Novel Architecture of 5G Network

Giorgi Akhalaia[a], Maksim Iavich[b]

[a] *Georgian Technical University, 77 Kostava str, Tbilisi, 0160, Georgia*
[b] *Caucasus University, 1 Paata Saakadze str, Tbilisi, 0102, Georgia*

Abstract

Over the last years 5G technology has definitely become one of the most important topics of communications, especially for people working on cyber security. Through persistent effort world leading telecom operators are trying to satisfy new requirements of 3GPP and implement 5G technology. By the three key concepts (Enhanced Mobile Broadband; Ultra-reliable and Low-latency Communications; Massive Machine Type Communications), 5G has exceed the limits of mobile network ecosystem and has started new era in wireless communications. It is an obvious that new features, technologies generate extra vulnerabilities and threats starting from software, design to implementation process. Being virtualization key concept of 5G, network is more software-based, than hardware-based. This structure makes 5G network more flexible but also inherits software vulnerabilities, that have to be solved. Even 5G uses 256 bit encryption and has improved authentication with base station than 4G, there are still gap that leaves it vulnerable for attacker. Using MITM attack can be sniffed and manipulated device capabilities. Thus, risk of sensitive information leakage and cyber attacks like MNmap, Battery Drain and etc. have increased. Solution mentioned in this article describes the scenario how should be done authentication between base station and user equipment to minimize the risk of fake base stations, which itself solves problems related to MITM. Checking the base station before attaching it is key concept of defense strategy from fake base stations.

Keywords 1

5G Security, Cyber Security, Battery Draining, MNmap, Authentication of Base station, MITM in 5G, 5G versus 4G

1. Introduction

Technical evolution has never been linear. Innovation progress scale and vector always depend on human's needs, demands and its rate of urgency. Diversity of Artificial Intelligence use case and huge amount of IoT devices have dramatically increased speed of developing automatization, self-maintained remote services and processes. Hence, there was a need of new communication standard which would overcome existing limitations. So, engineers have started working on 5th generation of telecom communication, which would have following general advantages.

- Ultra-Reliable-Low Latency Communication (URLLC) – up to 1 ms
- Enhanced Mobile Broadband (eMBB) – more than 10Gb/s
- Massive Machine-Type Communication (mMTC) – 1 Million Connections per km^2

Target groups of 5G general advantages are shown on the **Figure *1***.

IVUS2021: Information Society and University Studies 2021, April 23, 2021, Kaunas, Lithuania
EMAIL: gakhalaia@cu.edu.ge (A. 1); miavich@cu.edu.ge (A. 2);

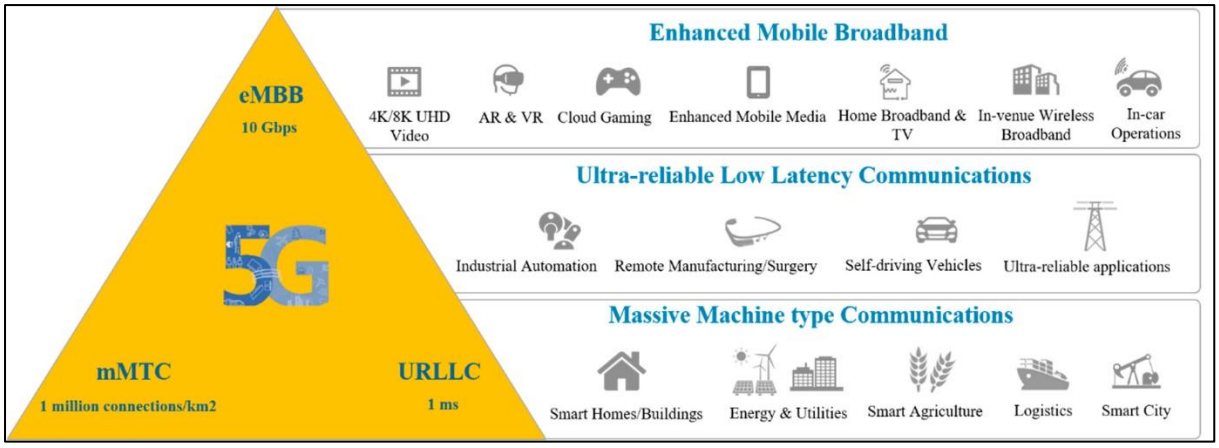

Figure 1: Target group of 5G advantages

To satisfy requirements mentioned above, 5G Network uses some new and improved techniques for both parts: for hardware and software. 5G operating spectrum range has been divided into 3 categories:

1. **Low-band** – below of 1GHz. It is generally used for high densely populated areas. Because buildings have less impact on quality of this frequencies. But, peak data speed is about 100 Mbps.
2. **Mid-band –** from 1GHz to 6GHz. It has more bandwidth and less latency than Low-band, but this band is more affected by buildings than previous one. Peak data rate is about 1 Gbps.
3. **High-band (mmWave) –** from 6GHz to 100 GHz. Actually this band has all new features promised by 5G Network. It is also called mmWave technology. Peak data rate is about several 10 Gbps.

Massive MIMO (mMIMO – Massive Multiple-input Multiple-output) and Flexible Beamforming are key techniques of 5G communication. Concept of mMIMO is simple: arrays of antennas are attached to the base station to serve huge number of terminals at the same time. By using multi-power beams engineers optimize 5G Network coverage and download/upload speed. They provide different transmit power for each antenna array to achieve standard requirements. This technique also does 5G more energy-efficient. Architecture of flexible beam forming is shown on **Figure *2***. [2]

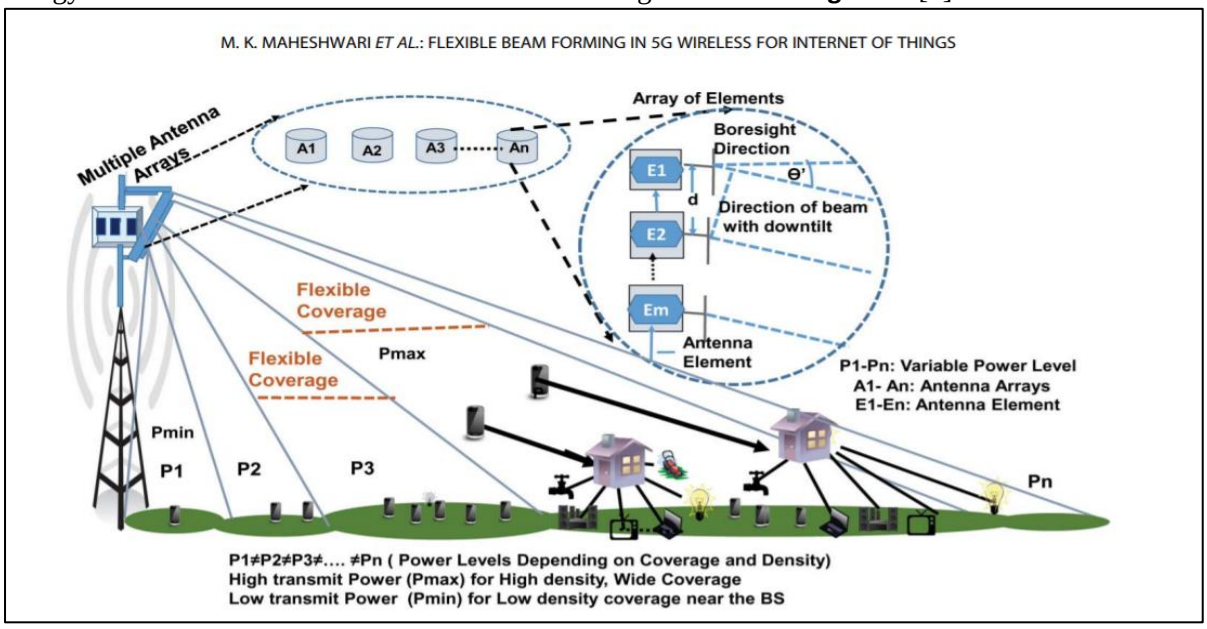

Figure 2: Flexible Beam Forming

But, nowadays it's just an experimental work and full 5G capabilities can be delivered only near the cell towers.

5G Network inherits some technologies from previous generations, but there are important changes that should be over checked to assess cyber risks and minimize potential threats. By providing predefined requirements, 5G technology has become more complicated (Hardware, Software, Logical) than its ancestors. There is no doubt that, we get extra vulnerability as we increase system's complexity.

We would like to mention that one of the most important and vulnerable update – Network Virtualization. As virtualization is a key technique of 5G architecture, it is going to use Network Functions Virtualization and Technologies of Software based Architecture: like Software Defined Access; Software Defined Networks; and Software Defined Radio. [3] Setting up network architecture using virtualization and AI have lots of advantages, like: reduced number of physical devices/base stations; effective power-consumption; Network-slicing – provides network more flexible and manageable; enabling resource rescheduling; auto-optimization and so on. Therefore, 5G network will be likely more software-based than hardware-based. Thus, all software related threats should be considered.

2. 5G comparison with previous generations

As it was mentioned above, 5G will cross the limits of telecom service and will take a reasonable part in future end-to-end communication, from end users to robots operating by AI. However, despite of it's huge step in standard specifications, there are set of techniques which are transferred from previous generation - 4G network. Majority of them are improved, but there are still some methods which were transported with it's vulnerabilities.

2.1. Technical Improvement

Before diving into 5G improvement, start with a brief overview about how mobile network generations were developed and came to the 5^{th} generation of telecom communication:

1. 1G – Analog voice was delivered (1980s)
2. 2G – Digital voice was introduced (early 1990s)
3. 3G – Mobile data was deployed (early 2000s)
4. 4G – New era: Mobile Broadband has started.
5. 5G – Unified system, with more capabilities to deliver superior reliability, extremely low latency, the highest speed and huge amount of connectivity.

Architecture of existing telecom networks was designed to provide voice and conventional mobile broadband services. However, previous organization has proven that it could not totally support diversity of 5G services. Huawei, the giant company working on 5G deployment lists the aspect that's stand behind network architecture transformation: [4]

- Various standards, services and site types have to been supported and simultaneously operated by complex networks.
- Multi-type connection coordination.
- Flexible management of NFs
- Service anchors distribution upon request
- Service deployment in shorter period

Market researchers are talking about positive effects of 5G on global economy. According to Qualcomm 22.8 million new jobs will be created and 13.1 trillion USD will be global economic outcome. Generally, it is most interesting and frequently asked question, how is 5G better than previous generation - 4G network? The very first aspect is speed. By combination of up to 20Gbps (peak data rate) and more than 100 Mbps (average data rate) 5G will be considerably faster than 4G. By the requirements, latency of 5G will be 10 times decreased than in previous standard. There will be 100

times more traffic capacity than used to be. Important changes come to spectrum, it can natively support licensed, unlicensed and shared spectrum types. 5G technology is designed so, that operable spectrum is divided into 3 categories (Low: below to 1GHz; Mid: 1GHz – 6GHz; High: upper than 6GHz – known as mmWave) which makes its usability in more efficient way. [5]

It should be mentioned that 5G use CUPS - Control and User planes separation. Actually, this is not new technology but in case of 5G it will be core element of the system architecture.

To summarize functionality improvement of 5G versus 4G, it is designed to be more capable, unified network that will support massive IoT and mission-critical communications.

2.2. Security aspects of 5G versus 4G

New functionality and technologies always rise additional threats and vulnerabilities. However, there are some methods that were transferred from 4G without resolving security issue. Andy Purdy, CSO for Huawei Technologies USA, in Forbes has written, that 5G implement new security protocols to resolve security issues imported from previous network. According to the paper 5G will use 256-bit encryption while 4G uses 128-bit. Also, it should be mentioned that, in case of 5G, user's location and identity will be encrypted too, while in 4G technology they used not to. [6]

Researchers have talked about different security flaws. It is well known fact that some of issues let attacker to perform "Downgrade attack". This is a case when victims connection is manipulated so, that it downgrades to slower connection/service, for example to 3G or 4G network. As a result, attackers can compromise well known vulnerabilities of older networks. Even it has stronger encryption, there is a issue when user authenticates, sends attach request to base station. That gives attacker chance to create fake base station and then act as a MITM. As virtualization is a key concept of 5G, it is designed to be more software-based network than hardware-based. Hence it is more vulnerable to software-based threats. At the same time, network slicing promotes 5G to be easily and flexible manageable as well as to stronger security of the whole system.

CUPS is used by CRAN – Cloud Radio Access Network, which represents an innovative architecture(cloud-based) for Radio Access Networks. It has powerful advantages over older architectures, but as a wireless network, its vulnerable to the most wireless security threats.

Virtual Mobile Network Operators, Network Infrastructure Providers and Communication Service Providers are main actors of 5G ecosystem. All of them have diverse privacy and security priorities. So, their incorporation should be done carefully not to violate security of the system.

By the end, when all the requirement is satisfied and the final version of 5G is deployed, it will be more secure way of communication than 4G or any previous generations.

3. Security issues of 5G Network

IoT devices represent essential target for 5G communication. As it is promised, IoT devices operating on 5G network will achieve minimal power consumption. However, at this moment 5G technology suffers from battery drain problem. There are two factors that cause battery drain on 5G enabled devices: 1. Network Switch and 2. Network Attack – MiTM. Testers from different organizations have already tested battery consumption of devices working on 5G Network. Mike Elgan in his article has written that reason of battery draining is switches. Testers from CNET tested 2 smartphones with and without usage of 5G: Moto Z3 and Galaxy S10. In first case battery died after 4 hours and in case of Galaxy S10 battery dropped to half (in four hours). [7]

Samsung support team also approved battery drain issue and published small description. As it is written, nowadays 5G network is only for data transmission and it is not capable to carry messages and phone calls. So, 5G smartphones have to hold simultaneously connections with multiple networks to be available for phone calls while using mobile data. [8] As network engineers said it the trial issue and will be resolved by the time after 5G capabilities will grow and support both: phone type communications (calls, messages) and data transmission.

Second factor, Network Attack - MITM, has higher cyber risk. It gives ability not only battery draining, but also other manipulations like packet injection, script injection, session hijacking and so on. So, it would be better solution to try minimizing probability of MITM attack. Altaf Shaik in his

article describes vulnerabilities and experimental setup of 5G network.[9] He has used MITM (setting up fake base station (BS)) for compromising security of 5G and making attacks like battery draining, MNmap and Bidding Down.

Idea of MNmap is quite simple, it is used to fingerprint and identify device type by scanning it's capabilities. It is like an OS fingerprinting, when hacker scans open ports on the host to identify running services. By knowing reference model, he/she or automated software identifies host OS and other details. Same mechanism works for MNmap attack. Using rogue BS, which acts as intermediate between UE and BS Altaf Shaik modified device capabilities and disabled Power Saving Mode. Hence device's modem was continuously measuring signal and running some processed, that was draining battery. Battery draining process is shown on **Figure *3***. [9]

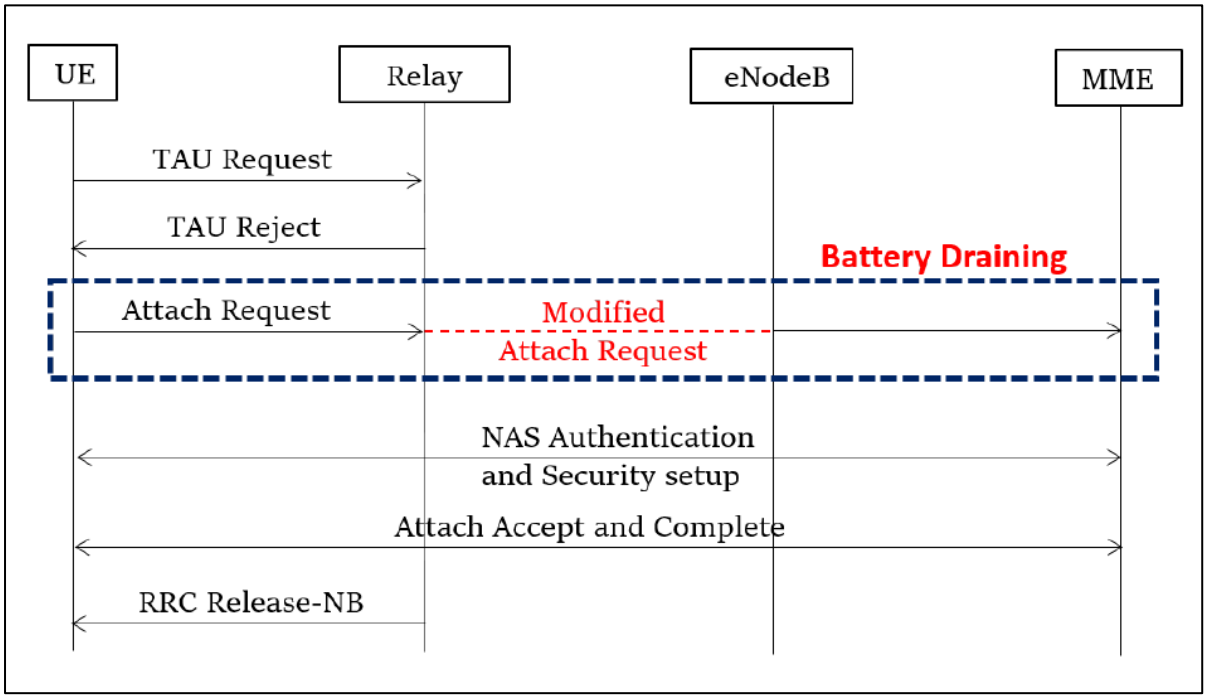

Figure 3: Battery Draining

As attach request from User Equipment to the BS is sent without encryption, there should be protection, that will prevent devices from attaching to fake BS. This can be software or hardware method, that will prove BS authenticity. Scenario should be following:

- All BSs have information about nearest BSs and have algorithm to approve genuine of each other.
- Before sending unprotected data (clear text) while UE tries to attach to BS, it must recheck legitimate of desired BS with already connected BS. This will prevent UE from attaching to fake BS. However, it will redirect attack vectors to BS, in trying to poison legitimate BS records. But, in general it is the safer way for UE and BS connection.

In normal case SIM (Subscriber Identity Module) based mechanism is used for authentication between BS and UE. SIM card role is to validate user on network and make payment processes.[7] In some countries SIM base authorization is used for e-governance, like certifying users for eservice. So, it is crucial to avoid rogue base station that acts as MITM and sniffs the conversation. Device has to send EMEI (International Mobile Equipment Identity) and EMSI (International Mobile Subscriber Identity) to base station while making handover or just after switching off flight mode. So, these details are easily obtainable over the air. IMEI code is unique and represents fingerprint of device (like a MAC). IMSI uniquely identifies each user of mobile network. Knowing EMEI and IMSI gives ability to identify device and its location. Also, with a little modification attacker can unlock stolen devices.

Adding checking element of BS genuineness, authenticity before attaching to the new BS in 5G architecture will significantly decrease probability of Rogue BS.

The very important point is implementation. No matter how strong and well-organized standard will be, if Network Operators make mistakes in process of deployment. Somehow, in some cases Network Operators skip steps in implementation process to reduce cost of deployment. Which itself increases risks and makes networks more vulnerable.

4. Future Plans

As a future plan, we are going to implement BS checking mechanism in 5G lab and measure how it affects on performance and productivity of the network and device. That will be part of my PhD. We will create simulated network from array of fake base stations and implement algorithm that will reevaluate genuineness of base stations. Which will assess authenticity of BSs for devices and will decide: grant access to connect or redirect attach request to another legitimate BS.

5. Conclusion

Successfully implemented 5G network will play a significant role in many aspects of physical world. Specifications required from 3GPP actually represents prerequisites of modern world and not only advantages of new standard. New and enhanced capabilities trigger new methods and technologies. Which themselves initiate vulnerabilities, threats and higher risk. Because of the nature of 5G architecture it is more vulnerable to software-based threats. Huge targe group of 5G is critical infrastructure, so security of the network is crucial. 5G inherits some technologies and weakness from 4G network. Even 5G has better (256 bit) encryption, than 4G (128 bit) network, it leaves holes for attackers while authenticates with base station. Test results mentioned in article shows that using fake base stations and making MITM attack sensitive information can be stolen. In our scenario of 5G architecture software element, algorithm will operate as a controller. Every time device requires to attach base station it has to reexamine legitimate of desired base station with already connected station. This will minimize chance of attaching fake base stations and MITM attack on this stage of 5G network.

6. References

[1] SK Telecom, in “5G architecture design and implementation guideline”, 2015.

[2] 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

[3] M. Ivezic, L. Ivezic, “5G Security & Privacy Challenges” in 5G.Security Personal Blog, 2019. https://5g.security/cyber-kinetic/5g-security-privacy-challenges/

[4] Huawei Technologies CO,. LTD in “5G Network Architecture – A high Level Perspective”, 2016

[5] Qualcomm Technologies inc. “What is 5G”, in online article. https://www.qualcomm.com/5g/what-is-5g

[6] 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

[7] 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/

[8] Samsung in online report “Samsung Phone Battery Drains Quickly on 5G Service” https://www.samsung.com/us/support/troubleshooting/TSG01201462/

[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] S. Mishra, Dr. N. Modi. “GSM Mobile Authentication Based On User SIM” in International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 6, 2014
[11] P. Razmjouei, A. Kavousi-Fard, M. Dabbaghjamanesh, T. Jin and W. Su, "Ultra-lightweight Mutual Authentication in the Vehicle Based on Smart Contract Blockchain: Case of MITM Attack," in *IEEE Sensors Journal*, doi: 10.1109/JSEN.2020.3022536.
[12] Yaseen, M., Iqbal, W., Rashid, I. *et al. MARC*: A Novel Framework for Detecting MITM Attacks in eHealthcare BLE Systems. J Med Syst 43, 324, 2019. https://doi.org/10.1007/s10916-019-1440-0
[13] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua and P. Haskell-Dowland, "Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks," *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand, 2019, pp. 1-6, doi: 10.1109/ITNAC46935.2019.9077977.