Alma Mater Studiorum · Università di Bologna

Wireless Systems and Networks

5G
Architecture Overview and Security

Professore:
Luciano Bononi

Simone Bonfante
Matricola: 819606

Anno Accademico 2018-2019

Contents

Chapter 1

Introduction

1.1 5G Overview

The evolution of the cellular network generations is influenced primarily by continuous growth in wireless user devices, data usage, and the need for a better quality of experience (QoE). More than 50 billion connected devices are expected to utilize the cellular network services by the end of the year 2020. However, state-of-the-art solutions are not sufficient for the challenges mentioned above. In short, the increase of 3D ('D'evice, 'D'ata, and 'D'ata transfer rate) encourages the development of 5G networks.

Specifically, the fifth generation (5G) of the cellular networks will highlight and address the following three broad views: (i) user-centric (by providing 24x7 device connectivity, uninterrupted communication services, and a smooth consumer experience), (ii) service-provider-centric (by providing a connected intelligent transportation systems, road-side service units, sensors, and mission critical monitoring/tracking services), and (iii) network-operator-centric (by providing an energy-efficient, scalable, low-cost, uniformly-monitored, programmable, and secure communication infrastructure).

The revolutionary scope and the consequent advantages of the envisioned 5G networks, therefore, demand new architectures, methodologies, and technologies (fig 1.1), e.g., energy-efficient heterogeneous frameworks, cloud-based communication (software-defined networks (SDN) and network function virtualization (NFV)), full duplex radio, self-interference cancellation

(SIC), device-to-device (D2D) communications, machine-to-machine (M2M) communications, access protocols, cheap devices, cognitive networks (for accessing licensed, unlicensed, and shared frequency bands), dense-deployment, security-privacy protocols for communication and data transfer, backhaul connections, massive multiple-input and multiple-output (mMIMO), multi-radio access technology (RAT) architectures, and technologies for working on millimeter wave (mmWave) 30–300 GHz. Interestingly, the 5G networks will not be a mere enhancement of 4G networks in terms of additional capacity; they will encompass a system architecture visualization, conceptualization, and redesigning at every communication layer.

This report will describe the limitations of 4g and compares it with the

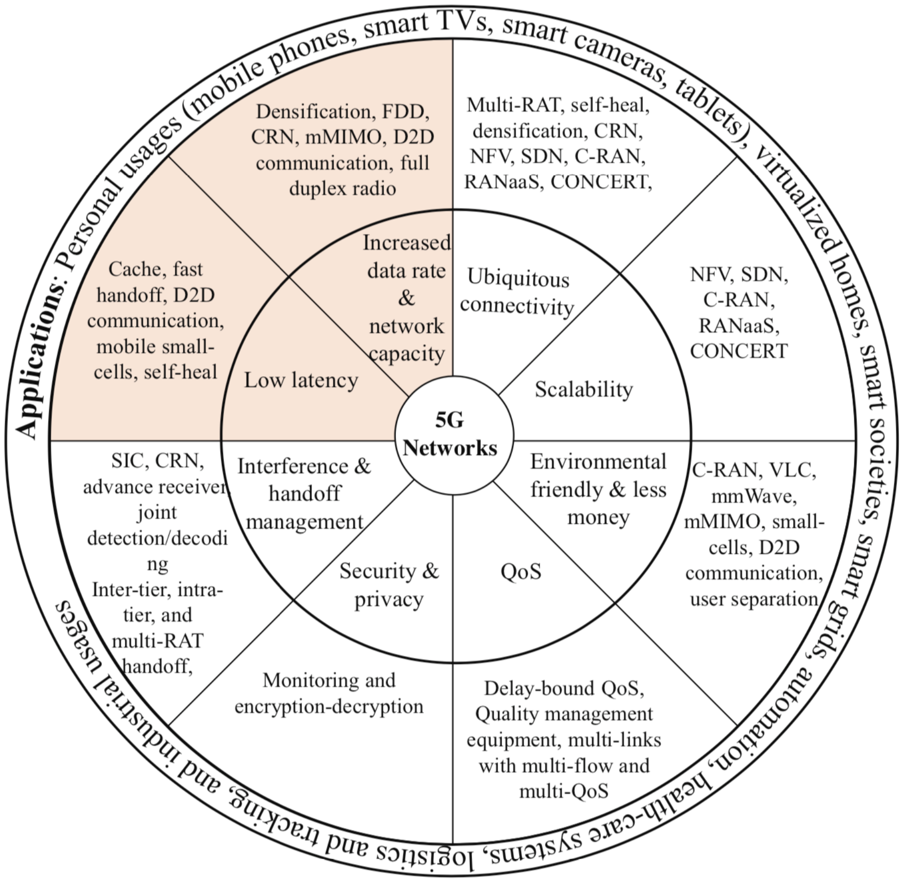

Applications: Personal usages (mobile phones, smart TVs, smart cameras, tablets), virtualized homes, smart societies, smart grids, automation, health-care systems, logistics and tracking, and industrial usages
Densification, FDD, CRN, mMIMO, D2D communication, full duplex radio
Multi-RAT, self-heal, densification, CRN, NFV, SDN, C-RAN, RANaaS, CONCERT,
Cache, fast handoff, D2D communication, mobile small-cells, self-heal
NFV, SDN, C-RAN, RANaaS, CONCERT
Increased data rate & network capacity
Ubiquitous connectivity
Low latency
Scalability
5G Networks
Interference & handoff management
Environmental friendly & less money
Security & privacy
QoS
SIC, CRN, advance receiver joint detection/decoding Inter-tier, intra-tier, and multi-RAT handoff,
C-RAN, VLC, mmWave, mMIMO, small-cells, D2D communication, user separation
Monitoring and encryption-decryption
Delay-bound QoS, Quality management equipment, multi-links with multi-flow and multi-QoS

Figure 1.1: 5G applications

security of 5G, possible architecture (s) of the 5G network in Chapter 3 and then talk about security in 5G networks (Chapter 4). Finally i'll provide a conclusion describing possible applications in Chapter 5.

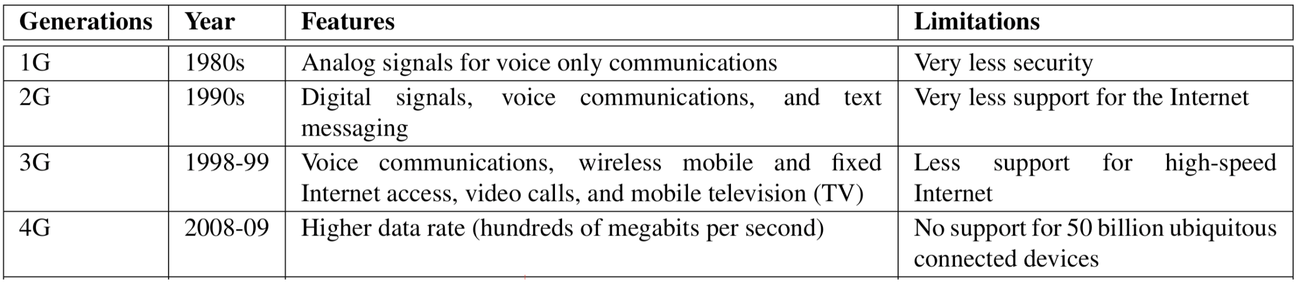
Chapter 2

4g vs 5G

The mobile technology has evolved a lot in the recent years. The handheld devices were initially in the form of pagers and now they have evolved to become devices with embedded features for social networking, photography and what not. All this is possible due to the advances in mobile phone generations [10].

These generations started back with 0G. The 0G did not have any support for wireless mobile technology. It was succeeded by 1G which was officially called the first generation of mobile telecommunications. It basically used analog radio signals. It was gradually replaced by 2G technology. The major difference between 1G and 2G was the presence of digital networks. SMS and MMS services were introduced in this generation. The third generation was called as 3G. It had numerous advantages over their 2G predecessors. These advantages were in the form of multimedia and internet applications with a much larger speed of connectivity. The 4G has support for very high speed internet connectivity as well as for cloud computing.

The world is now considering the vision for 5G which would solve a majority of Smartphone issues and would also be much more secure and high in performance than its predecessors (see fig. 2.1).



Generations	Year	Features	Limitations
1G	1980s	Analog signals for voice only communications	Very less security
2G	1990s	Digital signals, voice communications, and text messaging	Very less support for the Internet
3G	1998-99	Voice communications, wireless mobile and fixed Internet access, video calls, and mobile television (TV)	Less support for high-speed Internet
4G	2008-09	Higher data rate (hundreds of megabits per second)	No support for 50 billion ubiquitous connected devices

Figure 2.1: from 1G to 5G

2.1 Security issues in 4G

If we consider the MAC layer of the network architecture of 4G systems then we will observe that Wi-max is highly prone to the following attacks [8]:

- **DOS attacks:** These attacks make sure that a particular network resource is not available to the end user.
- **Replay attacks:** They involve a malicious user that spies the message transmission between two legitimate users and extracts the shared information between them. He then uses that piece of information to show that he is the legitimate sender / receiver.
- **Eavesdropping:** It refers to the activity which ensures that the communication between two authentic users is intercepted by any malicious user / third party.

Security Issues of LTE

Considering the MAC layer of the network architecture of 4G systems, LTE suffers from major security hurdles. These include unauthenticated user making use of the hand held device, faulty geographical location tracking, denial of service attacks and data modification. In a wireless scenario, data modification can occur in the form of message modification. Malicious user tries to change the packets header of data and even tries to target the message to other destination. The message can also be modified. At the physical level, LTE is highly prone to scrambling attacks. These attacks are implemented when the attacker has adequate knowledge about the time slots and particular frames which are to be infected.

Information security in 5G networks

The 5G mobile technology is still evolving and hence there is a lot of scope for incorporating the security factors in its framework. The drivers have only been concentrating on the latency and throughput factors but we can modify them to provide better support for user's authentication. These drivers can be grouped into categories according to their use and then their privacy policies can be re defined. Since cloud computing forms a part of the 5G framework hence its privacy will also be maintained [7].
The basic point of difference between the security of 4G and 5G networks is the establishment of new trust models. In the earlier generations, all devices were able to establish 'Trust' if they belonged to a particular organization. But under 5G, this won't be the case. This is because all the devices under the same managing organization are not equal. The devices can be termed as "trustworthy" only if they are free from all sorts of malicious associations.

2.2 Limitation of 4G

The 4G networks are not substantial enough to support massively connected devices with low latency and significant spectral efficiency, which will be crucial in the future communication and computing [5].

- **No support for bursty data traffic:** only one type of signaling/control mechanism is designed for all types of the traffic in the current networks, creating high overhead for bursty traffic.

- **Inefficient utilization of processing capabilities of a base-station:** the almost idle BSs consume an identical amount of power as over-subscribed BSs; hence, the overall cost of the network increases.

- **Co-channel interference:** Uplink channel and Downlink channel creates interference mostly if they have the same frequency.
- **No support for heterogeneous wireless networks:** The HetNets are already standardized in 4G; however, the basic architecture was not intended to support them.
- **No separation of indoor and outdoor users:** the communication between an indoor UE and an outside BS is not efficient in terms of data transfer rate, spectral efficiency, and energy-efficiency, due to the attenuation of signals passing through walls.
- **Latency:** $>$ 100 ms, No 0-latency.

2.3 Desideratum of 5G Networks

A growing number of UEs and the corresponding surge in the bandwidth requirement for the huge amount of data transmission certainly necessitate the novel enhancement to the current technology [8].

- **Dramatic upsurge in device scalability:** A rapid growth of smartphones, gaming consoles, high-resolution TVs, cameras, home appliances, laptops, connected transportation systems, video surveillance systems, robots, sensors, and wearable devices (watches and glasses) is expected to continue exponentially in the near future.
- **Massive data streaming and high data rate:** vast growth in a number of wireless devices equals higher amount of data trading. 2020 $>$ 100 times respect of 2014.
- **Spectrum utilization:** The two different channels (one for a UL and another for a DL) seem redundant from the point of view of the spectrum utilization. Furthermore, the spectrum utilization and efficiency have already been stretched to the maximum. It definitely requires

spectrum broadening (above 3 GHz) along with novel spectrum utilization techniques.

- **Ubiquitous connectivity:** 5G networks are envisioned for seamless connectivity of UEs over HetNets.
- **Zero latency:** 5G networks are envisioned to realize real-time and delay-bound services with the optimal QoS and QoE experiences.

Chapter 3

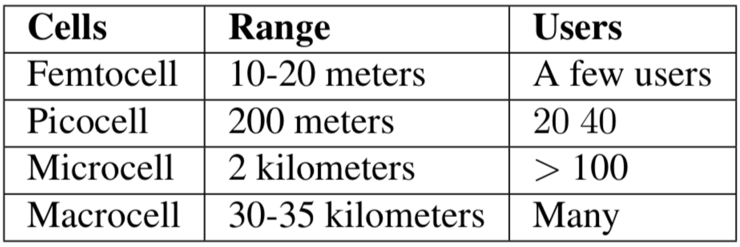
Architecture 5G

In this section, i will explicit the existing architectures for 5G networks, namely multi-tier, Massive MIMO, CRN-based, D2D communication based, and the cloud-based architectures. These proposed 5G architectures will be explained in the light of relevant advantages, disadvantages, and the challenges that are yet to be resolved [8].

3.1 Two-tier Architectures

Several two-tier architectures have been proposed for 5G networks, where a MBS stays in the top-tier and SBSs work under the supervision of the MBS in the lower tier.
A macrocell covers all the small-cells of different types (fig. 3.1).

Both the tiers share an identical frequency band and small-cell enhances the coverage and services of a macrocell.



Cells	Range	Users
Femtocell	10-20 meters	A few users
Picocell	200 meters	20 40
Microcell	2 kilometers	> 100
Macrocell	30-35 kilometers	Many

Figure 3.1: Classification of the cells.

In addition, D2D communication and CRN-based communication enhance a 2-tier architecture to a multi-tier architecture (fig. 3.2).

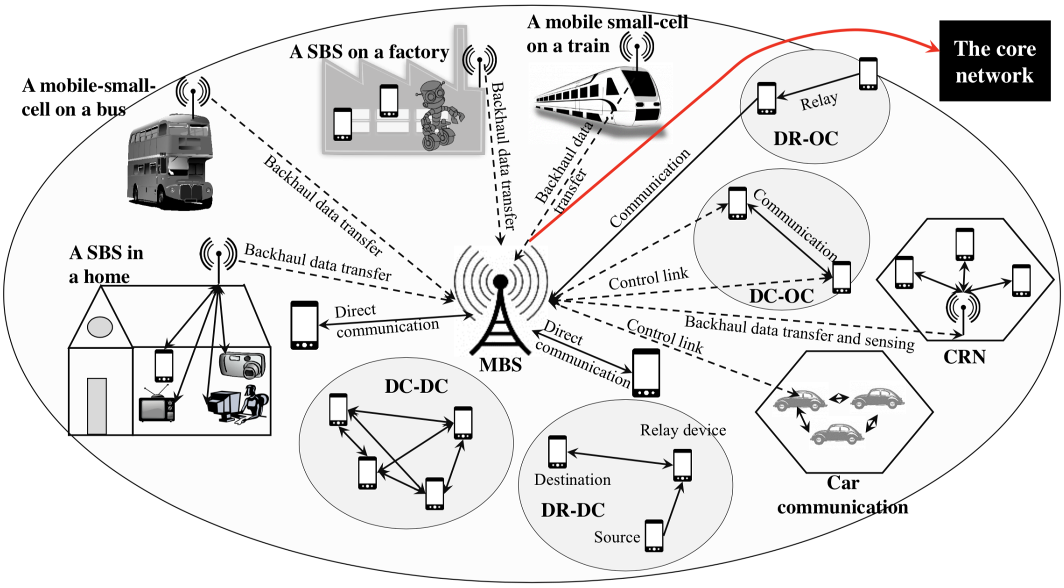


Figure 3.2: A multi-tier architecture for 5G networks with small-cells, mobile small-cells, and D2D- and CRN-based communications.

There's a tradeoff between the transmission power of a macrocell and the coverage area of small-cells: on the one hand, if the transmission power of a macrocell is high, then many adjacent UEs to a small-cell may find themselves in the service area of the macrocell, and hence, it will decrease the coverage area of that small-cell. On the other hand, if the transmission power of a macrocell is low, then the coverage area of the small-cell will increase.

Advantage

- **High data rate and efficient spectrum use**: the small physical separation between a SBS and UEs leads to a higher data rate and a better coverage. Also, the spectrum efficiency increases due to fewer UEs in direct communication with a MBS

- **Energy and Money saving**: the use of small-cells reduces the energy consumption of the network and of UEs, and also it is more economical to
- **Less congestion to a MBS**
- **Easy handoff**: handoff time overheads reduced since a mobile small-cell is capable to do the handoff on behalf of all related UEs

Disadvantage

- **Cost and operational reliability**
- **Frequent authentication**

3.2 Massive MIMO

One of the goals of 5G is to allow good communication between inside and outside. This will be supported with the help of **mMIMO**: The Massive MIMO system uses antenna arrays containing a few hundred antennas that are simultaneously at the same time, frequency slots that serve many tens of user terminals.

Remark: most wireless users remain inside for about 80% of the time and outside for about 20% of the time. To date, so that internal users can communicate with the external base station, the signals will have to pass through the interior walls and this will result in a very high loss of penetration. The improvement occurs with the use of mMIMO.

External mobile users are usually equipped with a number of antenna units, but with cooperation it is possible to build a large array of virtual antennas, which together with the base station antenna arrays form massive virtual MIMO links. Secondly, large antenna arrays will be installed in each building to communicate with external base stations. These are connected via cables to wireless access points to communicate with users inside. This will increase performance, use of spectrum, energy savings but will significantly increase costs.

Since the 5G cellular architecture is heterogeneous, it must therefore include macrocells, microcells, small cells and relays. A small mobile phone concept is an integral part of the 5G wireless cellular network:
Small mobile cells are positioned inside moving cars to communicate with users inside the car, while the huge MIMO unit consisting of large antenna arrays is positioned outside the car to communicate with the base station external.

Advantages:

- **Excellent spectral efficiency**, obtained by spatial multiplexing of many terminals in the same time-frequency resource.
- **Superior energy efficiency**, thanks to the antenna arrays that allow a reduction in radiated power.
- **Array gain**

Beamforming

Beamforming is a subset of mMIMO. In general, beamforming uses multiple antennas to control the direction of a wavefront by appropriately weighing the amplitude and phase of the individual antenna signals in a series of multiple antennas.
Beamforming is the application of multiple radiating elements that transmit the same signal at an identical wavelength and phase, which combine to create a single antenna with a longer and more targeted flow that is formed by reinforcing the waves in a specific direction.

Full Duplex

For a long duration of the communication period, in the design of the wireless system it is assumed that the radios must operate in half duplex mode. It means that it will not be transmitted and received simultaneously on the same channel.

But the realization of full duplex radio has many implications. Cellular networks will have to reduce their spectrum needs in half, as only one channel is used to achieve the same performance. Separate channels must be used, both for uplink and downlink, of equal width to allow the radios to realize full duplex.

3.3 Cognitive Radio Network

A cognitive radio network (CRN) is a collection of cognitive radio nodes (or processors), called secondary users (SUs) that exploit the existing spectrum opportunistically. A CRN in 5G networks is used for designing multi-tier architectures, removing interference among cells, and minimizing energy consumption in the network.

A CRN creates a 2-tier architecture and it is assumed that either a MBS or a SBS has cognitive properties for working on different channels. Two types of architectures: *non-cooperative* and *cooperative*.

- The non-cooperative CRN establishes a multi-RATs system (multi Radio Access Technologies) having two separate radio interfaces that operate at the licensed and temporary unoccupied channels by PUs. The SUs work only on cognitive channels and form a CRN, which overlays on the existing licensed cellular network.
- The cooperative CRN uses only a licensed channel, where SUs access the channel in an opportunistic fashion when the PU of the channel is absent.

Interference Management using CRNs

A cognitive technique integrated at a SBS allows to avoid inter-tier interference. It consists of three components: (i) a cognitive module which senses the environment and collects information, (ii) a cognitive engine which analyzes and stores the collected information for estimating available resources and (iii) a self-configuration module, which uses the stored information for optimizing several parameters. Note that a CRN can be used to support D2D communication and mitigate interferences caused by D2D communication.

Advantages

- **Minimizing interference:** by implementing a CRN at small-cells, cognitive small-cells can avoid interference very efficiently by not selecting identical channels as the channels of neighboring small-cells.
- **Increase network capacity:** the spectrum holes can be exploited for supporting a higher data transfer rate and enhancing bandwidth utilization.

3.4 Device-to-Device Communication

Device-to-Device (D2D) communication allows close proximity UEs to communicate with each other on a licensed cellular bandwidth without involving a MBS.

Challenges in D2D communication

Interference
UEs involved in D2D communication, D-UEs, face (or create) interference from (or to) other UEs, or from (or to) a BS, based on the selection of a DL or UL channel, respectively. A simple solution may exist by implementing CRNs in D2D communication. Any mechanism of CRNs can be implemented in D2D communication for interference removal.
Resource allocation
When UEs involved in D2D communication, it is required to allocate a sufficient amount of resources, particularly bandwidth and channels and must be carried-out to avoid interference from D-UEs.
Delay-sensitive processing

Audio, video streaming, and online gaming, which are natural in close proximity UEs, require real-time and delay-sensitive processing. Hence, it is required to consider delay-sensitive and real-time processing in D2D communication.

D2D Communication types

- **Device relaying with operator controlled link establishment (DR-OC):** A UE at the edge of a cell or in a poor coverage area can communicate with a MBS by relaying its information via other UEs, which are within the stronger coverage area and not at the edge (fig. 3.2)
- **Direct D2D communication with operator controlled link establishment (DC-OC):** Source and destination UEs communicate directly with each other without involving a MBS, but they are assisted by the MBS for link establishment. (fig. 3.2)
- **Device relaying with device controlled link establishment (DR-DC):** Source and destination UEs communicate through a relay without involving a MBS, and they are also responsible for link establishment. (fig. 3.2)
- **Direct D2D communication with device controlled link establishment (DC-DC):** Source and destination UEs communicate directly with each other without involving a MBS, and they are also responsible for link establishment. (fig. 3.2)

Note that DR-OC and DC-OC involve a MBS for resource allocation and call setup, and hence, prevent interference among devices to some extent.

Advantages

D2D communication results in link reliability among D-UEs, a higher data rate to D-UEs, instant communication, an easy way for peer-to-peer file sharing, local voice services, local video streaming, local online gaming, an improved spectral efficiency, decreased power consumption of D-UEs, and the traffic offload from a MBS.

3.5 Cloud-based radio access network

Cloud computing infrastructure provides on-demand, easy, and scalable access to a shared pool of configurable resources, without worrying about the management of resources. The inclusion of the cloud in the mobile cellular communication can provide its benefits to the communication system.
Il primo C-RAN è fornito da *China Mobile Research Institute* [4]: the basic idea is to execute the functionality of a MBS into a *control layer* and a *data layer* (fig 3.3). A C-RAN provides a dynamic service allocation scheme for scaling the network without installing anything. A MBS has two main components, as: (i) a baseband unit (BBU, for implementing baseband processing using baseband processors), and (ii) a remote radio head (RRH, for performing radio functions). In most of the C-RANs, BBUs are placed in the cloud and RRHs stay in MBSs. Thus, a C-RAN provides an easily scalable and flexible architecture.

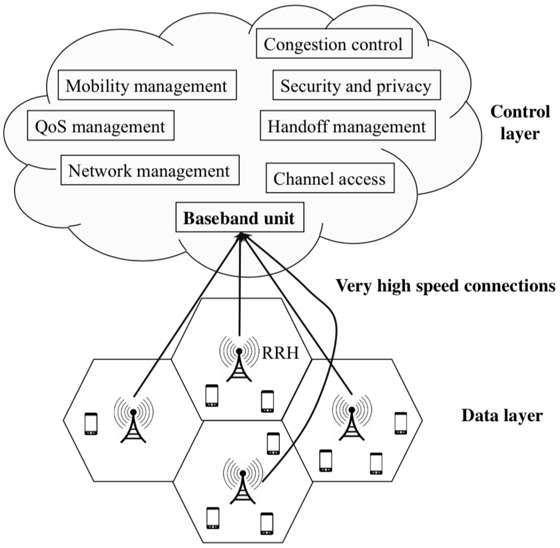


Figure 3.3: A basic cloud-based architecture for 5G networks.

Certainly a problem to be faced is the real time data transfer, *reliability* (hardware and software) and *security*.
The authors [4] provide two C-RAN architectures: (i) *full-centralized* C-RAN where BBU is located in the cloud while RRH is only located in the MBS, and (ii) *partially-centralized* C-RAN where RRH and some of the functionalities of a BBU are located in the MBS while all remaining functions of BBU and higher level functionalities of MBS are located in the cloud.
This architecture uses only two layers, control layer which performs baseband processing and resource management (application delivery, QoS, real-time communication, etc..) and data layer that contains heterogeneous physical resources and performs signal processing tasks (e.g., channel decoding, demultiplexing, etc..) The same architecture otherwise has some disadvantages, as: continuous exchange of raw baseband samples between the data and the control layers, and the control layer is usually far away from the data layer resulting in a processing delay. Liu et al. [6] proposed convergence of cloud and cellular systems (CONCERT). In this architecture, one more layer, called a software-defined service layer, is introduced at the top of the control layer. Software-defined services layer works as a virtual BS and provides services to the data layer (e.g., application delivery, QoS, real-time communication etc..).

Advantages

- **An easy network management:** C-RANs facilitate on-demand installation of virtual resources and execute cloud-based resources that dynamically manage interference, traffic, load balance, mobility, and do coordinated signal processing.
- **Reduce cost:** the deployment of C-RANs involves less cost, while it provides usual services like a MBS
- **Save energy:** C-RANs allow UEs and MBSs to offload their energy-consuming tasks to a nearby cloud, which saves energy of UEs and MBSs.

Chapter 4

5G Security

Due to the broadcast nature of the wireless medium, wireless information transmission is vulnerable to various malicious threats. In this section, we discuss four types of attacks, i.e., eavesdropping and traffic analysis, jamming, DoS and DDoS, and MITM, in 5G wireless networks, security services and the state of the art solutions.
Fig4.1 illustrates all four attacks, each of which is individually discussed in the following three aspects, type of the attack (passive or active), security services provided to fight against this attack, and the corresponding methods applied to avoid or prevent this attack. I focus on security attacks at the PHY layer and MAC layer, where the key differences on security between wireless and wire-line networks occur [3].

- EAVESDROPPING AND TRAFFIC ANALYSIS
- JAMMING
- DoS AND DDoS
- MITM

4.1 Security Services

The new architecture, new technologies, and use cases in 5G wireless networks bring in new features and requirements of security services [2].

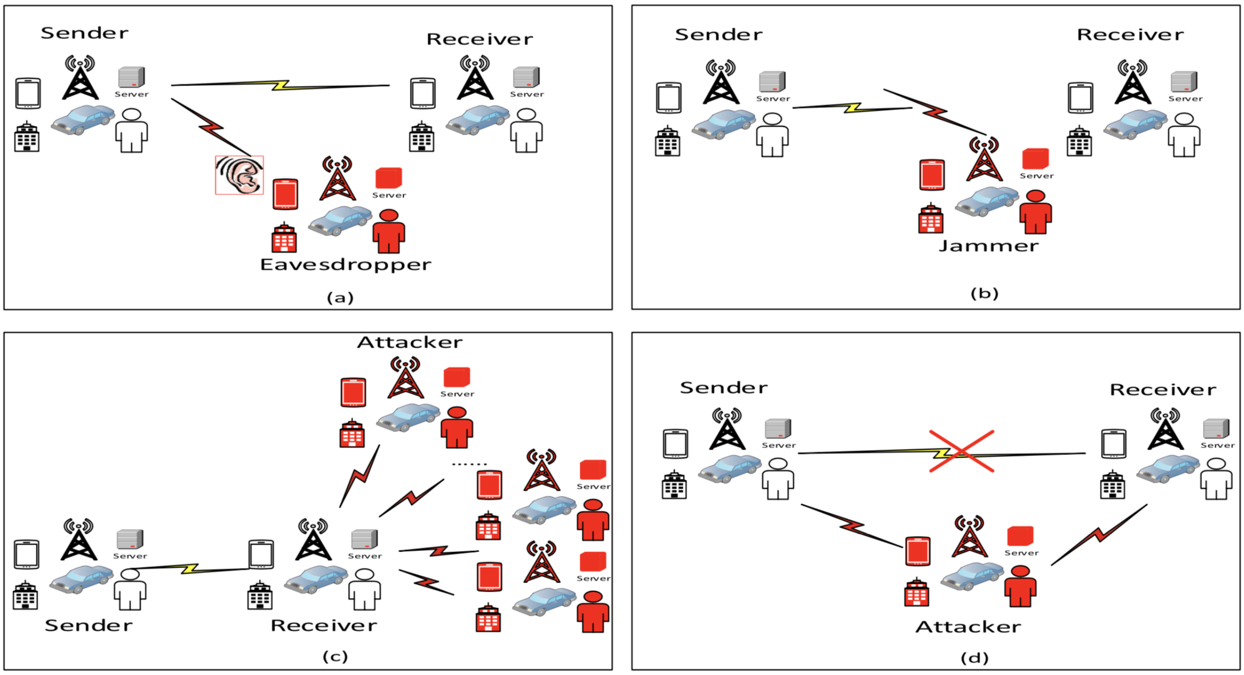


Figure 4.1: Four types of attacks.

4.1.1 Authentication

There are two kinds of authentications, namely, entity authentication and message authentication. Entity authentication is used to ensure the communicating entity is the one that it claims to be. **In the legacy cellular networks, mutual authentication between user equipment (UE) and mobility management entity (MME) is implemented before the two parties communicating to each other**.
The authentication and key agreement (AKA) in 4G LTE cellular networks is symmetric-key based. However, 5G requires authentication not only between UE and MME but also between other third parties such as service providers. Authentication in 5G is expected to be much faster than ever, moreover, the multi-tier architecture of the 5G may encounter very frequent handovers and authentications between different tiers in 5G.

4.1.2 Confidentiality

Confidentiality consists of two aspects, *data confidentiality* and *privacy*. Data confidentiality protects data transmission from passive attacks by limiting the data access to intended users only and preventing the access from or disclosure to unauthorized users. Privacy prevents controlling and influencing the information related to legitimate users, for example, privacy protects traffic flows from any analysis of an attacker.

Data encryption has been widely used to secure the data confidentiality by preventing unauthorized users from extracting any useful information from the broadcast information.

4.1.3 Availability

Availability is defined as the degree to which a service is accessible and usable to any legitimate users whenever and wherever it is requested. Availability evaluates how robust the system is when facing various attacks and it is a key performance metric in 5G. Typically availability attack: DoS, Jamming. For the availability at PHY, DSSS and FHSS are two classical PLS solutions: A pseudo noise spreading code is multiplied with the spectrum of the original data signal in DSSS. Without knowledge on the pseudo noise spreading code, a jammer needs a much higher power to disrupt the legitimate transmission. For FHSS, a signal is transmitted by rapidly switching among many frequency channels using a pseudorandom sequence generated by a key shared between transmitter and receiver.

4.1.4 Integrity

Although message authentication provides the corroboration of the source of the message, there is no protection provided against the duplication or modification of the message. The integrity of data is one of the key security requirements in certain applications.

Integrity services can be provided by using mutual authentication, which can generate an integrity key.

4.2 Solutions in 5G wireless security

4.2.1 Authentication

Authentication is one of the most important security services in 5G wireless networks. Following the authentication, a cipher key and an integrity key are generated to ensure both data confidentiality and integrity between the mobile station and the base station.

SDN

Due to the low latency requirement of 5G networks, authentication schemes are required to be more efficient in 5G than ever before. One way to exploit the advantages of SDN is to use weighed secure-context-information (SCI) transfer as a non-cryptographic security technique to improve authentication efficiency during high frequent handovers in a HetNet: it is based on the user-inherent physical layer attributes, hence hard to compromise. Many small cells scattered everywhere. The reduced cell size has prompted frequent handovers that could introduce more latency. The SDN controller

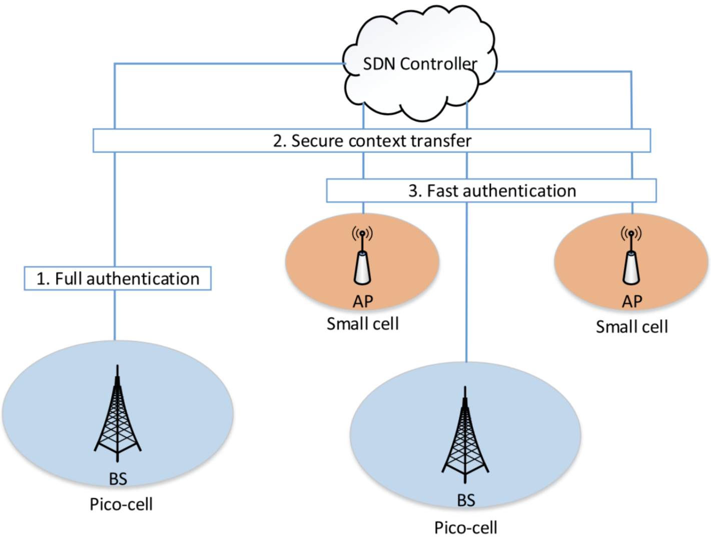


Figure 4.2: SDN scheme authentication.

implements an authentication model to monitor and predict the user location in order to prepare the relevant cells before the user arrival. Physical layer attributes are used to provide unique fingerprints of the user and to simplify authentication procedure.

However, relying completely on a physical layer attribute is not considered a reliable solution because the selected feature may not have a sufficient dynamic range for accurate differentiation. For applications such as banking or e-commerce it is necessary to consider more than one characteristic of the physical layer as Secure-context-information (SCI) and verify the identity of the device claimed in multiple aspects. Generally there are three types of fingerprints for mobile UEs, that is, software-based, hardware-based and channel / location-based features.

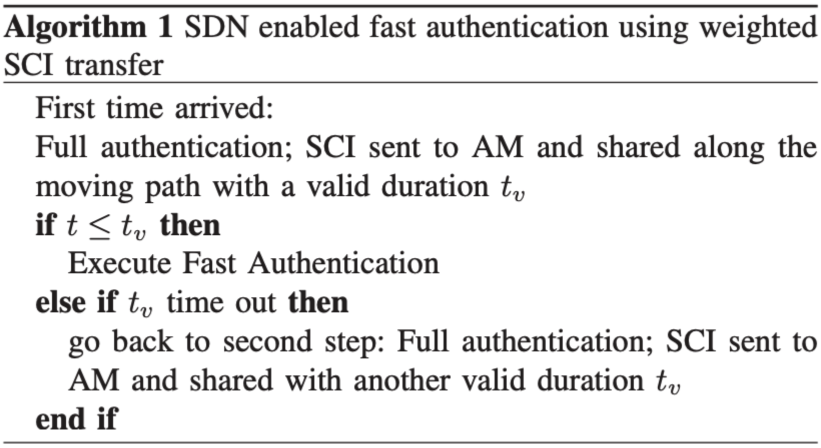
Combined SCI is provided for secure authentication and low latency. With SDN, the control logic is removed from the underlying infrastructure of a controller in the control layer.

The authentication module (AM) is implemented in the SDN controller to monitor and predict the users' location and prepare relevant cells for uninterrupted authentication The proposed fast authentication protocol includes full authentication and weighted SCI transfer based fast authentication. After the first full authentication in one cell, it can be readily applied in other cells with MAC address verification, which only needs local processing (fig 4.3).

The SDN enabled fast authentication has a better delay performance owing to SDN flexibility and programmability in 5G networks.

CRC (Cyclic redundancy check)

CRC can detect any double-bit errors in a single message. The message authentication algorithm outputs an authentication tag based on a secret key and the message. It is assumed that the adversary has the family of hash functions but not the particular polynomial *g(x)* and the pad *s* that are used to generate the authentication tag. The generator polynomial is changed periodically at the beginning of each session and pad s is changed



Algorithm 1 SDN enabled fast authentication using weighted SCI transfer

```
First time arrived:
Full authentication; SCI sent to AM and shared along the moving path with a valid duration $t_v$
if $t \leq t_v$ then
  Execute Fast Authentication
else if $t_v$ time out then
  go back to second step: Full authentication; SCI sent to AM and shared with another valid duration $t_v$
end if
```

Figure 4.3: SDN enabled fast authentication using weighted SCI transfer

for every message

4.2.2 Availability

Availability is a key metric to ensure the ultra-reliable communications in 5G. However a jammer can degrade the performance of the mobile users. To avoid DoS attacks can be applied a frequency hopping scheme, but it requires that users have access to multiple channels and it may not work efficiently for dynamic spectrum access users due to the high switching rate and high probability of jamming.

To reduce the switching rate and probability of jamming can be applied a pseudorandom time hopping anti-jamming scheme [1]. However, a pre-shared key is required for the time hopping anti-jamming technique. Considering the limited computational capabilities at certain nodes a fusion

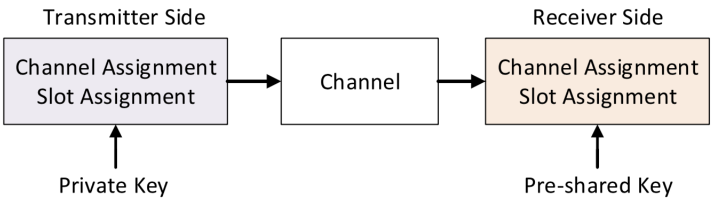


Figure 4.4: Pseudorandom timehopping.

center can be used to defend these nodes from a malicious radio jamming attack. Fig. 4.5 shows the resource allocation model between fusion center and the malicious jammer. The jammer aims to jeopardize the network without getting detected by distributing its power among the nodes intelligently. On the other hand, the fusion center as a defender aims to detect such an attack by a decentralized detection scheme at a certain set of nodes. The fusion center can allocate more bits to these nodes for reporting the measured interference. A hierarchic degree is assigned to each node based on its betweenness centrality. Once the attack is detected, the fusion center will instruct the target node to increase its transmit power to maintain a proper SINR for normal communications.

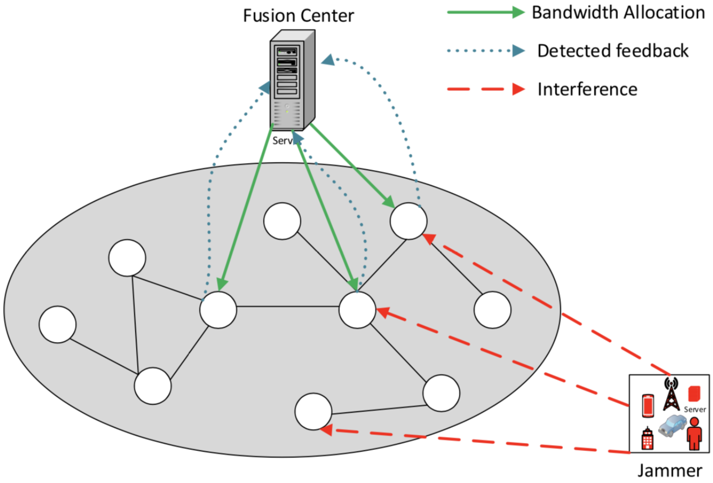


Figure 4.5: Resource allocation model.

4.2.3 Data Confidentiality

Data confidentiality service is commonly required to tackle eavesdropping attacks. The general system model with eavesdropping attacks is shown in Fig.4.6. In this subsection, i discuss data confidentiality based on power control, relay, artificial noise, signal processing, and cryptographic methods.

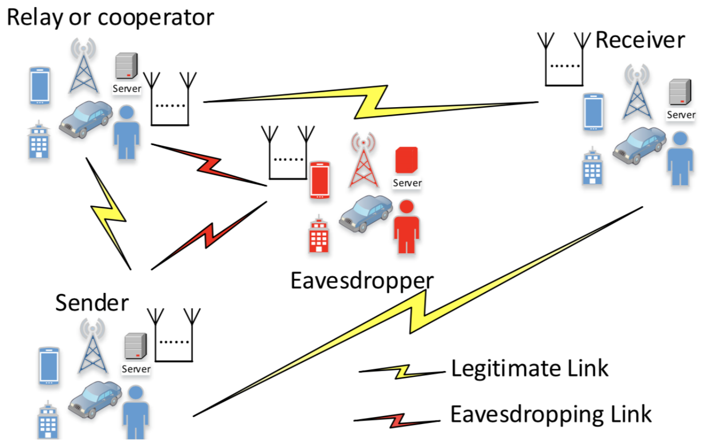


Figure 4.6: A general system model with eavesdropping attacks.

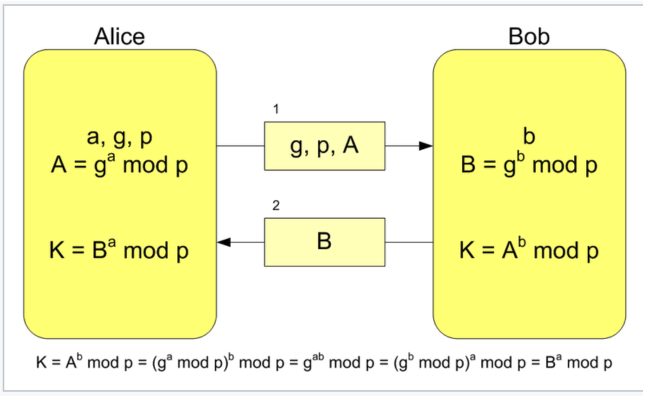
- **Power control:**
  Power control for security aims to control the transmit power to ensure that the eavesdropper can not recover the signal. Based on the most simple eavesdropping attack model with a single eavesdropper armed with a single antenna, is proposed a distributed algorithm to secure D2D communications in 5G, which allows two legitimate senders to select whether to cooperate or not and to adapt their optimal power allocation based on the selected cooperation framework.
  A shared bi-directional link is applied between Sender and Relay.
  All the advantages are lost by increasing the distance between transmitter and receiver.

- **Artificial noise:**
  Artificial noise can be introduced to secure the intended signal transmission.
  Assuming the sender is armed with multiple antennas an artificial noise transmission strategy is proposed to secure the transmission against an eavesdropper with a single antenna in millimeter wave systems. In this approach, the legitimate receiver generates artificial noise (AN) to impair the intruder's channel. This method is robust because it does not need the feedback of channel state information (CSI) to the transmitter.

- **Signal Processing:**
  Besides the three methods above to provide data confidentiality, is proposed an original symbol phase rotated (OSPR) secure transmission scheme to defend against eavesdroppers armed with unlimited number of antennas in a single cell. Perfect CSI and perfect channel estimation are assumed. The BS randomly rotates the phase of original symbols before they are sent to legitimate user terminals. The eavesdropper can not intercept signals, only the legitimate users are able to infer the correct phase rotations recover the original symbols.
  Massive MIMO can be applied to HetNets to secure the data confidentiality in the presence of multiple eavesdroppers for improving significantly the secrecy performance.

4.2.4 Key Management

Key management is the procedure or technique that supports the establishment and maintenance of keying relationships between authorized parties. The common data can be public or secret keys, initialization values, and other non-secret parameters. To provide flexible security, in [9], are proposed three novel key exchange protocols, which have different levels of computational time, computational complexity, and security, for D2D communications based on the Diffie-Hellman (DH) scheme (see fig. 4.7).

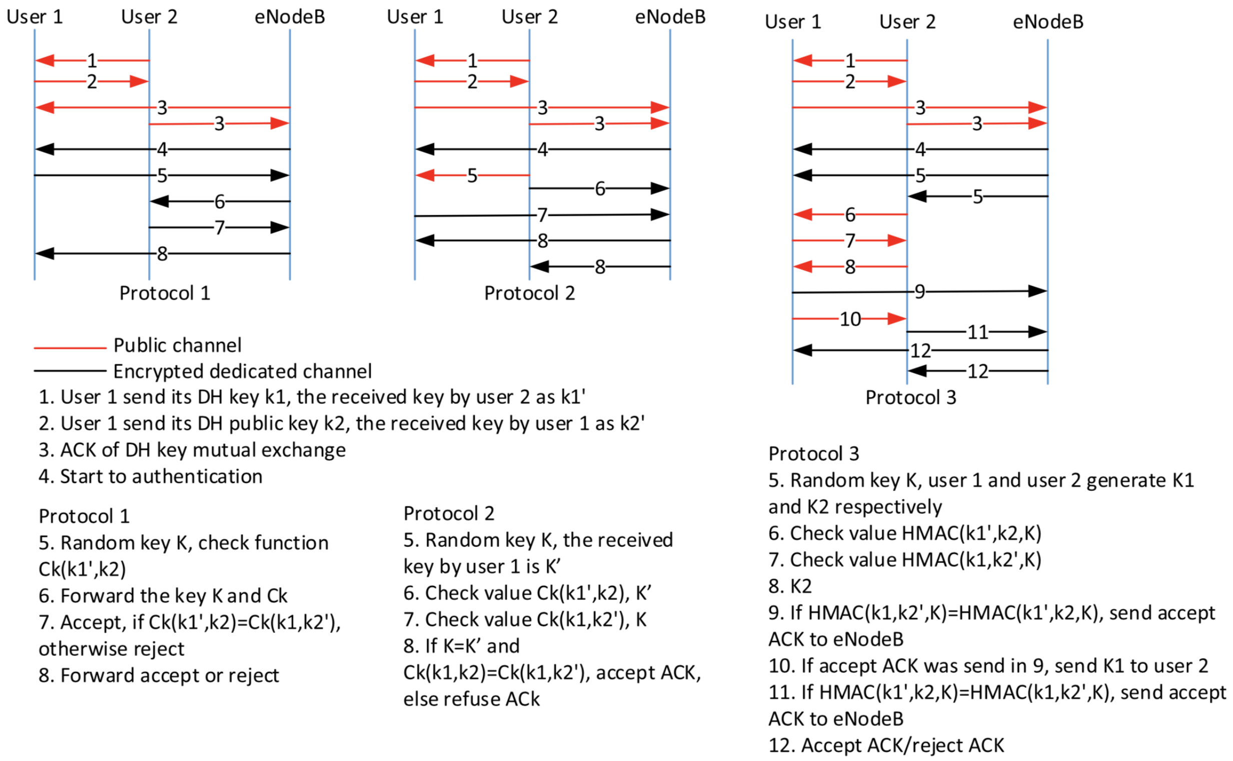


Alice
Bob
a, g, p
$A = g^a \bmod p$
$K = B^a \bmod p$
1
g, p, A
2
B
b
$B = g^b \bmod p$
$K = A^b \bmod p$
$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Figure 4.7: Diffie-Hellman scheme.

A summary image of the key exchange schemes is shown in fig. 4.8. Further, through numerical results, is demonstrated that the proposed protocols have low computational time and low communication overhead in comparison with existing key exchange protocols for D2D communication. The proposed protocols address the typical vulnerability of D2D scenarios, i.e., the man-in-the-middle (MITM) attack.

For all scenarios (i.e. *Traffic Offload, Social Networking*, etc..) there are two kinds of channels used in key exchange process: Public Channel, insecure channel through which the public keys are sent and received by both devices and eNodeB, and *Encrypted Dedicated Channel*, the same as P.C. but with data encryption.



1. User 1 send its DH key k1, the received key by user 2 as k1'
2. User 1 send its DH public key k2, the received key by user 1 as k2'
3. ACK of DH key mutual exchange
4. Start to authentication

Protocol 1
5. Random key K, check function Ck(k1',k2)
6. Forward the key K and Ck
7. Accept, if Ck(k1',k2)=Ck(k1,k2'), otherwise reject
8. Forward accept or reject

Protocol 2
5. Random key K, the received key by user 1 is K’
6. Check value Ck(k1',k2), K’
7. Check value Ck(k1,k2'), K
8. If K=K’ and Ck(k1,k2)=Ck(k1,k2'), accept ACK, else refuse ACk

Protocol 3
5. Random key K, user 1 and user 2 generate K1 and K2 respectively
6. Check value HMAC(k1',k2,K)
7. Check value HMAC(k1,k2',K)
8. K2
9. If HMAC(k1,k2',K)=HMAC(k1',k2,K), send accept ACK to eNodeB
10. If accept ACK was send in 9, send K1 to user 2
11. If HMAC(k1',k2,K)=HMAC(k1,k2',K), send accept ACK to eNodeB
12. Accept ACK/reject ACK

Figure 4.8: Summary of the key exchange schema.

Protocols

1. **Protocol 1:**
   The process is simple. Two devices, UE-1 and UE-2, exchange their DH public keys (g^b and g^a). Then an acknowledgement (ACK) is sent by both the devices to the eNodeB about the mutual exchange.
   eNodeB responds to both either and choose one of them to start the auth, i.e. UE-2; hence UE-2 generates a random Key K used for generating the check function: $c_k(g^{\hat{}a}||g^b)$. Both the key and check value are sent to the eNodeB. UE-1, once received, computes the value of $c_k(g^a||g^{\hat{}b})$ and compares it with the value received. Then sends ACK Accept(**D2D established**)/Reject(**D2D NOT established**) to eNodeB, and it sends this to UE-2 (see fig. 4.9).

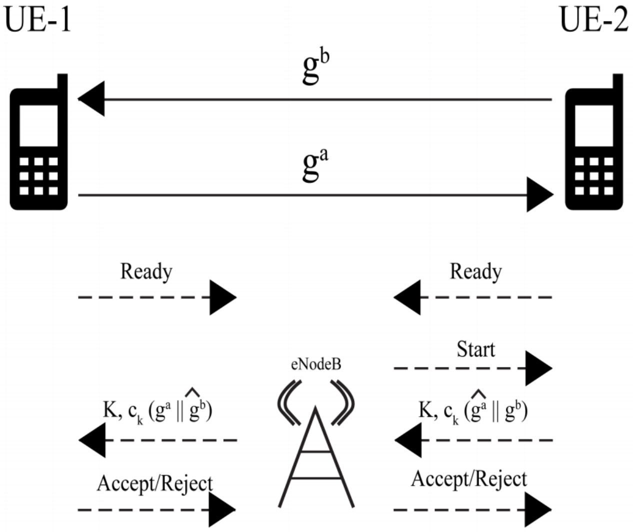


Figure 4.9: Key exchange - protcol 1.

2. **Protocol 2:**
   In this protocol eNodeB has an added comparison function for more security at the coded of slightly more computational complexity. The initial process is equal to Protocol 1 described above.
   UE-2 generates a random Key K (16-20 bits) and sends it through the

public channel. This key can be accessed by anyone.
The UE-1 computes the check value using the check function $c_k(g^a \, || \, g^{\wedge b})$ and the received key K^ and sends both the values to the associated eNodeB. UE-2 does the same.
eNodeB compares all and send ACK Accept(**D2D established**)/Reject(**D2D NOT established**8) to UE-1 and UE-2 (see fig. 4.10).

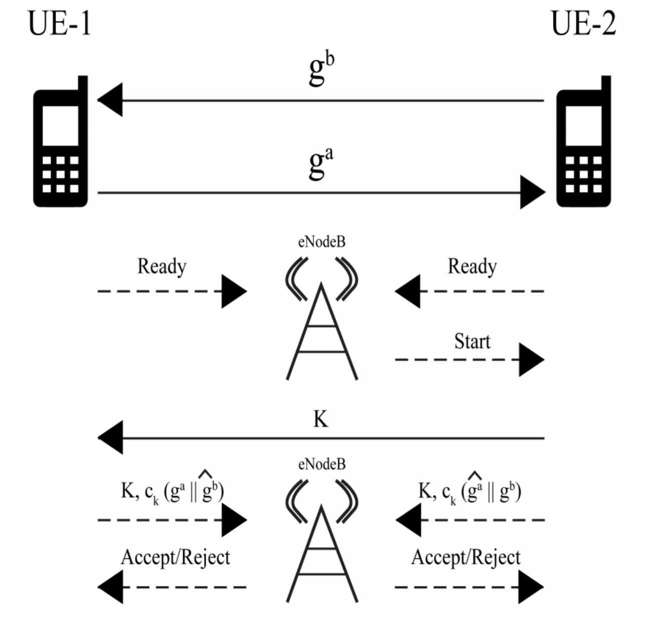


Figure 4.10: Key exchange - protcol 2.

3. **Protocol 3:**
   In this protocol eNodeB generates a random key K (16-20 bits) and sends it to both UE-1 and UE-2 through the encrypted channel. This key should not be exploited by the adversary. Then UE-1 and UE-2 generate K_1 and K_2 and calculate HMAC (*HMAC has a stronger property of being a pseudo-random function (PRF)*) values of (g^a $||g^b$ $||$K) and send it to each other on the public channel. UE-2 recalculates the HMAC value and compares it with the value that it received. If both match then it sends the key K2 to UE-1 along with an accept ACK to the eNodeB.

UE-1 does the same.
Depending on the ACK of both the UE-1 and UE2, the eNodeB send an accept/reject ACK to both the devices and a D2D link is established between them (see fig. 4.11).

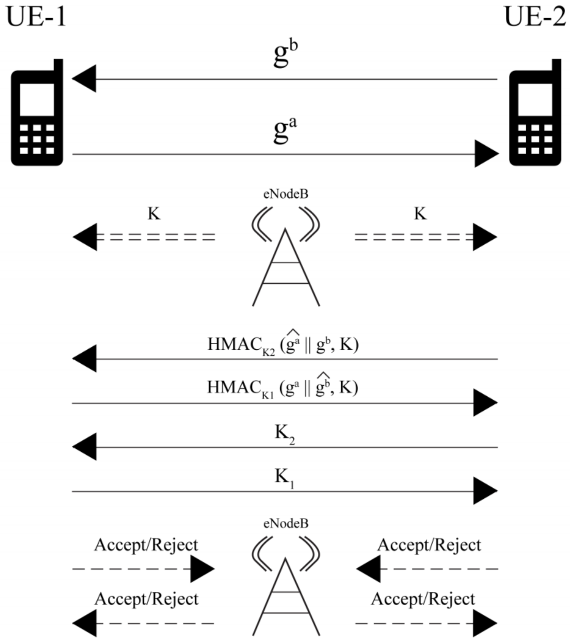


Figure 4.11: Key exchange - protcol 3.

Chapter 5

Conclusion

In this survey, i discussed salient features, requirements, and challenges involved in the development of the fifth generation (5G) of cellular mobile communication. I reviewed some architectures for 5G networks based on the inclusion of small-cells, cognitive radio networks, device-to-device communication, and cloud-based radio access networks. I compared 4G technology to 5G and finally i discussed about 5G security: services, issues and possible solutions.

5G wireless networks are expected to provide advanced performance to enable many new applications. In this report, i have presented a comprehensive study of recent development of 5G wireless security. The current security solutions mainly based on security services such as authentication, availability, data confidentiality, key management and privacy have been introduced. Many new security aspects are expected in 5G to the applications of technologies such as HetNet, D2D, massive MIMO, SDN and IoT [8].

Concluding, the zero latency, high speed data transfer, and ubiquitous connectivity are the salient features of 5G networks that are expected to serve a wide range of applications and services:

- **Personal usages:** multimedia data, voice communication, and Web surfing
- **Virtualized homes:** set-top box for TVs and residential gateways for accessing the Internet

- **Smart societies:** temperature maintenance, warning alarms, printers, LCDs, air conditioners, physical workout equipment, and door locks, would be interconnected in a way that the collaborative actions would enhance the user experience

- **The tactile Internet:** The tactile Internet improves the user experience in a virtual environment to an extent of only milliseconds of interaction latency.

- **Healthcare systems:** frequent data transfer from patients' body to the cloud or health care centers

- **Industrial usages:** The zero latency property of 5G networks would help robots, sensors, drones, mobile devices, users, and data collector devices to have real-time data without any delay

- **Vehicle-to-Vehicle:** Self-driving vehicles would take place in the near future, and as a requirement, vehicles would communicate with each other in real-time. Moreover, they would communicate with other devices on the roads, homes, and offices with a requirement of almost zero latency. Hence, an interconnected vehicular environment would provide a safe and efficient integration with other information systems

Bibliography

[1] N. Adem, B. Hamdaoui, and A. Yavuz. Pseudorandom time-hopping anti-jamming technique for mobile cognitive users. In *2015 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, Dec 2015.

[2] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. K. Nakarmi, M. Näslund, P. O'Hanlon, J. Papay, J. Suomalainen, M. Surridge, J. Wary, and A. Zahariev. A security architecture for 5g networks. *IEEE Access*, 6:22466–22479, 2018.

[3] D. Fang, Y. Qian, and R. Q. Hu. Security for 5g mobile wireless networks. *IEEE Access*, 6:4850–4874, 2018.

[4] China Mobile Research Institute. C-ran: The road towards green ran. In *white paper*, Sep. 2011.

[5] F. Liu, J. Peng, and M. Zuo. Toward a secure access to 5g network. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 1121–1128, Aug 2018.

[6] J. Liu, T. Zhao, S. Zhou, Y. Cheng, and Z. Niu. Concert: a cloud-based architecture for next-generation cellular systems. *IEEE Wireless Communications*, 21(6):14–22, December 2014.

[7] V. S. Pandi and J. L. Priya. A survey on 5g mobile technology. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pages 1656–1659, Sep. 2017.

[8] Nisha Panwar, Shantanu Sharma, and Awadhesh Singh. A survey on 5g: The next generation of mobile communication. *Physical Communication*, 01 2016.

[9] R. Sedidi and A. Kumar. Key exchange protocols for secure device-to-device (d2d) communication in 5g. In *2016 Wireless Days (WD)*, pages 1–6, March 2016.

[10] S. Vij and A. Jain. 5g: Evolution of a secure mobile technology. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 2192–2196, March 2016.