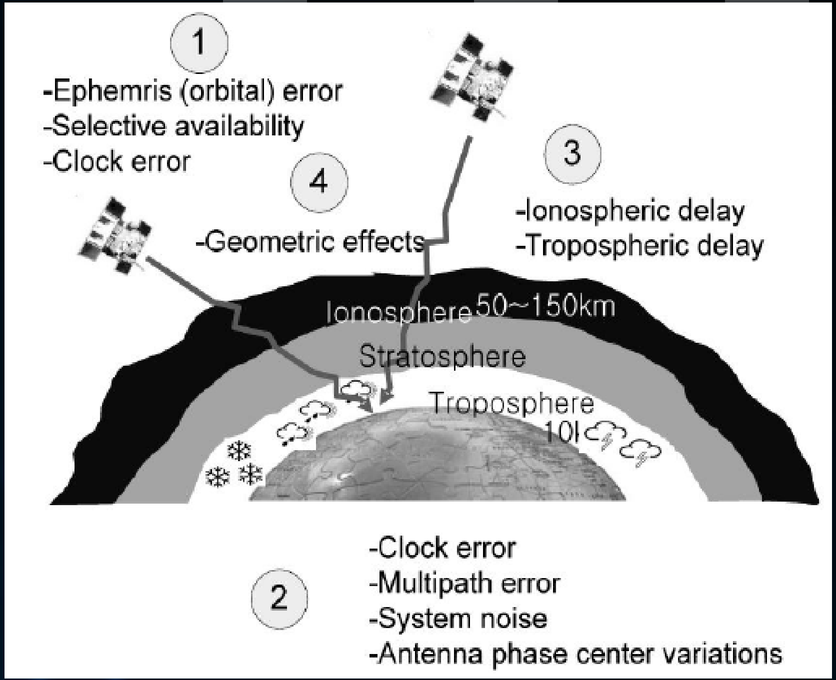






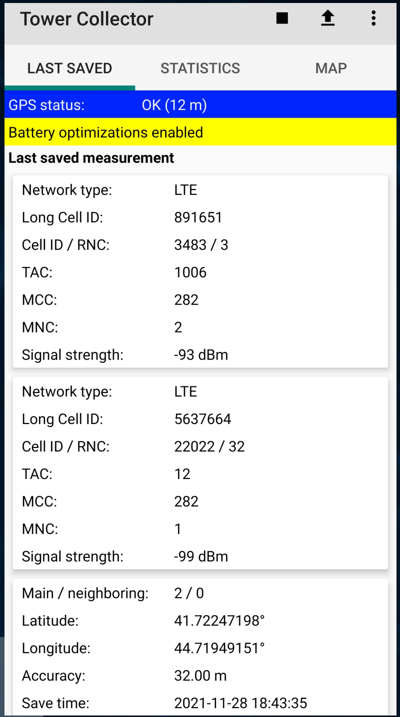
Limitations of this method

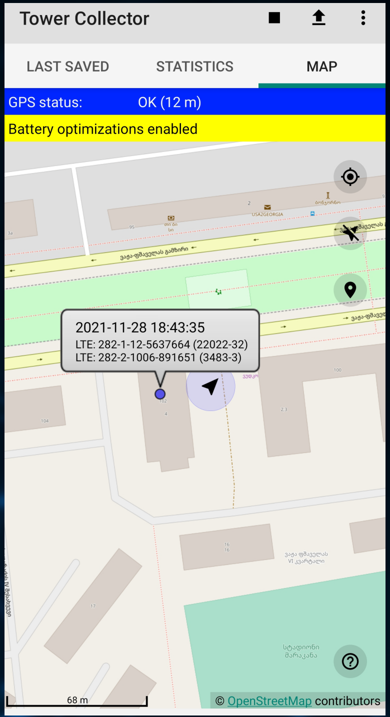
- Open sky is required for good satellite view
- Satellite positions should be with a good geometry
- TEC – should be considered
- Effects from earth atmospheric conditions
- GPS module must be an active
- User interaction is required !

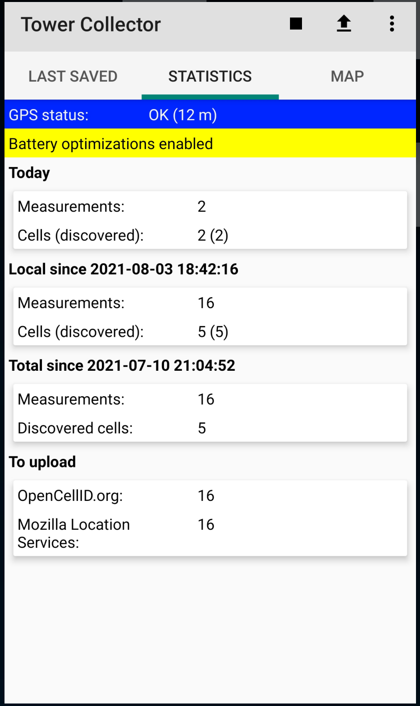


Case 2: A-GPS

Collecting Cell-Towers



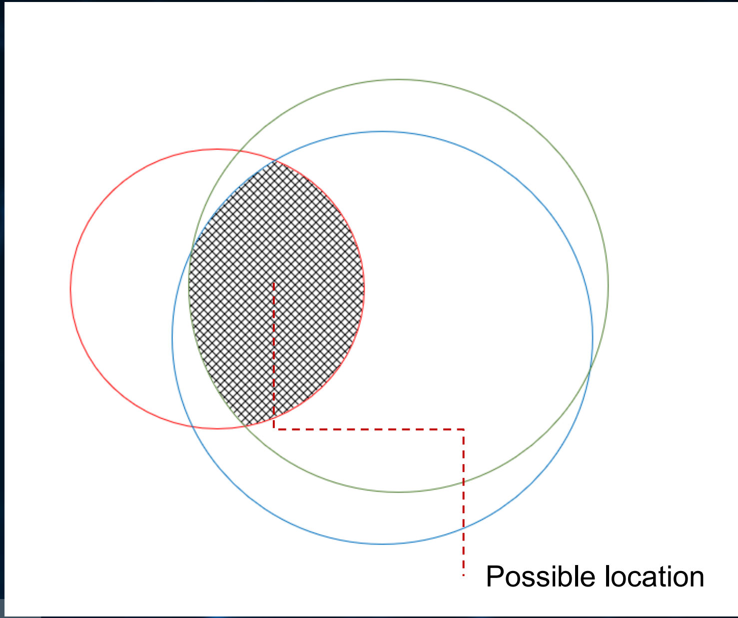


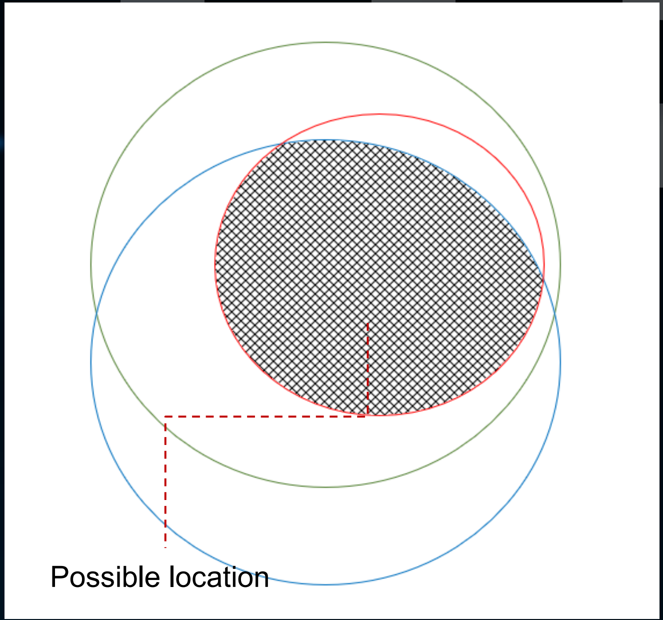


1. This method does not require to enable GPS module on mobile, as it uses data from cell-towers
2. Process of scanning cell-towers is always activated and running in background.

Drawbacks for Case 2

Mapping coverage circles of cell-towers





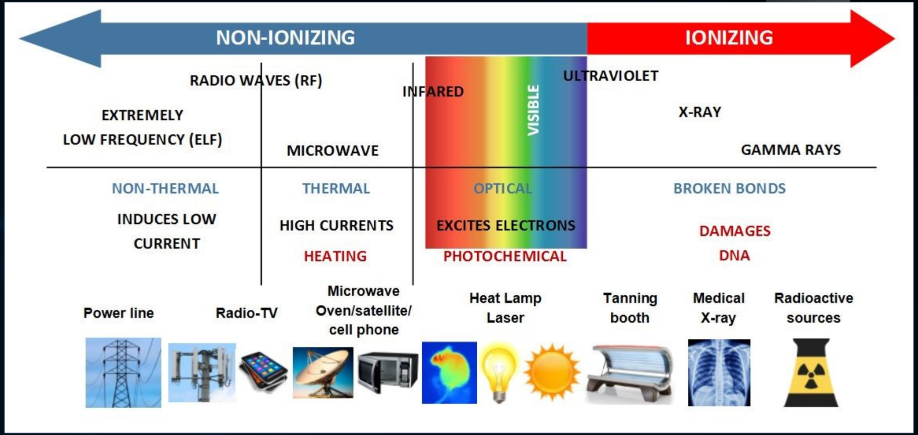
1. Towers that are very close to each other, might harden the process of locating device.

Radio Frequency

Electromagnetic fields represent significant component of the modem environment. It also called as an electroclimate

Radio frequency (RF) waves are a form of electromagnetic waves used in the communication bandwidths defined by the Federal Communications Commission (FCC)

With the widespread use of these technologies the exposure levels of electromagnetic field have raised.



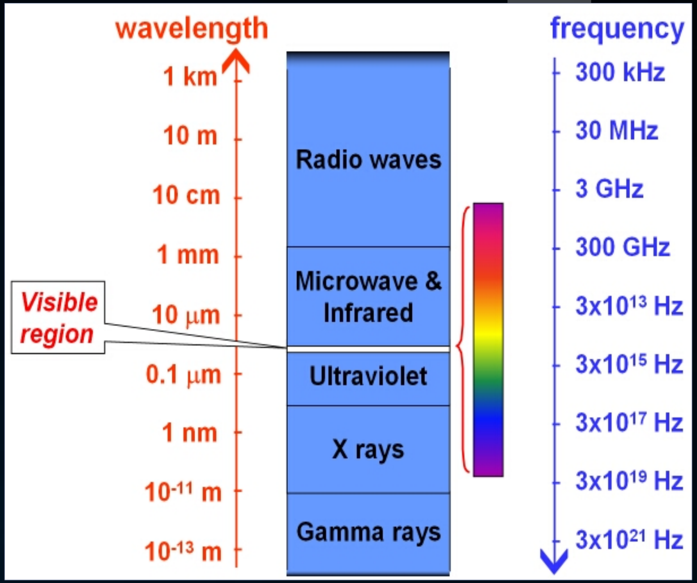
Radio Frequency

By understanding of health effect from RF EMFs, a conception of risk group has been determined.

Protecting children form RF EMFs has been seen as most relevant

In an occupational environment, the new legislative acts define risk groups as female workers being pregnant or workers carrying medical implants.

The functionality of active medical implants ay be at risk if the electromagnetic field is very strong

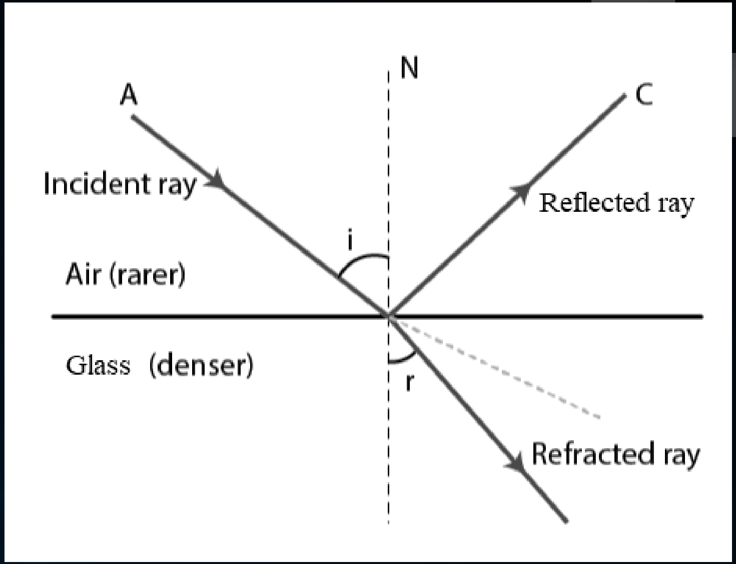


Limitations of Radio Wave

Today a variety of construction materials exist that are used to reduce the level of EMFs.

Dependent on the composition and the structure of the building materials , these may significantly affect the microwave propagation.

Typically, three types of microwave behavior are observed: transmission, reflection and absorption.

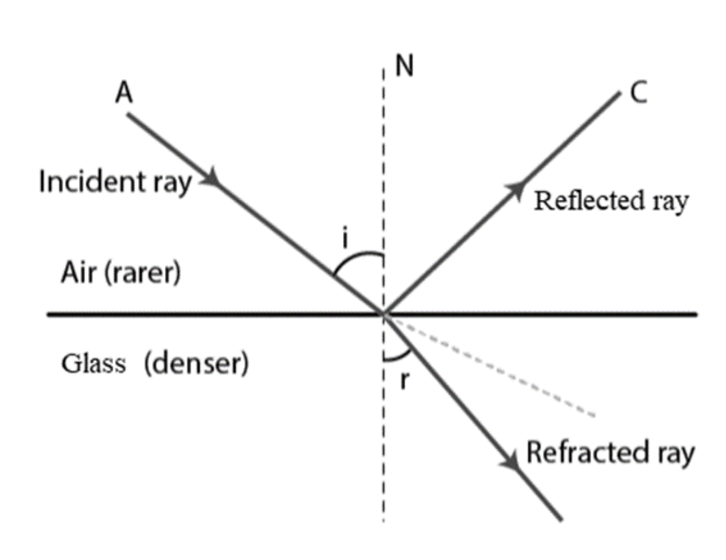


Limitations of Radio Wave

Wireless communication systems use free-space propagation of electromagnetic waves to affect transmission of their respective systems.

Free-space propagation generally is propagation through Earth's atmosphere, not through a vacuum.

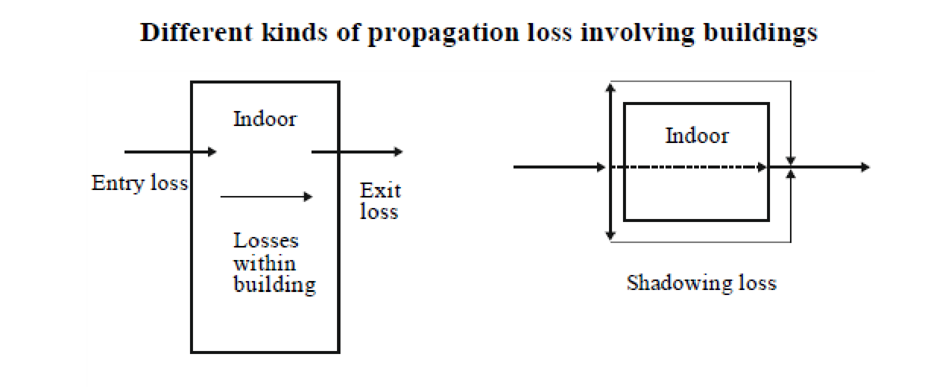
The difference is in signal loss through the Earth's atmosphere, which is not encountered in a vacuum.



Propagation Loss

That electrical properties of material and their structures strongly affect radio wave propagation

Radio waves that interact with a building will produce losses that depend on the electrical properties of the building materials and material structure.

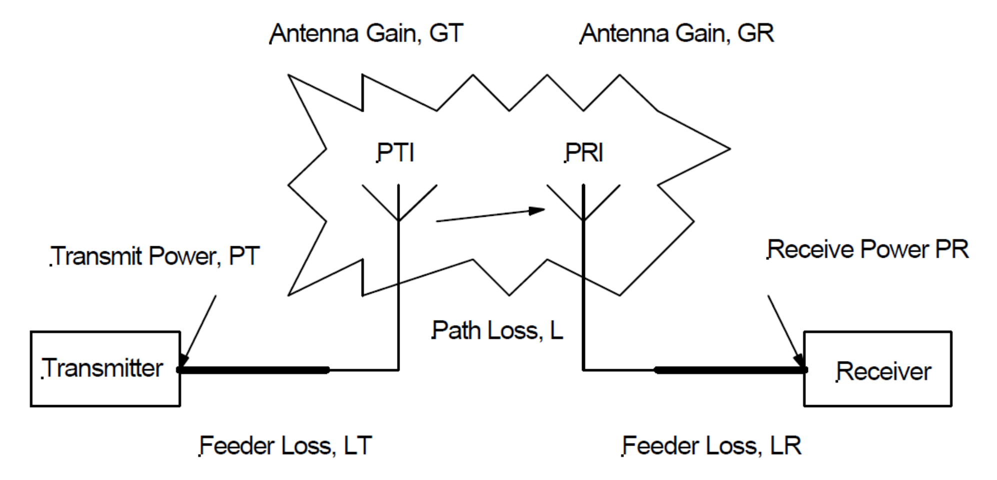


Limitations of Radio Wave

Basic transmission loss, or path loss, is the signal attenuation between a transmitter and receiver due to separation and multi-path (scattering). Basic transmission loss determines the range of a wireless link.

The path loss, L, can be found through the following relationship:

$$L = PT + GT + GR - PR - LT - LR$$



The free space path loss or atmospheric path loss is given by the following equation:

$$L_a = -32.45 + 20 * \log(freq) + 20 * \log(dist)$$

Limitations

- ✓ Limitations with buildings and building materials
- ✓ Free space/path loss
- ✓ Limitations with the nature of radio wave
- ✓ Limitations with geographic factors, like terrain

Packet Details

Signaling and data packets can be broken down into at least 5 logical channels:

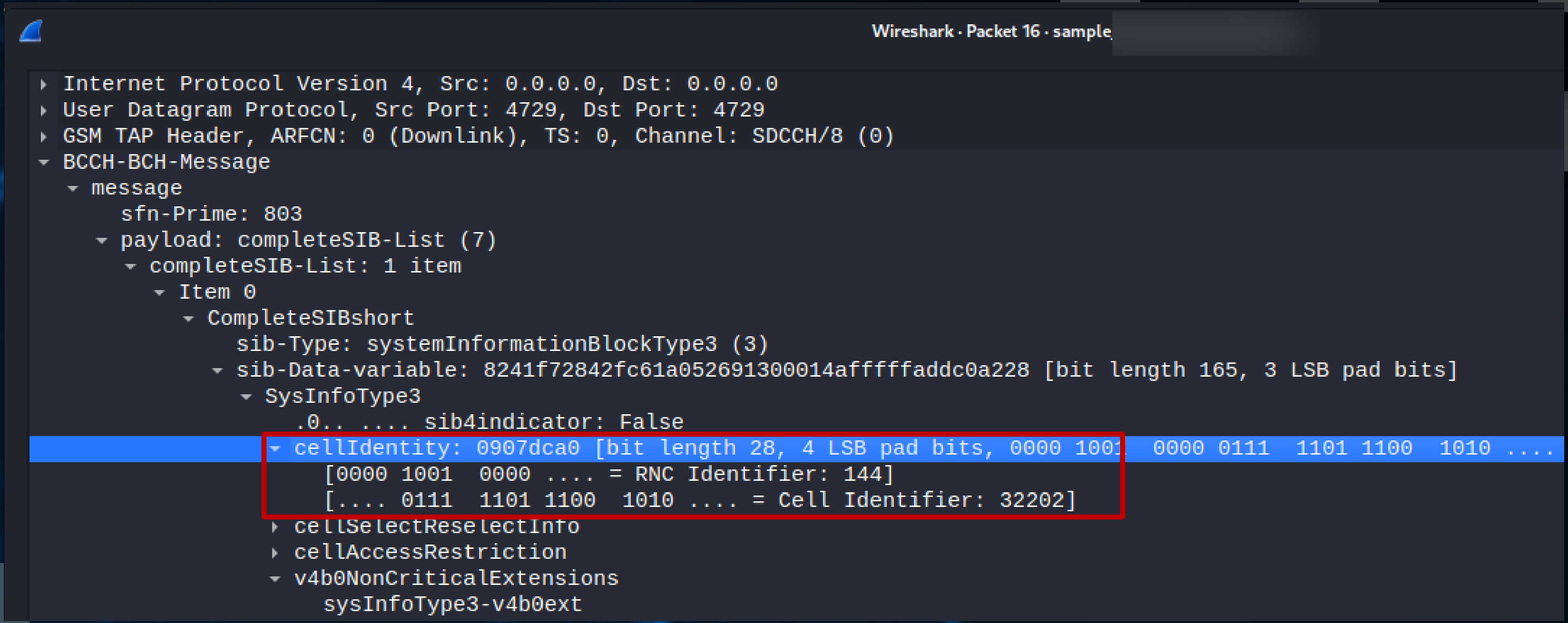
- BCCH (Broadcast Control): used by the antenna to broadcast its general characteristics (which operator it belongs to, which frequencies it supports, which area it is located in, etc.)
- PCCH (Paging Control): used by the antenna for telling an idle mobile to wake up and establish a new channel (because it receives an SMS or call for example)
- CCCH (Common Control): used to request dedicated radio resources to exchange more signalling (unencrypted)
- DCCH (Dedicated Control): all signalling after that (unencrypted then encrypted)
- DTCH (Dedicated Traffic Channel): all your data + telephony (it is commonly encrypted – except emergency calls)

Summarize

- ✓ Network scanning is a background process, by which devices are trying to find cell-tower with the strongest signal.
- ✓ When we increase the frequency, we got high bandwidth. But we are limited with distance and by the objects which prevents proper propagation of radio wave
- ✓ Device must be very close to the high-band antenna to operate at this level
- ✓ Cell-Towers are spreading their details.

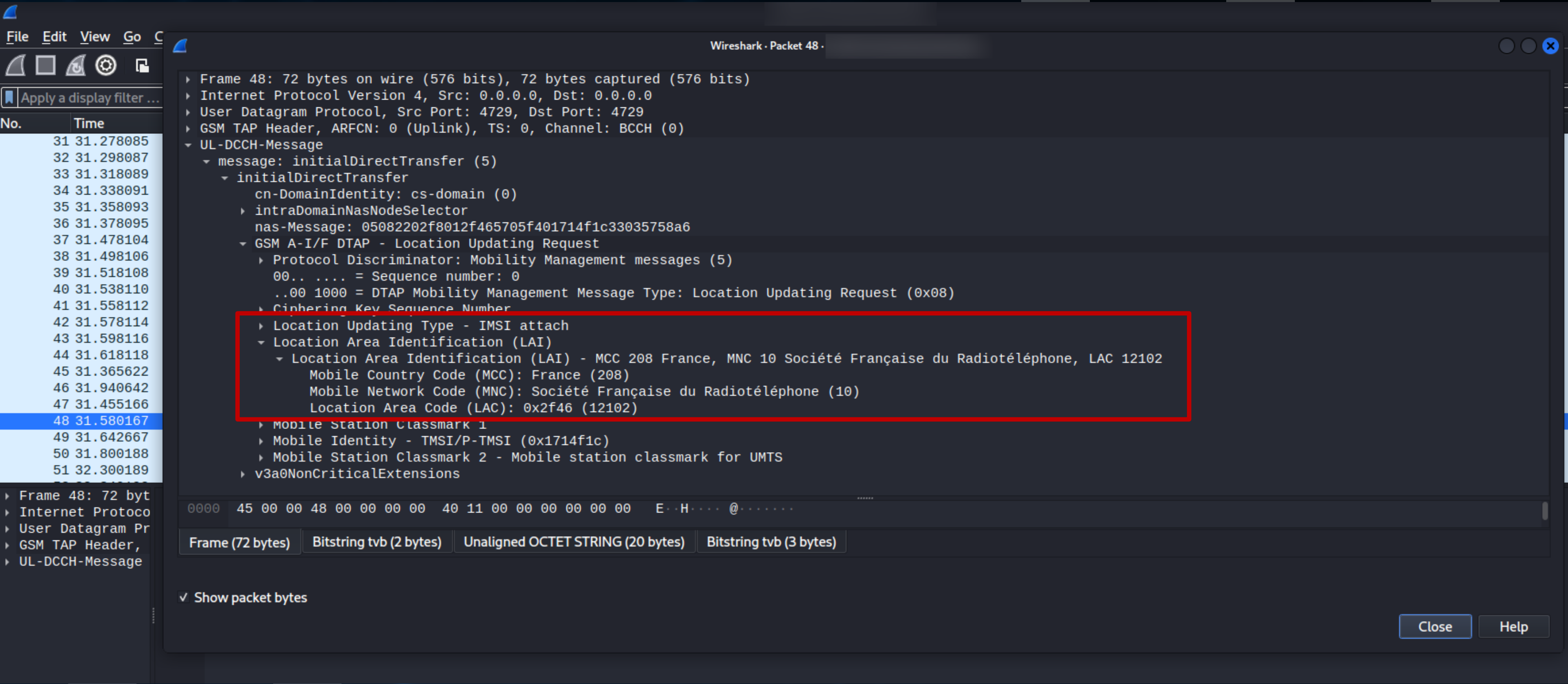
Limitations

Network details in captured file



Limitations

Network details in captured file



Results/Conclusion

- ✓ From theoretical aspects, according to our study and analyzing results of other researchers, technical changes in 5G architecture can cause more significant cyber threats related to location privacy than it was transferred from previous generation networks.

- ✓ MITM in 5G network can cause to relocate UE location and decrease the accuracy.

- ✓ Requesting GPS info from device is much noisier than just info related to cell-towers

- ✓ Locating device using A-GPS, by the knowing details about nearby cell-towers was more effective as it does not require user interaction.

- ✓ Upper-band (mmWave) in 5G network lets to determine UE location only by one active tower.

- ✓ When device is forced to connect 3rd band (Upper band), it can be located by only one cell tower.

Thank you for attention !

DEEPSEC.NET

email: gakhalaia@cu.edu.ge