International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

# Analysis of 5G Mobile Technologies and DDOS Defense

**Fareena Pathan, Komal Shringare**

*Student, Department of MCA, YMT College of Management, Institutional Area, Sector-4, Kharghar, Navi Mumbai, Maharashtra 410210*

---

**Abstract -** *5G will provide broadband access all over, consider higher user quality, and enable connectivity of large range of devices. Huge growth is expected in connected devices to continue—even speed up—leading to significantly more connection points, and web traffic. The most common 5G technologies are Photonic & NOMA.*

*Photonic technologies are mostly utilized in optical communication systems and networks because of their unique characteristics in terms of bandwidth, immunity to electromagnetic fields, compatibility with the optical fiber and flexibility.*

*In 5G transport layer, it will allow the transmission and routing of giant amounts of data traffic at an appropriate cost and additionally the transformation of the radio access network. In data center, photonic interconnect and shift will allow the conclusion of a different design able to powerfully reduce the energy consumption whereas providing a high level of flexibility in resource utilization.*

*The fifth generation (5G) networks face challenges in terms of supporting large-scale heterogeneous information traffic. The advanced conception of Non-orthogonal Multiple Accesses (NOMA) has been proposed order to support more users than the amount of available orthogonal time-, frequency-, or code-domain resources. The basic idea of NOMA is to support non-orthogonal resource allocation among the users at the final word cost of enhanced receiver complexity, which is required for separating the non-orthogonal signals. Using NOMA, 5G networks are going to be able to provide enhanced throughput and massive connectivity with improved spectral efficiency.*

*The main aim of DDoS defences is to detect the attack as early as possible, and to kill it. It can be source-based, destination-based, network based, or a hybrid. They can be deployed at prevention level, detection level, and after the attack (source identification and response).*

*This paper proposes DDoS detection and mitigation mechanisms: Software-Defined Networking (SDN)/ Network Function Virtualization (NFV) based approaches and cloud based approaches.*

***KeyWords*: 5G Technology, 5G transport layer, Photonics, NOMA (Non-orthogonal Multiple Access), DDOS (Distributed Denial-of-Service), Attacks, SDN, NFV.**

## 1. INTRODUCTION

5G is the upcoming mobile technology which has the possibilities to transform the economies, societies and our fast rate lifestyle. This technology has data consumption and a faster data rate. The 5G can stream 4k videos without buffering. The 5G technology main goal is to achieve a high data rate, low latency, low power consumption, improved system capacity and the most important thing—huge device connectivity.

### 1.1 5G System Architecture:

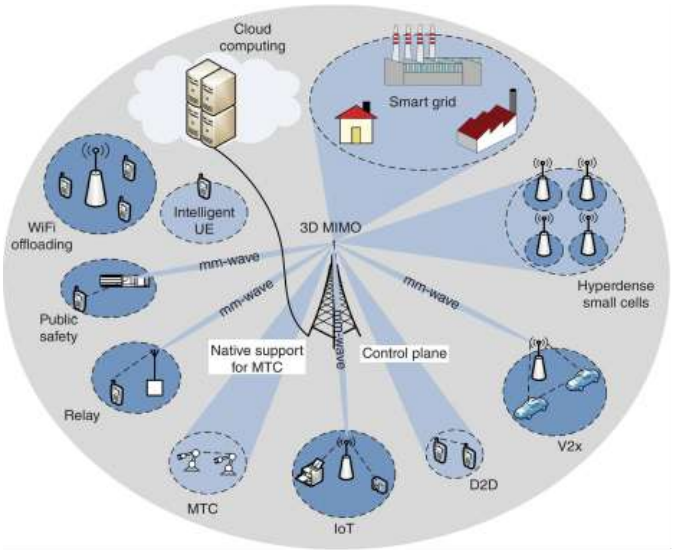


**Figure-1** 5G system architecture[1]

As illustrated by Figure one, 5G are a very system supporting a large vary of applications from mobile voice and multi-Giga-bit-per-second mobile net to D2D and V2X (Vehicle-to-X; X stands for either Vehicle (V2V) or Infrastructure (V2I)) communications, furthermore as native support is used for MTC and public safety applications.

3D-MIMO (Multiple Input, Multiple Output) are enclosed at BSs to boost the info rate and also the capability at the macro-cell level. System performance in terms of coverage, capability and increase in dead and hot spots using relay transmitters, Hyperdense small-cell deployments or Wi-Fi offloading; directional mmWave links are used for Telecommunication using the relay and/or small-cell BSs.

D2D (Device to Deice) communications are motor-assisted by the macro-BS, providing the management plane. Good grid application expected for 5G, enabling the electricity grid to control in a very additional reliable and economical method[1]. Cloud computing will be applied to the RAN, (Radio Access Network) the mobile users which will kind a virtual pool of resources managed by the network. The applications cloud is nearer to the top user which can scale back the communication latency to support delay-sensitive period of time management applications.

## 2 Next Generation of 5G Technology:

The latest wireless mobile technology is 5g mobile Network.

### 2.2 Photonics of 5G Networks:

Photonic technology can play a key role in 5G technology in several contexts. In 5G transport it'll permit the transmission and routing of big amounts of knowledge traffic at a suitable value and also the transformation of the radio access network. In knowledge center, photonic interconnect and shift can permit the conclusion of a brand new design able to powerfully cut back the energy consumption whereas offer a high level of flexibility in resource utilization. In future hardware platforms, photonic chip-to-chip interconnect can permit a major increase of information measure density resulting in dramatically scaled up world capability of these platforms.


**Figure-2:** Transport network evolution towards 5G. [4]

As Illustrate by Figure 2. Fiber optic transmission links became commercially available within the second half of 80s and shaped the supposed photonic layer of PDH (plesiochronous digital hierarchy) networks 1st and SDH/SONET (synchronous digital hierarchy), and distance (from many tens of km up to lots of and thousands Km) to modify a dramatic fall of the value per transmitted bit. Then the arrival of optical switch devices, largely based on WSS (wavelength selective switch) technology [2], has allowed any price saving, due to: reduction of the amount of optical-to-electrical-to optical (OEO) create sites; risk of rerouting individual optical channels in a reconfigurable mesh topology; implementation of prices effective protection schemes. More, optical switches work and offload work of the digital cross-connects [3], whatever based on SDH, optical transport network (OTN) or packet technologies. In this method, the optical layer consists each of optical transmission lines also as optical cross-connect (OXC) or reconfigurable optical add-drop electronic device (ROADM).

### 5G transport network architecture and photonic systems

A relevant modification is diagrammatical by the evolution of the radio access network and, specifically, by the transformation of the radio base station (RBS). Figure represents the most steps of that transformation. A base station primarily consists of a baseband unit (BBU) and a radio unit (RU). The previous includes all process functions performed on the baseband signal, whereas the latter works on the frequency (RF) signal, and contains the antenna part, the RF power and low noise amplifiers, and therefore the electronic equipment for digital-to-analog and analog-to-digital conversion of the downlink and transmission signals, severally. Within the traditional monolithic implementation, each BBU associated metal are integrated within the same rack and connected via an RF cable. Afterwards, the RBS was split so one BBU handles a particular variety of remote RUs (RRUs), saving instrumentation value. This transformation simplifies the preparation as a result of the RRUs are less complicated to put in and tack together, therefore reducing the operational expenditures, and permits an improved coordination among RRUs connected to constant BBU. The everyday distance between BBU and RRU is of the order of some hundred meters up to few kilometers.

To allow that transformation, it had been necessary to introduce a replacement form of interface, named fronthaul, and connected communication protocols. the foremost common one is called CPRI (common public radio interface) [5], supported a frame ready to carry digitized ratio antenna samples whereas respecting tight necessities in terms of clock frequency accuracy, latency and synchronization of information in transmission and downlink. That interface will adapt to any radio customary however information measure is angry. For example, to hold forty MHz of radio information measure, comparable to concerning a hundred and fifty Mbit/s of true traffic, results to two. 5 Gbit/s CPRI rate. For this reason, the new 5G radio can introduce new fronthaul interfaces, supported a unique split of functions between BBU and RRUs.

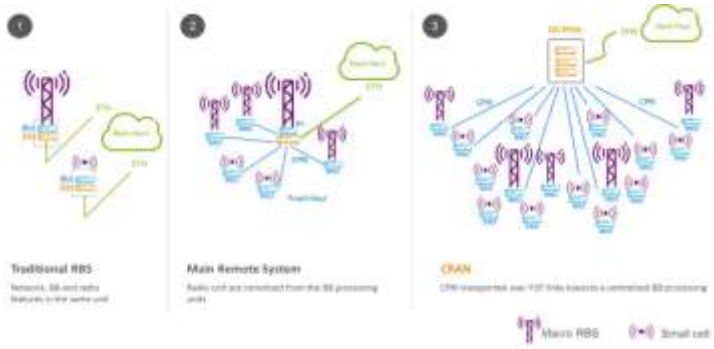


**Figure-3**: Radio access network evolution.[4]

A second step of transformation was the introduction of the centralized RAN (C-RAN). In a C-RAN, the packet process options asynchronous to the Hybrid Automatic-Repeat-Request (HARQ) loop, like the Packet knowledge Convergence Protocol (PDCP) are centralized, moreover as most of the Radio management Functions (RCF), that are guilty of the load sharing among system areas and completely different radio technologies, the policies to manage the schedulers in baseband and packet process functions, the negotiation of QoS, etc. The centralization of these functions permits network operators to modify their specification and management and to scale back the amount of websites to steer to an additional value reduction particularly in terms of operational expenditures. Packet process and management functions will eventually be virtualized on generic purpose processors (GPPs), for instance hosted in an exceedingly knowledge center, resulting in the idea of cloud RAN. Even time crucial baseband process functions (BBFs) may be centralized however virtualization is a lot of crucial during this case so they're a lot of appropriate for specific purpose processors (SPPs). The time sensitivity of the fronthaul interface between RRU and BBU, the most distance between RRU and BBU ranges from few kilometers up to few tens of kilometers.

All these transformations of the RBS and of the RAN cause vital changes in transport network. Probably, the foremost vital one is that fronthaul, that was introduced as a point-to-point link between one BBU and one RRU, becomes a replacement transport section with its peculiar necessities, distinguished by the backhaul section answerable for the communication between the RBS and therefore the remainder of the network up to the mobile core network. Backhaul networks sometimes accommodate aggregation nodes and links supported local area network transmission frames and packet switches (either local area network switches or MPLS/IP routers).

Fronthaul network instead, having to meet the tight necessities such as on top of, needs new design, nodes, and connected photonic part and modules.

### Photonics for data centers

The evolution towards flat architectures can eliminate a large variety of OE/EO changing parts so, besides photonic interconnect, photonic change can emerge as a key technology [2,3,8,9]. The inside packet aggregation interconnect network consisting of packet switches, within the future photonic change may offload a part of the work by introducing a given quantity of circuit change, as an example to route long information flows that are most of internal information traffic volumes [6,10]. During this method the long lasting information flows are photonic switched whereas all the opposite area unit separately (packet-by-packet) switched in the electrical domain. The offloading of packet switches work conjointly ends up in improvement in the performance of short-lasting flows routing. Photonic change gives an increased flexibility within the intra-DC interconnection among servers and storage parts to optimize the resources utilization. These days there are units static optical shuffles that area unit chargeable for that operate. Instead, a flexible and reconfigurable optical information center may give a coordinated management of network resources and also the capability to portion dynamically the network capability. This can be created possible by re-applying the idea of SDN management and network operates virtualization within the DC domain, in conjunction with a flexible photonic switched information plane.

### 2.3 NOMA (Non-Orthogonal Multiple Access):

Non-orthogonal multiple access (NOMA) schemes have received important attention for the fifth generation (5G) cellular networks [11]-[12]. The first reason for adopting NOMA in 5G owes to its ability of serving multiple users using constant time and frequency resources. There exist 2 main NOMA techniques: power-domain and code-domain.1 Power-domain NOMA attains multiplexing in power domain, whereas code-domain NOMA achieves multiplexing in code domain.

**2)**As shown in Fig. 4, the base station (BS) sends the superposed signals to 2 users, wherever User one has higher channel gain than User two. In NOMA, the user with higher channel gain and also the user with lower channel gain are sometimes referred to as the robust user and also the weak user, severally. The robust user initial subtracts the signal of the weak user through set, so decodes its own signal; the weak user considers the signal of the robust user as noise and detects its own signal directly. With worse channel gain and additional interference, the weak user is appointed additional power in NOMA to make sure fairness.

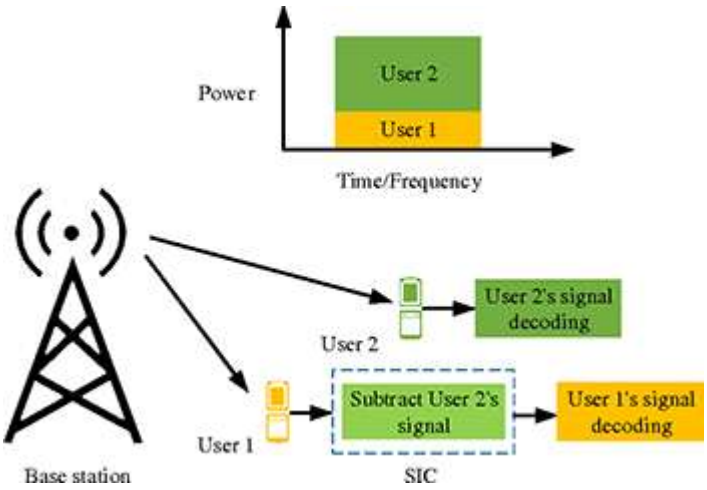


**Figure-4**: Downlink NOMA in a single cell with one BS and two users.

- **Benefits of NOMA**

NOMA dominates typical orthogonal multiple access (OMA) in many aspects, such as: **1)**Frequency resource, and mitigating the interference through SIC; **2)** It will increase the quantity of at the same time served users, and thus, it will support large connectivity; **3)** because of the coincident transmission nature, a user doesn't would like go through a regular time interval to transmit its data, and hence, it experiences lower latency; **4)** NOMA will maintain user-fairness and various quality of service by flexible power management between the strong and weak users [13]; particularly, as additional power is allotted to a weak user, NOMA offers higher cell-edge throughput and therefore enhances the cell-edge user experience.

## Limitations of NOMA

Various limitations and implementation problems need to be self-addressed to take advantage of the total benefits of NOMA, such as: **1)** every user has to rewrite info of all alternative users with worse channel gains (which are in the same cluster) before coding its own information [1], resulting in extra receiver complexity and energy consumption compared with OMA; **2)** once a mistake happens in attack at a user, the following coding of all alternative users' data can doubtless be distributed mistakenly. this suggests keeping the quantity of users in every cluster fairly low to cut back the impact of error propagation; **3)** to get the claimed edges of power-domain multiplexing, a substantial channel gain distinction between the strong and weak users is needed. This intuitively restricts the effective range of user pairs, that successively reduces the sum-rate gain of NOMA; **4)** every user has to challenge its channel gain data to the SB, and NOMA is inherently sensitive to the uncertainty within the measure of this gain [12].

## Research Challenges

Noticeably, a main analysis challenge is to overcome the limitations of NOMA mentioned within the previous section. Additionally, many different open problems got to be addressed.

• Firstly, because the density of BSs and client devices will increase, the matter of ICI could become severe in multi-cell networks. The problem of interference mitigation can be even harder for heterogeneous networks. As such, determining techniques that mix helpful interference cancellation and management approaches with NOMA is of noteworthy importance.

• Secondly, the combination of carrier aggregation (CA) with the NOMA-based system wills additional increase the information rates of the targeted users. However, what CA kind is suitable for NOMA solutions isn't however determined.

• Thirdly, developing low-complexity resource allocation algorithms is important, as they play a important role for NOMA performance optimisation. User pairing and power allocations, beside subband assignment are thought of in [14].

• Fourthly, the combination of NOMA with different enabling technologies for 5G, i.e., large MIMO and mmWave is of significance, and additional efforts are needed to explore NOMA solutions appropriate for large MIMO and mmWave networks; [15] presents an initial study during this direction.

• Finally, a way to understand physical layer security for NOMA is a motivating analysis direction; [16] investigates this issue in large-scale networks.

## 3. Defence from DDOS:

There are four forms of attacks, i.e., eavesdropping and traffic analysis, jamming, DoS and DDoS, and MITM, in 5G wireless networks.

Denial of Service (DoS) attacks take as objective to disable computer systems or networks. The DoS attacks with origin in multiple sources are referred as Distributed Denial of Service (DDoS) attacks.

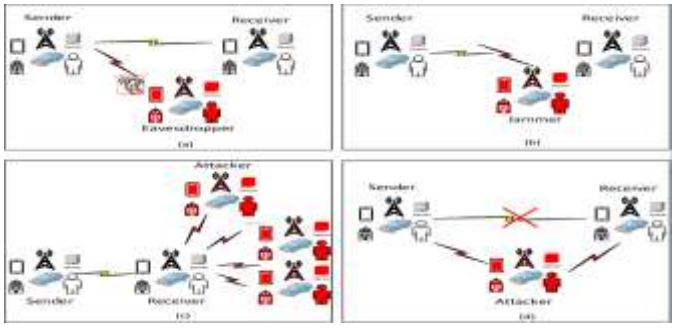

Fig. 5: Attacks in 5G wireless networks[ 17]

(a). Eavesdropping; (b). Jamming; (c). DDoS; (d). MITM

(a) **Eavesdropping:** Eavesdropping is an attack that's utilized by an unplanned receiver to intercept a message from others. Eavesdropping may be a passive attack because the traditional communication isn't affected by eavesdropping, as shown in Fig. 5a. Thanks to the passive nature, eavesdropping is tough to discover. Secret writing of the signals over the communication system is most commonly applied to fight against the eavesdropping attack. Traffic analysis is another passive attack that an unplanned receiver uses to intercept in-formation like location and identity of the communication parties by analyzing the traffic of the received signal while not understanding the content of the signal itself. In different word, even the signal is encrypted, traffic analysis will still be used to reveal the patterns of the communication parties. Traffic analysis attack doesn't impact the legitimate communications either.

(b) **Jamming:** Unlike eavesdropping and traffic analysis, jamming will fully disrupt the communications between legitimate users. Fig. 5b is an example for jamming attack. The malicious node will generate intentional interference which will disrupt the information communications between legitimate users. Jamming can also prevent approved users from accessing radio resources. The solutions for active attacks are commonly detection primarily based. However, direct sequence spread spectrum(DSSS) and frequency hopping unfold spectrum(FHSS) primarily based anti-jamming schemes might not match into some applications in 5G wireless networks. In [18], a pseudorandom time hopping anti-jamming theme is planned for cognitive users to enhance the performance compared to FHSS. Usually the characteristics of jamming, detection is feasible.

(c) **DoS and DDoS:** DoS attacks will exhaust the network resources by an someone. DoS could be a security attack violation of the supply of the networks. Jamming may be used to launch a DoS attack. DDoS may be shaped once over one distributed someone exists. Fig.5c shows a DDoS model. DoS and DDoS square measure each active attacks which will be applied at completely different layers. Currently, detection is generally used to acknowledge DoS and DDoS attacks. With a high penetration of huge devices in 5G wireless networks, DoS and DDoS can probably become a heavy threat for operators [17]. DoS and DDoS attacks in 5G wireless networks will attack the access network via a really sizable amount of connected devices. A DoS attack against the network infrastruc-ture will strike the communication plane, user plane, management plane, support systems, radio resources, logical and physical resources . A DoS attack against device/user will target on battery, memory, disk, CPU, radio, mechanism and sensors [17].

(d) **MITM:** In Man-in-the-middle attack (MITM), the attacker in secret takes control of the communication between 2 legitimate par-ties. The MITM attacker will intercept, modify, and replace the communication messages between the 2 legitimate parties. Fig. 5d shows a MITM attack model. MITM is an energetic attack which will be launched in several layers. Especially, MITM attacks aim to compromise knowledge confidentiality, integrity, and availableness. Supported the Verizon's knowledge investigation report [20], MITM attack is one of the most common security attacks. Within the gift cellular network, false base station based mostly MITM is an attack that the attacker forces a legitimate user to make a connection with a fake base transceiver station [21].

### 3.1 Security Challenges in SDN NFV and cloud are as follows:

#### 3.1.1 Security Challenges in Mobile Cloud

Cloud computing systems comprise various resources which are shared among users, it's possible that a user unfold malicious traffic to destroy the performance of the full system consume additional resources or stealthily access resource of different users. Similarly, in multi-tenant cloud networks wherever tenants run their own control logic, interactions will cause conflicts in network configurations. Mobile Cloud Computing (MCC) migrates the ideas of cloud computing into the 5G eco-systems. This creates variety of security vulnerabilities that largely arise with the field and infrastructural modifications in 5G. Now we Divided the MCC threats in targeted cloud segments into front-end, back-end and network based mobile security threats. The front-end of the MCC architecture is the consumer platform that consists of the mobile terminal on that applications and interfaces needed to access the cloud facilities run. The threat landscape on this section could vary from physical threats; wherever the particular mobile device and different integrated hardware elements are primary targets, to application-based threats; wherever malware, spyware, and different malignant software system are utilized by adversaries to disrupt user applications or gather sensitive user data [23].

**3.1.2 Security Challenges in SDN (Software Defined Network)** centralizes the network management platforms and allows programmability in communication networks. These 2 troubled options, however, produce opportunities for cracking and hacking the network. As an example, the centralized management are a good alternative for DoS attacks, and exposing the important Application SDN Programming Interfaces (APIs) to unplanned software package will render the full network down [22]. The controller modifies flow rules within the information path, therefore the controller traffic will be simply known. This makes the controller a clear entity within the network rendering it a favorite alternative for DoS attacks. The centralization of network management may also create the controller a bottleneck

for the full network thanks to saturation attacks as given in [22]. Since most network functions will be enforced as SDN applications, malicious applications if granted access will unfold disturbance across a network.

### 3.1.3 Security Challenges in NFV (Network Function Visualization)

Is extremely necessary for future communication networks, it's basic security challenges like confidentiality, integrity, credibility and nonrepudiation [24]. From the purpose of read of its use in mobile networks, it's conferred in that this NFV platforms don't give correct security and isolation to virtualized telecommunication services. One in all the most challenges persistent to the employment of NFV in mobile networks is that the dynamic nature of Virtual Network Functions (VNFs) that ends up in configuration errors and therefore security lapses [25].

### 3.2 Security Solutions in Mobile Cloud, SDN and NFV are as follows:

**3.2.1 Security Solutions for Mobile Clouds:** Most planned security measures in MCC revolve around the strategic use of virtualization technologies, the plan of secret writing ways and dynamic allocation of knowledge process points. Hence, virtualization comes as a natural possibility for securing cloud services since every end-node connects to a spe-cific virtual instance within the cloud via a Virtual Machine (VM). This provides security through the isolation of every user's virtual association from different users. Similarly, service-based restriction also will modify secure use of cloud computing tech-nologies. . In contrast to existing solutions wherever users with shared links are able to access such on-line video feeds, this design restricts access to only licensed viewers.

**3.2.2 Security Solution for SDN:** SDN facilitates fast threat identification through a cycle of gathering intelligence from the network resources, states and flows. Therefore, the SDN design supports extremely reactive and proactive security watching, traffic analysis and response systems to facilitate network forensics, the alteration of security policies and Security Service insertion [26]. Consistent network security policies will be deployed across the network because of international network visibility, whereas security systems like firewalls and Intrusion Detection Systems (IDS) will be used for specific traffic by change the flow tables of SDN switches.

**3.2.3 Security Solutions for NFV:** The security of VNFs through a security adapter in correspondence with the ETSI NFV design is bestowed in [27]. The projected design provides security not only to the virtual functions in a very multi-tenant surroundings, however additionally to the physical entities of a telecommunication network. Using sure computing, remote verification and integrity checking of virtual systems and hypervisors is projected in to supply hardware-based protection to non-public info and detect corrupt software system in virtualized environments.

## 4. CONCLUSIONS

In this paper we've planned 5G System architecture that is that the main contribution of the paper. There are many enhancements from 1G, 2G, 3G, and 4G to 5G within the world of telecommunications. Photonics is that the basic technology for several of the photonic parts and modules mentioned during this paper: integrated transceivers, photonic switches for transport and for data centers. NOMA in this article the superior spectral potency of noma is very promising for 5G radio access. The application of noma is additionally penetrable into different communication systems, as well as mmWave and visual light-weight systems. The potential of noma isn't restricted to only SISO systems; its capability will be additional increased by applying noma in MIMO systems. 5G can use mobile clouds, SDN and NFV to fulfill the challenges of huge property, flexibility, and costs. With all the benefits, these technologies even have inherent security challenges. Therefore, during this paper we've got highlighted the most security challenges which will become additional threatening in 5G, unless properly addressed. We've got additionally given the security mechanisms and solutions for those challenges

## REFERENCES

[1] "Fundamentals of 5G mobile Networks" by Jonathan Rodriguez, Publisher John wiely &Sons,June 2015.

[2] T. A. Strasser, and J. L. Wagener, "Wavelength-Selective Switches for ROADM Applications", IEEE Journal of Selected Topics in Quantum Electronics, vol. 16, Issue 5, Sept.-Oct. 2010.

[3] V. Eramo, M. Listanti, R. Sabella, and F. Testa, "Definition and Performance Evaluation of a Low-Cost/High-Capacity Scalable Integrated OTN/WDM Switch", IEEE Journal of Optical Communications and Networking, vol. 4, Issue 12, pp. 1033-1045 (2012)

[4] RoberoSabella , Ericsson IEEE 5G Tech Focus: Volume 2.

[5] CPRI Specification V7.0 (2015-10-09) Interface Specification [Online]. Available: http://www.cpri.info/downloads/CPRI_v_7_0_2015-10-09.pdf.

[6] R. Sabella, F. Testa, P. Iovanna, and G. Bottari, "Flexible packet-optical integration in the cloud age: Challenges and opportunities for network delayering", IEEE Communications Magazine, vol. 52, Issue 1, Jan 2014

[7] W. Miao, F. Yan, N. Calabretta, "Towards Petabit/s All-Optical Flat Data Center Networks Based on WDM Optical Cross-Connect Switches with Flow Control", IEEE Journal of Lightwave Technology, vol. 34, Issue 17, Sept.1, 2016.

[8] F. Testa, L. Pavesi, Optical Switching in Next Generation Data Centers, Springer International Publishing, 2018.

[9] A. Vahdat, H. Liu, X. Zhao, C. Johnson, "The emerging optical data center," in Proceedings of OFC, 2011.

[10] N. Farrington, G. Porter, S. Radhakrishnan, H.H. Bazzaz, V. Subramanya, Y. Fainman, G. Papen, A. Vahdat, "Helios: a hybrid electrical/optical switch architecture for modular data centers." in SIGCOMM'10, New Delhi, India, 30 August–3 September 2010.

[11] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges," IEEE Commun.. Surveys Tuts., vol. PP, no. 99, pp. 1-1, Oct. 2016.

[12] 3GPP, R1-163111, "Initial views and evaluation results on non-orthogonal multiple access for NR uplink," Apr. 2016.

[13] Z. Wei, J. Yuan, D. W. K. Ng, M. Elkashlan, and Z. Ding, "A survey of downlink non-orthogonal multiple access for 5G wireless communication networks," ZTE Commun., vol. 14, no. 4, pp. 17-25, Oct. 2016.

[14] M. R. Hojeij, J. Farah, C. A. Nour, and C. Douillard, "Resource allocation in downlink non-orthogonal multiple access (NOMA) for future radio access," Proc. IEEE VTC Spring, 2015, pp. 1-6.

[15] Z. Ding et al. "NOMA meets finite resolution analog beamforming in massive MIMO and millimeter-wave networks." arXiv preprint arXiv:1702.08783, 2017.

[16] Y. Liu et al., "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1656-1672, Mar. 2017.

[17] "Security for 5G Mobile Wireless Networks"Dongfeng Fang, Yi Qian, and Rose Qingyang Hu, IEEE ACCESS, AUGUST 2017

[18] N. Adem, B. Hamdaoui, and A. Yavuz, "Pseudorandom Time-Hopping Anti-Jamming Technique for Mobile Cognitive Users", 2015 IEEE Globe com Workshops (GC Wkshps), 2015, pp. 1-6.

[19] W. Baker et al., "Data breach investigations report", Methodology, vol. 36, pp. 1-63, 2011.

[20] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle

[21] Attacks", IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, 2016.

[22] 3GPP. (2017, May) SA3-Security. The Third Generation Partnership Project (3GPP). [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security

[23] S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, "Mobile cloud computing: Security threats," in 2014 International Conference on Electronics and Communication Systems (ICECS), Feb 2014, pp. 1–4

[24] A. van Cleeff, W. Pieters, and R. J. Wieringa, "Security Implications of Virtualization: A Literature Study," in 2009 International Conference on Computational Science and Engineering, vol. 3, Aug 2009, pp. 353–358.

[25] W. Yang and C. Fung, "A survey on security in network functions virtualization," in 2016 IEEE NetSoft Conference and Workshops (NetSoft), June 2016, pp. 15–19

[26] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defifined networks," IEEE Communications Magazine, vol. 51, no. 7, pp. 36–43, July 2013.

[27] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture," in 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug 2015, pp. 1255–1260