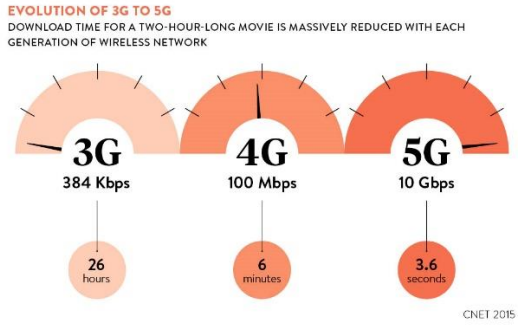
A REVIEW STUDY ON 5G NETWORK EMERGING SECURITY AND CHALLENGES

rana kumar saini[1], bhanu sharma[2], ashutosh sharma[3]
B.Tech(CSE), CGC Technical Campus,Jhanjeri (Mohali),India[1]
Assistant Professor, CSE Department., CGC Technical Campus,Jhanjeri (Mohali),India[2]
B.Tech(CSE), CGC Technical Campus,Jhanjeri (Mohali),India[3]
ranakumarsaini@gmail.com[1]
bhanu.sharma0989@gmail.com[2]
ashutoshv146@gmail.com[3]

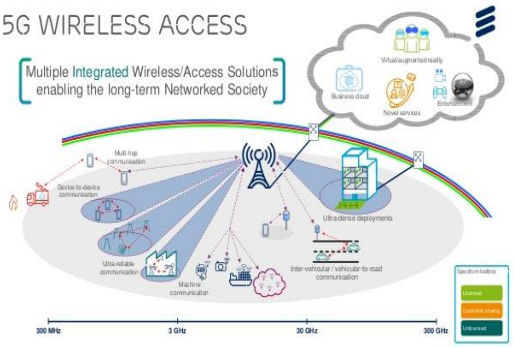
Abstract—
5G Network is more modulated form of network technology. It enhances the security and data transfer rate. Increase bandwidth means loss in coverage area. Cloud security provide by 5G network is major challenges in the field of network security. Rapid growth of subscribers in the network and servers are weak the regrowth of new generation technology implemented more secure and more reliable network.5G network performs smart work in internet of everything. It improve data rate 10GBPS .It have feature of100% coverage capacity and execute 100 time more capacity then 3G and 4G network. It have very low latency network and strong battery life up to 10 years. Multiple services run in parallel way to detects the natural resources.

Keyword: Development challenges, SDN, Radio security, Cloud security, Identity manager, benefits.

Introduction: 5G is fifth generation mobile communication technology. In future will use integration of many technologies that will be provide the high data rate and 2GHZ to 8GHZ frequency band used. The signification of mobile wireless communication is reflected is a fast speed of technological innovation the second generation mobile communication system that start in near to end of 20th century and the 3G system was launched in 2001, uses a sophisticated radio interface for 4G.



The generation growth of technology with respect to years and bandwidth ranges for different eras of communication. More specifically, there are eight advanced features of 5G wireless systems, 1-10 GBPS connections to end points in the field 1 millisecondlatency,1000xbandwidthperunitarea,10- 100 x no. of connected devices, 99.999% availability, 100% coverage,90% reduction of network energy usage and up to ten years battery life for low power devices. To achieve these performance requirements, various technologies are applied to 5G systems, such as heterogeneous networks, massive multiple-input multiple-output, millimetre wave, D2D communications, software defined network, network functions visualization and networking slicing. The standardization process for 5G wireless systems is just at the very beginning. Figure illustrates a generic architecture of 5G wireless systems.



5G wireless systems can provide not only traditional voice and data communications, but also many new use cases, new industry applications, and a multitude of devices and applications to connect society at large. Different 5G use cases are specified such as vehicle-to-vehicle and vehicle-to-infrastructure communications, industrial automation, health services, smart cities, smart homes and soon. It is believed that 5G wireless systems can enhance mobile broadband with critical services and massive IoT. Then architecture, new technologies, and new use cases in 5G wireless systems will bring new challenges to security and privacy protection.

1. Key Challenges For Deployment of 5G Network:

A. Increased **Bandwidth means Loss Coverage Area:** One of the key advantages of 3G cell towers was that they could cover immense territory with relatively few cells. This is because the network did not require as much bandwidth, meaning networks had to deploy fewer cells. When technology progressed to 4G networks, the cells were producing more bandwidth, meaning the coverage radius of each cell was smaller. People may have noticed that their coverage may drop more often than on their 3G network. As the 5G network gets rolled out, this trend will continue. More cell towers will be required to produce this immense bandwidth because the cells are not able to cover as much space as a 3G or 4G cell. Because more cells will need to be rolled out, 5G user should expect that their coverage may not be as widespread at first.

B. Data/Signal Losses: We have the probable losses in the 5G millimetre wave. These losses can happen due to different reasons – right from penetration problems, to foliage losses, rain attenuation, and a host of other factors. It also remains to be seen whether the ‘speed advantage’ of 5G indeed matches the expectations of software developers and

end-users. The technology is still under development, the final specifications are yet not confirmed by the IEEE – and the speeds that can be achieved in a controlled test environment might be impossible to achieve in a real-world scenario, thanks to technological shortcomings. The first full 5G network might arrive in the US in early-2019 – but expecting it to be fully operational immediately will be too naïve.

C. **Uncertainties over Coverage and Radio Frequencies:** There are reports indicating that 5G macro-optimized will, in all probability, use the 6 GHz (maybe, slightly lower) frequency. The catch over here is, this radio frequency band is already being used by satellite links and many other different signal types. This particular frequency range is already overcrowded – and it is very much possible that there will be some lingering problems with data transmissions (i.e., in sending/receiving signals) in this radio frequency. Complicating matters further is the fact that the 5G network cells will offer lower coverage than those of 4G (in spite of the exponentially higher bandwidth). This would mean that more cell towers will be needed to make 5G technology mainstream over time. The coverage of 5G can be up to 300 meters in the outdoor environment and a rather lowly 2 meters indoors.

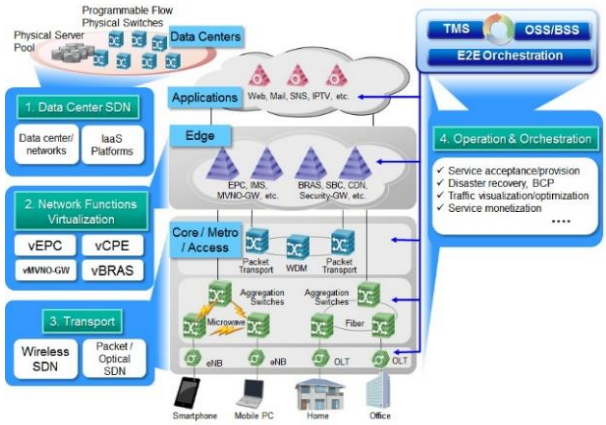
D. **Access to Spectrum:** Although cognitive radio was often touted as a solution to the problem of frequency spectrum shortage, it is seldom adopted as there are always concerns about the impact on the primary user or license holder of the spectrum. An alternative solution proposed which can potentially solve this dilemma is Authorized Spectrum Access (ASA) also known as Licensed Spectrum Access (LSA). The concept of LSA is to allow autho

B. users to access licensed spectrum based on certain condi set by the licensee of the spectrum. This would allow u utilized spectrum to be more effectively used and also s the problem of quality of service for the primary user.

2. Security services of 5G Network:

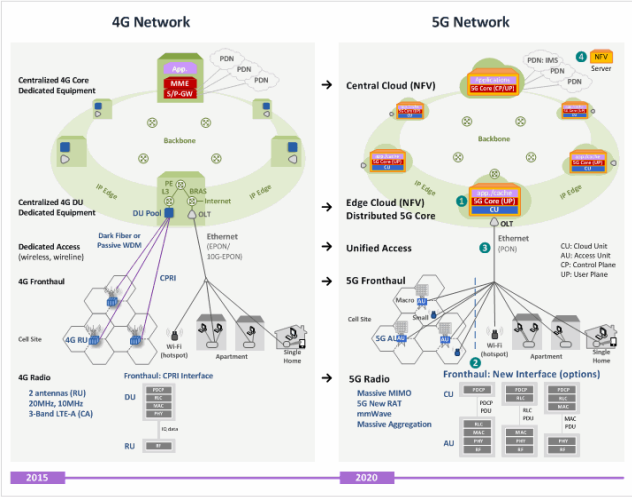
A. Software define network: Software-De Networks (SDNs) ease network configuration and evol as well as policy enforcement. SDN is based on principles that enable faster provisioning and configur of network connections:

I. Decoupling of control and data plane: Data plane n (switches) query the control plane (SDN controller) to forwarding instructions when new packet flows emerge.
II. Programmability of network services: the administ may introduce complex rules and programs for the co layer, which are then consistently executed in the data pl
III. Logically centralized control: network administrator program the behaviour of the traffic in a centralized man SDN is typically used with network function virtualiz (NFV) technologies. NFV provides a virtualiz framework where it is possible to create mobile netwo entities and services as Virtual Network Functions (VNFs) on demand and place them at the most suitable location using the most appropriate amount of resources.



Network slicing is a concept based on SDN. It enables the deployment of multiple logical networks independently on a common physical infrastructure platform. Network slices are created on-demand and they are isolated and restricted to the assigned resources. Micro-segmentation is a concept originating from data centres, but its viability has been considered for mobile networks as well. In a 5G network, a micro-segment can be defined as a network portion, which has been dedicated to a particular application or user and which protects particular (critical) network functions with the same security requirements. While an end-to-end slice contains all functions needed to create 5G connectivity, micro-segments may contain only one or a few functions that are secured using micro-segment specific means and policies. Micro-segments may be utilized to deploy fine-grained isolation, specific access controls, and tuned security policies and controls that fulfil application-specific trust models.

B. 5G Radio Security Network: 5G networks need to be better equipped to proactively find threats and vulnerabilities before they become an issue with application / L7 visibility and controls across all layers including application, and data, at all locations. With billions signaling of connected devices and critical enterprise applications now relying on 5G networks, MNOs cannot wait to address attacks and security incidents after they have already happened. Due to the evolved threat landscape and new technology that provides users with low-cost alternatives to program their own devices (even at radio access level), the attack resistance of radio networks should be a more clearly outspoken design consideration in 5G, analyzing threats such as Denial of Service from potentially misbehaving devices, and adding mitigation measures to radio protocol design. Although LTE radio access has excellent cryptographic protection against eavesdropping, there is no protection against modifying or injecting user plane traffic. With 5G radio access as a building block in, for example, industrial automation, the potential benefits of adding integrity protection seem worthy of investigation.



C. Cloud Security: With virtualized and highly distributed networks, effective 5G security outcomes will require actionable insights at cloud-scale. Cloud based threat prevention mechanisms powered by advanced big data analytics and machine learning techniques is critical to provide swift response to known and unknown threats in real-time. With device-initiated botnet attacks becoming more likely in 5G, cloud automated prevention mechanisms allow MNOs to not only find but isolate infected devices. Cloud security will be added to the list of 5G concerns. Develop hypervisors and network virtualization with high assurance on isolation. As mentioned, investments in this area could pay off, as this would greatly simplify the handling of diverse security requirements in the same infrastructure. Build useful ecosystems and architectures from existing trusted computing tools and concepts for remote attestation, for example. Provide more efficient solutions for cloud-friendly data encryption. Develop easy-to-use, trusted management of cloud systems and the applications.

D. Identity Manager: The 4G LTE standard requires USIM on physical Universal Integrated Circuit Cards to gain network access. This way of handling identity will continue to be an essential part of 5G for reasons such as the high level of security and user friendliness. Embedded SIM has also significantly lowered the bar for deployment issues related to machine-to-machine communication. Still, there is a general trend of bring-your-own-identity, and the 5G ecosystem would generally benefit from a more open identity management architecture that allows for alternatives. One example would be to allow an enterprise with an existing, secure ID management solution to reuse it for 5G access. Examining new ways to handle device/subscriber identities is therefore a key consideration that should enter the investigation of the new trust models for 5G. Concepts such as network slicing can provide an enabler for securely allowing different ID management solutions side-by-side by confining usage to virtual, isolated slices of the network. The threat of IMSI catching, where rogue radio network equipment requests mobile devices to reveal their identity, was discussed during the 3G and 4G standardization process. However, no protection mechanism was introduced at that time, as the predictable threats did not seem to justify the cost or complexity involved. It is not clear whether this risk analysis is still valid, and enhanced IMSI protection deserves consideration for 5G.

3. Benefits of 5G Networks: Three main benefits categories have been defined for 5G Network:

A. Enhanced Mobile Broadband: Builds on the existing 4G mobile broadband model by providing higher bit rates and improved efficiencies. Mobile operators recognise this need given the expected growth in general mobile usage of internet-based content and services. Several markets, like Japan and South Korea, are driving MBB to support the growing density of traffic in their major cities. In addition, several early initiatives are underway to use mobile systems to provide cost efficient alternatives to fixed services to homes and offices.

B. Massive Internet of Things: Addresses the support for high density of connected devices, e.g. related to smart cities, smart energy grids, and so forth. Sensors, control units, and other connected devices will be used to optimise time, effort and performance in various contexts. Besides supporting a huge number of devices, power consumption of the devices is reduced to allow for extended battery operation of up to 10 years. Many companies and the public sector deem IoT as interesting for addressing new business verticals such as health monitoring, transport management and production control.

C. Ultra-Reliable Low Latency: Is designed to support business or mission critical communication scenarios, such as during emergency situations. Remotely operated or autonomous vehicles or robots also belong to this category. Many use cases are still to emerge, and we expect governmental agencies and specific industries and possibly gaming to drive this. Examples include public safety services, remote operation of excavator/mining vehicles, industrial robots and virtual and augmented reality used for remote inspection, remote medical intervention, and entertainment.

4. Conclusion: 5G is an emerging technology with a concept of wireless networks. 5G wireless network are expected to provide advanced performance to enable many new applications. In this paper, I am first discuss various security services and challenges include high cost and loss data rate/ data signals. Based on the fact that the impact of the data loss in 5G Network. Data loss and coverage area for major issues for 5G Network.

REFERENCES:

[1].www.acma.gov.au/theACMA/~/media/47F68EC7164A4BBD88D29D1420ADA3A4.ashx
[2]. www.cora.ucc.ie/handle/10468/5072
[3].www.digitalcommons.usu.edu/cgi/viewcontent.cgi?article=120&context=ece_facpub.
[4].www.iamanonymous.com/5g-security/
[5].www.ieeexplore.ieee.org/document/67296589.
[6].www.ieeexplore.ieee.org/document/6812298.
[7].www.ieeexplore.ieee.org/document/8125684.
[8].www.lightreading.com/mobile/5g/5g-and-millimeter-wave=band-challenges/a/d-id/735852.

[9].www.researchgate.net/publication/284027607_key_technologies_and_problem_in_deployment_of_5g_mobile_communication_system.
[10].www.uk5g.org/discover/read-article/the-problem-with-5g-deployment/