# 5G Security Artifacts (DoS / DDoS and Authentication)

M Awais Javed
*Information Security Deptt*
*(Researcher)* MCS NUST
Rawalpindi, Pakistan
awaiswill@gmail.com

Sohaib khan Niazi
*Information Security Deptt*
*(Researcher)* MCS NUST
Rawalpindi, Pakistan
Sohaib.niazi99@mcs.edu.pk

**Abstract. 5G will deliver a wider broadband access, higher and faster mobility, unprecedented connectivity and coverage to massive matrix of personal devices, mobility based (vehicular/ commercial UAVs/ Drones) and Internet of Things / Everything (IoT / IoE) nodes with ensured availability and optimum reliability. Availability is targeted through multipronged Active/Passive attacks using DOS / DDOS (RF jamming / Bandwidth jamming with malformed packets) and reliability is targeted through exploiting existing architectural weaknesses of radio and data communication protocols (LTE-A / IP based Networking). In prevailing threat landscape, concepts of adoption and integration of Software Defined Networking (SDN) and Network Function Virtualization (NFV) in 5G networks will open gateways of new networking paradigms with a focus on centralized security dynamics (overall visibility and substantial controls). These network security dynamics in diversified use cases (Internet of Everything /smart grids) will provide an optimum centralized control with a global overview, vigilant monitoring as well as prompt reaction (detection and prevention) to these prevailing threats. In this purview of the 5G cellular security matrix with a centralized SDN and NFV, this document has reviewed on 5G cellular secure communication channels to unearth the effectiveness of conventional DOS/DDoS and Authentication attacks within environment of SDN and NFV. This research will also present proposed mitigation of DOS / DDOS and incorporation of advanced authentication mechanism for more reliable cellular communication networks.**

Keywords—***5G Security; SDN; NFV; LTE-A; Communication Channels; DoS/ DDoS; Authentication; Dual-homed Switching Network (DSN)***

### *Introduction – 5G Transformation Preamble*

5G communications and networks has emerged as promising and an advanced technology for future data communication**.** 5G networks and systems are ready to hit commercial, public and corporate sectors with highly advanced features to its predecessors, which includes definitely the higher speeds (upto 10 Gbps), minimum latency (1 millisecond), broader Bandwidth, massive matrix of interconnected IOT devices, almost 100% coverage and availability, optimum usage of network energy and an extended battery life up to ten years. This complex network matrix of billions of connected devices and smart nodes will definitely supersede the concept of conventional networking. In this futuristic pressing networking requirements Software Defined Networking (SDN) and (Network Virtualization Function) NFV will come into play to upgrade this network management challenges to simplify the complex network controlling of these billions of devices / nodes [1]. As such networks will be transforming/ upgrading from 4th generation of cellular standard of Long Term Evolution–Advanced (LTE-A) standard towards 5th generation based LTE-A cellular standard, so 5G will be blending LTE-A protocols with advanced complex networking design to be accommodated within SDN architecture. This blend will result in existing hardware infra structure of LTE-A combined with readily available networking devices / solutions with optional upgradations of SDN and NFV. On other hand interestingly it will also affect the vendor specific monopoly to shift their tilt to software based solutions. Moreover 5G wireless cellular networks with Internet Service Providers (ISPs) will be switching all services to IP based core networks. In transition of this shift, conventional threats are likely travelling in parallel with this transition with more sophistication and advanced tools of penetration. This will open gateways of multipronged threats of radio spectrum as well as networking protocol exploitation in an IP based core network. This will blend the classical computer and network threats with the wireless channel of User equipment (UEs) /devices and giving more freedom of operation to attackers due to limited processing power of these UEs / devices /nodes. However, introduction of SDN based 5G networks will centralize the network control through software programming and virtualize the deployment of the core networking policy. SDN networking slicing [2] is the virtual deployment of logical / virtual networks as slices created as and when required within predefined domain of resources of core networking devices. The concept of Micro-segmentation [3] has been driven from data centers, however its implementation as a network slice in mobile / cellular networks are considered viable**.** In this logical network segmentation, one complete slice will provide minimalistic functionality to make a 5G networking cell, while micro segments may be limited to few functions within emblem of the specified programs. Micro segments may be deployed for fine-tuned isolation, specific access controls and security policies, and their centralized control for application specific trust models in 5G diversified use cases [4]**.**

### *Document Outline*

Section-I shall explains the multipronged threat landscape with security challenges to cellular communications both in LTE-A based RF channels and followed by conventional networking threat statement , possible threats in SDN and challenges in authentication mechanisms. Section-II further elaborate these threats in a cohesive manner to assess their

987-1-5386-5106-3/19/$31.00 ©2019 IEEE

effectiveness in a foreseeable future of cellular and IP based networking convergence. Section-III will add possible countermeasures and mitigation techniques. Document will be culminated with future research directions and conclusion.

# I. Security Challenges

## A. *Security Challenges in RF Channels*

As it is imminent that any wireless transmission channel is prone to intentional or unintentional disclosure and disruption through radio frequency (RF) interference. Here focus is on intentional or deliberate interference (disruption and sniffing / eavesdropping) in LTE-A cellular networks as same infrastructure is going to support upcoming 5G standards.

TABLE-I

| **LTE-A Cellular Communication Channel** | **Signals** | **Functions** | **Vulnerability** |
|---|---|---|---|
| Synchronization Signals channel | Primary Synchronization Signals (PSS) | Downlink Synchronization signal to UE | High power transmission can jam PSS /SSS as by default design these signals are detectable at low SNRs |
| | Secondary Synchronization Signals(SSS) | Provide Physical Cell identity (PCI) to UE | |
| Downlink Reference signals channel | Cell –specific Reference Signal (CRS) | OFDM transmission carries pilot or reference signals called CRS for synch | Jamming a carrier reference signal will yield a higher data error rate by misaligning the reference |
| Downlink Broadcast signals channel | Physical Broadcast Channel (PBCH) | Carries Message information Block (MIB) and use Cyclic redundancy Check (CRC) for error detection | PBCH requires low power jamming to target only 10% of downlink sub carriers and may leads to a very efficient synchronization attack |
| | Physical Downlink Control Channel (PDCCH) | Carries system information Block (SIB) which possess complete cell information and critical information of network (e.g, eNodeB idle timer, PRACH,PCLI) | Ideal for attacker to sniff and extract information of the cell and network configurations |
| Downlink control channel | Physical Control Format Indicator channel (PCIFCH) | Contains Uplink and Downlink resource allocation information | Being a sparse channel, highly prone to an efficient jamming attack |
| Hybrid-ARQ Indicator channel | Physical Hybrid-ARQ Indicator channel (PHICH) | Gives Positive and negative acknowledgements of uplink packets on a downlink channel | Being a sparse channel, highly prone to an efficient jamming attack |
| Downlink and Uplink Use Data | Physical Downlink shared channel (PDSCH) and Physical Uplink shared channel (PUSCH) | Use to transmit date from eNodeB to User and from User to eNodeB | Least important threats as requires a complex attack combing jamming and network details |
| Uplink Control Channel | Physical Uplink control channel (PUCCH) | Sends uplink control information (UCI) | Jamming requires only 25-30% of bandwidth of PUCCH |

LTE-A standard communication is generally divided in two channels i.e, LTE-A Downlink (from base station (eNodeB) to User device or equipment) and LTE-A Uplink (from User device or equipment to base station (eNodeB)). Targeting either way communication channel (Uplink and downlink channels) for jamming and spoofing can be undertaken by an attacker even with limited available capabilities. Moreover it has also been learnt that LTE-A broadcast transmission messages are in plaintext and has no encryption. Attacker can easily access all type of network configuration of the desired LTE-A system. This will definitely enhance the attacking capability of an attacker to next level. LTE broadcast message frame has mappings of physical channels to give an attacker the initiative of selecting a specific physical channel downlink. Table-I derived from [5] explains all signaling channels of LTE-A functioning and their respective vulnerabilities. Table-I give a brief description of various attack vectors on LTE-A communication channels/signals.

## B. *Security Challenges in IP Based Networks*

Networks are generally considered quite susciptable to unavailability due to easily manipulated attacks of Denial of service (DoS) with limited volume of traffic while Ditributed Denial of Service (DDoS) becomes a higher volume of traffic to choke the bandwidth either on wire or wireless. Anyway both are considered an easy to implement and nasty attacks to adversely affect the networking operations. Present day attackers are focusing more on cellular smart devices in shape of making part of their botnets with Advanced Persistent Threat (APT) due to limited defence capability of the cellular device or nodes as well as lack of security awareness in the user. Conversely these compromised UEs / devices are very handy in generating DDoS and DoS. In addition to such attacks, such UEs and devices are potentially beneficial as Theft of Service (ToS) and networking protocol's misuse / abuse results in degraded Quality of Service (QoS) (which closely related to from poor availability of service reaching again to some small scale of DoS). One such example is malformed text messages to freeze or crash the targeted device. More likely threats which are spreading through non legitmate mobile apps updates or asking the extention of unprecedented previliges. Once such updates executed or previlliges granted, these updates compromises the targeted device and make it a part of a mobile botnet / potential threat to existing cellular and networking operations. All these devices part of a botnet are ever ready to participate in an unaware DOS/DDOS attacks from command and control of the attacker or their services are stolen resulting degradtion of an assured QoS. Either way service provider (LTE-A or ISPs) and normal user/consumer will suffer. Conventional networks attacks has undergone in transformation with passage of time. Latest trends of such threats are presented in Table-II.

Generally these attacks are broadly in two classes of flooding and logical attacks. Flooding attacks are the first one described in Table-II which are volume based attacks. Logical attacks are explained as protocol based attacks or application based attacks which simply exploit the weaknesses of the programming of the network based services while the first attack exploits the inherent trust factor.

TABLE-II

| **Network specific DOS / DDOS Attacks** | **Brief Description** |
|---|---|
| Volume Based Attacks | These attacks target network bandwidth and consume it in for undesired resources. Examples of such attacks are UDP Flood attack, ICMP flood attack etc. |
| Protocol Based Attacks | Purpose is to exhaust the network device functioning. Network devices may include servers, firewalls, load balancer and routers etc. |

| | |
|---|---|
| Application Based Attacks | These are considered to be more sophisticated and serious attacks. They target the legitimate applications running on machine OS and exploit the code vulnerabilities of specific applications. Such attacks include Session Initiation Protocol (SIP) Flood Attack , Browser application through Hyper Text Transfer Protocol (HTTP) Flood Attack |

### C. *Security Challenges in SDN*

SDN has built-in monitoring tools in which network flow information is fed to a centralized controller for analysis to detect threats in that particular data flows . Attacks vectors presented in [6] which will be coming with SDN with their implementation in mobile networks. The 5G framework will support SDN and NFV to enhance scalability of network analysis with additional algorithms like machine learning and optimum management control. Prevailing security threats will be identified with correlation of 5G domains in comparison to presently enforced security standards and 3GPP LTE-A framework [7]. Security critical information is related to network configuration, network condition, data / IP based traffic statistics, cyber-attacks, application specific data reports, commercial / consumer data leakage and other detected incidental reports. 5G security threats are also going to surge with a greater concern for availability as more bandwidth means more Theft of Services (ToS). The 5G wireless channels will provide easy accessibility for exploitation by network based jamming attacks (DOS or DDOS) and there are no concrete solutions which even exist till date.

Moreover, multi domain authentications in 5G will be implemented as diversified use cases of horizontal and vertical technologies will exist between subscribers, operators and other relevant services providing parties. However, authentication in 5G will get much more complex with massive devices connected within these services than it has been imagined. In addition, security automation is also needed to make the 5G system robust against various security attacks [4],[8]. MITM attack exploited at different layers to compromise data confidentiality, integrity, and availability (CIA). In present cellular network, a false base station based MITM attack forces a legitimate user to create a connection with a fake base transceiver station [8]. Mutual authentication is introduced to neutralize the false based station attacks. Unsecured pre-authentication traffic is instrumental in extending such attacks as MITM in cellular GSM services. These attacks are successfully implemented on all past cellular generations. The basic GSM design specifications lacks network authentication and has an inbuilt potential of MITM like attacks leading straight to compromise of privacy and confidentiality.

### D. *Security Challenges in Authentication*

Authentication session is initiated to authenticate the end user/service provider or network operator using AKA (Authentication and Key Management) protocol. After authentication session is successfully completed, a session key is generated for the communicating piers for rest of the communication. Later generations of GSM like UMTS and LTE-A have adopted the concept of mutual authentication rather than user only authentication. AKA (Authentication and Key Management) protocol used in 4G LTE cellular networks are symmetric key based. It is interesting that 5G networks with multi-tier architecture due to massive nodes connections matrix will be demanding a very fast and rapid switching between authenticating piers at all ends. As the key management protocols in such multi-tier or heterogeneous networks with the requirement of a fast and a rapid authentication modes will be difficult to manage, a secure context information using SDN platform may be adopted as mentioned in [9]. The scheme of secure-context Information (SCI) will use attributes and signatures of physical layer including the MAC address of a device.

## II. COHISIVE OVERVIEW OF THREATS

LTE-A cellular communications, Network Data communication and SDN networks require secure channels for business continuity to impede the prevailing threats. Almost all communication channels today preferably deploy IPSec protocol for securing the communication lines. To impart secure tunneling in 5G communication channels, IPSec may be implemented with little alterations as described in [10]. Other security algorithms like authentication, integrity and encryption may also be integrated in LTE cellular communications as discussed in [11] to enhance the security of communication channels. Primarily such security algorithms will also produce higher overheads as well as resource exhaustion, so applying such security solutions in 5G framework are not considered workable in terms of both higher throughput and energy efficient requirements respectively. Thus a higher level of security for critical communication is achievable by utilizing novel security features such a physical layer security parameters (RF signatures/ RF fingerprints) [12], using asymmetric security schemes [13] and dynamic security parameters which can alter with the environment [14].

### A. *SDN Communication Flow Monitoring*

To monitor data channels in SDN, different methods are marked by researchers to supervise the flow of communication e.g, OpenNetMon for monitoring data flows, OpenTM to optimize load balancing and to detect anomalies in SDN, OpenSAFE for deeper analysis and altogether all these technologies are well characterized in [15]. All these SDN based appliances are focused on quality and performance as well as monitoring security threats which are degrading quality and performance. SDN based monitoring framework has been further proposed and tested by segregating the functions of monitoring data flows, data distribution, data inference, and data control. However, it is pertinent to mention that results of all these appliances revealed that each appliance performs better in singularity for its optimum output in any SDN platform. This is depicting a new picture for application based SDNs to streamline the autonomous control in handling and decreasing the false positives and negatives. Definitely opening new avenues for the demoralized vendor based monopolies.

### B. *SDN Network centralization*

As SDN network centralization will transform to a virtual control and programming with opening the doorways for potential hackers/attacker's community. For example, the centralized control is ideal for DoS or DDoS and exposing whole network to a compromise as mentioned in [16] [17].

As the SDN has the ability to control data flowing paths with a centralized controller in various communication channels, this controller will visible to network for its operations and ultimately lead to an ideal choice for DoS / DDoS attacks. The centralization of network control can also make the controller a congestion in case of saturation attacks on networks as mentioned in [17]. Moreover any malware once entered SDN networking application, will bring down the whole network to a state of disruption and disparity until detected and rectified [18]. In addition, flawed implementations expand surface of attack vectors with potential RF capabilities or have direct access to the desired networks. Sustainable protection is required to be focused in forthcoming research work to upgrade the classical security paradigm to new generation of data communication protocols. Even NFV being an integral part of SDN networks, still requires the prime security parameters like confidentiality, integrity and non-repudiation [19]. For mobile networks, these security challenges are presented in [20] to show that NFV lacks fundamental security in an isolated environment for NFV services. Basic NFV challenge is configuration flaws leading to security vulnerability in a cellular mobile network [21]. Further SDN network is completely compromised if the network centralization hypervisor is hacked [19].

### *C. **SDN Based Network Authentication***

As 5G networks will have a complex networking ecosystem evolving to FANETS (Flying ad hoc networks), MANETS (Mobile Adhoc networks) and VANETS (Vehicular Adhoc Networks), HETNETS (Heterogeneous networks) and D2D (Device to Device) including smart grids, smart infrastructure and smart cities concepts all converging in one better place of 5G. Thus, such convergence of technologies will be welcoming all black hats to one destinations and contrariwise direly demanding safe and secure networking ecosystem. Likewise this security of end user will be *initiated and* supported with a rapid and instant authentication between end piers regardless of who all are switching in which technology from any other technology with an extra out efforts for throughput and latency issues. After a foolproof authentication, these 5G actors will develop a factor of trust to further the exchange of sensitive and critical data. As of today IPsec tunneling is predominant for secure communication interfaces used in legacy cellular networks and reason of predominance is self-explanatory as attacking these interfaces require exceptional skills to intrude these interfaces. IPsec role in 5G will not be the same especially once SDN based networking will be enforced, this will open gates for potential threat surface to intrude in SDN. SDN based cellular networks can be divided in data communication channel, data control channel and internetworking channel as discussed in [22]. Presently SDN based networks are deploying TLS (Transport Layer Security)/ SSL (Secure Socket Layer) for securing these channels [6]. It is however, important to highlight that TLS/SSL are vulnerable to IP based attacks, SDN Scanner attacks [23] and absence of substantial authentication procedures to withstand networking attacks [11]. Legacy SIM cards will be transforming into embedded SIM card in which users' credentials are configured through Internet [24]. It is important to undertake security penetration testing for this embedded SIM technology before deployment in the 5G infrastructure. Flawed appliance of such innovation like embedded SIM can easily be exploited using side channel attacks and once secret key is revealed to an attacker, he can either eavesdrop passively and decrypt the communication or undertake MITM by a simple impersonation of the victim inside the network. Moreover SIM cloning cannot be ruled out in such embedded systems.

Normally it is customary that a symmetric-key based authentication is used in the mobile networks. The mutual authentication is initiated and utilized in 3G cellular networks to upgrade the one way authentication procedure in legacy cellular networks. After the authentication, to maintain data confidentiality and data integrity between cellular devices and base stations a cipher key and an integrity key are generated to provide security of communication channel on both ends. In contrary to the cryptographic mutual authentication, concept of a non-cryptographic fast authentication scheme is introduced in SDN [4], in which weighed secure-context-information (SCI) transfer to reduce latency with an efficient authentication during rapid handovers in a HetNet. Physical layer characteristics are primers of SCI used to enhance the authentication reliability with provision of unique attributes (fingerprints) of the end user. The first user-specific physical layer attribute is making a statistical model of arriving traffic as a Pareto distribution in which authentication delay is analyzed with various network scenarios. Scheme of fast authentication is proposed which will address authentication procedure using weighted secured context information (SCI) [4]. Once the first full authentication in carried out in one cell of network, that is easily implemented and propagated in surrounding / neighboring cells with verification of cellular device MAC address including physical layer attributes, with local processing.

## III. Culmination Strategy

### *A. **Mitigation Techniques For DoS / DDoS***

It is pertinent to mention that UE chipset is a firmware with specific cellular technology (GSM/ UMTS/ CDMA etc), so any upgradation in existing technology of Base stations (eNodeB) will also require the firmware of that cellar technology to be updated . These changes or upgradations may also require replacement of both ends of service provider and user equipment. Such changes may be foreseen as reallocation of RF spectrum or LTE-A technology itself. Somehow this greater shift must consider all the prevailing vulnerabilities and needed to be addressed once for all. Cellular Technology vulnerabilities as described in Table-I is countered in Table-III, however no channel is safer in LTE-A once attacker is determent to disrupt the LTE-A network.

Network based attacks are used to be protected through using anti malware systems , Firewalls , Intrusion Detection / Protection systems (IDS / IPS) followed by Unified threat management products (UTMs). However all these defensive systems are conventional techniques failed to dynamically changing threat landscape in Next Generation networks (NGNs). The main reason of failure was not the effective protection rather diversified nature of multi facet threats attacking the network in any single point of time. However, luckily later part of this decade has introduced the concept Security Operations Centre (SOC) with a centralized security control platform with long term logging, real-time monitoring and analysis of reported threats by using all conventional security systems more effectively and appropriate prevention techniques. SOC amalgamation with SDN will further the concept of a robust and proactive security mechanism for both cellular and IP based networking. 5G standards will further improve its security architecture and will be able to provide the promising services as discussed in preamble of this document.

Table-III

| **LTE-A Cellular Communication Channel** | **Mitigation** |
|---|---|
| Downlink Broadcast signals channel | Spread spectrum techniques like using Dynamic Spread Spectrum sequence (DSSS) will spread the signals on the all available Bandwidth (from 6-10 M Hz) |
| Primary Synchronization Signals (PSS) | PSS spoofing can be counter by staggering receiver timing for SSS. It may be time dependent and in case whenever time expires, the UE should not accept the PSS and select any other stronger cell within the same frequency. |
| Uplink Control Channel | Scrambling the RF spectrum allocated for PUCCH with an encryption which will hide the shared sequence of PUCCH and will not be available on band edges of uplink band. Only an authentic user will be allowed to decrypt the scrambling of frame continents. |
| Network Based Attacks | As networking attacks will degrade services by only option of absorbing it. However such attacks mitigation include dropping of IP packets from attacker by using Firewalls / IPS / NGN FW, deflect the attack to Honeypots / Honey farms , Load balancing services and the last option is shutting down the services.<br>Moreover SDN will be already equipped all such mitigation technologies as SDN have a better capabilities of analysis for network traffic flow and behavior. Same may be considered quite effective for Network based attacks. Same is explained in more depth in next paragraph of this article. |

## B. *Mitigation Techniques For Authentication Misuse*

SDN is characterized with three basic attributes logical intelligent centralization , centralized virtual programming and a high level of abstraction of complex networking functions [25]. All these attributes contributes in improvement in 5G networking key factors in terms of scalability and flexibility and ultimately the cost of deployment such networks will significantly reduce. Software Defined mobile Networking (SDMN) architecture comprise in three distinct planes (an application plane, control plane, and data plane), to integrate SDN, NFV and cloud computing all together. Though the key management is exhaustive with user rapidly switching in network cells in 5G, a controller of SDN is optimized to map the user locations for predicting his future locations. There are various physical layer attributes which constantly being sampled by SDN controller in order to analyze the multiple SCI combination for prediction. These physical layer attributes are fetched in terms of predetermined weighted SCI design of a connecting node with predefined decision rules for joining and leaving the SDN networks. The SDN utilizes Pareto distribution model for arriving and queuing traffic. Moreover, SDN as a centralized system with global visibility of the users' locations and activities as well as the network traffic behavior, desired policies can be formulated for these roaming security scenarios and broader network security. Presently NGN / advanced network security systems include Firewalls systems and Intrusion Protection systems (IPS) / Intrusion Detection systems (IDS) can be incorporated and implemented in the flow tables of SDN for a specific network traffic. In addition, such security policies needed to be incorporated in the network with a global view of the network. However, with these SDN and NFV service delivery model implementation, network vulnerabilities may also exist [26]. The separation of hardware platform specified security attributes will definitely increase the threat surface by decoupling software from hardware [2]. The concept of Network slicing is produced for isolation of a specific network in [27] and essentially to meet the increasing demand of isolation functionalities SDN and NFV. As SDN will sub divide networks into slices and each slice security may be attributed with SOC for better monitoring and prevention. As discussed earlier these networking defensive or protective systems are not beneficial if working in an isolation.

## C. *Dual-Homed Switching of Networks (DSN)*

Likewise it is proposed that Wi-Fi is now available almost in every building and corner of a street and paving its way in all future smart infrastructures (smart cities / smart grids). This all around ubiquitous availability of a wireless medium may be used more judiciously in parallel of LTE-A communication channel. As a one of function of SDN is multi domain authentications in 5G which may be utilized to integrate LTE-A and Wi-Fi in a separate network slices for one single UE. LTE-A based communication devices may be provided with a Dual-Homed Switching of Networks (DSN) facility. DSN facility will switch to Wi-Fi channel preferably when in range of friendly / authenticated Wi-Fi network and will substantially decrease the load on LTE-A base station, however core cellular network will be aware of UE presence through attached IP-based network. Service provider will maintain handover session of all UE devices once entering or leaving within predefined / friendly identified Wi-Fi networks to and from a base stations (eNodeB). This concept of DSN if implemented in coming LTE-A networks and Wi-Fi networks will provide two manifolds to 5G cellular standard.

To understand this concept let us suppose whenever UE enters in friendly identified Wi-Fi networks, it will prefer switching friendly/ identified Wi-Fi to connect over LTE-A Transmission channel once it is available. Now service provider is in picture that a particular UE has switched to Wi-Fi IP based network. First manifold is security against compromise of any wireless channel (DoS / DDoS / RF Jamming) that it will greatly enhance the redundancy in case a second channel is available for back up. Second manifold is rather more cost beneficial by reducing the ever increasing LTE-A nodes overload in near future and thus will greatly be improving QoS as well as Energy Efficiency (EE) for both the base station and user devices. This proposal is simply an amalgamation of legacy LTE-A and IP based networking with Dual homed Switching Networking (DSN) capability to address the already stated multipronged threats in a robust and greener manner as depicted in the Figure-I.

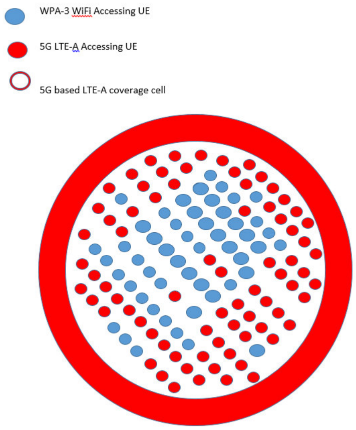

**Figure-I** 5G single Cell with dense UE while traffic load is balanced with concept of DNS (Dual homed switching of networks) using potential Wi-Fi WPA-3 standards

Further this proposal may require engagement of both the vendor specific UEs and the service providers. It is also added that Wi-Fi Alliance has announced the next generation of Wi-Fi standard in late 2018 and will ensuring its availability. In this purview, WPA-3 launching is in progress by 2019 which is also adding an additional layers of security and considered it to be much suitable for dual homed switching of cellular devices. DSN implementation with SDN may be experimented for real-time analysis with launch of 5G in production system.

### *D. Future Directions*

As discussed in beginning, LTE-A broadcast messages are in plaintext with their cellular network information available further for exploitation and to be considered as open check for a willing attacker. Same situation prevails for DoS and DDoS attacks, however SDN and NFV will be addressing all available threats in landscape of networking domain. It means that DoS / DDoS and authentication attacks will remain dominant even in coming ages of 5G. Future research shall consider this paradigm shift of all technologies at one platform of 5G as an opportunity to come out of this persistent threatening environment prevailing both in cellular and networking technologies. Innovation together with intuitions suggest that cellular technology architecture redesigning which is already in progress may be cashed optimistically, as in such prevailing threats how to trust the concepts of evolution as smart grids smart infrastructures and smart cities? These concepts to be designed in keeping all such threats at bay to ensure widespread availability without any deniability as well as a guaranteed authentication without the worries of a compromise by any stack holder (consumer / UE or administrator or a service provider).

## Conclusion

5G networks are anticipated be implemented highly advanced and innovative features of network connectivity with automation, virtualization and centralization of resources. However, exceptions of security vulnerabilities are also highlighted caused by unsecured re-authenticated traffic and ubiquitous wireless channel which is needed to be overcome by some fundamental changes to provide security against network based jamming attacks. Such novel security aspects will also appear in 5G applications wrt HetNet, D2D, M-MIMO, SDN and IOT, but we touched only SDN side for an autonomous security and centralized control of 5G ultra dense networks (UDN). We focused only communication channel, DOS and basic authentication scenarios in 5G. For this 5G may implement SDN, NFV and cloud computing to overcome problems of massive connectivity with flexibility, network security and definitely the cost factors. While highlighting inherent security challenges in 5G, some of security mechanisms and solutions for those specified challenges are also presented like effectiveness of IPSec protocol can be enhanced with a little improvement. However, limited deployment scenarios of these security mechanisms in 5G networks, the potential threat surface cannot be summarized**.** Similarly with practical implementation of new application services offered in 5G in line with massive IOT devices, the real facets of communication security and privacy challenges will be highlighted. 5G technologies and services will bring a new wave of security challenges with on scene comforts of technology and researchers must prepare to face and address it in a befitting manner.

At last not the least, the proposal of dual homed switching network (DSN) proposal is highly recommended for research community for consideration.This paper is to be considered a generalized reviewed effort to these challenges and prevailing threats against security of cellular and networking technology.

## References

[1] N. Alliance, "5G White Paper," *By NGMN Alliance 1.0*, p. 124, 2015.

[2] NGMN Alliance, "5G security recommendations Package #2: Network Slicing," *Ngmn*, pp. 1–12, 2016.

[3] J. Kindervag and A. Kindness, "Three Technical Innovations Will Ignite Zero Trust," 2015.

[4] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G Mobile Wireless Networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[5] R. P. Jover, "Security Attacks Against the Availability of LTE Mobility Networks : Overview and Research Directions," no. January 2013, 2017.

[6] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," *IEEE Secur. Priv.*, 2016.

[7] U. M. Tel, "ETSI TS 13 Digital cellular teleco communications system ( Pha 3GPP System A Architecture Evolution ( SAE," vol. 0.

[8] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[9] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," *2016 IEEE Int. Conf. Commun. ICC 2016*, 2016.

[10] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, "Secure communication channel architecture for Software Defined Mobile Networks,"

*Comput. Networks*, vol. 114, pp. 32–50, Feb. 2017.

[11] M. Y. Ijaz Ahmad∗, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, *5G Security: Analysis of Threats and Solutions*. 2018.

[12] G. Baldini, R. Giuliani, and E. C. Pons, "An Analysis of the Privacy Threat in Vehicular Ad Hoc Networks due to Radio An Analysis of the Privacy Threat in Vehicular Ad Hoc Networks due to Radio Frequency Fingerprinting," no. May, 2017.

[13] Caidan Zhao ; Lianfen Huang ; Yifeng Zhao ; Xiaojiang Du, "Secure Machine-Type Communications toward LTE Heterogeneous Networks," *Publ. IEEE Wirel. Commun.* , vol. Volume: 24, no. 1, 2017.

[14] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," *IEEE Secur. Priv.*, vol. 14, no. 4, pp. 34–44, Jul. 2016.

[15] F. Z. Y. ; M. G. ; V. F. ; B. G. ; D. von H. ; Bessem, "Network slicing with flexible mobility and QoS/QoE support for 5G Networks," *IEEE*, 2017.

[16] I. Ahmad, S. Namal, M. Ylianttila, S. Member, A. Gurtov, and S. Member, "Security in Software Defined Networks : A Survey," no. January, 2015.

[17] S. Shin, "AVANT-GUARD : Scalable and Vigilant Switch Flow Management in Software-Defined Networks," 2013.

[18] and P. V. D. Kreutz, F. M. Ramos, "Towards Secure and Dependable Software-defined Networks," *ACM SIGCOM*, 2013.

[19] A. Cleeff, W. Pieters, and R. Wieringa, "Security implications of virtualization: A literature study," *Proc. - 12th IEEE Int. Conf. Comput. Sci. Eng. CSE 2009*, vol. 3, pp. 353–358, 2009.

[20] M. M. ; V. K. ; A. Gurtov, "NFV security considerations for cloud-based mobile virtual network operators," *IEEE*, 2016.

[21] B. Yi, X. Wang, K. Li, S. k. Das, and M. Huang, "A comprehensive survey of Network Function Virtualization," *Comput. Networks*, vol. 133, pp. 212–262, 2018.

[22] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN)*, no. August 2017. 2015.

[23] S. Shin and G. Gu, "Attacking Software-Defined Networks: A First Feasibility Study," *Second ACM SIGCOMM Work. Hot Top. Softw. Defin. Netw. (HotSDN 2013)*, pp. 165–166, 2013.

[24] C. Notice and A. Notice, "Remote Provisioning Architecture for Embedded UICC Technical Specification," 2014.

[25] O. N. F. Solution and B. September, "深入研究---Sb-Wireless-Mobile.Pdf," 2013.

[26] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: Pros and cons," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 73–79, 2015.

[27] "5G security - enabling a trustworthy 5G system - Ericsson." [Online]. Available: https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system. [Accessed: 15-Dec-2018].