

The Mobile Network

An overview

Table of Contents

Introduction **1**
Development History 1
Challenges and answers 1
The basic structure of a mobile network 2
The basic principles applying to the design and operation of a mobile network 3
Details of network architecture **5**
The radio access network 5
Mobile radio cells 6
Frequencies 6
Components of a base station 7
Changes in connection with the introduction of 5G 7
The core network 8
Mobility management entity 9
Gateway units 9
Central database 9
Other central network components 9
Developments toward 5G 10
The transport network 10
The operation and maintenance center – the network control center **11**
Core tasks: 11
OMCs' OSS 11
Interfaces to business support systems 11
Terminal devices **12**
Types of devices 12
Device applications and security 12
Security in mobile networks **13**
The air interface – for communications between devices and base stations 13
The transport network – communications between base stations and the core network 13
Separation of communications relationships 14

Access control (= authentication) in connection with use of services (such as telephony, SMS, Internet access) 14
General security considerations 14
Secure introduction of new technology, and secure operation 15
Remote maintenance and support provided by manufacturers 15
Standardization of security for mobile communications 15
Summary 17
Abbreviations 18

Introduction

Development History

The first digital mobile networks in Europe went into operation in 1992. Since then, the GSM (Global System for Mobile Communications) standard, which originated in Europe, has become established worldwide, and it remains one of the key bases for mobile voice communications. The GSM standard, which succeeded purely national, analog cellular networks, is referred to as the 2nd generation (2G) standard. The further development of cellular communications proceeded via the "UMTS" (3G) and "LTE" (4G) standards and technologies, with new technology generations being introduced at intervals of about 10 years. Other technologies, such as "GPRS" and "EDGE," can be seen as intermediate steps in a development moving from network architectures designed solely for voice communications to architectures that can support increasingly capable data services. Mobile data communications began with text messaging (short message service – SMS), at very low bit rates, and has progressed to the point at which mobile broad-band Internet access has become routine. This level of development has been made possible by new features in core networks, in combination with increasingly powerful mobile devices; by growth of the available spectrum for wireless access; and by the use of fiber optics in transport networks.

Challenges and answers

On the one hand, this continuous technological development, and the ongoing expansion of mobile networks, have been driven by extreme growth in use of mobile data services. The quantities of data transported via mobile networks are currently forecast to grow annually by 40-50 %. While those quantities of data are still considerably smaller, in absolute terms, than the quantities being transported via fixed networks, they are still large enough to require ongoing massive investments in network expansions and upgrades and in new technologies.

On the other hand, apart from the continual expansion of mobile network use, capacities and coverage, the global development in mobile communications has been driven, and is being driven, by innovation, and by related ever-greater requirements. 5G will bring new features and new intelligent solutions for both private customers and business customers (especially with regard to applications for enterprises). Industry 4.0, Smart City and Smart Home are some of the current buzzwords in this context. These new possibilities can be divided into three major application areas:

- Ultra-high-speed broadband services, i.e. data services offering significantly higher data transmission rates. Such services will be required for video transmissions and for AR/VR applications.
- Interconnection of extremely large numbers of devices and sensors. The Internet of Things is just starting to take off. (M2M, massive IoT)
- Fundamentally new mobile network capabilities, via controllable quality of service, lower latencies (shorter response times), new security characteristics, network-based positioning, and much more.

The basic structure of a mobile network

All mobile networks have digital, hierarchical network structures. What does this mean? Simply put, it means that a network, on one end, consists of a small number of components with central, overarching tasks – its core network – and, on the other end, of a very large number of base stations – the radio access network. These two major parts are interconnected via transmission lines – the transport network. Yet another component, a control and monitoring network, ensures that all the other mobile network components operate reliably. The network is completed by subscriber devices, such as telephones, smartphones and connected sensors.

The following section briefly describes these various main parts of a mobile network. The section that follows it then presents greater detail. Readers should note that this article does not focus on telecommunications services and applications.

- The radio access network provides the connections between a) subscribers and their devices and b) the network itself. In a fixed network, connections to private and business customers are normally provided via fixed landlines (primarily optical fiber, coaxial cables, copper wires). In a mobile network, such connections are provided via radio waves. This portion of a network is referred to as the "radio access network" (RAN). Radio waves support wireless bidirectional connections between base stations in the network and subscribers' terminal devices. In the interest of redundancy and reliability, the base stations in this part of the network are sited so that their "mobile radio cells" overlap, geographically, to some extent.
- The network's command center is referred to as its core network (CN). A core network consists of numerous sub-components with dedicated tasks. The core network's main tasks are to control communications within the network, including access, and set-up and termination of connections, and to facilitate customers' mobility. In addition, core network components control the nature and scope of the services provided.
  The components of the core network are relatively small in number and are distributed over small numbers of sites. This contrasts with the radio access network's large number of base stations, each with limited geographic coverage. The core network's network elements are seen as critically important. Any disruption or fault in these elements can have major impacts either on the network as a whole or on large geographic sections of it. Normally, critical elements are installed redundantly, to help ensure that any disruptions do not affect (all) network subscribers.
  The core network also manages handovers to the Internet, to other telecommunications networks (national and international) and to the operating company's own services platforms.
- The transport network links all base stations with the core network and handles data transmissions between the access network and the core network. All traffic streams (voice and data) are encrypted. As is the case for the access network, the transport network has only the task of transferring data; it does not process data.
- Mobile networks also have another highly important level: network monitoring and control. This level is not involved in managing communications relationships between subscribers and in handling the signaling data that such management requires. Its task is to carry out overarching monitoring and control of all network components involved in such

management. It monitors the network's stability and stability, responds to any problems and disruptions and serves as the pathway for basic changes to the network. This level thus represents a separate monitoring and control network for the mobile network as a whole.

- To be complete, communications relationships must encompass both network components and mobile terminal devices. The range of devices found on the subscriber side includes telephones, smartphones, computers, routers and sensors. SIM cards play an important role in identifying subscribers and devices and in encryption of communications.

The basic principles applying to the design and operation of a mobile network

- Open, global standards: The global success of digital mobile communications has been made possible through international standardization. Standardization bodies (such as ETSI, 3GPP, ITU, …), working in the framework of international teams of experts, and in cooperation with representatives of network operators, manufacturers of infrastructure, equipment and terminal devices, and services developers, develop standards and their underlying architectural and design principles. The resulting standards and principles enter directly into the development and design of networks and components. The key achievements of such efforts – in addition to unified network architectures, binding services characteristics and open interfaces – include transmission protocols, which define the manner in which mobile networks "speak." Since the establishment of GSM, standardization has enabled mobile-network operators to combine network elements of different manufacturers and to introduce globally standardized services that function seamlessly across network (and network operators') boundaries. The numbers, quality and reliability of the resulting open standards have improved continuously over the years. Via various industry initiatives, efforts are currently underway to open up standards still further.
- Separation of subscriber data and control data: Communications operate on the basis of separation of usage data (for voice calls, text messages and data transmissions) from control data, which is also referred to as "signaling data." Signaling data play an essential role in establishing connections, in enabling communication between two or more subscribers (people or devices), and in controlling the mobility of communication relationships. The data needed to control the network are kept clearly separate from subscriber data (which are also encrypted).
- Decoupling of hardware and software: Since the beginnings of digital communications, such communications have been based on software – computer programs and algorithms – installed on hardware, i.e. specially designed computers. In certain kinds of network elements, system suppliers have linked the software and hardware within a closed system ("black box"). Various industry initiatives are now aiming to decouple hardware and software within network elements, in order to achieve the kind of openness that prevails in interfaces. The advantages of such openness include greater transparency, and greater flexibility in combining components of different manufacturers and in using standardized computer hardware. This approach is referred to as "virtualization." Although aspects of it are still under development, this technology is already being used to some extent in regular network operations ("Network Function Virtualization" – NFV)).

- Cloudification: The above-described decoupling is a basic prerequisite for "cloudification," which will play an important role especially in connection with 5G. Cloudification entails a shift to cloud-based operation, in which a mobile network's functions and services are operated and managed, in various constellations, within a network operator's data center. The data centers used for this purpose are special, protected centers that meet the most stringent requirements pertaining to availability, security and scalability.
  The advantages of this technology – which does present challenges with regard to operational reliability – include easier adjustments to usage/load profiles and faster implementation of new services. This technological innovation stands ready for full-scale introduction and use.

Details of network architecture

The following section describes the various areas of a mobile network in greater detail. The basis for all components of a network – also referred to as network elements – consists of a suitable combination of hardware (cables, antennas, special computers) and software, and of the proper interaction of the various network elements via standardized interfaces and protocols.

Originally, networks for digital communications were designed primarily for transmission of voice communications (as was the case for ISDN). Today's networks are high-performance, IP-based data networks, however.

The radio access network

The radio access network has the task of accepting subscriber data into the network and sending data from the network to subscribers. A network's base stations are transmission components that, for the sake of simplicity, may be likened to radio modems – or, at a highly abstract level – to the base stations used with cordless phone systems. Base stations are equipped with control logic for distribution of available transmission capacities among mobile subscribers and for assurance of quality of service. They accomplish the second of these tasks by controlling transmission power, antenna orientation and other quality parameters. Apart from carrying out such configurations, modern access networks do not create any services or modify any data. Most of the base stations in modern networks are connected via fiber optic connections to the other parts of the mobile network.

The most resource-intensive aspects of setting up and operating a mobile network include the initial installation, ongoing network modernization (S-RAN; see below), and – now – further network expansions and upgrades to the 5G standard. This is true in terms of the required infrastructure investments (for example, infrastructure upgrades for additional antennas / new antenna technology), of the ongoing costs (such as location rentals, energy costs), and of the personnel expenses for installation and maintenance. Because radio access networks tend to be spread out over considerable areas (even nationwide), all adjustments and adaptation that have to carried out in a harmonized manner require large investments of time and materials. In any given case, different versions of base stations, spread throughout the entire country, can be affected. What's more, tasks such as network upgrades have to be carried out without negatively affecting service for subscribers. In "worst-case" situations, every one of the thousands of base stations in a network will have to be visited at least twice!

With a view to speeding up the installation process and – in light of the enormous investments needed for setting up and operating a network – to reducing dependence on individual partners, multiple system suppliers for the access network will normally be chosen, via selection procedures.

Mobile radio cells

The area that a base station covers, with the radio waves emitted by its antenna, is referred to as a "mobile radio cell." For simplicity's sake, one can picture the coverage pattern formed by adjacent mobile radio cells as a hexagonal, honeycomb pattern. The size and range of individual cell is on the order of a hundred meters. In rural areas, cells can be up to several kilometers in size. A cell's radius depends on numerous factors: the transmission power of its antenna, the frequency being used, the type of antenna involved and the surrounding structures. Other factors that affect network coverage, apart from these key influencing factors, include the capacity of cells and the manner in which cells are arrayed. Coverage is optimized via careful placement and orientation of antennas. Depending on the required or desired size of a cell, its antennas can be placed on a dedicated antenna mast or on roofs of buildings, or even integrated within facades or billboards, etc. In general, the higher an antenna is placed, the larger will be its range. For some years now, antenna sites have commonly served multiple sub-cells, primarily for the purpose of increasing network capacities. In such cases, the cells are said to be "sectorized."

Regardless of the coverage a mobile radio cell ultimately achieves, it will always serve only a small subset of the relevant network operator's total number of active mobile subscribers.

Frequencies

A mobile radio cell's propagation behavior is determined largely by the frequency band that has been chosen for it.

The higher the frequency band, the more capacity is available, in principle – but the poorer is the cell's propagation behavior. High-frequency radio waves quickly weaken and fall prey to interference, with the result that they are no longer properly received. Walls of buildings, especially solid, dense walls, and certain types of steel structures, often prove to be impenetrable barriers. This explains why the 3.5 GHz frequency band, in which most European, American and Asian countries are currently auctioning spectrum for 5G, is suitable for fast data services, but not for wide-area coverage.

The lower frequency bands (such as 900 MHz) that have been used since the introduction of GSM boast good ranges, also into buildings. But because such bands offer much smaller spectrum resources, they are ill-suited to the task of transmitting large quantities of data.

While high-frequency-band mobile radio cells offer advantages such as high capacity and bandwidth, they have to be closely "interwoven." They are best used as "small cells," meaning cells with a radius of just a few hundred meters or even less. Higher frequency ranges will gradually be phased in also for coverage within structures (industrial structures, shopping centers, stadiums). Needless to say, installation of large numbers of mobile radio cells requires large investments. In addition, planning of the denser 5G networks presents its own set of challenges, in ensuring that large numbers of cells do not interfere with each other. Once network planners identify a theoretically ideal location for a base station, they have to find a corresponding real-world location that they can lease and obtain approval for. Then they have to actually install the base station and commission it. For today's mobile-network operators, who are seeking to provide the

best-possible coverage and service in the shortest-possible time, and as cost-effectively as possible, this overall, complex and involved process thus presents both technical challenges and time challenges.

Components of a base station

Base stations were referred to above, for simplicity's sake, as "components." In actuality, a base station is of course not just a single device but a combination of different modules that carry out different technical tasks.

A base station's antennas, for example, convert electrical signals into radio signals – and vice versa. The size – and, thus, the weight – of a base station's transmission and receiving antennas are determined in part by the frequency spectrum for which the antennas need to be designed. The lower the spectrum, the larger the antennas. In the early phase of digital communications, each base station was equipped with one transmission antenna and one receiving antenna. The antenna housings found on today's base stations (the housings are the small white boxes on the antenna masts) contain multiple individual antennas. Currently, 4x4 antennas, i.e. units in which four transmission antennas and four receiving antennas are combined within a single component, are already in service, and the first 64x64 antennas are now available. Such new multiple-antenna units are referred to as "MIMO" ("multiple input, multiple output") and (in the latter case) "massive MIMO" antennas. These new antenna types are not passive in their function, but active; they integrate beamforming systems for concentrating and directing their beams, and they can dynamically adjust their power levels in keeping with applicable standards.

A base station requires components and functionalities for the handover from line-bound transmission to a radio interface. Such functionalities can be provided either by a combined unit or by physically separate units. A radio unit, with amplifiers and filters, carries out bidirectional conversion of digital signals into analog electromagnetic waves. A base band unit, logically separate from the radio unit (and physically separable from it, in principle), carries out digital signal processing.

Another important technical term in this context is "Single Radio Access Network" (S-RAN). Previously, every mobile network generation required its own separate transmission and receiving components within the access network. S-RAN technology now enables combinations of different generations (GSM, UMTS, LTE) to use the same components. This is a key basis for flexible use of the available spectrum, with respect to applicable technology. It is now supporting migration to LTE, for example, and it will soon support migration to 5G. In the framework of S-RAN modernization, existing base stations are being upgraded with new future-proof network elements.

Changes in connection with the introduction of 5G

The first phase of the introduction of 5G networks involves the adoption of the "New Radio" (NR) standard, a more-efficient radio-transmission standard. This requires retrofits to base stations, to enable them to support the new standard.

In this phase, the new 5G network is being set up as an expansion of the existing LTE network. The 5G base stations are being connected to the LTE core network, and that network is being upgraded to incorporate 5G functionalities. With this approach, the LTE network will function as a sort of "anchor network" for the new 5G network. As a result, wherever, in this phase, complete-coverage 5G is not yet in place, subscribers will automatically be shifted back to the LTE network. This implementation approach is referred to as a "Non-Stand-Alone" (NSA) approach.

Initially, 5G will also be used within a new frequency band, in the 3.5 GHz range. As a result, new antennas will be required that support that band. The added bandwidth that the new spectrum is expected to provide for mobile networks will increase the capacity of the access network. The new system, in combination with special antenna technologies, and even with use of multiple frequency bands, will be able to achieve very high bandwidths, i.e. subscribers will perceive it as being very fast.

As explained above, use of higher frequency ranges, and fulfillment of higher capacity requirements (for transmission of larger quantities of data, and for higher speeds), will be possible only through network densification. In comparison to the development of previous networks, the process of expanding 5G networks will necessitate finding considerably larger numbers of suitable and available antenna locations, even before complete-coverage 5G ever becomes available.

Also, the issue of "cloudification" (see above) will ultimately influence the design of components for the access network. This means that gradually, in the coming years, the trends toward open interfaces, and toward further decoupling of hardware and software systems, will continue and will reach into the cloud-based parts of networks, which thus far have tended to be largely proprietary.

The core network

The core networks in place as of LTE differ from the comparable parts of earlier generations of mobile networks in that they use packet-switched transmission that is completely IP-based. In GSM networks – as in ISDN networks – voice transmissions were digital, but they involved dedicated connections between two subscribers. Following the introduction of LTE, a technology for packet-switched voice transmission via LTE – "Voice over LTE" (VoLTE) – was introduced. It represents an evolutionary step forward from 2G and 3G transmission of voice conversations.

The new, IP-based network architectures are a key basis for efficient provision of new services. LTE core networks also have considerably "flatter" structures than earlier core networks had. This provides considerable improvements, over earlier networks, with regard to network latency.

Because of their complexity, core network components are considerably more expensive than base station components, in terms of both investments and ongoing overhead. Owing to their centralized network placement, however, and to the relatively small numbers of such components that networks require, the total costs for core network components will normally be lower than those for the attached access network. Core networks ac-count for about 15-20 % of the total investments and costs for a network

Due to the central role that a core network plays, any disruptions, changes or modernizations in it can have significantly greater implications and impacts than disruptions in other network parts normally have. For this reason, great care and attention must be given to the planning, implementation and operation of core networks, and key components of such networks must always be redundantly in place.

The key components of modern core networks include:

Mobility management entity

The "mobility management entity" (MME), a control node in modern LTE networks, is responsible for authenticating users. It adjusts the network's behavior according to whether a subscriber is in the "idle" or "connected" (making a call) mode, and also in accordance with the subscriber's mobility. Networks provide MME functions for both their own subscribers and roaming subscribers. MMEs also manage interactions with second-generation (GSM) and third-generation (UMTS) networks, and they control a range of network security mechanisms.

Gateway units

Serving gateways (SGW) forward subscribers' data packets both within the network and to earlier-generation sub-networks. PDN gateways (PGW) control data transfers into external data networks, i.e. to other mobile and fixed networks. Modern PGWs support all of the different functionalities that such transfers involve.

Central database

A core network has a central database, known as a "home subscriber server" (HSS), that stores subscriber information. The information involved consists not of names and addresses but of technical information relating to the subscriber identities linked to SIM cards. In each case, the data includes an ID number and a profile linked with the relevant identity. Each profile includes such information as which services the subscriber has booked and is entitled to use. Such information plays a key role in connection with network login, subscriber mobility within the network and use of communications services such as voice calling.

Other central network components

The above-described components are complemented by additional components with special tasks, such as protecting the network (firewalls), enabling secure communications for devices connected via WiFi networks, and many others.

The major sub-systems of the central network include the "IP multimedia subsystem" (IMS), which is normally a separate unit that consists of multiple sub-modules. The IMS provides IP-based voice services such as VoLTE.

Developments toward 5G

As explained above, the introduction of 5G will begin with the integration of new base stations, within the access network, that support the 5G "New Radio" standard. Initially, this new 5G radio network will be linked with the existing core networks of the current LTE networks.

The new core networks designed especially for 5G ("5G Core") are currently still in the final stages of development. They will be integrated within networks in a subsequent step. The full range of the many new features that 5G promises to bring will not become available until the new core networks are in place. As in past evolution of mobile network services, development and provision of 5G services will take place in stages, via "3GPP" releases. Release 15, which has now been approved, and Release 16, which is still in the specification process, are especially important with regard to the introduction of 5G. (Note: Smaller release numbers relate to LTE and to earlier standards.)

The transport network

This part of the network is responsible for proper and orderly data transfers between individual network elements. Transport networks are not special features of mobile networks per se, since their primary task is to transport encrypted usage and signaling data transparently between the access network and the core network. Every LTE base station, for example, has a dedicated link, encrypted with IPsec, to the core network.

A transport network aggregates data from the various base stations and transfers them into the core network – and transfers data vice-versa, from the core network to base stations. Like access networks, transport networks do not process data. Active components within transport networks maintain data integrity in transport – even over large distances. The active components involved in this task are standard network components, such as switches and routers. In general, transport networks have star-shaped, tree-like structures (combining different topologies).

Transport networks also have redundancies, to ensure that data will automatically be rerouted within the network in the event of any failures of individual segments. The transport pathways themselves are now implemented over fiber-optic links. In some cases, directional radio links – i.e. special types of point-to-point radio links, within dedicated frequency spectrums – are also used.

The operation and maintenance center – the network control center

Core tasks:

A mobile-network operator's "operation and maintenance center" (OMC), also referred to as a network control center, has the task of ensuring that the network operates properly, disruption-free and securely, 24/7. This includes monitoring the network's performance data (traffic volumes and streams, proper functioning and load distribution of/in network elements), monitoring for any problems and responding to disruptions and failures. The OMC also serves as the conduit for adjusting and optimizing the network configuration, via installation of new software releases and network parameters in the various network components.

An OMC has connections to all elements of its mobile network, so that it can collect all necessary measurement data for monitoring and optimization and adjust the network configuration as required. OMC processes are increasingly being automated.

While the core network is responsible primarily for the network's actual functionality and communications relationships, the OMC is chiefly responsible for the network's proper end-to-end operations. The OMC is thus a security-critical element in the best sense, since the network operator uses it to maintain control and configuration authority over all the different components – supplied by different suppliers and industrial partners – within the network.

OMCs' OSS

OMCs are supported by computer programs known as "operation support systems" (OSS). As a rule, an OMC will have numerous such systems, for many different sub-tasks. In such systems, manufacturer-provided, proprietary configuration systems and interfaces are combined with systems of IT partners that support overarching, manufacturer-independent network monitoring and control. Experts working the realm of OSS thus need both a sound knowledge of their network and good IT skills.

Interfaces to business support systems

A network operator's "business support systems" (BSS) are IT systems for such tasks as billing, customer acquisition, customer care, etc. BSS require interfaces to network functions, because they have to carry out such tasks as configuring subscriber accounts, including all booked features, within the network, and drawing billing data from the network and processing it for subscribers.

Terminal devices

Types of devices

Permanently installed car phones figured prominently among the devices seen in the early days of mobile communications. Such phones were followed by portable phones and then by increasingly smaller mobile phones. Beginning in about 1996, the first devices for data communications, which was beginning to emerge on the mobile front, were introduced by companies such as Nokia (the "Communicator") and HTC ("XDA"/"MDA"). Then, as of 1997, iPhones emerged on the scene, paving the way for the smartphone mass market. Phones using the competing Android operating system soon followed. Today, Android is the operating system of choice for most alternatives to iPhones, and it is widely used in vehicles and connected devices.

Radio technology is also used for establishing communications links within homes and in business premises. Special routers, installed in subscribers' own facilities, provide access to stationary voice and data services. In some cases, hybrid combinations of fixed and mobile services are used, to provide greater data throughput. In such configurations, use of new frequency bands, in connection with radio-based "fixed wireless access" (FWA) for the final hundred meters or so between the network and the subscriber, will provide still more options. Since mobility plays only a subordinate role in such configurations (what mobility is required is provided by the subscriber's WiFi system, sited behind the main access device), such configurations represent a borderline case between mobile and fixed network communications.

At the conclusion of this section, the growing numbers and diversity of connected devices and sensors should be mentioned; key terms in this context include machine-to-machine communications (M2M) and the Internet of Things (IoT).

Device applications and security

Basic network services, such as telephony / voice services and data services, are provided on highly secure basis (via redundancy and encryption).

Any discussion of security-relevant issues related to telecommunications networks should also consider the risks that applications can present for terminal devices. Applications, which are provided both by device manufacturers and by third-party suppliers, either come bundled with devices, as basic software (operating system, pre-installed applications) or are installed by users themselves. In addition, the risks that malware present for mobile data devices also have to be considered.

As is now widely known, certain smartphone applications, in addition to processing application data (such as text and voice messages), also collect user data and automatically forward it, without the user's knowledge, to remote servers. In this connection, cf. also the discussion about "over-the-top" services such as Facebook, Google, etc.

Security in mobile networks

Any complete security concept must consider all of the components, interfaces and communications relationships encountered in mobile networks. The following section provides a short outline in this connection.

The air interface – for communications between devices and base stations

The three most important security measures in this network area are:

- Encryption of all confidential communications;
- Mutual authentication in interactions between mobile devices and base stations;
- Secure storage of cryptographic keys in SIM cards and in the core network.

Via air interfaces, mobile devices (such as smartphones) establish secure connections with base stations. To do so, they use cryptographic keys stored on their SIM cards. In each case, only the SIM card and the core network know the key. This system makes it possible to establish secure communications links, and it enables the components involved – i.e. the subscriber (represented by their SIM card) and the network (represented by the base station) – to authenticate themselves to each other. As a result, each side knows that it is speaking with the component that it expects to be speaking with. Unauthorized third parties can neither pretend to be one of the components involved nor eavesdrop on the communication.

- Pseudonymization of user identities via use of short-term identities.

Mobile communications calls for "technical" identities. To ensure that third parties cannot, for example, monitor and then reproduce a network user's motion profile, such identities are regularly and automatically replaced, without users' knowledge. No correlations with previous or subsequent identities can be established. This rules out any possibilities for unwanted tracking of users.

The transport network – communications between base stations and the core network

Two security measures in particular are especially important:

- Encryption of all confidential communications;
- Mutual authentication in interactions between base stations and the core network.

All further communications from base station into the mobile network's central core network are also protected by encryption. As a result, the core network sets up protected, secure communications links. In addition, all base stations are authenticated as well via such links. This ensures that only base stations belonging to the pertinent mobile-network operator are able to communicate with the operator's core network.

Separation of communications relationships

A mobile network maintains different types of communications relationships. Strict separation of its communications relationships from one another is yet another important security measure. Such separation ensures that no unwanted "mixing" takes place and that, for example, user-transmitted data have no possibility of influencing control of the network. A similar principle of separation applies to the different types of traffic within mobile communications. The transport and processing of customer data, signaling data and control data all take place as separate processes.

Access control (= authentication) in connection with use of services (such as telephony, SMS, Internet access)

Controls for mobile networks apply two basic principles to ensure that no unauthorized use of network services takes place.

- Firstly, the core network "knows" which services the network subscribers have booked, and it allows each subscriber to use only the services he/she has booked.
- Secondly, this approach is also used with individual network accesses, such as the dedicated company-network accesses that companies provide for their employees.

Every subscriber to a mobile network has a profile, within the core network, that shows what services they can use. The core network's components ensure that subscribers can use only those services for which they are authorized. Similar controls are applied to networks of closed user groups, such as those found within company networks. In each case, subscriber profiles are controlled by the above-described BSS and OSS systems, and they can be accessed solely by the network operator.

General security considerations

In addition to the above-listed security measures, which are specific to mobile networks (and other similar types of networks), mobile networks also employ security measures that are used in virtually all communications networks. The following is a selection of important measures in this group:

- Secure configuration of components, and deactivation of functions that are not required, or that are not secure;
- Required changing of manufacturer-preset, standard passwords;
- Use only of cryptographic procedures that are acknowledged to be secure;
- Regular software updates, for elimination of any detected security vulnerabilities;
- Use of secure network architectures that have interlocking security concepts; such concepts include keeping networks separate from individual functions (for example, via firewalls), filtering of data traffic, and use of control commands, in the network, that limit actions to what is permitted and required;
- Use of physical protection measures; for example, data centers are kept locked and have strict access-control systems;

- Use of redundancy concepts that ensure that functionalities are maintained when individual components fail;
- Required security checks for personnel working in critical areas such as network control and operations.

Secure introduction of new technology, and secure operation

All phases of projects for introducing new technologies and functionalities into mobile networks – including phases related to concepts, architecture, manufacturer selection, configuration, acceptance tests and commissioning – are supported and monitored by security experts. In such efforts, security experts ensure that every project phase gives adequate consideration to security and that all necessary security measures are implemented.

Acceptance tests are a standard part of all introductory projects. In such tests, security tests are carried out to ensure that no undesired functionalities, such as incorrect processing of non-standards-conformal messages, are active in any sub-systems being used.

The components of mobile network are operated in accordance with the principle of "minimal rights." Employees and IT systems receive only the access rights that they absolutely need in order to carry out their tasks. And different tasks have to be performed by different roles. This ensures that any incorrect actions, regardless of whether they are intentional or unintentional, can cause only minimal damages (at worst).

During runtime, monitoring data are collected and then correlated and processed in security monitoring centers, for the purposes of quickly detecting any cyberattacks, network anomalies and component malfunctions and of quickly addressing their underlying causes. Like the operations center for the mobile network, a security monitoring center is typically staffed with security experts around the clock, on 365 days of the year.

Remote maintenance and support provided by manufacturers

In cases in which a component manufacturer needs to remotely access individual components, for maintenance purposes (for example, to access them from his own network), such procedures are allowed only for the specific task in question, only for an explicitly defined group of users, and only temporarily, i.e. for a defined period of time. In addition, such access takes place over special, restricted, encrypted and authenticated access pathways. Furthermore, every work step is monitored by the network operator, to ensure that all work is carried out in keeping with the network operator's requirements.

Standardization of security for mobile communications

In addition to defining standards for equipment and radio transmission, international standardization bodies also define standards for relevant security measures and procedures. The 3GPP and GSMA formats play a particularly important role in this connection. The standards defined by those bodies are implemented in development and configuration of mobile network components and of terminal devices. In addition, they are mutually agreed in contractual

agreements between mobile-network operators, and they are implemented by other players in the mobile communications sector. These provisions and procedures play a key role in ensuring the security of mobile communications across the boundaries between individual mobile-network operators.

Summary

Mobile networks are complex structures that need to be planned, installed and operated with great care. The architecture for such networks, which is clearly structured and standardized, provides the basis for their stable operation and their coordinated, continuous further development. In conclusion, the following points also need to be emphasized:

- Today's telecommunications networks reflect the development and preparatory work of the past decades, including continuous investments. Interlocking update cycles are carried out, leading to regular replacements of network components at intervals of 5 – 10 years. The introduction of 5G, in the coming years, will bring about additional significant progress, and entail enormous network investments.
- Access networks play a central role in subscribers' experience of network quality. In light of their clearly defined, limited range of features, and of their geographic distribution, access networks can be considered non-critical and "under control," security-wise, in terms of the impacts of any failures. The situation is similar with transport networks.
- Core networks, on the other hand, are of critical importance in this regard, as a result of the services and network functions they control, and of their central, exposed placements. Network control centers, which monitor networks across boundaries between networks and manufacturers, are also critically important elements.
- The importance of security, in all its aspects, is great, and it continues to grow. Networks' logical, hierarchical structures, along with network-control entities, global standards and extensive function and security checks, all play important roles in the tasks of achieving, maintaining and guaranteeing reliability and transparency. In closing, we note that a complete perspective on this subject would need to include a third part, covering the terminal devices on the subscriber side and the applications they run.

Abbreviations

Abbreviation	Meaning	Explanation
3GPP	3rd Generation Partnership Project	Worldwide cooperation project for standardization; underway since UMTS/3G.
AR/VR	Augmented reality / virtual reality	Augmented: Enhanced via superimposed information; applied to the perspectives on real environments that are provided by devices such as data goggles. Virtual reality: Projection of artificial environments.
BBU	Base band unit	A base station component within the access network.
BSS	Business support systems	IT systems that support business processes.
CN	Core network	(German: Kernnetz)
EDGE	Enhanced Data Rates for GSM Evolution	A technique, introduced in the framework of evolution toward UMTS networks, for enhancing data-transmission speed.
ETSI	European Telecommunications Standards Institute	The European standardization body that paved the way for the GSM standard.
FWA	Fixed wireless access	A radio-based link between a household and a network.
GHz	Gigahertz	Hertz = Unit of frequency. 1 GHz = 1 billion oscillations per second.
GPRS	General Packet Radio System	System for adding data-transmission functionality to 2G networks.
GSM	Global System for Mobile Communications	The first global standard for digital mobile networks; also referred to as "2G."
GSMA	GSM Association	Mobile-network-operators' association.
HSS	Home Subscriber Server	Database that forms part of core networks.

IoT	The Internet of Things	Term applied to the "ecosystem" of connected devices, sensors, etc.
IP	Internet Protocol	The protocol used in computer networks. The foundation for the Internet.
IPsec	Internet Protocol Security	An encryption protocol that is used with IP connections.
ISDN	Integrated Services Digital Network	An international standard for a digital fixed network. In Germany, this was a key standard prior to the introduction of IP-based networks.
ITU	International Telecommunication Union	UN organization that focuses on technical aspects of telecommunications. The ITU sponsors the "World Radio Conference" (WRC), which discusses standards for global use of frequency bands.
LAN	Local Area Network	Local network in a home, in the premises of a company, …
LTE	Long Term Evolution	4th-generation mobile network.
M2M	Machine to Machine	Applied to communications between connected devices.
MHz	Megahertz	Hertz = Unit of frequency. 1 MHz = 1 million oscillations per second.
MIMO	multiple input, multiple output	Antenna system that combines multiple transmission and receiving antennas in a single unit.
MME	Mobility Management Entity	Forms part of core networks.
NFV	Network Function Virtualization	Decoupling of hardware and software.
NR	New Radio	New transmission standard for radio interfaces within 5G networks.
NSA	Non-stand-alone	The initial architecture chosen for the introduction of 5G. In it, the LTE network serves as an "anchor network" for the 5G network as it develops.
OMC	Operation and Maintenance Center	A mobile-network operator's network control center.

OSS	Operation Support Systems	Systems within a network control center.
OTT	Over the Top	Applied to transmission of voice, video and data content without direct control by the relevant Internet / telecommunications-services provider. Examples of OTT services include messenger services (WhatsApp, Facebook, iMessage, etc.).
PDN	Packet Data Network	Part of a core network.
PGW	Packet Data Network Gateway	A PDN gateway in a core network.
RAN	Radio Access Network	Radio-based access network.
RU	Radio Unit	A base station component within an access network.
SGW	Serving Gateway	A gateway in a core network.
SIM	Subscriber Identity Module	Chipcard for identification within a mobile network.
SMS	Short message service	Service for transmission/reception of short messages (texts) within mobile networks.
S-RAN	Single Radio Access Network	Network element, within the access network, for operation of several different mobile-network generations within a single unit.
UMTS	Universal Mobile Telecommunications System	3rd-generation mobile network.
VoLTE	Voice over LTE	Digitalized, IP-based voice transmission.
Wi-Fi	Wireless local area network	Private, public or commercial local radio network that uses unlicensed spectrum.



GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com