**NAME**:- Pratiksha Ravindra Zalte **ROLL NO:-** 4046A019 **CONTROL ID:-** 2023082897

V. G. Vaze Kelkar College, Mulund (E)

5G Security: Analysis of Threats and Solutions

\*Pratiksha Zalte

# Abstract

***This paper addresses the security and privacy***

***challenges in 5G technology, covering the development of security solutions and future directions. It also compares the security of 5G wireless network systems to traditional cellular networks, examining new security requirements and potential attacks. The integration of various technologies into 5G is explored, with a focus on identity management and flexible authentication.***

***Additionally, the paper investigates Multi-Access Edge Computing (MEC) technology's role and security***

***threats.***

# I INTRODUCTION

The vision of 5G wireless networks lies in furnishing veritably grandly data rates and advanced content through thick base station

deployment with increased capacity, significantly better Quality of Service( QoS), and extremely low quiescence. To give the necessary services

envisaged by 5G, new networking, service deployment, storehouse and processing

technologies will be needed. pall computing provides an effective way for drivers to maintain

data, services and operations without retaining the structure for these purposes. thus, mobile shadows using the same generalities will bring

technologically distinct systems into a single sphere on which multiple ser vices can be stationed to

achieve a advanced degree of inflexibility and

vacuity with lower Capital Expenditures( CapEx) and functional Charges( OpEx). Softwarizing the

network functions will enable easier portability and advanced inflexibility of networking systems and ser vices. Software Defined Networking( SDN)

enables network function softwarization by separating the network control and data

encouraging aeroplanes . SDN brings invention in networking through abstraction on one hand and

simplifies the network operation on the other hand.

Network Function Virtualization( NFV) provides

the base for placing colourful network functions in different network peripheries on a need base and

eliminates the need for function or service-specific tackle.

SDN and NFV, completing each other, ameliorate the network pliant ness, simplify network control and operation, break the hedge of seller specific personal results, and therefore are considered

largely important for unborn networks. Yet with these new technologies and generalities, network security and stoner sequestration remain a big

challenge for unborn networks.

Wireless communication systems have been prone to security vulnerabilities from the veritably

commencement. In the first word generation( 1G) wireless networks, mobile phones and wireless

channels were targeted for illegal cloning and

masquerading. In the alternate generation( 2G) of wireless networks, communication spamming came common not only for pervasive attacks but edging

in false information or broadcasting unwanted

marketing information. In the third generation( 3G) wireless networks, IP- grounded communication

enabled the migration of Internet security vulnerabilities and challenges in the wireless

disciplines. With the increased necessity of IP grounded communication, the fourth Generation( 4G) mobile networks enabled the proliferation of smart bias, multimedia business, and new services into the mobile sphere. This development led to further complicated and dynamic trouble

geography. With the arrival of the fifth generation( 5G) wireless networks, the security trouble vectors will be bigger than indeed before with lesser

concern

for sequestration. thus, it's pivotal to punctuate the security challenges that are hanging not only due to the wireless nature of mobile networks, but live in

the implicit technologies that are largely important for 5G. In this paper, we punctuate the security

challenges that are on the van of 5G and need prompt security measures. We further bandy the security results for the pitfalls described in this

paper. The rest of the paper is organized as follows Section II states various types of security

challenges .Section III describes the crucial

security challenges followed by security results for the stressed security challenges in Section IV. The paper is concluded in Section V.

# VARIOUS TYPES OF SECURITY CHALLENGES IN 5G

5G, the fifth generation of mobile communication technology, offers numerous advantages, such as faster data speeds, lower latency, and increased

capacity, but it also presents several key security challenges. Here are some of the primary security challenges in 5G:

1. Privacy Concerns: With the proliferation of

connected devices and the massive amount of data generated, there are concerns about user privacy. This includes the collection and potential misuse of personal data by service providers, as well as the

risk of unauthorized access to sensitive information.

1. Network Slicing: 5G enables network slicing, allowing multiple virtual networks to run on a single physical infrastructure. While this is

beneficial for customization, it poses security risks if one slice is compromised, potentially affecting others.

1. IoT Vulnerabilities: The Internet of Things (IoT) devices often lack robust security features, making them vulnerable to attacks. In 5G, the massive

expansion of IoT increases the attack surface and potential for security breaches.

1. Supply Chain Risks: 5G infrastructure

components are often sourced from various

suppliers and can involve complex supply chains.

This creates opportunities for malicious actors to

insert backdoors or other vulnerabilities at various points in the supply chain.

1. Distributed Edge Computing: Edge computing, a fundamental aspect of 5G, involves processing data closer to the source. While this improves latency

and efficiency, it also means that sensitive data is distributed across a broader geographic area,

making it more challenging to secure.

1. Network Function Virtualization (NFV) and

Software-Defined Networking (SDN): 5G networks increasingly rely on virtualization and software-

defined approaches, which can be exploited if not properly secured. Malware or vulnerabilities in

virtualized network functions can have widespread effects.

1. Authentication and Authorization: The

authentication and authorization mechanisms used in 5G networks need to be robust. Weaknesses in

these systems can lead to unauthorized access and data breaches.

1. Distributed Denial of Service (DDoS) Attacks: With the increased bandwidth in 5G networks, DDoS attacks can be more potent. It is crucial to have effective DDoS mitigation strategies in place.
2. Interconnection Security: 5G networks need to interconnect with existing 4G, Wi-Fi, and other

technologies. Ensuring secure transitions between these networks and preventing vulnerabilities in older technologies from affecting 5G is a

significant challenge.

1. National Security and Geopolitical Concerns:

The rollout of 5G infrastructure has raised

geopolitical concerns, particularly regarding the

involvement of specific vendors and their potential ties to governments. This can impact the security

and trustworthiness of the network.

1. Backhaul and Transport Network Security: The transport networks that connect 5G base stations to the core network are vulnerable to attacks. Securing these backhaul connections is critical to

maintaining the overall security of the 5G network.

1. Regulatory and Compliance Challenges: The evolving nature of 5G technology and the rapid deployment of new services can make it

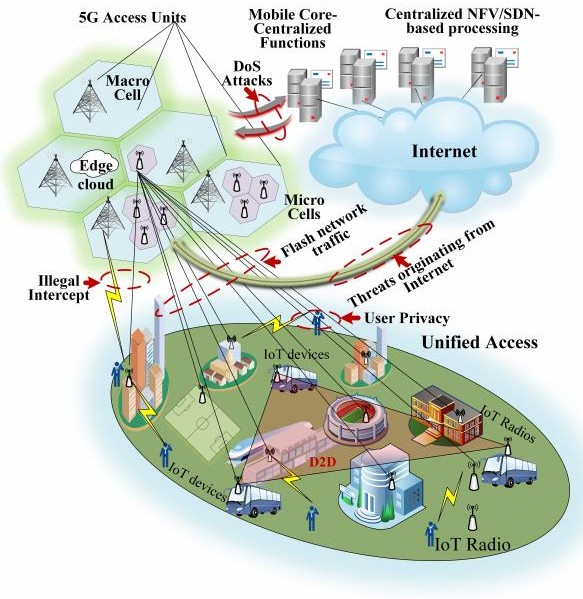
challenging to keep up with regulatory and

compliance requirements, which are essential for maintaining security standards.

To address these security challenges, collaboration between governments, service providers,

equipment vendors, and cybersecurity experts is

essential. Ongoing research, development, and the implementation of robust security protocols and practices are crucial to ensuring the integrity and security of 5G networks.



**Fig 1.** 5G network and the threat landscape.

# KEY SECURITY CHALLENGES IN 5G

5G will connect critical infrastructure that will require more security to ensure safety of not only the critical infrastructure but safety of the society as a whole. For example, a security breach in the online power supply systems can be catastrophic for all the electrical and electronic systems that the society

depends upon. Similarly, we know that data is critical in decision making, but what if the critical data is corrupted while being transmitted by the 5G networks? Therefore, it is highly important to investigate and highlight the important security challenges in 5G networks and overview the potential solutions that could lead to secure 5G systems. The basic challenges in 5G highlighted by Next Generation Mobile Networks (NGMN) and highly discussed in the literature are as follows:

* **Flash network traffic:** High number of end- user devices and new things (IoT).

Flash network traffic refers to sudden and intense bursts of data or traffic on a network. These abrupt spikes in network activity can occur due to various reasons, such as sudden increases in user demand, large-scale data transfers, or distributed denial of service (DDoS) attacks. Flash traffic can strain network resources and potentially lead to network congestion or disruptions. Managing and mitigating flash network traffic is essential to ensure the network's stability, performance, and security during such high-impact events.

* **Security of radio interfaces:** Radio interface encryption keys sent over insecure channels. The security of radio interfaces is a critical aspect of telecommunications and wireless technology. It refers to the protection of data and communication over wireless channels, including mobile networks like 5G, 4G, and earlier generations.
* **User plane integrity:** No cryptographic integrity protection for the user data plane.

User plane integrity protects against data tampering and ensures that the data received by the end user is unchanged and originates from a trusted source. It employs cryptographic mechanisms like message authentication codes (MACs) and digital signatures to verify the data's integrity, making it difficult for malicious actors to modify or inject unauthorized content into the data stream.

* **Mandated security in the network:** "Mandated security in the network" refers to the practice of requiring specific security measures within a network environment. In this context, "service-driven constraints on the security architecture leading to the optional use of security measures" means that certain network services or applications may have different security requirements and constraints. While

some security measures are mandatory for critical services, others are optional based on the specific needs of a service or application.

* **Roaming security:** "Roaming security" involves the security measures and protocols in place to ensure the safety of user data and communications when a mobile device moves from one operator's network to another, particularly in a foreign or roaming network. The statement "User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming" highlights a potential security challenge in this context.
* **Denial of Service (DoS) attacks on the infrastructure:** Visible nature of network control elements, and unencrypted control channels. With the increased bandwidth in 5G networks, DDoS attacks can be more potent. It is crucial to have effective DDoS mitigation strategies in place.
* **Signaling storms:** Signaling storms" in the context of telecommunications refer to situations where a distributed control system, such as the Non-Access Stratum (NAS) layer in the Third Generation Partnership Project (3GPP) protocols, experiences an excessive volume of signaling messages or control traffic. These signaling storms can result from various factors, including network failures, network congestion, or abrupt changes in device or user states.

When signaling storms occur, they can overload network resources, disrupt service, and negatively impact the efficiency and responsiveness of the communication system. In the case of NAS, which manages the control and signaling functions for mobile devices, signaling storms can lead to delayed call setup, increased latency, and inefficient network utilization.

* **DoS attacks on end-user devices:** No security measures for operating systems, applications, and configuration data on user devices.

Denial of Service (DoS) attacks on end-user devices occur when malicious actors target vulnerabilities in operating systems, applications, and configuration data on these devices. The statement "No security measures for operating systems, applications, and configuration data on user devices" underscores a significant security challenge.

Without adequate security measures, end-user devices like smartphones, computers, and IoT devices can be vulnerable to DoS attacks. These attacks aim to overwhelm or exploit weaknesses in the device, rendering it inaccessible or unusable. Attackers can flood the device with excessive traffic or malicious code, causing it to slow down or crash

## Security challenges in mobile clouds

Security challenges in mobile clouds refer to the unique vulnerabilities and risks associated with using cloud computing services on mobile devices. Mobile cloud computing combines mobile devices with cloud-based services, and this fusion creates specific security concerns:

* 1. Data Privacy: Storing and accessing data in the cloud from mobile devices can expose sensitive information to potential breaches. Ensuring data privacy through encryption and access controls is crucial.
  2. Network Security: Mobile devices often connect to public and untrusted networks, making them more susceptible to eavesdropping and man-in-the- middle attacks. Secure network connections and protocols are essential.
  3. Device Loss and Theft: The portability of mobile devices increases the risk of loss or theft. Remote wipe and tracking features are necessary to protect data in such situations.
  4. Authentication and Authorization: Ensuring the identity and authorization of users on mobile devices is a challenge. Multi-factor authentication and strong access controls help mitigate this risk.
  5. Malware and Phishing: Mobile devices are prime targets for malware and phishing attacks. Security software and user education are crucial to prevent such threats.
  6. Compliance and Legal Issues: Handling regulatory compliance and legal matters, especially in the context of data stored and processed in the cloud, can be complex and requires careful consideration.
  7. Data Synchronization: Keeping data consistent across multiple devices while maintaining security can be challenging. Proper synchronization mechanisms are needed.

Addressing these challenges involves a combination of technological solutions, user education, and effective policies to protect data, devices, and cloud services while enjoying the benefits of mobile cloud computing.

## Security Challenges in SDN and NFV small description

Security challenges in Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) revolve around the transformation of traditional network architectures into more flexible, dynamic, and software-driven models:

* 1. Control Plane Security: Separating the control and data planes in SDN introduces a new layer of complexity and the potential for unauthorized access to control plane elements. Securing the

control plane is crucial to prevent unauthorized control over the network.

* 1. Virtualization and Isolation: In NFV, network functions are virtualized and run on shared infrastructure. Ensuring strong isolation and security between these virtual instances is essential to prevent one compromised function from affecting others.
  2. Network Service Chains: SDN and NFV can create complex network service chains. Coordinating and securing the flow of traffic through these chains while maintaining performance and availability is a challenge.
  3. Centralized Controllers: SDN centralizes network control in a single controller or a few controllers, making them attractive targets for attacks. Protecting these controllers is critical to the security of the entire network.
  4. Dynamic Configuration: The dynamic nature of SDN and NFV environments can make it difficult to maintain consistent security policies and configurations. Automation and security policies are essential to keep up with changes.
  5. Interoperability : Integrating legacy and SDN/NFV-enabled devices can create security gaps. Ensuring interoperability while maintaining security is a challenge.
  6. Network Monitoring: With dynamic network changes, it can be challenging to monitor and detect security threats effectively. Advanced threat detection and analytics are needed.

Addressing these challenges requires robust security practices, including encryption, access controls, segmentation, threat detection, and proactive monitoring. Additionally, a deep understanding of the unique security considerations of SDN and NFV is vital for organizations transitioning to these technologies.

## Security Challenges in Communication Channels

5G will have complex ecosystem involving drones and air traffic control, cloud driven virtual reality, connected vehicles, smart factories, cloud driven robots, transportation and

health. Thus the applications need secure communication systems that support more frequent authentication and exchange of more sensitive data. Also, many new players such as public

service providers, Mobile Network Operators (MNOs), and cloud operators will get involved with these services. In such an eco-system several layers of encapsulated authentications are required at both network access and service levels, and frequent authentication is required between actors. Before 5G networks, mobile

networks had dedicated communication channels based on GTP and IPsec tunnels. The communication interfaces, such as X2, S1, S6, S7, which are used only in mobile networks, require significant level of expertise to attack these interfaces. However, SDN-based 5G networks will not have such dedicated interfaces but rather common SDN interfaces. The openness of these interfaces will increase the possible set of attackers. The communication in SDN based 5G mobile networks can be categorized in to three communication channels i.e. data channel, control channel and inter-controller channel . In current SDN system, these channels are protected by using TLS (Transport Layer Security)/ SSL (Secure Sockets Layer) sessions . However, TLS/SSL sessions are highly vulnerable to IP layer attacks , SDN Scanner attacks and lack strong authentication mechanisms .

## Privacy Challenges in 5G

From the user’s perspective, the major privacy concerns could arise from data, location and identity .

Threats such as semantic information attacks, timing attacks, and boundary attacks mainly target the location privacy of subscribers . At the physical layer level, location privacy can be leaked by access point selection algorithms in 5G mobile networks . International Mobile Subscriber Identity (IMSI) catching at tacks can be used to reveal the identity of a subscriber by catching the IMSI of the subscriber’s User Equipment (UE). Such attacks can also be caused by setting up a fake base station which is considered as preferred base station by the UE and thus subscribers will respond with their IMSI. Moreover, 5G networks have different actors such as Virtual MNOs (VMNOs), Communication Service Providers (CSPs) and network infrastructure providers. All of these actors have different priorities for security and privacy. The synchronization of mismatching privacy policies among these actors will be a challenge in 5G network . In the previous generations, mobile operators had direct access and control of all the system components.

However, 5G mobile operators are losing the full control of the systems as they will rely on new actors such CSPs. Thus, 5G operators will lose the full governance of security and privacy . User and data privacy are seriously challenged in shared environments where the same infrastructure is shared among various actors, for instance VMNOs and other competitors.

Moreover, there are no physical boundaries of 5G network as they use cloud based data storage and NFV features. Hence, the 5G operators have no direct control of the data storing place in cloud environments. As different countries have different level of data privacy mechanisms depending upon their preferred context, the privacy is challenged if the user data is stored in a cloud in a different country.

# POTENTIAL SECURITY SOLUTIONS

In this section, we highlight security solutions for the security challenges outlined in the previous section. The challenges of flash network traffic can be solved by either adding new resources or increasing the utility of existing systems with novel technologies. We believe that new technologies

such as SDN and NFV can solve these challenges more cost effectively. SDN has the capability to enable run-time resource, e.g. bandwidth, assignment to particular parts of the network as the need arises.

In SDN, the controller can gather network stats through the south-bound API from network equipment to see if the traffic levels increase. Using NFV, services from the core network cloud can be transferred

towards the edge to meet the user requirements. Similarly, virtual slices of the network can be dedicated only to areas with high density of UEs to cope with flash network traffic. The security of the radio interface keys is still a challenge, that needs secure exchange of keys encrypted like the proposed Host Identity Protocol (HIP) based scheme in . Similarly, the user plane integrity can be achieved by end-to end encryption technologies suggested in . Roaming security and network-wide mandated security policies can be achieved using centralized systems that have global visibility of the users’ activities and network traffic behavior e.g. SDN. The signaling storms will be more challenging due to the excessive connectivity of UEs, small base stations, and high user mobility. C-RAN and edge computing are the potential problem solvers for these challenges, but the design of these technologies must consider the increase in signaling traffic as an important aspect of the future networks as described by NGMN. Solutions for DoS attacks or saturation attacks on network control elements are presented in the following sections.

## Security Solutions for Mobile Clouds

In the realm of Mobile Cloud Computing (MCC), security measures are increasingly centered around the strategic use of virtualization technologies, redesigned encryption methods, and the dynamic allocation of data processing points. Virtualization is a natural choice for enhancing security, as it ensures that each end-node connects to a specific virtual instance in the cloud via a Virtual Machine (VM). This approach provides security through the isolation of each user's virtual connection from others, reducing the risk of unauthorized access.

Moreover, service-based restrictions are emerging as a key strategy for secure cloud computing. For example, a proposed infrastructure leverages cloud platforms and 5G technology to secure cloud services, allowing mobile users to share real-time videos while restricting access to only authorized viewers.

To address specific security threats like HX-DoS (Hybrid Crossfire Denial of Service), tailored solutions such as learning-based systems are more effective than generic approaches. These learning- based systems analyze a set of packet samples, examining various known attributes to detect and mitigate threats efficiently.

In addition to cloud-based security, securing mobile terminals is crucial. Anti-malware solutions, whether installed directly on the mobile device or hosted and served from the cloud, can significantly bolster resistance to malware attacks. Furthermore, the MCC data and storage security framework includes energy-efficient mechanisms for data and storage service integrity verification, public provable data possession schemes, and lightweight compromise-resilient storage outsourcing.

For application security, several innovative frameworks have been proposed, ranging from securing elastic applications on mobile devices for cloud computing to dynamic credential generation mechanisms for user identity protection, in-device spatial cloaking mechanisms to safeguard privacy, and secure cloud frameworks like Mobi-Cloud.

These multifaceted approaches collectively contribute to a robust security ecosystem within the MCC domain.

## Security Solutions for SDN and NFV

The advantages of Software-Defined Networking (SDN) go beyond just network flexibility and control; they extend to enhancing network security. With a logically centralized control plane offering a global view of the network and programmability, SDN is well-suited for rapid threat identification.

By collecting intelligence from network resources,

states, and flows, SDN facilitates highly responsive and proactive security monitoring, traffic analysis, and response systems. This capability supports network forensics, the adaptation of security policies, and the seamless insertion of security services. Furthermore, the global visibility provided by SDN allows for the deployment of consistent network security policies throughout the network, making it easier to manage and secure.

In addition, the security of Virtual Network Functions (VNFs) is addressed through a security orchestrator within the context of the ETSI NFV architecture. This innovative architecture not only protects virtual functions in multi-tenant environments but also extends security to physical entities within telecommunication networks. To enhance security, it employs trusted computing, remote verification, and integrity checking for virtual systems and hypervisors. This approach ensures hardware-based protection for private information and the detection of compromised software in virtualized environments, thereby fortifying security within the network.

These advanced security measures, underpinned by SDN and NFV capabilities, empower networks to better respond to and defend against emerging threats while maintaining a high degree of flexibility and adaptability.

## Security Solutions for Communication Channels

In the context of 5G, ensuring the security of communication channels is essential not only to mitigate identified security threats but also to harness the additional benefits offered by Software- Defined Networking (SDN), including centralized policy management, programmability, and global network state visibility. While IPsec is the predominant security protocol used in current telecommunications networks, such as 4G-LTE, it can also be adapted to secure 5G communication channels with slight modifications, as discussed in and .

In contrast, securing LTE communications relies on the integration of various security algorithms, encompassing authentication, integrity, and encryption. However, these conventional security solutions often entail high resource consumption, significant overhead, and a lack of coordination.

Consequently, they may not be well-suited for the critical infrastructure communication requirements of 5G networks.

To address this challenge and achieve a higher level of security for critical communications in the 5G era, innovative security mechanisms are being

explored. These mechanisms encompass strategies like physical layer security that adopts Radio- Frequency (RF) fingerprinting , the use of asymmetric security schemes , and the dynamic adaptation of security parameters in response to changing situations . Similarly, end-to-end user communication can be fortified through the deployment of cryptographic protocols like the Host Identity Protocol (HIP). These forward- looking security measures are instrumental in meeting the evolving demands of 5G networks and safeguarding critical communication.

## Security Solutions for Privacy in 5G

In the context of 5G, safeguarding privacy is of paramount importance, and it necessitates a "privacy-by-design" approach. This entails considering privacy as a fundamental aspect right from the beginning of system design, with a range of essential features inherently built-in to enhance privacy.

A hybrid cloud-based approach is being explored to address privacy concerns effectively. This approach allows mobile operators to store and process highly sensitive data locally, while less sensitive data can be handled in public clouds. This strategy empowers operators with greater control and access to data, enabling them to make informed decisions about data sharing. Furthermore, service-oriented privacy in 5G networks is emerging as a promising solution for preserving privacy, ensuring that users' personal information remains protected.

To meet the stringent privacy requirements of 5G, the development of robust mechanisms for accountability, data minimization, transparency, openness, and access control is imperative. During the standardization of 5G, it is crucial to consider and incorporate strong privacy regulations and legislation. These regulations can be classified into three categories:

1. Government-Level Regulation: Governments establish country-specific privacy regulations, often in collaboration with international organizations such as the United Nations (UN) and the European Union (EU).
2. Industry-Level Regulation: Various industries and groups, including standards organizations like 3GPP, ETSI, and ONF, work collaboratively to draft best practices and principles to protect privacy.
3. Consumer-Level Regulation: Privacy measures should be designed to meet consumers' specific privacy requirements, ensuring that their preferences and data protection needs are considered.

For location privacy, techniques like anonymity- based approaches are essential. These methods allow the subscriber's real identity to be concealed and replaced with pseudonyms. Encryption-based practices, such as encrypting messages before sending them to Location-Based Services (LBS) providers, enhance privacy. Techniques like obfuscation, which reduce the quality of location information to protect privacy, and location cloaking algorithms are instrumental in countering major location privacy threats like timing and boundary attacks. These approaches collectively contribute to robust privacy protection in the 5G landscape.

# CONCLUSION

5G will use mobile shadows, SDN and NFV to meet the challenges of massive connectivity, inflexibility, and costs. With all the benefits, these technologies also have essential security challenges. thus, in this paper we've stressed the main security challenges that can come more hanging in 5G, unless duly addressed. We've also presented the security mechanisms and results for those challenges. How ever, due to the limited standalone and intertwined deployment of these technologies in 5G, the security trouble vectors can not be completely realized at this time. also, the communication security and sequestration challenges will be more visible when further stoner bias e.g. IoT are connected and new different sets of services are offered in 5G. To add it up, it's largely probably that new types of security pitfalls and challenges will arise along with the deployment of new 5G technologies and services. still, considering these challenges right from the original design phases to the deployment will minimize the liability of implicit security and sequestration setbacks.

# REFERENCES

1. M. Agiwal, A. Roy, and N. Saxena, “Next Generation 5G Wireless

Networks: A Comprehensive Survey,” *IEEE Communications Surveys*

*Tutorials*, vol. 18, no. 3, pp. 1617–1655, third

quarter 2016.

1. N. Alliance, “NGMN 5G white paper,” *Next Generation Mobile Net*

*works, White paper*, 2015.

1. 3GPP. (2017, May) SA3-Security. The Third Generation Partnership Project (3GPP). [Online]. Available:

<http://www.3gpp.org/Specifications-groups/sa-> plenary/54-sa3-security

1. Security for 5G Mobile Wireless Networks - Dongfeng Fang, Yi Qian, and Rose Qingyang Hu AUGUST 2017