

# Identification of the Location in the 5G Network

**Giorgi Akhalaia**

Caucasus University  
Scientific Cyber Security Association



## 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

# Introduction

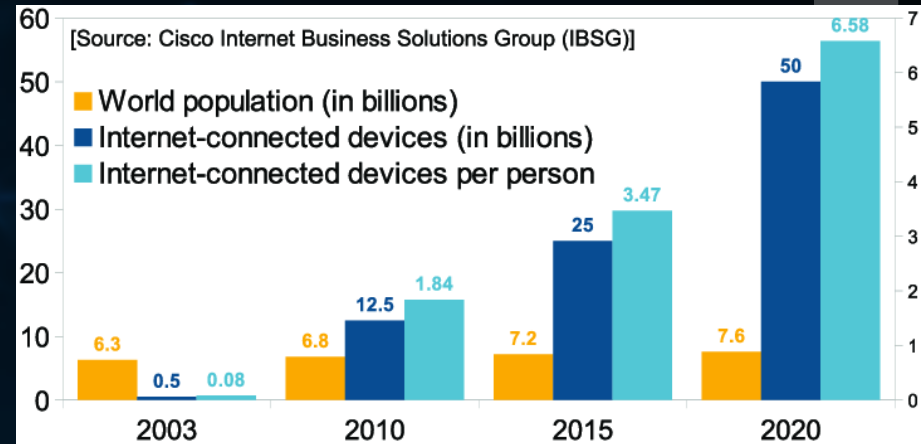
n

DeepSec 2022 – Vienna, Austria

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



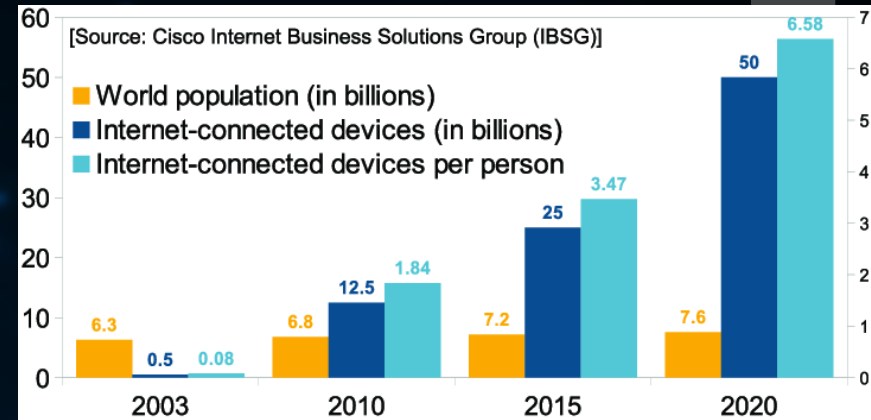
# Introduction

DeepSec 2022 – Vienna, Austria

**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

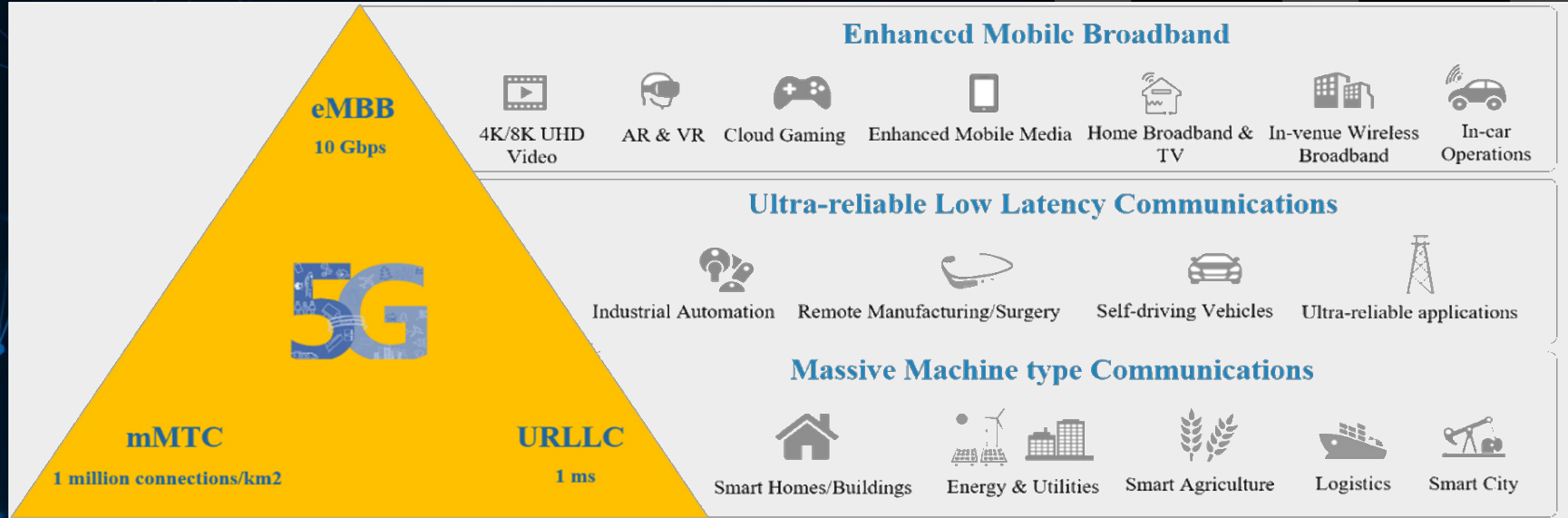
DeepSec 2022 – Vienna, Austria

- ❑ 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

DeepSec 2022 – Vienna, Austria



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

## Low-band -- < 1 GHz

## Mid-band -- 1 GHz – 6 GHz

## High-band -- 6 GHz – 100 GHz (mmWave)

The diagram illustrates a 5G network architecture with a Base Station (BS) and its coverage area. The BS is equipped with Multiple Antenna Arrays, which are connected to an Array of Elements (E1, E2, ..., Em). The coverage area is divided into Flexible Coverage regions, with Pmax representing High transmit Power for High density, Wide Coverage, and Pmin representing Low transmit Power for Low density coverage near the BS. The diagram also shows the direction of beam with downtilt and the boresight direction, with an angle  $\theta$  indicated. The coverage area is further divided into regions P1, P2, P3, ..., Pn, where P1-Pn represent Variable Power Levels. The diagram also shows the relationship between the BS, the antenna array, and the coverage area, including the direction of beam with downtilt and the boresight direction.

**Multiple Antenna Arrays**

**Array of Elements**

**Boresight Direction**

**Direction of beam with downtilt**

**Antenna Element**

**Flexible Coverage**

**Pmax**

**Pmin**

**P1-Pn: Variable Power Level**

**A1- An: Antenna Arrays**

**E1-En: Antenna Element**

**P1#P2#P3#... #Pn ( Power Levels Depending on Coverage and Density)**

**High transmit Power (Pmax) for High density, Wide coverage**

**Low transmit Power (Pmin) for Low density coverage near the BS**

M.K Maheshwari in "Flexible Beam Forming in 5G Network"

# Methods of locating Device

DeepSec 2022 – Vienna, Austria

**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.**

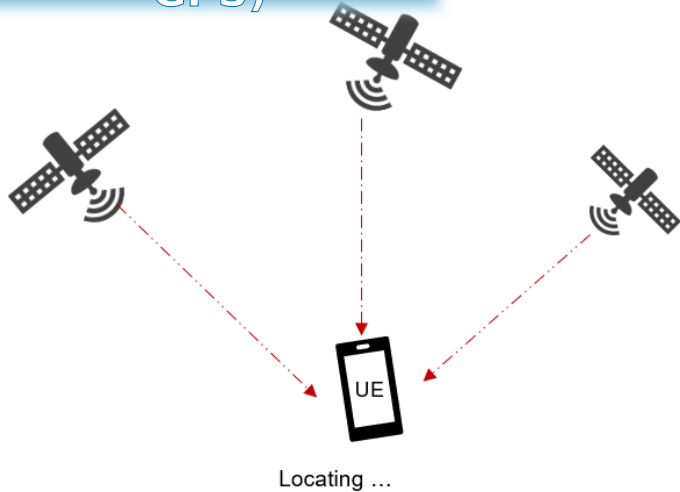
GNSS – Global Navigation Satellite System



# Locating Device

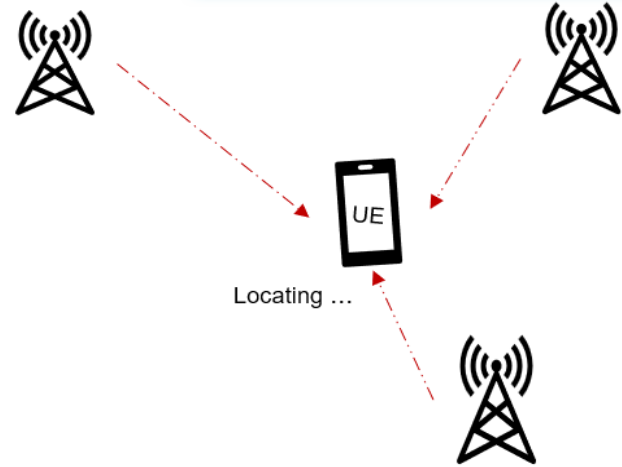
DeepSec 2022 – Vienna, Austria

## 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.



## Trilateration

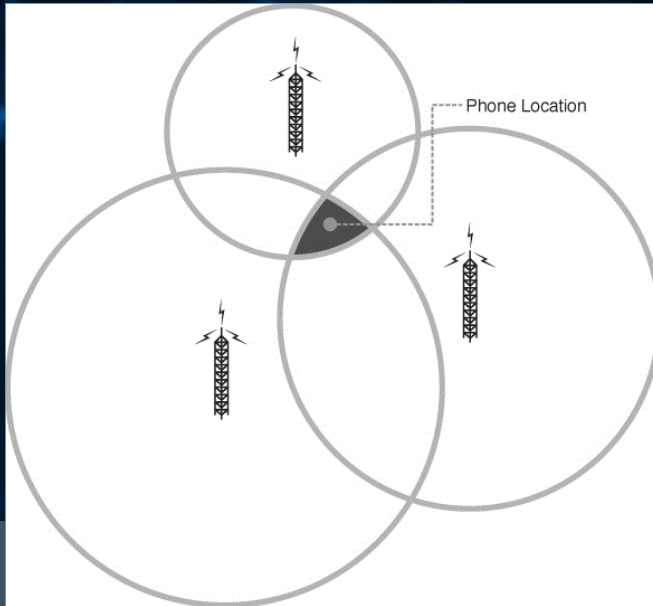


Illustration 1

## Triangulation

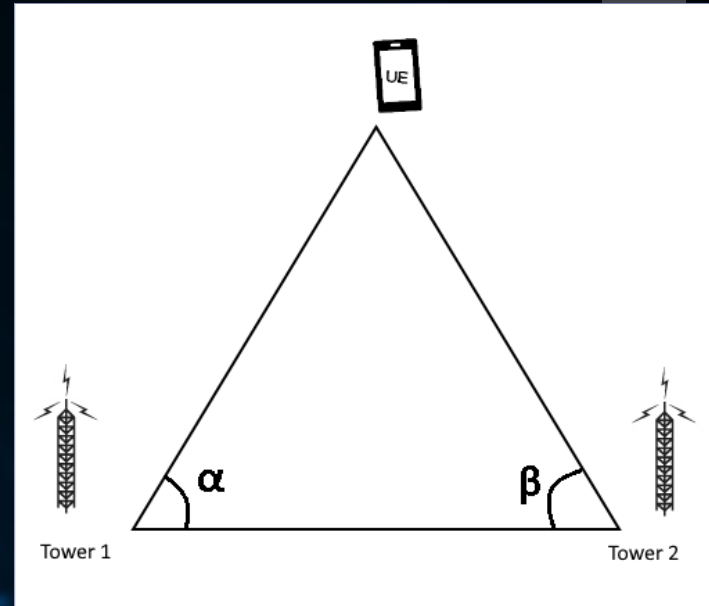
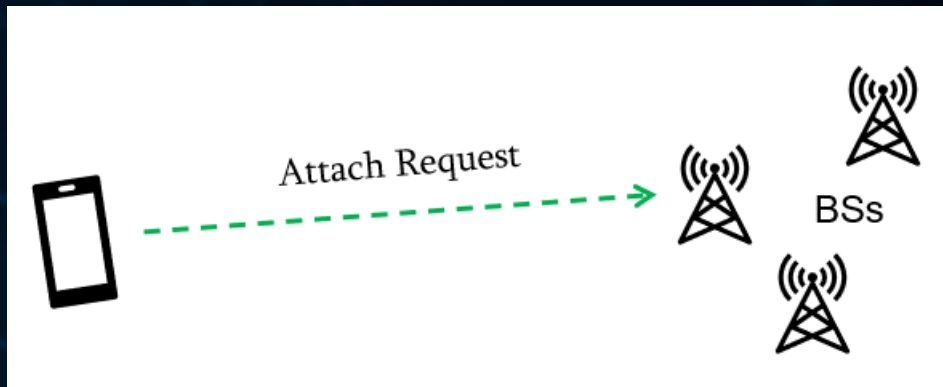


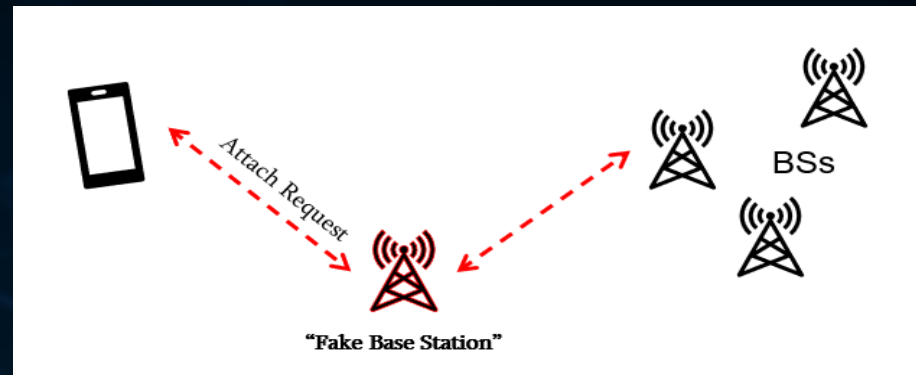
Illustration 2



## 1. Attach Process (Normal Case)

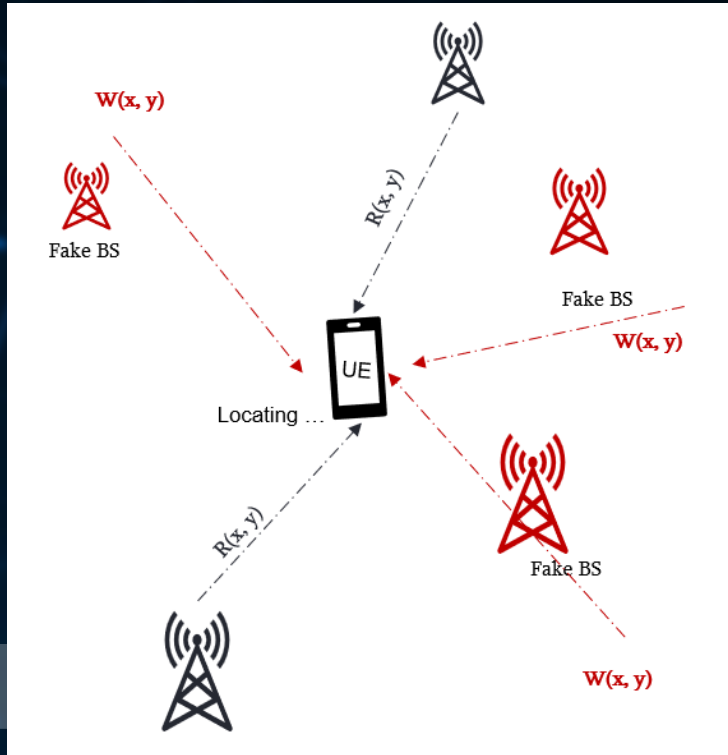


## 2. Fake BS - MITM – in 5G Network:



# Fake Base Stations in Network

DeepSec 2022 – Vienna, Austria



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

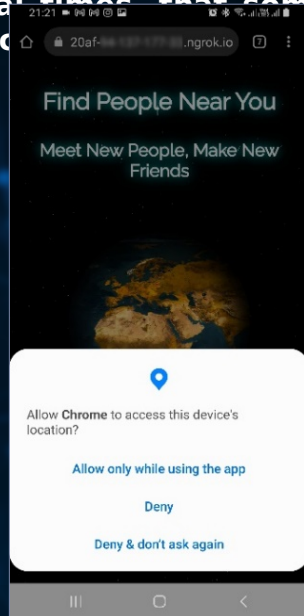
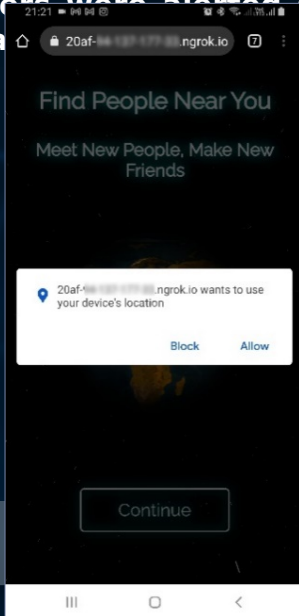
- Because of wrong inputs, device might be relocated or located with very low precision

# Experimental Work: Case 1: GNSS Method

DeepSec 2022 – Vienna, Austria

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 was on location.



```
Os IP : 192.168.1.100
Os Name : Android
Os Version : 10
CPU Cores : 8
Browser Name : Chrome
Browser Version : 96.0.4664.104
CPU Architecture : not Found
Resolution : 412x846
Time Zone : Georgia Standard Time
System Language : en-US
```

[!] Waiting for User Interaction

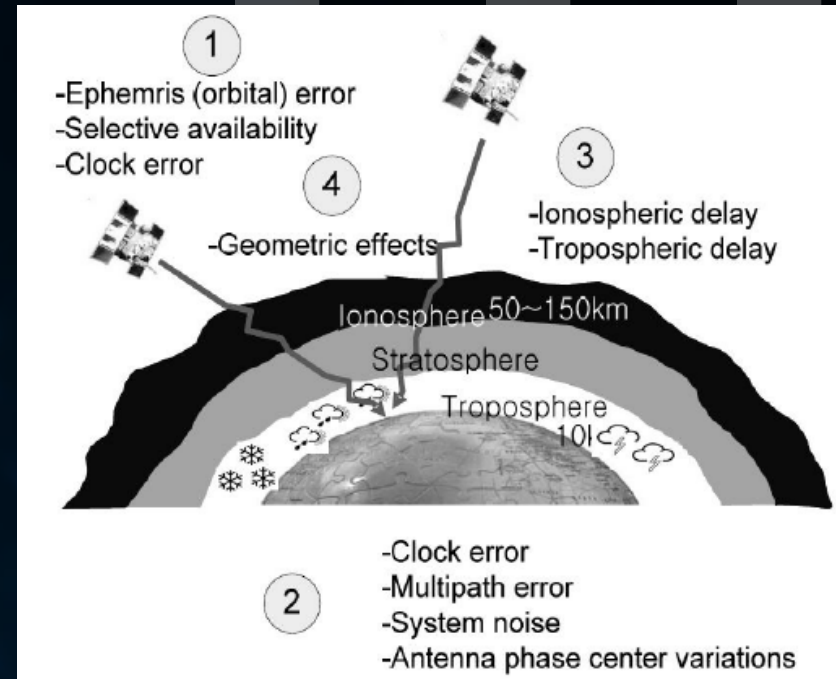
Google Map Link : <https://www.google.com/maps/place/41.7225356+44.7202972>



# Limitations of this method

DeepSec 2022 – Vienna, Austria

- **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 !**

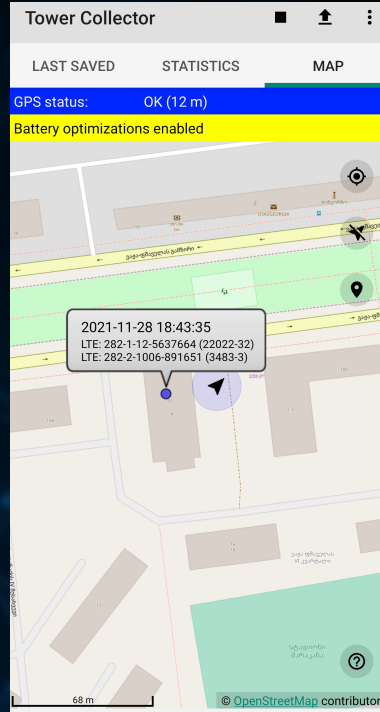


# Case 2: A-GPS

DeepSec 2022 – Vienna, Austria

## Collecting Cell-Towers

Tower Collector	
LAST SAVED	STATISTICS
GPS status: OK (12 m)	
Battery optimizations enabled	
Last saved measurement	
Network type:	LTE
Long Cell ID:	891651
Cell ID / RNC:	3483 / 3
TAC:	1006
MCC:	282
MNC:	2
Signal strength:	-93 dBm
Network type:	LTE
Long Cell ID:	5637664
Cell ID / RNC:	22022 / 32
TAC:	12
MCC:	282
MNC:	1
Signal strength:	-99 dBm
Main / neighboring:	2 / 0
Latitude:	41.72247198°
Longitude:	44.71949151°
Accuracy:	32.00 m
Save time:	2021-11-28 18:43:35



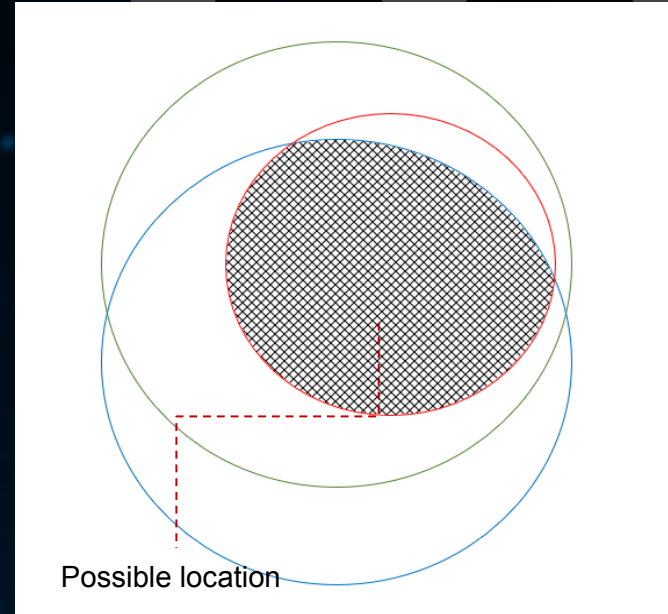
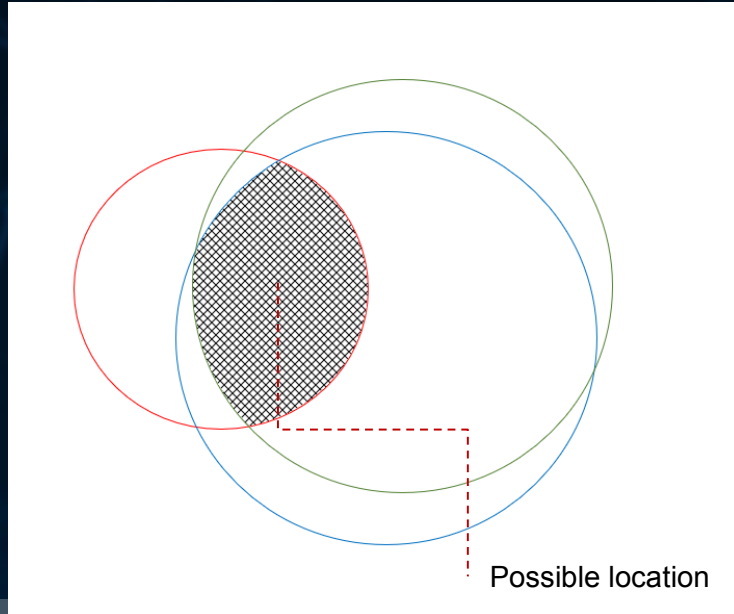
Tower Collector	
LAST SAVED	STATISTICS
GPS status: OK (12 m)	
Battery optimizations enabled	
Today	
Measurements:	2
Cells (discovered):	2 (2)
Local since 2021-08-03 18:42:16	
Measurements:	16
Cells (discovered):	5 (5)
Total since 2021-07-10 21:04:52	
Measurements:	16
Discovered cells:	5
To upload	
OpenCellID.org:	16
Mozilla Location Services:	16

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

DeepSec 2022 – Vienna, Austria

## Mapping coverage circles of cell-towers





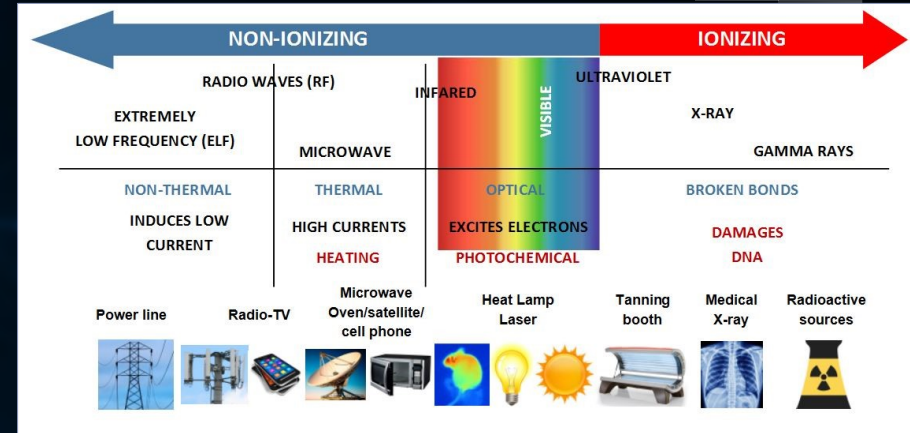
# Radio Frequency

DeepSec 2022 – Vienna, Austria

Electromagnetic fields represent significant component of the modern 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

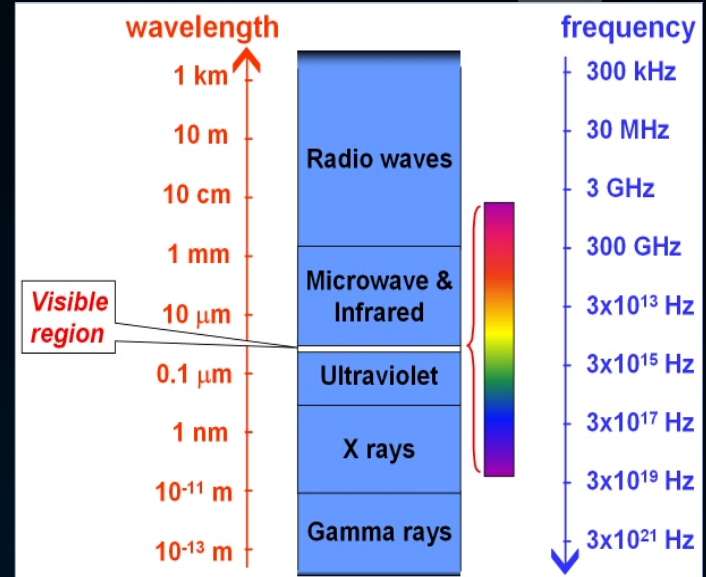
DeepSec 2022 – Vienna, Austria

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

Protecting children from 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 may be at risk if the electromagnetic field is very strong



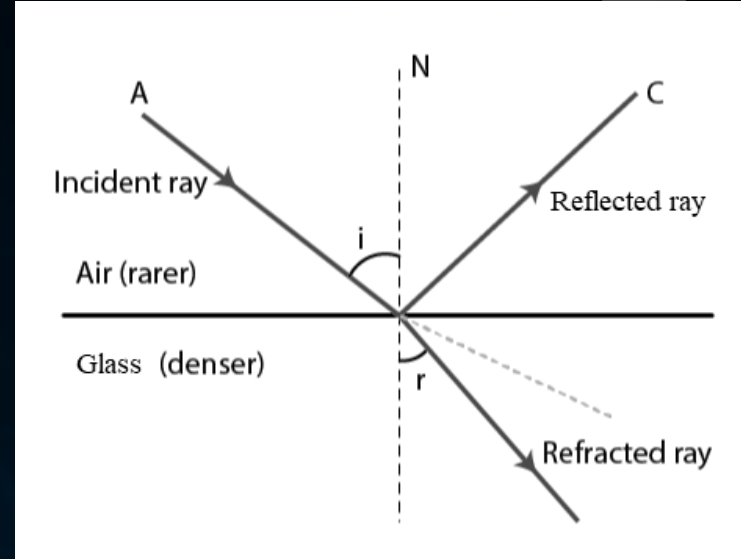
# Limitations of Radio Wave

DeepSec 2022 – Vienna, Austria

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.



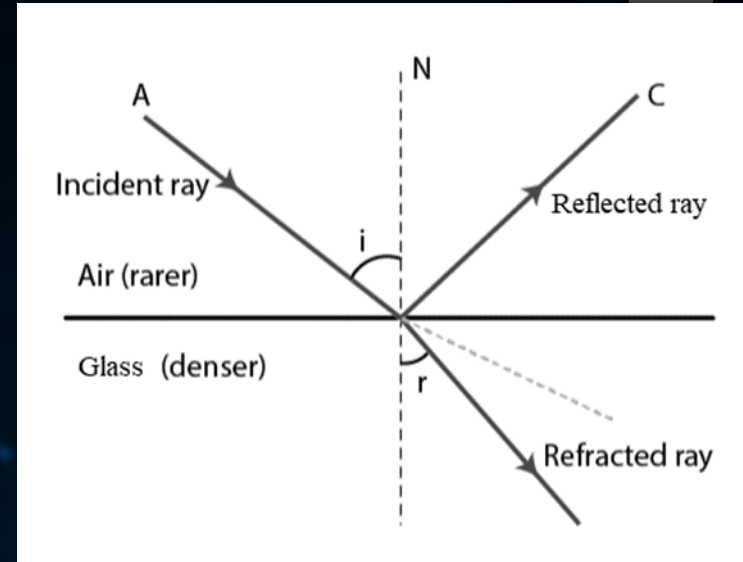
# Limitations of Radio Wave

DeepSec 2022 – Vienna, Austria

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.



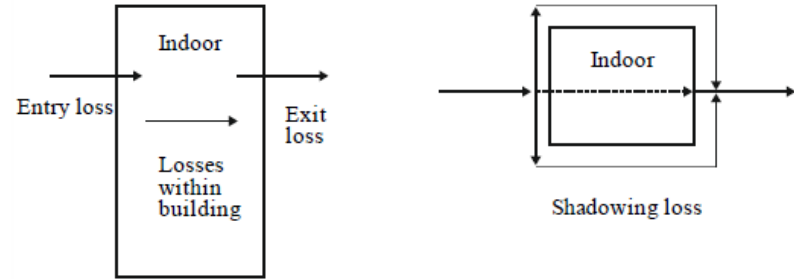
# Propagation Loss

DeepSec 2022 – Vienna, Austria

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.

**Different kinds of propagation loss involving buildings**



# Limitations of Radio Wave

DeepSec 2022 – Vienna, Austria

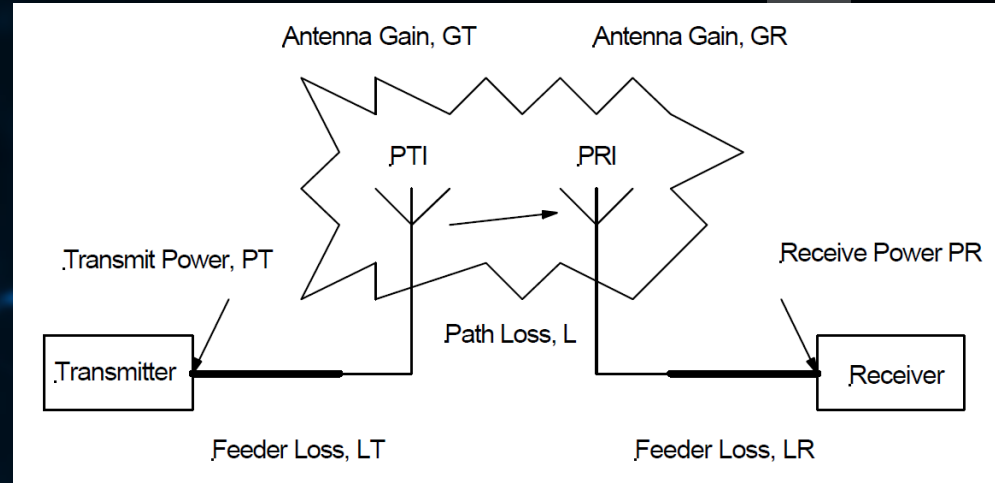
Basic transmission loss, or path loss, is the signal attenuation between a transmitter and receiver due to separation and multi-path (scattering). Basic transmission loss determines the range of a wireless link.

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

$$L = P_T + G_T + G_R - P_R - L_T - L_R$$

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

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





# Limitations

DeepSec 2022 – Vienna, Austria

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

**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

DeepSec 2022 – Vienna, Austria

- ✓ 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

DeepSec 2022 – Vienna, Austria

## Network details in captured file

```
Wireshark · Packet 16 · sample

▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 0.0.0.0
▶ User Datagram Protocol, Src Port: 4729, Dst Port: 4729
▶ GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: SDCCH/8 (0)
▼ BCCH-BCH-Message
  ▼ message
    sfn-Prime: 803
  ▼ payload: completeSIB-List (7)
    ▼ completeSIB-List: 1 item
      ▼ Item 0
        ▼ CompleteSIBshort
          sib-Type: systemInformationBlockType3 (3)
          ▼ sib-Data-variable: 8241f72842fc61a052691300014afffffaddc0a228 [bit length 165, 3 LSB pad bits]
            ▼ SysInfoType3
              .0.. .... sib4indicator: False
              ▼ cellIdentity: 0907dca0 [bit length 28, 4 LSB pad bits, 0000 100: 0000 0111 1101 1100 1010 ....
                [0000 1001 0000 .... = RNC Identifier: 144]
                [.... 0111 1101 1100 1010 .... = Cell Identifier: 32202]
              ▶ cellSelectReselectInfo
              ▶ cellAccessRestriction
              ▼ v4b0NonCriticalExtensions
                sysInfoType3-v4b0ext
```

# Limitations

DeepSec 2022 – Vienna, Austria

## Network details in captured file

Wireshark - Packet 48

File Edit View Go C

Apply a display filter ...

No.	Time
31	31.278085
32	31.298087
33	31.318089
34	31.338091
35	31.358093
36	31.378095
37	31.478104
38	31.498106
39	31.518108
40	31.538110
41	31.558112
42	31.578114
43	31.598116
44	31.618118
45	31.636522
46	31.940642
47	31.455166
48	31.580167
49	31.642667
50	31.800188
51	32.300189

Frame 48: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 0.0.0.0
- User Datagram Protocol, Src Port: 4729, Dst Port: 4729
- GSM TAP Header, ARFCN: 0 (Uplink), TS: 0, Channel: BCCH (0)
- UL-DCCH-Message
  - message: initialDirectTransfer (5)
    - initialDirectTransfer
      - cn-DomainIdentity: cs-domain (0)
      - intraDomainNasNodeSelector
        - nas-Message: 05082202f8012f465705f401714f1c33035758a6
    - GSM A-I/F DTAP - Location Updating Request
      - Protocol Discriminator: Mobility Management messages (5)
        - 00.. .... = Sequence number: 0
        - ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request (0x08)
      - Ciphering Key Sequence Number
      - Location Updating Type - IMSI attach
      - Location Area Identification (LAI)
        - Location Area Identification (LAI) - MCC 208 France, MNC 10 Société Française du Radiotéléphone, LAC 12102
          - Mobile Country Code (MCC): France (208)
          - Mobile Network Code (MNC): Société Française du Radiotéléphone (10)
          - Location Area Code (LAC): 0x2f46 (12102)
      - Mobile Station Classmark 1
      - Mobile Identity - TMSI/P-TMSI (0x1714f1c)
      - Mobile Station Classmark 2 - Mobile station classmark for UMTS
      - v3a0NonCriticalExtensions

0000 45 00 00 48 00 00 00 00 40 11 00 00 00 00 00 00 E..H....@.....

Frame (72 bytes) Bitstring tvb (2 bytes) Unaligned OCTET STRING (20 bytes) Bitstring tvb (3 bytes)

✓ Show packet bytes

Close Help

# Results/Conclusion

DeepSec 2022 – Vienna, Austria

- ✓ 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 3<sup>rd</sup> band (Upper band), it can be located by only one cell tower.



**Thank you for attention !**



*email:*  
***gakhalaja@cu.edu.ge***