5G Security: Concepts and Challenges

Poorna Pravallika Sriram, Hwang-Cheng Wang, Hema Ganesh Jami, and Kathiravan Srinivasan

Abbreviations

AKA	Authentication and Key Agreement protocol
AMTS	Advanced mobile telephone system
AN	Artificial noise
API	Application programming interface
ASM	Antenna subset modulation
BC-CM	Broadcast channel with confidential message
BER	Bit error rate
BS	Base station
BYOD	Bring your own device
CR	Cognitive radio
DNS	Domain Name System
DoF	Degrees of Freedom
EAP	Edge Automation Platform
eMBB	Enhanced Mobile Broadband

The original version of this chapter was revised. A correction to this chapter is available at https://doi.org/10.1007/978-3-030-03508-2_7

P. P. Sriram (✉)
Department of Electronics & Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

H.-C. Wang
Department of Electronic Engineering, National Ilan University (NIU), Yilan City, Taiwan

H. G. Jami
Vel Tech Rangarajan Dr. Sagunthala R&D Insititute of Science and Technology, Chennai, India

K. Srinivasan
School of Information Technology and Engineering, Vellore Institute of Technology (VIT), Vellore, TN, India

D. N. K. Jayakody et al. (eds.), *5G Enabled Secure Wireless Networks*,
https://doi.org/10.1007/978-3-030-03508-2_1

EPS	Evolved Packet System
ETCI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
HD	High Definition
HIP	Host Identity Protocol
HTTP	Hypertext Transfer Protocol
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunication
IMTS	Improved Mobile Telephone System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPWAVE	Internet Protocol Wireless Access in Vehicular Environment
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KKT	Karush-Kuhn-Tucker
LDPC	Low-density parity check
LTE	Long-Term Evolution
M2M	Machine to machine
MA-WC	Multiple access wiretap channel
MIMO	Multiple input, multiple output
mmWave	Millimeter Wave
MPWG	Mobile Platform Work Group
MTS	Mobile telephone system
NERC	North American Electric Reliability Corporation
NOMA	Non-orthogonal multiple access
NP	Network planning
ONF	Open Networking Foundation
PTT	Push to talk
QoS	Quality of service
RAN	Radio access network
RS	Relay stations
SDO	Standards Development Organization
SDR	Software-defined radio
SIC	Self-interference cancellation
SINR	Signal-to-interference-noise ratio
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TDD	Time division duplex
UAV	Unmanned aerial vehicle
USIM	Universal Subscriber Identity Module

WG	Working group
ZFBF	Zero-forcing beam-forming

1 Overview

1.1 Introduction

Wireless mobile communication has initiated its technology formulation, revolution, and development from the 1980s. In the last few decades, wireless mobile innovations have experienced third and fourth generations of technology development and revolution. The quality of services (QoS) and security are significantly promoted in 4G, while the cost per bit is low. In comparison with the previous network generations, there are some issues with 4G such as greater power consumption (battery use) and the high cost of the equipment needed to implement the next-generation network. 5G is going to be the next generation. Mainly, it aims to provide a complete wireless communication with almost no limitations. As six billion people own smartphones, we are going to dissect the different generations of cellular technologies. Moreover, the digital wireless communication systems are relentlessly determined to satisfy the developing need for individuals. Also, in the 5G technology, the rate of the data calls is made easy compared to the previous generations as the quality of the service is excellent and highly flexible and has significant spectrum management and improved efficiency with decreasing cost. This whimsical development represents not just the powerful need for individuals all over the globe to communicate and connect with each other and also to have access to the information but also the gigantic steps that innovation has made in satisfying the need [1]. All IP-based fourth-generation Long-Term Evolution (LTE) networks have become a portion of the day-to-day routine with the rapid rise in demand of the smart mobiles. As a result, a set of new user-oriented mobile multimedia applications, like video conferencing, streaming video, e-health care, and online gaming, has arisen. Furthermore, as the sphere prepares for the first commercial debut of 5G networks, many people are inquisitive about the security hazards and risks. 5G technology will reinforce a massive number of connected devices, which enables a colossal rise in bandwidth and create a next-generation hazard landscape that will irresistibly introduce 5G security challenges. These new applications are fulfilling user necessities as well as opening the new business skylines for remote operators to expand their income.

1.2 Evolution of Cellular Technologies

The evolution of the mobiles classifies various technologies into different "generations." The word "generation" indicates the change in the quality of service, adaptable transmission technology, and new frequency bands.

First Generation

The acronym 1G represented the first-generation mobile telecommunication and was first introduced in the 1980s and continued till 1990. These networks use analog systems for communication. Mobile devices are simple voice-only cellular phones. Moreover, the first generation of analog mobile phones has a speed of 2.4 Kbps and 14.4 Kbps. It allows its consumers to make voice calls only within the same country. Voice call modulation is performed using a technique called frequency division multiple access (FDMA). It proposes many mobile technologies like mobile telephone system (MTS), advanced mobile telephone system (AMTS), improved mobile telephone system (IMTS), and push to talk (PTT) [2]. On the other hand, it has low capacity, deceptive hand-off, and weak voice links and does not offer security.

Advantages of 1G technology

1G represents the initial success in the attempt to achieve mobile communication. In retrospect, 1G has few advantages. Nevertheless, it signifies an important step in the development of mobile technology, and many of the fundamental ideas such as cells, frequency reuse, and multiple access have remained in subsequent generations of mobile communication.

Limitations of 1G Technology

- Constrained limit: It has a very little coverage area cellular network.
- Low calling limit: The quality of the call service is low because of its low capacity.
- No space for range development: There is no room for the spectrum growth.
- Poor data communications: The data rate speed is low.
- Negligible security: Privacy and security assurance is minimum.
- Deficient extortion security: Protection toward fraud sites is not guaranteed.

Second Generation

2G refers to the second generation, which is based on the global system for mobile communication (GSM). 2G networks use digital signals, and its data speed is in between 14.4 Kbps and 64 Kbps [3]. This network offers unique services such as short message services (SMS), picture messages, and multimedia messages (MMS). It cannot handle complex data such as video which is the most notable drawback. The network capacity of 2G is very much better than 1G. The primary distinction between 1G and 2G is that 1G uses analog signals whereas 2G uses digital signals for communication.

Advantages of 2G Technology

- Improved privacy is the added advantage of 2G technology.
- 2G technology introduces the digital data services such as SMS and email that have allowed the world to shrink and people to get closer.

- It enables users to place a call on hold in order to access another call.
- The digital data service is used to assist the mobile network operators to introduce short message service over the cellular phones.

Disadvantages of 2G Technology

- 2G technology requires powerful digital signals to help the mobile phones work, but the digital signals could be weak if there is no network coverage in any specific area**.**
- The data rate is low. The downloading and uploading speeds available in 2G technologies are up to 236 Kbps.

Limitations of 2G Technology

- It demands intense digital signals to assist the connections of mobile phones.
- Complex data types such as videos are not supported.

Third Generation

In the third generation, the wireless communication terrace has voice and data potency. It was established in 2000. 3G is the first international standard system released from ITU, in divergence to the previous generation systems. It works in frequency division duplex (FDD) and time division duplex (TDD) modes. As compared to 1G and 2G, it provides a higher speed which ranges from 144 Kbps to 2 Mbps. It has a bandwidth of 25 MHz. Also, it is referred to as Mobile Telecommunication 2000. It introduced data services, expanding the functionality beyond voice and including multimedia, text, and some limited Internet access. The foremost technological dissimilarity that differentiates 3G technology from 2G technology is the use of packet switching rather than circuit switching for data transmission [4].

Advantages of 3G Technology

The 3G network uses a wide range of radio spectrum that allows faster data transmission. It also allows location-based services like weather reports on the mobile phones.

Limitations of 3G Technology

- The price for 3G services is expensive – It provides better-quality services compared to 2G technology services.
- Expensive in nature – Due to the voice and data rate services, the rate of 3G is a little more expensive.
- Higher bandwidth requirements – The requirement for the bandwidth is high due to the heavier usage of data calls.

Fourth Generation

The fourth generation of mobile communication is a packet switched wireless system with colossal area coverage and high throughput. It is designed to provide high spectral profitability. It provides communication with higher data rates and high-quality video streaming in which Wi-Fi and WiMAX are combined [3]. This network can provide a speed of upto 50 Mbps. The quality of service (QoS) and security are symbolically promoted in 4G, while the cost per bit is low.

The primary 4G protocol – LTE – was designed to reinforce the mobile broadband and is the dominant industry standard today. The significant frequency band range is between 2 and 8 GHz. It also provides the ability for worldwide roaming to allow access to cellular communication anywhere.

Advantages of 4G Technology

The most apparent benefit of the 4G mobile network is its prodigious speed. Expanded bandwidth leads to much higher data transfer speed, which is particularly advantageous for mobile gadgets. 4G offers coverage of 30 miles and more. The uploading speed in 4G is upto 5 Mbps and the downloading speed is upto 50 Mbps.

Limitations of 4G Technology

- It is expensive and hard to implement.
- It demands more battery usage.
- It needs complex hardware.

Fifth Generation

This 5G technology merges all the upgraded benefits of mobile phones like high-speed dialing, music recording, cloud data storage, and high-definition (HD) downloading instantaneously. New radio bands above 20 GHz are being designated for 5G. 5G networks are also intended to meet new use cases, such as the Internet of Things, services, and lifeline communication in times of natural catastrophe. It will be crafted for an extraordinary system to broadcast immense amount of information in gigabits per second (Gbps), enabling media news feeds and TV programs with HD quality [3].

Even though 4G has not been around for a very long time, it is found to be inadequate in dealing with the various necessities in terms of denser networks and increased capacity factors such as the widespread use of smartphones, in terms of data rates, speed, coverage, battery life, and the emergence of the Internet of Things (IoT). This is not the technology’s flaw; the smartphone revolution had not started when the 4G requirements and technologies were considered and selected. New applications are always developing. Nevertheless, overcoming the current limitations of 4G is the primary goal of 5G. The concept is to meet future demands for data rates, speed, coverage, and battery life in architecture to enable a cost-effective network that can be efficiently scaled.

Issues and Challenges of 5G

The key challenges in meeting the performance of these future networks using affordable technologies that are still in research and investigation are:

- Number of supportive devices
- Data volumes
- Lower cost with higher capacity
- New air interface
- Speed

Features of 5G Technology

- Faster data transfer rates compared to the previous generations
- Large memory
- Swift dialing speed
- HD quality impression
- More attractive and effective
- Peak uploading and downloading speed
- Remote diagnostics
- Up to 25 Mbps connection speed
- High-quality services to prevent errors
- Bidirectional large bandwidth

As the world embraces for the first commercial debut of 5G networks, many people are contemplating about the security hazards and risks that the new standard is going to encounter. 5G networks will feature a vast number of connected devices, see a substantial increase in bandwidth, and create a next-generation hazard landscape that will inevitably introduce unique security challenges [5].

1.3 The Significance of 5G Security

The 5G standard will bring the towering benefits such as upgraded speed and performance, low latency, longer battery life, greater capacity, and superior efficiency. Further, the 5G networks are not only preferred for faster data rates but also provide a backbone for many new services in the networked society, such as IoT and the industrial Internet. These services will provide connectivity for autonomous cars and unmanned aerial vehicles (UAVs), remote health monitoring through body-attached sensors, smart logistics through item tracking, remote diagnostics, and preventive maintenance of equipment [6]. However, immensely increased number of devices and high usage of virtualization and cloud will lead to many multifaceted 5G security threats, hazards, and attacks. Moreover, to realize healthy and robust communication in the future, the industry should strive to maintain a high standard of 5G security.

1.4 The Need for Security

The strategies to attack telecommunication systems have changed from war dialers to viruses to modern-day sophisticated, steady risks. The devices to protect multimedia transmission have likewise advanced from physical access control to modern applications and firewalls. Expanded utilization of cell phones for data services and applications has presented these gadgets with similar security dangers that were once known and confined to personal computers (PCs). Bring your own device (BYOD) and cloud technologies have additionally lifted the enterprise limits and regularly invited security specialists to work out novel solutions [7]. Mobile devices have not yet replaced personal computers but have turned into a perfect place where individual data can be found for depraved use. Therefore, security should be architected to shield from the present dangers as well as to address the expanding and developing risk landscape. Sufficient security ought to incorporate danger intelligence, visibility, and real-time protection [7].

Likewise, seeing to the presumable results of an assault, the harm may not be restricted to a business or notoriety, it could even severely affect open security. Besides, this prompts a need to increase particular security functional zones. Attack resistance should be a plan thought when characterizing new 5G protocols [8]. Applications for 5G are beyond traditional mobile connectivity needs to new public communication, IoT, smart world based on smart cities, smart transportation, and more. One of the principal challenges for 5G adoption is security-related challenges. Although security is a mandatory requirement of 5G networks, many of the 5G security-related issues are still under development. However, the rapid adoption of 5G network will soon raise the requirement of a comprehensive handbook of 5G security.

2 5G Security Standardization

In February 2017, 3GPP published “Service Requirements for the 5G System” (TS22.261) that defines performance targets in various scenarios such as indoor, urban, rural, and different applications (intelligent transport, remote monitoring, and so on) [9]. 3GPP publishes 5G Phase-1specifications in 2018 as Release 15 and plans to publish Phase-2 in 2020 as Release 16. Since 5G is expected to be completely converged with Internet protocols, the standards produced by the Internet Engineering Task Force (IETF) are expected to play a vital role [9].

2.1 Internet Engineering Task Force

The IETF is an open standards organization that develops and promotes the center Layer-3 and higher protocols for the Internal and Intranet standards. It has existed as a formal Standards Development Organization (SDO) since mid-1986, yet the principal guidelines and demand for remarks had been formulated in the late 1960s. A portion of the eminent IETF benchmarks include the Internet Protocol form IPv4 and IPv6, Domain Name System (DNS), Transmission Control Protocol (TCP), and Hypertext Transfer Protocol (HTTP) [8]. The 3GPP has incorporated a large number of IETF protocols in the cellular framework design throughout the years. IETF and 3GPP keep in close contact to track specialized topics.

The relevant working groups are, for example, IP Wireless Access in Vehicular Environments (IPWAVE) working group (WG) and Host Identity Protocol (HIP) working group on secure mobility protocols. If 5G networks serve safety crucial applications as envisaged, the ISO (International Organization for Standardization) will introduce standards such as Common Criteria (ISO 15408). For instance, for car connectivity, a specific standard is ISO 26262, which covers car safety requirements. ETSI (European Telecommunications Standards Institute) was the initiator of GSM standard and critical contributor of W-CDMA as 3G standard within 3GPP. As a co-founder of 3GPP, ETSI is actively involved in developing 5G through organizing such events as ETSI Summit on 5G network infrastructure, which focused on 5G standardization in 2017 [10]. ETSI identified priority applications for 5G as mobile broadband evolution, massive M2M communication, and ultra-reliable low-latency communication.

ETSI is also a known contributor to the Network Functions Virtualization Industry Specification Group (ISG) and is currently forming a group focusing on 5G security [9]. ITU (International Telecommunication Union) receives input from regional organizations such as ETSI in Europe and ARIB in Japan and develops recommendations for standards defining bodies. ITU Telecommunication Standardization Sector (ITU-T) created a Focus Group on International Mobile Telecommunications (IMT-2020), which operated in 2015–2016 and analyzed requirements and framework for the 5G ecosystem [10]. ITU Study Group 17 (SG 17) focuses entirely on security aspects of telecommunication. Several other relevant standardization bodies include IEEE 802, TCG, and ONF [10]. Interoperability and mobility with third-party networks such as Wi-Fi involve standards from the IEEE (Institute of Electrical and Electronics Engineers) such as 802.11. At Trusted Computing Group (TCG), the Mobile Platform Work Group (MPWG) develops use cases, frameworks, and analysis of 5G security. Open Networking Foundation (ONF) promotes the use of software-defined networking protocols and network operating systems. Its specifications, including OpenFlow, could become part of 5G core architecture and therefore are also important from the security point of view.

3 Security Characteristics of 5G

Basic Security Characteristics of 5G

- *Prevention of threats*: Reducing the ground issues for most security incidents. The firewalls are used to protect the network and control access to reduce the user-based risk. Intrusion detection and prevention tools are considered for blocking basic 5G security threats.
- *Terminating and fixation of advanced malware*: Going beyond signature-based tools helps to spot the attacks designed to evade basic filters. Behavior-based checks on endpoints – possibly using sandboxing – are important. Once a threat is detected, all the instances of it on the network should be removed.
- *Detecting anomalies:* Usage of the packet capture, big data, and machine learning to identify threats that are not detected by the basic filters. When inserted into the network switches and routers, it is more effective as it turns those devices into 5G security sensors.
- *Incorporate DNS (Domain Name System) intelligence*: DNS activity is monitored and protected against any malicious attacks.
- *Making threat intelligence paramount*: In order to understand the malicious efforts of hackers, providers must look for vendors that can profile hackers.

3.1 Drivers of 5G

The drivers for security have set up to give a reliable fundamental availability benefit. This fundamental trust will keep on being a driving force for 5G that organizes, as a high information rate, portable broadband administration. 5G systems will not be composed exclusively to provide new capacities for individuals and society but also to interface ventures (e.g., assembling and preparing, intelligent transport, and smart grid). With 5G, it is possible to foresee new models of how network and transmission services are provided. For instance, an automaker may wish to give management services to vehicles. Setting up coordinate wandering concurrences with different access arrangement for suppliers could be a cost-effective approach to accomplish this. Correspondingly, the idea of terminal/gadget will change: unattended machines and sensors will associate. Moreover, at times whole hairlike systems containing one or many individual gadgets will connect to the 5G network. Cloud and virtualization advancements will be utilized to lower the costs and improve the benefits more quickly. Telecom systems will uncover application programming interfaces (APIs) [8] toward users and outsider specialist organizations to a higher degree. Besides, general consciousness of user security in the public eye has expanded, prompting a more prominent spotlight on the assurance of user meta-data and correspondence. This issue turns out to be significantly more focal with the improvements in big data analytics. What describes 5G, considerably more than 4G, is that it will have a significant part in the task of society. The full extent of security, protection, and flexibility will be a change that comes a long way past innovation. It will impact legal systems and direction and activities of business elements and people.

3.2 Significance of Security and Privacy

The four characteristics of 5G networks and their usage, each with suggestions for security and protection, are:

- Modern confide models
- New relevance transmission models
- Emerging risk prospects
- Raised privacy concerns

Modern Confide Models

Confide models change over time. For instance, consider bring-your-own-device (BYOD) tendency in business. Beforehand, all user gadgets were thought to be reliable, as they were the greater part of a similar kind, all issued and overseen by the corporate IT division. Today, users need to utilize their own gadgets, thereby causing dangers like potential Trojan horses behind corporate firewalls [8].

Since 5G is going to support new plans of action, trust models will change. For example, for new basic administrations, what security necessities will be anticipated onto the 5G systems? The new kinds of gadgets will traverse a greatly extensive variety of security necessities and will in the meantime have completely different security requirements. Gadgets have so far been accepted to consent to models and not to intentionally endeavor to assault networks.

The current confide model does not explicitly capture this evolving business and technological scenery of 5G. To guarantee that 5G can bolster the requirements of new plans of action and guarantee adequate security, the trusted display outline is redrawn [8]. In that capacity, this does not really mean totally upgrading security. Nonetheless, it is urgent to distinguish any huge weaknesses.

Security for New Relevance Transmission Models

The utilization of clouds and virtualization underlines the reliance on protected programming and prompts different impacts on security. Current 3GPP-characterized frameworks depend on practical hub details and unique interfaces (reference focuses) among them, and all things considered, give a decent beginning stage to virtualization. Recently, committed/exclusive equipment has still regularly been utilized for these hubs and interfaces. Decoupling hardware and software implies that telecom software can never again depend on the particular security properties of a committed telecom hardware. For a similar reason, standard interfaces to the computing/network stages – for example, those characterized by ETSI (the European Telecommunications Standards Institute) in their Network Functions Virtualization work – are important to guarantee a sensible way to deal with security [8]. At the point where operators having third-party applications in their communication fabric and executing on hardware indistinguishable from local telecom services, there are demands on virtualization with solid detachment properties.

Emerging Risk Prospects

5G networks will considerably play an important part as the basic foundation. Numerous individuals have experienced events when phone lines, web access, and TV have all stopped working at the same time during a large-scale system blackout. The quality facilitated in and created by the 5G framework is evaluated to be much higher, and the advantages (hardware, software, and information) will be considerably more appealing for various sorts of attacks. Besides, thinking about the conceivable outcomes of an assault, the harm may not be restricted to a business or community; it could even severely affect the society as a whole. This prompts a need to reinforce certain security measures. Attack resistance should be a key ingredient when designing new 5G protocols [8]. Faulty validation strategies, for example, username/password should be eliminated. However, in a general sense, the new risks stress the requirement for quantifiable security affirmation and consistency; in other aspects, checking the presence, accuracy, and adequacy of security capacities is also important. Those utilizing 5G will require answers to inquiries, for example, is it safe to set up a virtual machine on a given equipment? What security tests have been conducted on a product? A key resource of the Networked Society will be information. As the carriers of information, 5G networks should give satisfactory assurance as separation and productive transport of ensured (scrambled/verified) information. The all of 5G gadgets and network won't simply influence innovative attack patterns; the social engineering attacks will likewise increase. Individuals asserting to be work associates or repair experts, for example, may contact an individual and demand different sorts of access to the person's data as well as to his/her gadgets.

Raised Privacy Concerns

There have been a few recent news stories that reported fraud base stations tracking users in urban communities and extracting individual information without user's knowledge [8]. The security of individual information has been examined inside EU. It is being audited in standardization bodies, for example, the 3GPP and the

IETF, and debated in many other forums. An especially delicate resource is the user identifier(s). As far back as 2G, user security has been a huge concern. However, the International Mobile Subscriber Identity (IMSI) assurance has so far only provided limited protection.

4 Network Planning

The steady growth in demand for better mobile experience, higher data rates, and lower latency is promoting the development of the upcoming generation of wireless systems, namely, 5G [11]. Network planning (NP) is one of the essential stages in deploying a wireless network that meets certain coverage, capacity, and quality of service (QoS) requirements. The planning process can minimize and optimize the locations of base stations (BSs) in a selected geographical area [11].

The precise planning for network establishment consists of:

- Preplanning
- Detailed planning
- Post-planning or optimization

Preplanning The output of preplanning is a surmised number of base stations required to cover an area of interest.

Detailed Planning The detailed planning stage permits the decision of the actual positions of the BSs inside the zone to be served [12].

Post-planning In the optimization stage, which happens after the system has been deployed and is running, the network performance is inspected, potential problems are detected, and network operations are enhanced by the improvement [12].

4.1 Objectives

The objective of NP mostly depends on the business strategy of the operators. The coverage targets for different types of services, taking into account billing and throughput policies, regulatory constraints, market share goals, and competition [11]. Ultimately, the objectives can be boiled down to the following set of optimization goals identified in the cell planning phase.

1. *Minimize TCO*: In addition to minimizing the overall network cost, this objective may also include minimizing economic costs related to deployment and parameter optimization.

2. *Maximize capacity*: For a single service, this goal can be defined as the number of clients who can be served at once. On account of multi-service traffic, the capacity can be approximated with respect to worldwide throughput.
3. *Maximize coverage*: This includes satisfying coverage policy requirements for various services. Uplink (UL) and downlink (DL) coverage must be balanced. Both traffic channels and coverage of standard channels must be considered [13].
4. *Minimize power consumption*: Health concerns have motivated the radiated power minimization objective. However, the recent awakening of a desire for greener wireless systems has added more depth to this objective. Consequently, power consumption, including fixed circuit power as well as variable transmission power, must be minimized.

Optimize Handover (HO) Zones In a well-planned cellular system, a certain proportion of the area of each cell should overlap with neighboring cells to satisfy HO conditions. HO zones are essential to ensure the continuation of service between sectors. It also strengthens the radio connection against fast fading and shadowing [14]. However, too much overlap may result in wastage of power and radio resources and increase in interference and electro-smog, making it a tricky planning objective.

4.2 Planning Inputs

Various inputs are required to solve the cell planning difficulty depending on objectives in focus and phase of planning. The following inputs need to be known for planning the network.

Traffic Models

User traffic distribution is a primary factor that ultimately determines the cellular system plan and, hence, is a crucial input in the network planning process. In GSM (mono-service systems), for instance, geographical characterization of traffic distribution is sufficient. However, with multi-service systems supporting data, traffic characterization based on types and level of service is needed. Test point-based traffic models are often used for network planning traffic modeling, for the sake of practicality [15, 16]. In this model, an area is characterized by a time interval, and all located mobile terminals are bundled into a single test point [17]. This point represents the increasing traffic, or traffic intensity, from all those terminals, over the determined interval.

Potential Site Locations

Theoretically, a base station can be installed anywhere. However, in the real world, a set of candidates is first predetermined and used as input to the cell planning, to incorporate the real estate constraints [15]. The objective is to find the optimum subset of base station locations. These potential BS locations are determined by taking into account constraints such as socioeconomic feasibility and availability of site(s), traffic density, building heights, terrain height(s), and preexistence of a site(s) by the same or other operators.

BS Model

There are many parameters that define the base station model, like antenna type and height, receiver sensitivity, load capacity, transmit power, and capital and operational costs [16]. Moreover, heterogeneous networks necessitate modeling of new types of nodes, for instance, relay stations (RS), picocells, femtocells, and small cells.

Propagation Prediction Models

A key input to the planning process is the signal propagation model. The potential of this model is to incorporate reflection, diffraction, absorption, and propagation of the signal in a real environment [17]. The natural and human-made structures, vegetation, and topography of an area largely determine the accuracy of the network planning outcomes. Very sophisticated planning tools rely on actual measurement-based propagation maps, or ray tracing-based complex analysis, to predict the propagation. However, obtaining complete propagation maps of a large area using these methods is a very cumbersome, time-consuming, and expensive process [15]. For this reason, different empirical models have been proposed in the literature. Such models abstract the experimental and statistical data in the form of deterministic expressions that can easily be used in network planning. Okumura, Hata, and COST 231 are a few examples of such well-known propagation models used in network planning to depict propagation loss in different environments and scenarios [16]. Fine-tuning of these models is done by setting parameters within these models to reflect the real-world conditions as closely as possible. While propagation models for sub-5 GHz frequencies are well established, research on developing such models for higher frequencies such as mmWaves is still in progress [18].

4.3 Planning Outputs

The network planning process intends to provide one or more of the following outputs:

- The ideal number of base stations
- The best areas to fix base stations
- The kind of base station ideal for each area
- The configuration of parameters such as antenna height, number of sectors, and sector orientation, tilt, and power
- Frequency reuse pattern
- Capacity dimensioning, e.g., number of carriers or carrier components per sector

4.4 Types of Network Planning

The objectives, input, and output of the network planning process also depend on the type of planning. There are two types of network planning as described in the follows.

Rollout Network Planning

This is the network planning where no prior networks exist, and a logical state approach can be used to meet all the objectives of interest. Regarding input parameters, in this phase, the traffic distribution is not exactly known yet [18]. Estimates of traffic based on geo-marketing forecasts are used for planning in this phase.

Incremental Network Planning

This type of network planning is carried out after the first rollout planning to meet the increasing demand. Unlike the plane state approach, planning in this phase is bounded by additional constraints imposed by existing sites. However, in this phase, the traffic distribution can be modeled with much better accuracy using measurements from existing network reports. It is anticipated that 5G deployment will mostly require incremental planning by building on LTE/UMTS/GSM network [18].

5 5G Roadmap

5G is not just a progressive upgrade of the previous generation of cellular but a revolutionary technology envisioned to defeat the bounds of access, bandwidth, performance, and latency limitations on connectivity worldwide. It has the potential to enable fundamentally new applications, industries, and business models and dramatically improve quality of life around the world.

5.1 Need for Roadmap

Remarkably, it is fundamental to comprehend which innovative disruptions are required to empower mobiles to last as well as to flourish in an undeniably competitive technology and business landscape. Understanding that innovative disruption is firmly coupled to advancement, this community IEEE innovation roadmap lays out the technology and development vision for the telecommunications industry and a significantly more far-reaching industry stakeholder system. With appropriate direction, it is foreseen that 5G and beyond will have the capacity to realize the financial advantages envisioned in various studies [19].

The critical benefits of the IEEE 5G technology roadmap are to:

- Focus endeavors toward future solutions, with the goal that advantages are boosted for the industry.
- Amortize R&D costs through coordinated efforts and associations.
- Analyze unique developments to obtain potential solutions which serve stakeholders in the business.
- Align with peer-competitive arrangements that can be executed in synergistic environments and also in the competitive domain.
- Contribute and be educated on normal points of view to address the mutual needs and difficulties involved in the evolution to the future state.
- Empower visibility into future innovation patterns.
- Enhance venture methodologies for R&D.
- Make important contributions to the standards.

Building up a time allotment of projections when presenting new innovations might be needed to convey basic advantages like:

- Gives essential lead time to gear and interface improvement
- Enables time for solutions to be displayed and tested
- Empowers research opportunities to be explored and financed

5.2 Roadmap Process

In mid-2016 the community found that there is a need to build up an arranged vision for the wireless connectivity ecosystem. The IEEE 5G Initiative was hence forth presented under the sponsorship of IEEE with a commencement meeting in August 2016, in Princeton in the United States [19]. Also, a significant workshop was held in conjunction with IEEE GLOBECOM 2016, where the vision was enunciated in broad daylight and supporters were urged to contribute to the developing roadmap ecosystem. From these workshops and conferences, a working philosophy has been set up. Generally, the focus of this IEEE innovation guide is to recognize basic needs, difficulties, and potential solutions/zones of development. The point is to build partnerships and coordinated efforts among industry groups, be comprehensive of all divisions of the wireless community and to be driven by industry trends. The goal is to refresh it intermittently; in particular, an arrangement of advance reports is to be routinely delivered and conveyed to the business at large.

The following topics reflect the roadmap working group:

- Massive multiple input, multiple output (MIMO)
- Hardware
- Edge Automation Platform (EAP)
- Millimeter Wave (mmWave)
- Security
- Standardization building blocks
- Applications and services

6 Existing Concepts of 5G

6.1 Multiple Input and Multiple Output

Using multiple transmit and receive antennas, MIMO method is used to increase the capacity of the channel in radio link. MIMO has turned into an essential component of remote correspondence framework benchmarks including IEEE 802.11ac (Wi-Fi), WiMAX (4G), and so on [20]. The advantage of MIMO is that a greater amount of data can be sent across the wireless channels, thereby improving the energy efficiency, spectral efficiency, and reliability. In MIMO configuration, both the transmitter and receiver sides may contain a huge number of antennas [21]. In the current days, “MIMO” refers to a pragmatic system for sending and accepting in excess of one information stream on a radio channel simultaneously through multiple propagation paths, as illustrated in Fig. 1.

In a MIMO system, the transmitting antennas as well as the receiving antennas are distributed to many devices. Further, one of the main benefits of MIMO technology is that intracellular interference and noise can be reduced. Because of these benefits, MIMO is considered to be a key technology.

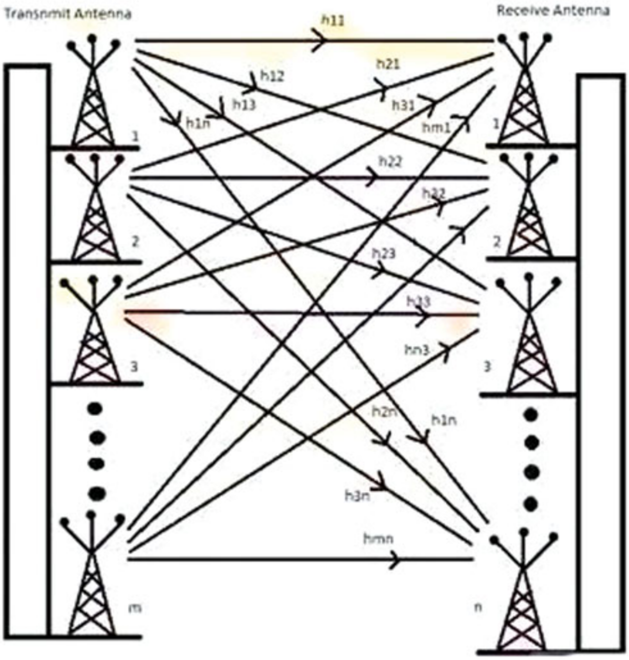


Fig. 1 MIMO system

6.2 Cognitive Radio Network

Cognitive radio (CR) is a vigorous, keen radio and system technology that can automatically recognize available channels in a remote range and furthermore change transmission parameters, thereby enabling more communications at the same time and enhancing radio-operating behavior. Innovations like adaptive radio and software-defined radio (SDR) [20] are utilized in a CR network. Adaptive radio is a technology where the communication system operates and changes its performance. As for SDR, various hardware components like modulator, demodulator, amplifier, and mixer are replaced by an intelligent software system [22]. Cognitive radio network is used to improve the utilization of radio-frequency spectrum as shown in Fig. 2.

As shown in Fig. 3, in one cognitive radio cycle, a device monitors the spectrum bands to detect blank spectrum spaces (white spaces or holes). From the qualities of the spectrum spaces that are recognized through spectrum sensing, a suitable range of band is picked based on the radio characteristics and user requirements [22]. If a band of the operating spectrum is determined to be available for use, communication can be executed over that spectrum band.

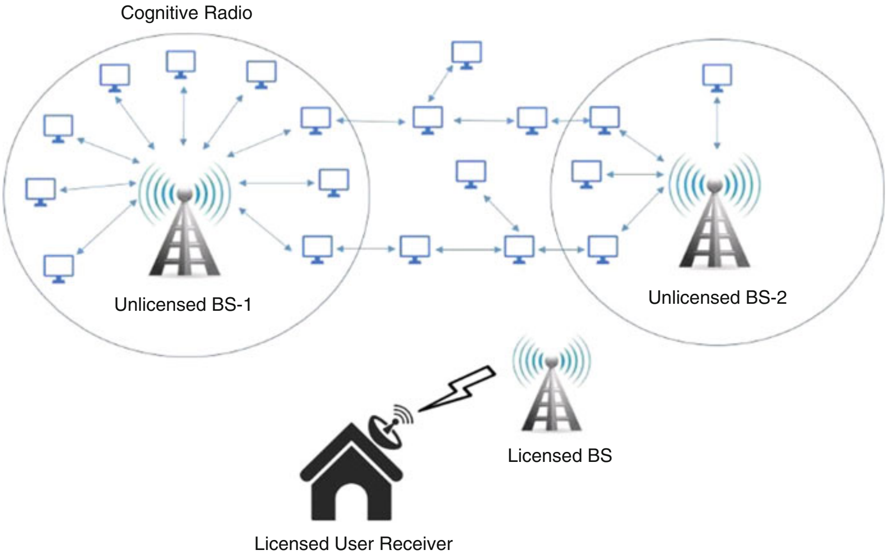


Fig. 2 Cognitive radio system

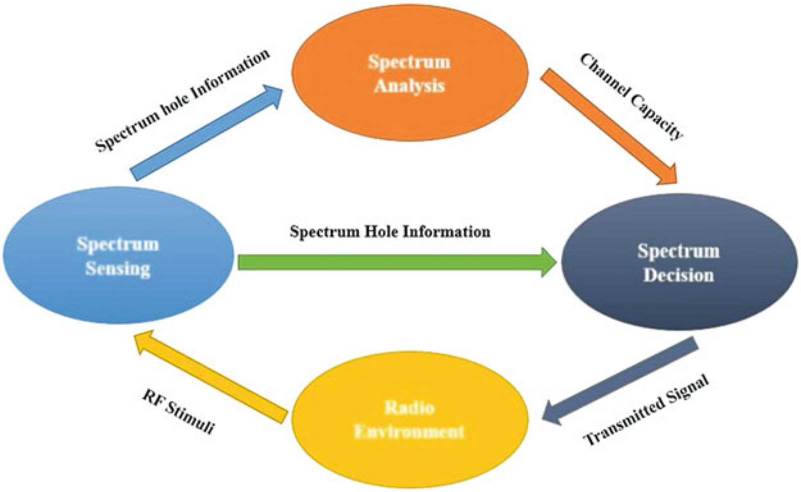


Fig. 3 Cognitive radio cycle

7 Security Models

5G frameworks are the next stage in the advancement of mobile communication and will have a crucial empowering influence on the Networked Society [8]. This advancement engenders new security situations and requires new security arrangements. 5G networks will bring a massive number of connected devices, interoperability of new and legacy access technologies, significant increase of bandwidth, and new business cases that will usher in new challenges from the security perspective [23]. 5G security will not only be defined by quantitative aspects such as bit-rates and latency but also by subjective perception, for example, new business and trust models, better approaches for delivering services, a developed risk landscape, and an expanded concern for protection.

7.1 Identity Management

The 4G LTE standard needs USIM (UMTS Subscriber Identity Module) on the universal integrated circuit card to gain network access [8]. This way of handling the identity will continue to be an essential part of 5G for reasons such as abnormal state of security and ease of use. Embedded SIM has likewise brought down the bar for organization issues identified with machine-to-machine communication. In any case, there is a general pattern of bring-your-own-personality, and the 5G ecosystem would for the most part benefit from a more open identity administration system. The risk of IMSI retrieval, where fraud radio system hardware demands cell phones to reveal their personality, has been talked about amid the 3G and 4G institutionalization process [23]. In any case, no insurance instrument was presented around them, as the anticipated dangers did not appear to justify the cost or multifaceted nature involved. It isn't clear whether this hazard examination is as yet legitimate and improved IMSI security merits thought for 5G.

7.2 UE Security

In the next-generation system, the storage of credentials and identities for both human and machine-type devices is required in the UE. The credentials and identities may be stolen from attacks by software or hardware. Such security threats can impact the subscriber or operator network [23]. 3GPP SA3 has currently agreed that a secure element for credential storage in UEs must provide:

1. Integrity protection of the subscription credential(s)
2. Confidentiality protection of the long-term key(s) of the subscription credential(s) (e.g., Key (K) in EPS AKA (authentication and key agreement)) [23]
3. Execution of the authentication algorithm(s) that make use of the subscription credentials

The above requirements should be achieved within the UE, with the use of a tamper-resistant secure hardware component. Implementations of these requirements shall allow security evaluation/assessment. The Subscriber Identity Module (SIM) functions for 5G, i.e., next-generation USIM will inherit from previous standards [23]. In a similar manner to LTE system, the next-generation USIM will be able to generate symmetric keys. It may also be able to generate new asymmetric key pairs and even new trusted public keys.

7.3 Radio Network Security

Due to the emerging risk landscape and new innovation that furnishes users with minimal effort to program their own gadgets (even at radio access level), the attack resistance of radio systems ought to be an all the more blunt plan thought in 5G, examining risks, for example, Denial of Service from conceivably getting out of hand gadgets, and adding moderation measures to radio protocol outline [23]. In spite of the fact that LTE radio access has phenomenal cryptographic assurance against eavesdropping, there is no security against changing or infusing user plane traffic. With 5G radio access as a building block in, for instance, mechanical automation, the potential advantages of including integrity assurance appear to be deserving of investigation [8].

7.4 Flexible and Scalable Security

With virtualization and more unique setups entering the zone for 5G, it is opportune to consider a more powerful and adaptable security design for it. Security for synchronous RAN signaling [8] could have a higher level of freedom than asynchronous security aspects. New security outlines with higher adaptability can better address clashes between convenience and security.

7.5 Network Slicing Security

Network slicing not only requires the necessary security from UE accessing the slice but also poses new security challenges. Isolation should be assured for network slices, without which attackers who have access to one slice may launch an attack to other slices. Proper isolation will enable integrity and confidentiality protection. Additionally, it should be ensured that resources of the network infrastructure or a network slice instance are not impacted by another slice instance, to minimize attacks and provide availability [23]. A 5G UE can simultaneously access different network slices for multiple services. Such access can be via various types of radio access networks including both 3GPP and non-3GPP. When the network slice access information is tampered, unauthorized UEs may use such information to establish a connection with the network slice and consume resources.

On the other hand, the advantage of network slicing is that operators can provide tailored security for each slice. Different access authentication and authorization can be provided for tenants of different network slices.

7.6 Vitality Effective Security

While security services such as encryption come with a cost, the cost is no longer an issue for cell phones and comparable gadgets. The vitality cost of encoding one bit is similar to transmitting one bit. In any case, for battery-operated gadgets with a long target lifetime, there might be a need to consider significantly more lightweight arrangements, as each joule devoured could be of significance.

7.7 Cloud Security

Cloud security is a critical concept and will be added to the list of 5G security concerns.

- *Integrity Management*

  Each service provider will have its own integrity management system to control access to data and other assets. Cloud suppliers either incorporate the user's integrity management framework into their own foundation using federation or SSO technology or a biometric-based framework or develop an integrity management arrangement of their own [24]. Cloud ID, for example, gives protection, safeguarding cloud-based biometric distinguishing proof. It connects the private data of users to their biometrics and stores them in a scrambled manner. Making utilization of an accessible encryption method, the biometric distinguishing proof is performed in the scrambled area to ensure that the cloud suppliers or potential aggressors don't access any sensitive information or the contents of individual inquiries.
- *Physical Security*

  Cloud specialist advocate the idea of physically securing the IT hardware (servers, switches, links, and so on.) against unapproved access, obstruction, burglary, fires, surges, and so forth and guaranteeing that fundamental resources such as power are adequately protected to diminish the likelihood of interruption. This is regularly accomplished by serving cloud applications from "world-class" [24] (i.e., professionally conceived, designed, built, overseen, and maintained) server centers.
- *Faculty Security*

  Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.

- *Privacy*

  Service providers should guarantee that every single basic datum (credit card numbers, for instance) is properly masked or encoded and that exclusive access are granted to approved users only [24]. Any information that the supplier gathers or delivers about user action in the cloud should also be carefully protected.

8 Security Protocols

Many security protocols have been introduced. We focus mainly on authentication and key exchange protocols for 3GPP network.

8.1 Informal Security Protocols

It is often useful to discuss security protocols informally before proceeding with formal analysis. Therefore, we establish an informal understanding of threat model, security properties, channels, and protocols.

Before going to study about open security protocols, we need to know about Dolev-Yao adversary.

Dolev-Yao Adversary

Large messages are thought to be components of some theoretical variable-based math, and cryptography is a unique activity on that polynomial math [25]. The adversary is thought to be a particular (yet non-deterministic) state machine, and the main route for the enemy to deliver new messages is to play out specific activities on messages it definitely "knows." This model has a to a great degree pleasant component called as straightforwardness. Since all members (genuine and noxious) can be spoken to as state machines, they can be created together to deliver a solitary expansive "framework" machine. Security properties can be communicated as well-being properties about this machine, and such properties can be confirmed consequently. This model likewise has a downside: the Dolev-Yao adversary is entirely frail.

Threat Model

In particular, the Dolev-Yao adversary controls the network, i.e., it can read, intercept, and send messages. Moreover, the adversary can compromise clients, i.e., it can reveal their secrets. Furthermore, the adversary is allowed to apply public functions such as hashing, encryption, or signing on values that she knows. Also, the threat model allows unbounded message lengths, an unlimited number of fresh nonces, and an unlimited number of protocol sessions.

Security Properties

An informal definition of some fundamental security properties is given first and formalized.

Definition (Authenticity) Information is authentic if the original message sender is whom he or she claims to be and the message is unchanged [26].

Definition (Confidentiality, Secrecy) Confidentiality (also called secrecy) is the property of information being protected from disclosure to unauthorized parties.

Definition (Integrity) Information has integrity if it is not modified in any way by unauthorized parties.

Authentication Properties for Protocols

Definition (Aliveness, Informal) A protocol assures to an agent “x” in role X the aliveness of another agent “y” if whenever “x” accomplishes a run of the protocol, apparently with “y” in role Y, then “y” has previously been running the protocol [25].

Definition (Weak Agreement, Informal) A protocol assures to an agent “x” in role X weak agreement with another agent “y” if whenever agent “a” accomplishes “x” run of the protocol, apparently with “y” in role Y, then “y” has previously been running the protocol, apparently with “x” [25].

Definition (Non-injective Agreement, Informal) A protocol assures to an agent “x” in role X non-injective agreement with an agent “y” in role Y on a message M if whenever “x” accomplishes a run of the protocol, apparently with “y” in role Y, then “y” has previously been running the protocol, apparently with “x,” and “y” was acting in role Y in his run, and the two agents agree on the message M.

Definition (Injective Agreement, Informal) The injective agreement is defined to be non-injective agreement with the additional property that each run of agent “x” in role X corresponds to a unique run of agent “y” in role Y. The intuitive understanding of injective agreement is that it prevents replay attacks.

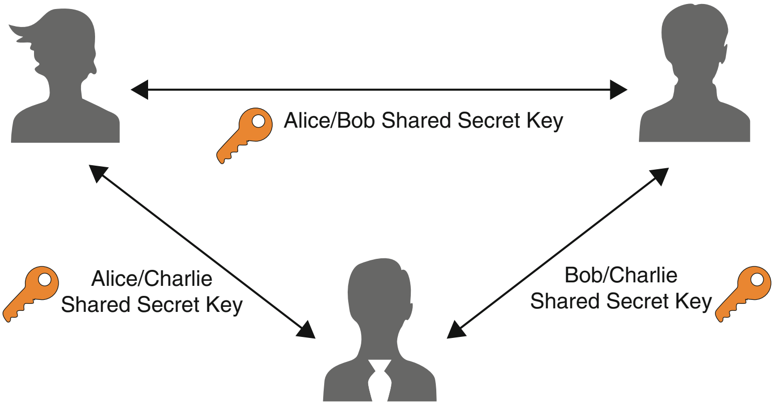


Fig. 4 Alice and Bob message transmission

Channels

For two parties to exchange messages, it is crucial that they be connected in some way.

Definition (Channel) A channel is a logical connection between two parties that can be used to transmit messages.

Recall that the threat model assumes that the adversary controls the network, i.e., it can read and send arbitrary messages over a regular channel. Further, this motivates the following definition of an essential type of channel, making use of the defined notions of informal security properties.

Definition (Secure Channel) A secure channel is a channel that provides confidentiality and authenticity. However, it does not protect messages from being replayed or reordered by the adversary.

Alice and Bob Notation

Protocols will be first specified in an extended form so-called Alice and Bob notation before specifying them formally. Protocols are specified as a set of roles, where every part comprises of a number of steps. Each step sends or receives messages. Moreover, the protocol participants are called agents. Each agent has a name and can execute a protocol in different roles with other agents.

Figure 4 demonstrates the process followed by the Alice and Bob concept. The message which is to be transmitted to the other end is encrypted so that only the person at the other end of will know how to decrypt it regardless of whether it is an insecure communication medium.

In a nutshell, Alice and Bob notation is a compact and succinct description of the messages that the protocol agents exchange in the presence of an attacker. The semantics of the Alice and Bob notation will not be defined rigorously. Instead, the principal conventions are explained, and simple example is given to furnish the understanding.

The following conventions are used:

- If an agent receives a message containing a term *x* and *x* is known to the agent (e.g., because it is the peer's agent name or the agent has sent or received x in an earlier message of the same protocol run), then it must verify that the values of both x's match. This check is implicit in the notation [27].
- If an agent receives a message, it will verify its structure up to the level required to recover all sub-terms it needs, for example, to match the values it knows already or to compute subsequent messages. Also, this is crucial, since the recipient's view may differ from the sender's view.

  For example, if an Alice and Bob protocol specification describes a message (x, hash(y)) for some hash function hash, then an agent who knows only x (and not y) will accept any pair t with x as first element, e.g., t = (x, 0) or t = (x, f ((h, 1))) for some function f.
- Messages marked with an asterisk * are optional, i.e., they can be skipped by both the sending and the receiving agents.
- {|x|}*k* denotes symmetric encryption of the message x with key *k*. The message x can be recovered from {|x|}*k* if and only if an agent knows *k*.
- {m}*sk* denotes the message m signed with key *sk*. A signature in Alice and Bob notation is always hiding, i.e., the message itself cannot be recovered from the signature.
- [[m]]*sk* is an abbreviation for (m,{m}*sk*). It can be understood as a form of non-hiding signature.
- → denotes a secure channel.
- Messages of a protocol are numbered consecutively, starting from 1.

Protocol Example 1

1. A → B: (A, {|n|}*k*)
2. B → A: {B, n}*k*
3. B → C: ({|n|}*k*, *k*)

How the above protocol example runs is informally described below. Assume agent "a" is executing the protocol in role A with an agent "b" in role B. Moreover, "b" is executing the protocol with role A and with an agent "c" in role C.

1. a starts by sending the message (a,{|n|}*k*) over an attacker-controlled channel to b. Here, n is to be understood as a fresh nonce and *k* is a long-term key shared between a and b. When b receives the message, it verifies the value of a in the message and tries to decrypt the value n.
2. If b has accepted the first message from a, it replies with the message {b, n}*k* over an attacker-controlled channel. When a receives the message, it verifies the value of band n as well as the signature.
3. After b has sent the second message, it can optionally send the message ({n}*k*, *k*) to cover a secure channel. c will accept the message in any case, even if it has

the wrong structure (e.g., if it is a constant string). Further, this is because c does not know the key *k* or the term {n}*k* and it does not need to extract one of those terms to compute a subsequent message.

Attack Scenarios

The term attack scenario is used to outline protocol attacks. An attack scenario uses the same notation as Alice and Bob protocols. Additionally, we use the following conventions.

- We write Adv(R) to denote the adversary masquerading as agent R.
- Parallel protocol instances are indented in case an attack requires multiple instances.
- Messages that are not relevant to the attack are omitted.
- We distinguish different runs of the same agent A (if there is more than a single run) with indices A [0], A [1]...

Assume that in the protocol example, B would claim injective agreement with A on n after it received the first message. It is easy to see that the property is violated because the adversary can masquerade as A and resend the first message to B.

Attack Scenario 1 outlines the attack.

Attack Scenario 1 (Example)

1. A → B [0]: (A, {|n|}*k*)
2. Adv (A) → B [1]: (A, {|n|}*k*)

The outlined attack violates injective agreement of B with A on the value n. It is a trivial replay attack that makes B accept the same value n twice.

9 Channel Security

Physical layer security achieves information confidentiality based on data theoretic methodologies and has got significant progress. The key idea behind physical layer security is to utilize the normal haphazardness of the transmission channel to guarantee security in the physical layer. The move toward 5G mobile communication poses new challenges for physical layer security to look into.

9.1 Introduction

These days, mobile communication systems have been broadly utilized in regular citizen and military applications and have become a vital piece of our day-to-day life. Individuals depend intensely on the systems for transmission of vital/private data, for example, credit card data, e-well-being information, and control messages.

As a result, security is a key issue for future 5G mobile networks. Normally, existing security measures depend on bit-level cryptographic techniques and associated protocols at different levels of the data processing stack. These solutions have several disadvantages. First, standardized protections within public wireless networks are not safe enough, and many of their weaknesses are well known. Second, even if enhanced ciphering and authentication protocols exist, they incur heavy constraints and high additional costs for the users of public networks. Therefore, new security approaches are rooted in information theory fundamentals and focus on the secrecy capacity of the propagation channel [28]. This is referred to as physical layer security.

The advantages of employing physical layer security techniques for 5G networks compared to that of cryptography techniques are twofolds.

- Initially, physical layer security systems don't depend on computational intricacy [29].
- Second, the structures of 5G networks are usually decentralized, which implies devices may randomly connect to or exit the network at any time instant.

As a result, physical layer security techniques can be used to either perform secure data transmission directly or generate the distribution of cryptography keys in the 5G networks. Specifically, we center on the following innovations.

9.2 Physical Layer Security Coding

Although the first physical layer security code appeared around 1970s, the design of specific security codes which can be used in practical communication systems is still challenging. We survey the best in class of three crucial physical layer security codes, including low-density parity check (LDPC) codes, polar codes, and lattice codes [30].

LDPC Codes

The LDPC codes are the first secrecy-capacity-achieving codes regarding weak secrecy. LDPC codes have been intended for the Gaussian wiretap channel. The physical layer security communication is fulfilled by punctured LDPC codes under the metric of bit error rate (BER), where the secrecy data bits are covered up in the punctured bits. In this way, these data bits are not transmitted through the channel but rather can be decoded at the recipient side in light of the non-punctured piece of the codeword.

This coding scheme can yield a BER close to 0.5 at the eavesdropper's (Eve Channel) side while significantly decreasing the security gap compared to the non-punctured LDPC codes. However, the punctured LDPC codes result in higher transmit power compared to the non-punctured LDPC codes. Further, to solve this problem, a nonsystematic coded transmission design by scrambling the information bits has been proposed. This scrambling technique achieves a security level comparable to the design based on puncturing without expanding the transmit control. This scrambling configuration has been applied to parallel Rayleigh dispersed channels by exploiting the equivocation rate of eavesdropper's channel as an optimization criterion. A summary of the attributes of LDPC codes is given in Table 1. 5G enhanced mobile broadband (eMBB) use case will adopt LDPC codes for channel coding on the data channel.

Polar Codes

For the weak secrecy criterion, a polar coding scheme is constructed to attain the secrecy capacity for the symmetric binary-input memoryless wiretap channel under the condition that the channel of the eavesdropper is degraded relative to the main channel of the desired user [31]. The main idea is to select only those bit channels which are suitable for both the desired user and the eavesdropper to transmit random bits. Moreover, [31] those bit channels which are suitable for the desired user but bad for the eavesdropper are used to transmit information bits.

This coding scheme is applied to a critical agreement problem over the block fading wiretap channel. The safe polar code is utilized for each fading block, from which the secrecy keys are produced in light of standard privacy amplification techniques [32].

Also, this coding scheme is extended to the multiple access wiretap channel (MA-WC), the broadcast channel with confidential message (BC-CM), and the interference channel with confidential message (IC-CM).

This coding scheme has been applied to accomplish the Shannon capacity of discrete memoryless BC-CM [32]. A summary of the attributes of polar codes is given in Table 2. 5G eMBB use case will adopt polar codes for channel coding on the control channel.

Table 1 LDPC codes for physical layer security

Main channel	Eve channel	Criterion	Constituent codes
Noiseless	BEC	Weak secrecy	Duals of LDPC
BEC	BEC	Weak secrecy	Two-edge LDPC
Noiseless	BEC	Strong secrecy	Duals of LDPC
Gaussian	Gaussian	BER	Punctured LDPC
Gaussian	Gaussian	BER	Non-punctured LDPC
Parallel Rayleigh	Parallel Rayleigh	BER	Non-punctured LDPC
Gaussian	Gaussian	Equivocation rate of Eve	Irregular LDPC

Table 2 Polar codes for physical layer security

Channel	Criterion	Main contribution
Symmetric binary-input memory less degraded wiretap channel	Weak secrecy	Achieve secrecy capacity
Symmetric binary-input memory less degraded wiretap channel	Weak secrecy	Achieve rate-equivocation region
Symmetric binary-input memory less degraded wiretap channel	Weak secrecy	Generate a key agreement
General wiretap channel MA-WC, BC-CM, IC-CM	Weak secrecy	Achieve secrecy capacity Achieve secrecy rate regions
Deterministic wiretap channel	Weak secrecy	Achieve secrecy capacity
Bidirectional relay networks with confidential messages	Weak secrecy	Achieve capacity-equivocation region
Symmetric binary-input memory less degraded wiretap channel	Strong secrecy	Achieves both security and reliability
General wiretap channel	Strong secrecy	Achieve secrecy capacity
Discrete memory less BC-CM	Strong secrecy	Achieve secrecy capacity

Table 3 Lattice codes for physical layer security

Channel	Criterion	Main contribution
Gaussian wiretap channel	Secrecy gain	Define secrecy gain
Gaussian wiretap channel	Secrecy gain	Propose a method to examine the secrecy gain
Gaussian wiretap channel	Secrecy gain	Construct best lattice codes for dimensions $8 < n \leq 23$
Rayleigh wiretap channel	Secrecy gain	Construct a wiretap lattice code
Gaussian wiretap channel	Weak secrecy	Construct a wiretap lattice code
Gaussian wiretap channel	Strong secrecy	Design wiretap lattice codes
Gaussian BC with a confidential message	Strong secrecy	Propose a superposition lattice code

Lattice Codes

For wiretap lattice codes, a notation of secrecy gain is defined, which reflects the eavesdropper's correct decoding probability [32]. Asymptotic analysis of the secrecy gain shows that it scales with the dimension of the lattice. A summary of the attributes of lattice codes is given in Table 3.

Other lattice code designs for the wiretap channel include nested lattice code for cooperative jamming, interference channels, and Gaussian relay networks.

Table 4 Secure massive MIMO with passive eavesdropper

System model	Main contribution
Multi-cell multiuser, one desired user, one eavesdropper	Matched filtering precoding and AN generation designs
Multi-cell multiuser, one desired user, one eavesdropper	Regularized channel inversion and AN generation designs
One desired user, multiple eavesdroppers	AN-aided secure transmission designs
Single-cell, multiple desired users, one eavesdropper	Distributed power allocation under security constraints
One desired user, one eavesdropper	Secure transmission with finite alphabet inputs
Relay-aided, one desired user, one eavesdropper	Secrecy performance analysis and power allocation designs

9.3 Massive MIMO

Deploying large antenna arrays significantly increases the capacity of channels. Massive MIMO is a promising technology for effective transmission of massive data and is viewed as one of the “big three” 5G technologies.

Passive Eavesdropper Scenarios

Physical layer security for massive MIMO systems with passive eavesdroppers has been newly studied [33]. The impact of multi-cell interference and pilot contamination on the achievable ergodic secrecy rate are analyzed, and several matched filtering, precoding and artificial noise (AN) generation designs are proposed to mitigate the eavesdropper’s channel [33] and protect the desired user’s channel.

For single-cell multiuser massive MIMO systems with distributed antennas, three security-constrained power allocation schemes are designed by maximizing the minimum user’s signal-to-interference-noise ratio (SINR) subject to the eavesdropper’s SINR and the sum power constraint and reducing the sum transmit power subject to SINR [34] constraints of the users and the eavesdropper, respectively.

A summary of secure massive MIMO systems with passive eavesdropper(s) is given in Table 4.

Other secure massive MIMO works with passive eavesdroppers include a secure transmission for massive MIMO systems with limited radio-frequency and hardware impairments, secure strategies in the existence of a massive MIMO eavesdropper, secrecy outage probability analysis for a massive MIMO system, and so on [35].

Active Eavesdropper Scenarios

Most physical layer security research work assumes that the perfect channel knowledge of the appropriate user is available at the transmitter and won’t delve into details of the procedure required to obtain this channel knowledge [31]. In time duplex division (TDD) communication frameworks, the users in an uplink

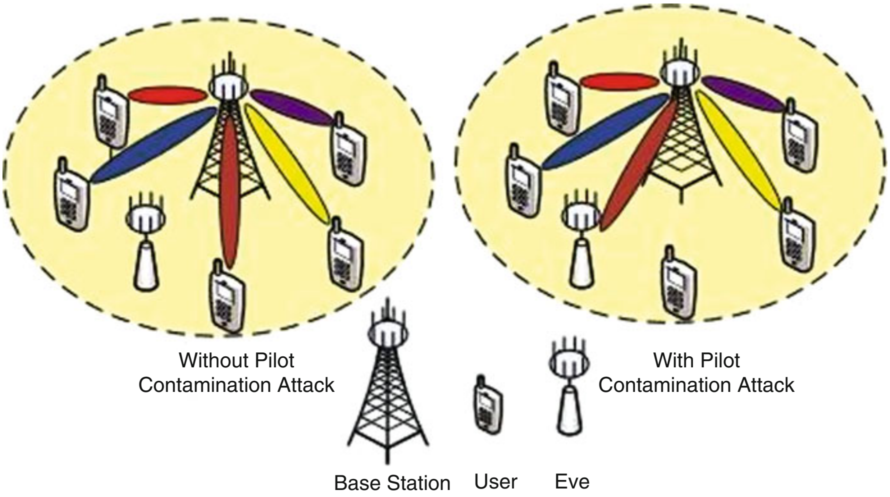


Fig. 5 Secure massive MIMO with active eavesdropper

preparing stage will send pilot signals to the base station (BS) to assess the channel for the ensuing downlink transmission. From the eavesdropper's perspective, it can effectively send a similar pilot signal as the clients to attack this uplink channel training stage and thus significantly increase its eavesdropping capability.

This pilot contamination attack causes a severe secrecy threat to TDD-based massive MIMO systems [32]. On one hand, large antenna arrays beam-forming leads to the hardening of the channel, which prevents the exploitation of channel fluctuations caused by fading to sharpen the secrecy performance. On the other hand, as illustrated in Fig. 5, the pilot contamination [36] attack causes the transmitter to beam form toward the eavesdropper instead of the desired user. If the eavesdropper's pilot power is sufficiently large, a desired secrecy rate may not be achievable. Systematical analysis of the secrecy threat caused by the pilot contamination attack for multi-cell multiuser massive MIMO systems over correlated fading channels has been performed [32]. Then, a matched filter precoding and AN generation design and a null space design are provided to nullify the pilot contamination attack for weakly correlated channels and highly correlated channels, respectively. A unified design which combines the matched filter precoding and AN generation design and null space design is also proposed. MIMO systems are the same as the maximum DoF (degrees of freedom) of massive MIMO systems when the eavesdropper does not exist. However, if the pilot contamination attack exists, the maximum secure DoF of massive MIMO systems could be zero. An estimator is designed at the BS side to evaluate the leakage [37].

Then, the BS and the desired user perform the reliable, secure communication by adjusting the lengths of the secret key based on the estimated information leakage. A summary of secure massive MIMO systems with active eavesdropper(s) is given in Table 5.

Table 5 Secure massive MIMO with active eavesdropper

System model	Main contribution
Multi-cell multiuser, one desired user one eavesdropper	Systematically analyze the secrecy threat caused by the pilot contamination attack Propose efficient schemes to combat the pilot contamination attack
Single-cell multiuser, multiple desired users one eavesdropper	Analyze maximum secure DoF with the pilot contamination attack Propose a plan to shield the pilot signal under the pilot defilement attack
Single-cell multiuser, one desired user one eavesdropper	Employ secret key agreement protocol with the pilot contamination attack Adjust the lengths of the secret key based on the estimated information leakage

9.4 Millimeter Wave (mmWave) Communications

Abundant spectra within the high-frequency band may result in significantly different propagation environments for physical layer secure communication. To understand mmWave secure transmission more clearly, research works for both point-to-point and network mmWave communication systems are introduced.

One of the most promising potential 5G technologies under consideration is the use of high-frequency signals in the millimeter-wave frequency band that could allocate greater bandwidth to deliver faster, higher-quality video and multimedia contents [38]. Compared to microwave networks, the mmWave networks have various new characteristics such as a large number of antennas, short range and highly directional transmissions, different propagation laws, sensitive to blockage effects, and so on. Therefore, secure mmWave communications will be different from conventional secure microwave communications.

The mmWave communication system is usually equipped with a larger number of antennas at the transmitter with a limited number of radio-frequency (RF) chains [39]. To take advantage of this point, let us consider another approach by using an antenna subset modulation (ASM) technique to reach secure mmWave communication at the physical layer. The proposed approach utilizes a subset of the antenna array to formulate a directional modulation signal intended for the desired user. By randomly choosing the antenna subset for each symbol, the received signal for the undesired user becomes a randomized noise. Therefore, secure transmission is achieved. This ASM technique can be further extended to mmWave vehicular communication systems.

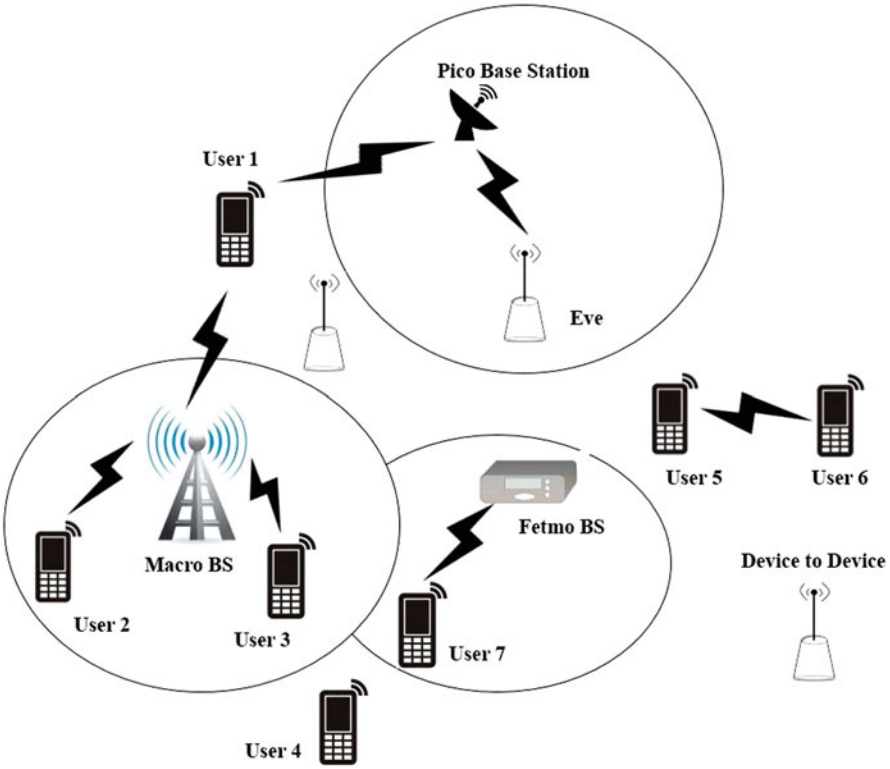


Fig. 6 A four-tier macro-/pico-/femto-/D2D heterogeneous network with users and eavesdroppers

9.5 Heterogeneous Networks

In general, a heterogeneous network is composed of various tiers of networks which operate in the same system bandwidth [37]. We describe in detail on how to design transmission schemes to secure multitier communications.

Physical Layer Security in Heterogeneous Networks

The 5G heterogeneous systems ought to insightfully and consistently incorporate different nodes to frame a multitier hierarchical architecture [40], including the macro-cell tiers with high-power nodes for extensive radio coverage regions, the small cell tiers with for small radio areas, and the gadget levels which bolster gadget-to-gadget interchanges. Figure 6 shows a typical four-tier macro-/pico-/femto-/D2D heterogeneous network with users and eavesdroppers.

This multitier architecture brings new challenges to the investigation of physical layer security compared to the conventional single-tier topology [41]. For example, the locations of the high-/low-power nodes will have a significant impact on the physical layer security design, which needs to be modeled and analyzed correctly. The optimal selection policy for each user among high-/low-power nodes under security constraints becomes difficult. The protection of confidential and privacy data between connected devices against data leakage requires sophisticated designs. Moreover, heterogeneous networks may introduce severe cross-tier interference. These aspects should be taken into consideration when designing reliable and secure data transmission schemes. Also, [40] users are accessible to [alternatively, should have access to] an arbitrary tier, e.g., open access. Therefore, particular user association policies that coordinate both quality of service and secrecy are necessary.

9.6 Non-orthogonal Multiple Access (NOMA)

As a multiple access technology, the security of NOMA communications is a paramount concern to which more attention should be paid [39]. The physical layer security technology can be combined with NOMA to tackle this issue.

Physical Layer Security of NOMA

NOMA plays a crucial role in providing substantial system throughput, high reliability, improved coverage, low latency, and massive connectivity in 5G wireless networks. As a result, NOMA has been recognized as an essential enabling technology in 5G wireless communication systems [42]. Because of the spectral efficiency benefit, NOMA has been newly incorporated into 3GPP Long-Term Evolution Advanced (LTE-A), which additionally proves the significance of NOMA in future communication systems. Consequently, giving an unrivalled level of security for NOMA innovation is one of the most urgent needs in the outline and execution of the 5G communication systems. Significant research is needed to efficiently consolidate physical layer security with NOMA [39]. However, a few difficulties should be addressed in the design process, for example, the different transmit powers and heterogeneous security requirements of users. Additionally, participation of clients offers an intriguing alternative to improve the secrecy execution.

In Fig. 7, an eavesdropper-exclusion zone is established. To reduce the SIC (successive interference cancellation) complexity at the receiver, a user paring scheme is employed, where one user in the internal zone and one user in the external zone are allocated in the same resource slot. When the base station only has a single antenna, the secrecy outage probability is analyzed.

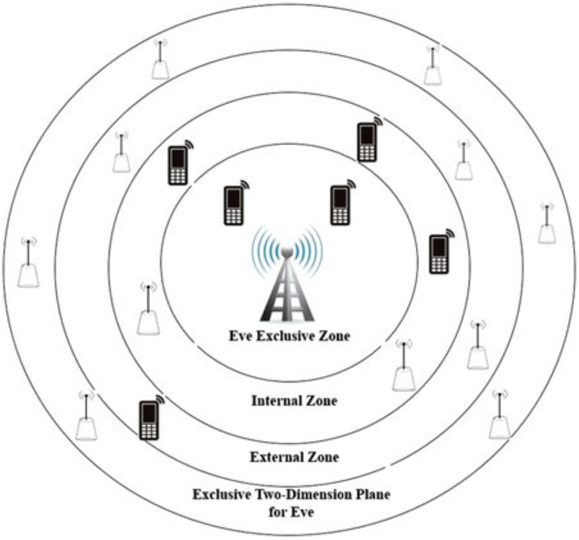


Fig. 7 Network model for secure NOMA transmission

9.7 Full Duplex Technology

Full duplex technology brings both opportunity and challenge for the physical layer security communication. On one hand, the full duplex innovation empowers the recipient to produce extra AN to interfere the eavesdropper. Then again, the eavesdropper with full duplex innovation can effectively attack the communication procedure while eavesdropping. In general, we talk about four classes of full duplex physical layer security interchanges, including the full duplex receiver, the full duplex transmitter and receiver, the full duplex base station, and the full duplex eavesdropper.

Full Duplex Receiver

Firstly, a single-antenna transmitter, a two-antenna full duplex receiver, and a single-antenna eavesdropper wiretap channel were studied [43], where the full duplex receiver uses one antenna to receive the signal and another antenna to send AN to the eavesdropper. Perfect self-interference cancellation (SIC) is assumed at the receiver.

The closed-form expression of the secrecy outage probability for the transmission scheme proposed in [44] is derived to investigate the joint transmit and receive beam-forming design for a single-antenna input, multiple-antenna output, and multiple-antenna eavesdropper (SIMOME) wiretap channel with imperfect SIC [45]. The full duplex receiver transmits AN to the eavesdropper while accepting data from the transmitter. For the global perfect CSI assumption, the linear receiver matrix and the AN generation matrix which boost the achievable secrecy rate are mutually designed. It is demonstrated that unlike the half duplex case, the secrecy rate no longer saturates at high SNR for the full duplex case.

Further, a closed-form expression is derived for the maximal achievable secure degrees of freedom of the MIMO ME (multiple-antenna eavesdropper) wiretap channel with a full duplex receiver under the global perfect CSI and perfect SIC assumptions [43]. Both the transmitter and the full duplex receiver will send AN to debase the channels of the eavesdroppers. For this situation, the precoding matrix and the AN generation matrix are streamlined mutually to boost the achievable secrecy rate. The secure communication in a single-input-single-output multiple-antenna eavesdropper (SISOME) wireless ad hoc network is analyzed where a hybrid full/half duplex receiver deployment strategy is employed [46]. The fractions of full duplex receivers which optimize the secure link number, the network-wide secrecy throughout, and the network-wide secrecy energy efficiency are derived.

Secure bidirectional communication is investigated where two multiple-antenna full duplex nodes communicate with each other in the presence of multiple-antenna eavesdroppers. Global perfect CSI and imperfect SIC assumptions are adopted. The beam-forming vectors are designed to reduce the total transmit power subject to the constraints of secrecy and QoS parameters. Assuming global perfect CSI and perfect SIC, the secrecy sum rate of bidirectional full duplex communication systems is maximized within the sight of a single-antenna eavesdropper under the sum transmit power constraint [46]. A null space-based suboptimal design is also proposed to reduce the computational complexity.

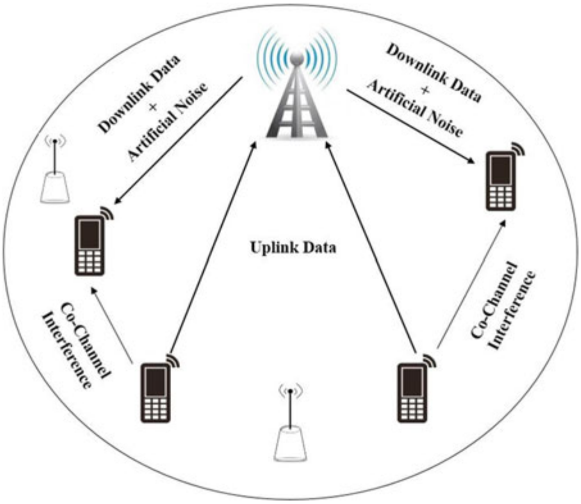
Full Duplex Base Station

Consider a multiple-antenna full duplex base station which communicates with a single-antenna transmitter and a single-antenna receiver simultaneously with single-antenna eavesdropper [47] (Fig. 8). The joint precoding and AN generation design at the base station with global perfect CSI and perfect SIC is investigated to guarantee both the uplink and downlink transmission security. It is expected that exclusive defective [48] CSIs of eavesdroppers are accessible to the base station. A vigorous asset designation is intended to limit the total of uplink and downlink transmit power subject to the uplink and downlink data rate and security rate requirements. As illustrated in Fig. 9, the proposed configuration accomplishes significantly higher-power efficiency compared to the baseline ZFBF (zero-forcing beam-forming) scheme.

Full Duplex Eavesdropper

Consider a multiple-antenna full duplex active eavesdropper which simultaneously eavesdrops and attacks the legitimate MIMO communication link. It is expected that

Fig. 8 Secure communication for the full duplex base station network



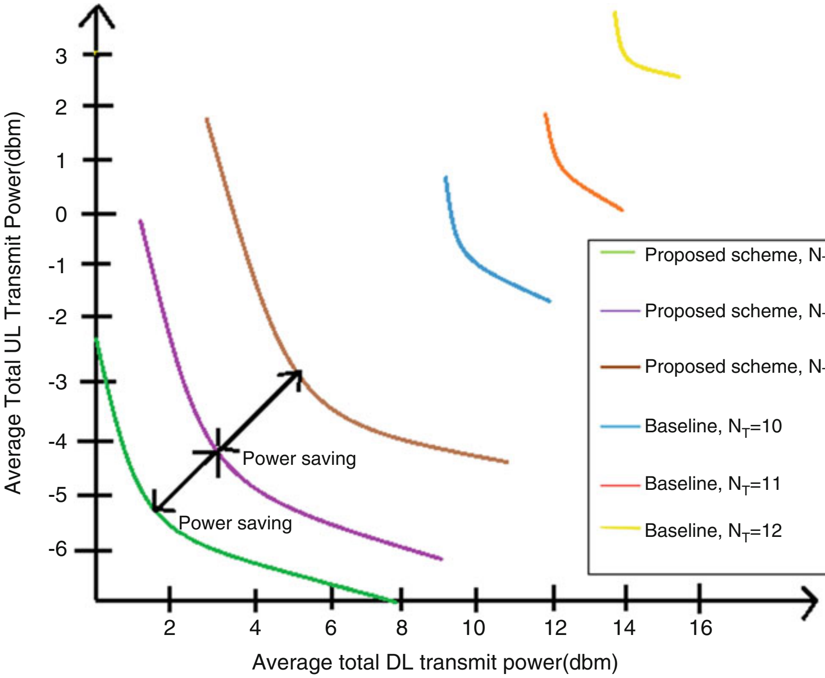


Fig. 9 Tradeoff between the downlink and uplink total transmit powers

the eavesdropper has information of the channels among all nodes and imperfect estimation of the self-interference channel. The jamming signals which minimize the secrecy rate are designed based on the Karush-Kuhn-Tucker (KKT) analysis.

Then, the optimal transmission strategies at both the eavesdropper and the legitimate user's sides are designed.

References

1. G. Asvin, H. Modi, S.K. Patel, 5G technology of mobile communication: A survey, in *IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)*, Gujarat, 2013, pp. 288–292
2. Internet source – isindexing.com
3. M.K. Arjmandi, 5G overview: Key technologies, in *Opportunities in 5G Networks: A Research and Development Perspective*, ed. by F. Hu (CRC Press, Boca Raton, 2016)
4. Internet source – www.nou.edu.ng
5. P. Sharma, Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation. Int. J. Comput. Sci. Mob. Comput. **2**(8), 47–53 (2013)
6. Internet source – scm-fallersleben.ciando.com
7. M. Chen, Y. Qian, S. Mao, W. Tang, X. Yang, Software defined mobile network security. Mob Netw Appl **21**(5), 729–743 (2016)
8. Internet source – www.ericsson.com
9. M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, M. Ylianttila (eds.), *A Comprehensive Guide to 5G Security* (Wiley, Hoboken, 2018)
10. V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, J. Taheri, 5G mobile networks -requirements, enabling technologies, and research activities, in *A Comprehensive Guide to 5G Security*, (Wiley). https://www.etsi.org/etsi-security-week-2017/5g-security
11. W. El-Beaino, A.M. El-Hajj, Z. Dawy, On radio network planning for next generation 5G networks: A case study, in *International Conference on Communications, Signal Processing, and Their Applications (ICCSPA)*, Sharjah, 2015, pp. 1–6. https://doi.org/10.1109/ICCSPA.2015.7081315
12. Y. Elias, Z. Dawy, LTE radio network planning with Het-Nets: BS placement optimization using simulated annealing, in *MELECON 2014–2014 17th IEEE Mediterranean Electro-Technical Conference*, 2014
13. C.Y. Lee, H.G. Kang, Cell planning with capacity expansion in mobile communications: A Tabu search approach. IEEE Trans. Veh. Technol. **49**(5), 1678–1691 (2000)
14. Internet Source – hal.inria.fr
15. Z. Ribeiro, L.A. DaSilva, A framework for the dimensioning of broadband mobile networks supporting wireless internet services. IEEE Wirel. Commun. **9**(3), 6–13 (2002)
16. K. Tutschku, P. Tran-Gia, Spatial traffic estimation and characterization for mobile communication network design. IEEE J. Sel. Areas Commun. **16**(5), 804–811 (1998)
17. R. Pattuelli, V. Zingarelli, Precision of the estimation of area coverage by planning tools in cellular systems. IEEE Pers. Commun. **7**(3), 50–53 (2000)
18. A. Taufique et al., Planning wireless cellular networks of future: Outlook, challenges and opportunities. IEEE Access **5**, 4821–4845 (2017)
19. Internet source – 5g.ieee.org
20. Internet source – pubs.sciepub.com
21. L. Hermann, MIMO OFDM space time coding – spatial multiplexing, increasing performance and spectral efficiency in wireless systems, Part I technical basis (Technical report), 2007
22. A. Agarwal, G. Misra, K. Agarwal, The 5th generation mobile wireless networks – key concepts, network architecture and challenges. Am. J Electr Electron Eng **3**(2), 22–28 (2015)

23. Xiaowei Zhang Detecon International GmbH, Cologne, Germany, Andreas Kunz Lenovo, Oberursel, Germany, Stefan Schröder T-Systems International GmbH, Bonn, Germany. 2017 IEEE Conference on Standards for Communications and Networking (CSCN)-Overview of 5G security in 3GPP (2017).
24. Internet Source – www.nosmut.com
25. Internet source – tamarin-prover.github.io
26. B. Schmidt, Formal Analysis of Key Exchange Protocols and Physical Protocols, PhD Thesis, ETH Zurich, 2012
27. S. Meier, Advancing Automated Security Protocol Verification, PhD Thesis, ETH Zurich, 2013
28. Internet source – www.phylaws-ict.org
29. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M. Di Renzo, Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. **53**, 20 (2015)
30. Internet source – www.faqs.org
31. M. Baldi, G. Ricciutelli, N. Maturo, F. Chiaraluce, Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel, in *Proc. Int. Conf. Commun. (ICC'2015),* London, June 2015, pp. 435–440
32. H. Mahdavifar, A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Trans. Inf. Theory **57**, 6428–6443 (2011)
33. Y. Wu, R. Schober, D.W.K. Ng, C. Xiao, G. Caire, Secure massive MIMO transmission with an active eavesdropper. IEEE Trans. Inf. Theory, 1–22 (2016)
34. K. Guo, Y. Guo, G. Ascheid, Security constrained power allocation in MU-massive MIMO with distributed antennas. IEEE Trans. Wireless Commun. **15**(12), 8139–8153 (2016)
35. Y. Zhang, A. Liu, C. Gong, G. Yang, S. Yang, Polar-LDPC concatenated coding for the AWGN wiretap channel. IEEE Commun. Lett. **18**, 1683–1686 (2014)
36. Y. Wu, R. Schober, D.W.K. Ng, C. Xiao, G. Caire, Secure massive MIMO transmission in the presence of an active eavesdropper, in *2015 IEEE International Conference on Communications (ICC)*, 2015
37. T.T. Do, H.Q. Ngo, T.Q. Duong, T.J. Oechtering, M. Skoglund, Massive MIMO pilot retransmission strategies for robustification against jamming. IEEE Wireless Commun. Lett. **6**(1), 58–61 (2017)
38. Internet source – www.scientificamerican.com
39. Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges. IEEE J Sel. Areas Commun. **36**(4), 679–695 (2018)
40. D.B. Rawat, K. Neupane, M. Song, A novel algorithm for secrecy rate analysis in massive MIMO system with target SINR requirement, in *Proc. INFOCOM'2016*, San Francisco, April 2016, pp. 1–6
41. H.-M. Wang, T.-X. Zheng, *Physical Layer Security in Random Cellular Networks* (Springer, Singapore, 2016)
42. Z. Ding, Z. Zhao, M. Peng, H.V. Poor, On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming. IEEE Trans. Commun. **65**(7), 3151–3163 (2017)
43. G. Zheng, I. Krikidis, J. Li, A.P. Petropulu, B. Ottersten, Improving physical layer secrecy using full-duplex jamming receivers. IEEE Trans. Signal Process. **61**, 4962–4974 (2013)
44. Wireless Networks, Springer, 2016. https://www.cs.cmu.edu/~prs/wirelessS16/
45. G. Chen, Y. Gong, P. Xiao, J.A. Chambers, Physical layer network security in the full- duplex relay system. IEEE Trans. Inf. Forensics Secur. **10**(3), 574–583 (2015)
46. L. Li, Z. Chen, D. Zhang, J. Fang, A full-duplex Bob in the MIMO Gaussian wiretap channel: Scheme and performance. IEEE Signal Process Lett. **23**, 107–111 (2016)
47. Z.H. Awan, A. Zaidi, L. Vandendorpe, Multi access channel with partially cooperating encoders and security constraints. IEEE Trans. Inf. Forensics Secur. **8**, 1243 (2013)
48. F. Zhu, F. Gao, M. Yao, H. Zou, Joint information and jamming-beam forming for physical layer security with full duplex base station. IEEE Trans. Signal Process. **64**(12), 6391–6401 (2014)

Poorna Pravallika Sriram is a B.Tech graduate in the Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. She has 3 years of work experience on IoT (Internet of Things) as she had a heed interest toward it. She had published papers in national and international conferences on PCB fabrication, image processing, and IoT domains. She had worked as a research analyst at National Ilan University (NIU) on Narrowband Internet of Things (NB-IoT) as a TEEP (Taiwan Education Experience Program) student.

Hwang-Cheng Wang received the M.S. degree in Computer Science and Ph.D. degree in Electrical Engineering, both from the University of Southern California, Los Angeles, California, USA. He is currently a professor in the Department of Electronic Engineering, National Ilan University (NIU), Taiwan. He is in charge of the Embedded Systems and Mobile Computing Laboratory at NIU. Prior to joining NIU, he had served at the Data Communication Institute, Ministry of Transportation and Communications, as a senior technician. He was a visiting scholar at the Next Generation Internet Research Center, Beijing Jiaotong University and Information Science Institute, Academia Sinica. His research interests are in wireless networks, mobile communications, RFID, embedded systems, and innovative combination of information and communication technologies.

Hema Ganesh Jami is from Andhra Pradesh, India. He studied Bachelor of Technology in Electronics and Communication Engineering at Vel Tech University and started master's at National Tsing Hua University, Taiwan, in Communication Engineering. He got selected for research internship at National Ilan University by Taiwan Experience Education Program in January 2018. He has done his internship on Narrowband IoT, with the guidance given by Prof. H.C Wang.

Kathiravan Srinivasan received his B.E., in Electronics and Communication Engineering and M.E., in Communication Systems Engineering from Anna University, Chennai, India. He also received his Ph.D., in Information and Communication Engineering from Anna University Chennai, India. He is presently working as an associate professor in the School of Information Technology and Engineering at Vellore Institute of Technology (VIT), India. He was previously working as a faculty in the Department of Computer Science and Information Engineering and also as the deputy director – Office of International Affairs at National Ilan University, Taiwan. He has won the Best Conference Paper Award at 2018 IEEE International Conference on Applied System Innovation, Chiba, Tokyo, April 13–17, 2018. Further, he has also received the Best Service Award, Department of Computer Science and Information Engineering, National Ilan University, Taiwan. In 2017, he has won Best Paper Award at 2017 IEEE International Conference on Applied System Innovation, Sapporo, Japan, May 13–17, 2017, and Best Paper Award at International Conference on Communication, Management and Information Technology (ICCMIT 2017), Warsaw, Poland. In 2016, he received the Best Service Award as the Deputy Director at Office of International Affairs, National Ilan University. He is presently serving as the associate editor for IEEE Access and Editorial Board Member and reviewer for various SCI, SCIE, and Scopus indexed journals. He has played an active role in organizing several international conferences, seminars, and lectures. He has been a key note speaker in many international conferences and IEEE events.