SECURITY CHALLENGES IN FIFTH GENERATION MOBILE COMMUNICATION

[1]VIJAYASANTHI S
[1]M.Phil Research Scholar,
M.Phil Computer Science,
[1]KG College of Arts and Science, Coimbatore, Tamil Nadu, India.

ABSTRACT: The advanced features of 5G mobile wireless network systems yield new security requirements and challenges.The potential attacks and security services are summarized with the consideration of new service requirements and new use cases in 5G wireless networks. The recent progress and the existing schemes for the 5G wireless security are accessible based on the corresponding security services, including confirmation, availability, data con- fidentiality, key management and privacy. This paper further discusses the new security features involving different technologies applied to 5G, such as heterogeneous networks, device-to-device communications, massive multiple-input multiple-output, software-defined networks and Internet of Things.

Keywords: 5G, D2D, MIMO, SDN, IoT, Network Security

I.INTRODUCTION

5G technology is the next step in the advance of mobile communication. 5G will not only provide voice and data communication but also present capabilities for new technologies such as Internet of Things. 5G is no longer curbed to provide faster mobile services for voice and data communication but as a substitute it will serve vertical industries, which will cultivate a new form of services. The new networking technologies such as such as Software Defined Network (SDN)/Network Functions Virtualisation (NFV) will further enhance the 5G capability to provide an effective platform for new services/businesses to flourish.[1]

These new technologies also bring new bullying. NFV establishes virtualised networking tone fanatical to provided that poles apart network military and the security of data hosted in these virtualised environments mostly depends on the degree of segregation between virtualised components. It always remains a challenge to provide a fully dependable secure NFV environment and hence next generation mobile networks should have security joystick in place to address the vulnerabilities imposed by NFV atmosphere. Similarly, SDN brings a new form of threats because of centralised software regulator controlling network flows. Although these issues are not specific to 5G technology but 5G security agenda should address these issues and provide a secure environment for next cohort network.

The varying network is another driver for 5G defence. In contrast to LTE network which is owned by a single network operator to have the funds for network services to its customer, 5G networks will be composed of a number of stakeholders given that specific services.

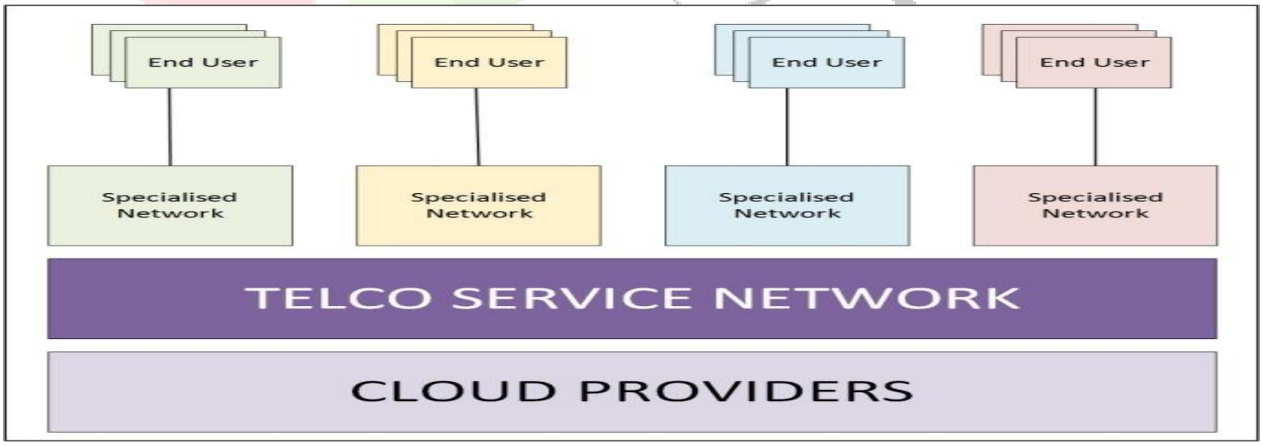

Fig 1.1.Cloud Providers

These new focused networks will result in new trust model for 5G networks with an further element of services compared to traditional 4G trust model shown below [1].

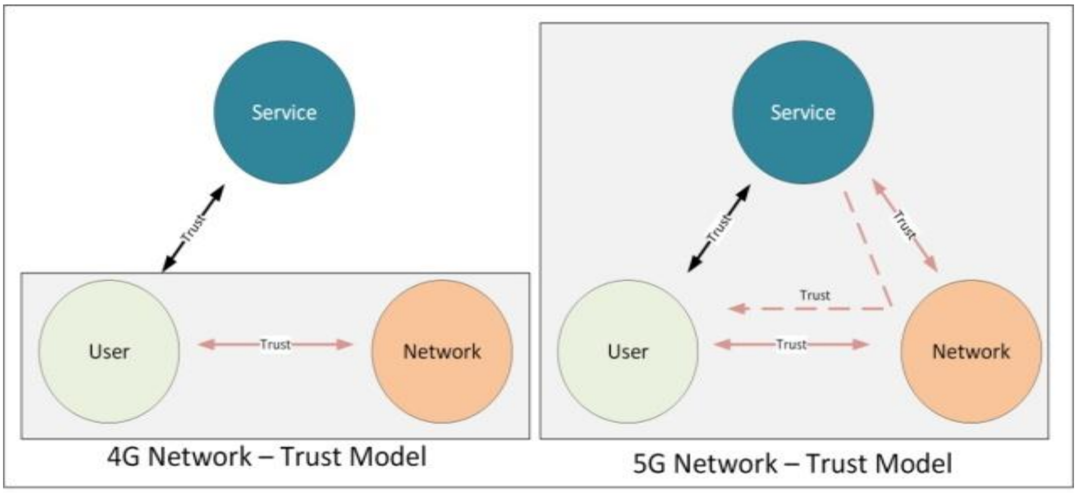

Fig.1.2 4g&5g Trust Model

The Next invention Mobile set of connections (NGMN) treaty highlights the following security requirements in 5G Whitepaper:

- Strong Subscriber Authentication
- Must provide the security mechanism for protecting diverse range of information.
- Bearer-independent (e.g., higher layer) security (end to end security)
- Secure network design
- Resilience and High Availability to provide 99.999% network availability
- Reliability

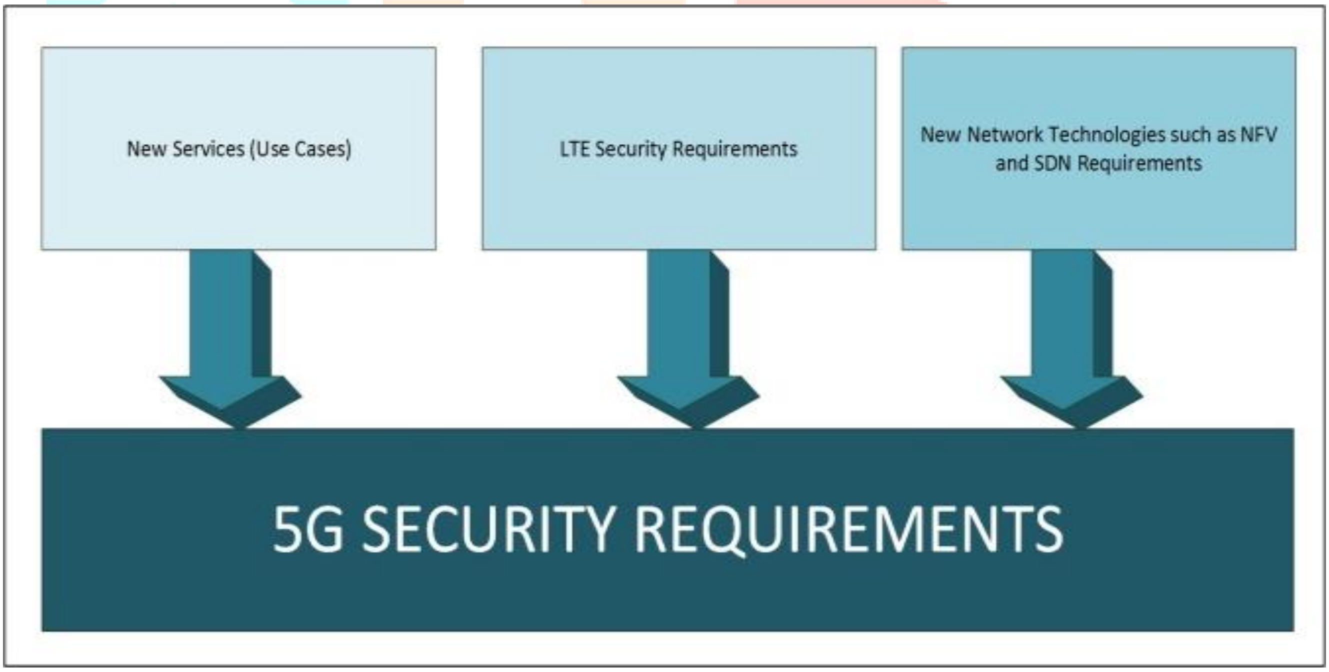
New Services (Use Cases)
LTE Security Requirements
New Network Technologies such as NFV and SDN Requirements
5G SECURITY REQUIREMENTS

Fig 1.1 5G Requirements

III.SALIENT FEATURES OF 5G

The features and its usability are much beyond the prospect of a normal human being. With its ultra-high speed, it is potential enough to change the meaning of a cell phone usability.

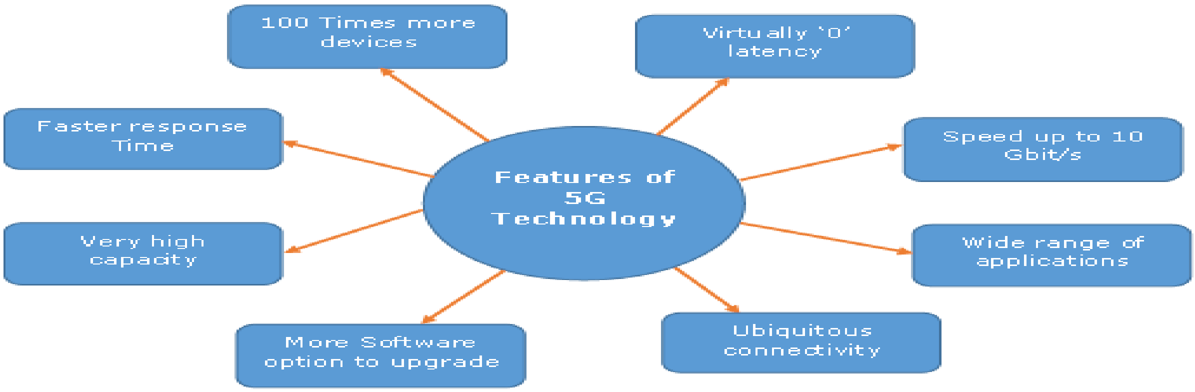

Fig.3.1 Features of 5G

Starting from the First invention (1G) in 1980s, Second invention (2G) in 1990s, Third invention (3G) in 2000s, Fourth invention (4G) in 2010s, and now Fifth invention (5G), we are advancing towards more and more sophisticated and smarter technology.

Fig.3.2 Mobile Generation

VI. CHALLENGES AND FUTURE DIRECTIONS FOR 5G WIRELESS SECURITY:

The challenges and future directions for 5G security research and development are presented in this section. According to the previous sections, part of the security solutions used in 4G will be evolved into 5G. However, with extensive use cases and various integrated technologies applied to 5G, security services in 5G face many challenges in order to address 5G advanced features. Several perspectives of the challenges and corresponding future directions are discussed as follows.[3]

A.NEW TRUST MODEL

With the advanced services offered by 5G wireless networks, not only new types of functions are provided to people and society, but also new services are applied to vertical indus- tries, such as smart grid, smart home, vehicular networks and m-health networks, etc. In the legacy cellular networks, user terminals, home, and serving networks are considered in the trust model. The trust models vary among different use cases which can involve new actors in 5G wireless networks . The authentication may need to be implemented between various actors with multiple trust levels.

There have been research work on trust models for dif- ferent use cases. Eiza *et al.* proposed a system model to facilitate secure data transmission over 5G wireless net- works for vehicular communications. DMV, TA, LEA, and vehicles are included in the proposed system model. The trust model between them is more complex than the trust model in the legacy cellular networks. [3]

With the massive number of devices over 5G wireless networks, new trust models are needed to improve the performance of security services such as IoT user cases authentication. However, it lacks a trust model between devices and fusion center in. For some applications, there are various types of devices connected to the same network, some of which may be used only to gather data and some of which may be used only to access internet. The trust requirements of different devices should be different. For different security demands, the corresponding trust model may have different security requirements. As an example, a high security level demand may require both devices.

B.PRIVACY PRODUCTION:

With data involved in various new applications in 5G, huge volume of sensitive data are being transmitted through the 5G wireless networks. 5G wireless networks raise serious concerns on privacy leakage due to the open network plat- forms of the privacy is an important requirement for implementing different applications.

The pri-vacy protection in different use cases can vary based on the security requirements, such as location privacy, identity privacy. For example, in , to secure the privacy of patients, the proposed protocol provides security of data access and mutual authentication between patients and physician

C. FLEXIBILITY AND EFFICIENCY

To address different security requirements for different appli- cations and dynamic configurations of the 5G architecture based on virtualization, the security mechanisms must be flexible. The security setup must be customized and optimized to support each specific application instead of an approach fitting all .[5]

Therefore, for each security service, different levels need to be considered for different scenarios. If differentiated security is offered, a flexible security architecture is needed . In our proposed security architecture, network functions in the control plane are various depending on the use cases.

D. UNIFIED SECURITY MANAGEMENT

Although there are different services, access technologies and devices over 5G wireless networks, a security frame- work with a common and essential set of security features such as access authentication and discretion shelter is needed.

The basic features of these security services may be similar to those in the legacy cellular networks. However, there are many new perspectives of these security features in 5G wireless networks, such as the security management across assorted access and security management for a large number of devices.[6]

V.CONCLUSION

The techniques and technologies discussed in section IV are mostly integrated in LTE-A, however mmW is still awaited. MIMO, CA, CoMP, C-RAN, HetNets are deployed, and enabled operators to achieve better throughput, and resource utilization. Moreover these techniques resulted in increased spectrum efficiency and reduction in cost per bit. They also meant to increase data rates to meet the promised limit of LTE-A.

Extension in IMT frequency spectrum is the key enabler of 5G; it can definitely provide targeted data rate of 5G. Successful experiments of cmW and mmW conducted by various vendors clearly show that 5G is reality about to happen. mmW has limitation of coverage due to its inherent characteristics.

VI.FUTUREWORK

To determine buffering requirements and queue management for 5G networks, we are conducting simulations to draw statistical results. Transmission impairments in mmW technology are a major hurdle. These instigate scientific community to come up with such solution that mitigates these problems.

Microwave and wire is already in use in backhauls, it is thought that fiber optic and mmW can be used for both fronthaul and backhaul. Future wireless networks might witness a total guided backhaul using fiber optic. The other promising areas for realization of 5G include orbital angular momentum encoding, full duplex, and non-orthogonal wave form seeks attention of research community.

REFERENCE

[1] “5G: A Technology Vision” huwaei technologies.

[2] Jawed Ibrahim, “4G Features” Bechtel Telecommunications Technical Journal, December 2002.

[3] H. Khan, M. A. Qadeer, J. A. Ansari and S.Waheed. 4G as a Next Generation Wireless Network. Future Computer and Communication, 2009. ICFCC 2009.International Conference, April 2009

[4] Engr. Muhammad Farooq, Engr.Muhammad Ishtiaq Ahmed, Engr. Usman M Al , “Future Generations of Mobile Communication Networks” Academy of Contemporary Research Journal V II (I), 15-21, ISSN: 2305-865, January 2013.

[5]P. Schulz et al., “Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture” in IEEE Communications Magazine, 55(2): 70-78, 2017.

[6] M. Simsek, D. Zhang, D. Öhmann, M. Matthé, G. Fettweis, “On the Flexibility and Autonomy of 5G Wireless Networks” in IEEE Access, 2017.

[7] Keerthana.V A “Survey paper on Security protocols of Wireless Detector Networks” International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 5, Issue IX, ISSN:2321-9653 September 2017