**I. INTRODUCTION**

5G provides a highly flexible and scalable network technology for connecting everyone and everything, everywhere.

enhanced mobile broadband (eMBB), URLLC, and massive machine type communications (mMTC).

**II. 3GPP Rel-16 and proposed Rel-17 5G System Architecture and Security Features**

The 5G system (5GS) architecture builds on a cloud native foundation by means of the Service Based Architecture (SBA) in the 5G core (5GC), with the objective to provide universal connectivity via all access technologies. 5GC also provides architectural agility by introducing compute-storage split and enablers for 1:N redundancy for control plane resiliency, efficient transaction processing and operational efficiency (enabling reduced CAPEX and OPEX).

The Rel-17 architecture will provide:

* further enhancements for analytics-powered networks and enablers for network automation (eNA),
* support for proximity services,
* a multicast and broadcast architecture,
* enhancements to support edge computing,
* enhancements to support the IIoT framework,
* support for NTNs and drones (also referred to as unmanned aerial systems - UAS) [1][3].

**Analytics-powered networks:** Rel-15 and Rel-16 specify the framework for data collection and data analytics in the 5GS by introducing the Network Data Analytics Function (NWDAF)

Advanced ML algorithms can utilize the information collected by the NWDAF for tasks such as mobility prediction and optimization, anomaly detection, predictive QoS and data correlation.

**Enhancements for Verticals and Industrial IoT:** Support for E2E IIoT in the 5GS is based on a set of enabling features for which the foundation is being specified in Rel-16:

* Support for Time Sensitive Communication
* Non-public (i.e. private) networks
* Support for 5G LAN-type services
* Enhanced location services

Time Sensitive Networking (TSN) is a communication service that supports deterministic communication and/or isochronous communication with high reliability and availability.

**Expansion of Mobility and Altitude:** One of the main drivers for 5G Evolution is to expand the reach of mobile connectivity beyond current boundaries. Several features are proposed to be introduced which will address this objective:

* Enhancements for NTNs [12], including both satellites and High-Altitude Platform Stations (HAPS) (see Section III for further details);
* Connectivity and control of Unmanned Aerial Vehicles (UAVs) [13] including identification, tracking and authentication.

**Proximity Services:** Support for proximity services (ProSe) is beneficial both for public safety and commercial services.

**Multimedia Broadcast and Multicast Services (MBMS):** Support for MBMS will be introduced for NR mainly for public safety use cases, V2X applications and railways [15]. These use cases require broadcasting/multicasting over an area potentially wider than a single cell.

**Edge computing enhancements:** The 5G System in Rel-15 introduces a strong foundation to enable edge computing [16] by means of support for local UPF (re-)selection,

**Security Evolution:** 5G networks ensure privacy of their users, confidentiality protection, integrity of the traffic they transport and protection against attacks that can affect availability, integrity of the network and confidentiality of stored data.

Network Slice Selection Assistance Information (NSSAI) for slice access can be protected, if necessary. Security for duplicated transmissions (for URLLC) is expected to provide support for new applications such as medical imaging.

The following are some of the key security features specified in Rel-15 and Rel-16:

* Unified authentication framework and access-agnostic authentication.
* Primary and secondary authentication in public and non-public networks (including support for slice-specific authentication).
* Increased home control, e.g. for authentication and steering of roaming.
* Enhanced subscriber privacy
* Enhanced Security for Radio Resource Control (RRC) and Non-Access Stratum (NAS) signaling
* Support for user plane integrity protection (covering all three use case domains, i.e. eMBB, URLLC and massive IoT).
* Secure service-based architecture and inter-PLMN interconnection
* Security for interworking between the 5GS and the Evolved Packet System (EPS) of 4G.

**III. 3GPP Rel-16 and proposed Rel-17 RAN Features**

MIMO enhancements for further improvement of eMBB, positioning enhancements, and sidelink operation for direct device-to-device communication.

**Industrial internet of thing (IIoT)**

Key components of the Rel-16 enhanced URLLC feature include:

1. Control channel enhancements including new compact downlink control information formats with improved reliability
2. Scheduling and HARQ enhancements to allow for out-of-order uplink scheduling and HARQ-ACK. That will reduce latency for the user which allow UE to manage second uplink packet.
3. Support for multiplexing and pre-empting different traffic types in the uplink En bild som visar skärmbild

   Automatiskt genererad beskrivning
4. Support for multiple active grant-free uplink transmission configurations to accommodate different service flows (e.g. one configuration for a robot arm and one configuration for a pressure sensor).
5. Support for the ability to schedule two or more uplink data repetitions that can be in one slot or across a slot boundary for improved reliability.

**Integrated Access and Backhaul:** IAB nodes may be deployed for four fundamental purposes:

1. to remediate تصحيح isolated coverage gaps,
2. (ii) to provide backhaul where fiber deployment is sparse,
3. (iii) to enhance system capacity and
4. (iv) to bridge coverage from outdoor to indoor.

IAB nodes use the same spectrum and air-interface for access and backhaul and create a hierarchical wireless multi-hop network between sites.

En bild som visar skärmbild, telefon, mobiltelefon, parkering

Automatiskt genererad beskrivning

The IAB architecture leverages the gNB logical split architecture with a centralized Unit (CU) at the IAB donor node and Distributed Units (DUs) at IAB nodes. (تستفيد بنية IAB من البنية المنقسمة المنطقية gNB مع وحدة مركزية (CU) في العقدة المانحة IAB والوحدات الموزعة (DUs) في عقد IAB.)

An IAB node contains a Mobile Terminal (MT) part which behaves as a UE towards the parent node, this means it monitors the Synchronization Signal Blocks (SSBs) transmitted by the parent node for beam discovery, it monitors Downlink Control Information (DCI) for scheduling, and it performs random access towards the parent node.

**NR for Unlicensed Spectrum (NR-U):** NR-U adds channel access procedures to enable fair coexistence with other systems such as IEEE 802.11 variants or LTE Licensed-Assisted Access (LAA).Access to unlicensed spectrum provides an important tool to increase capacity for both service providers and private networks. For service providers, NR-U enables access to additional spectrum to improve the cellular network operation by offloading traffic in hot-spots. NR-U also enables the operation of standalone networks in unlicensed spectrum without any access to licensed spectrum.

The narrower beams and higher attenuation at these frequencies will provide higher spatial isolation than is seen in lower frequency bands, which will change the coexistence mechanisms required.

**MIMO Enhancements:**

The 5G NR air interface provides extensive support for large scale antenna arrays often referred to as Massive MIMO [19]. The main reasons for deploying Massive MIMO are coverage and capacity enhancement, which are critical given the expected year-on-year increases in demand for mobile broadband data services [22]. The NR MIMO framework is scalable and flexible and supports arbitrarily large antenna arrays with arbitrary antenna configurations for both FDD and TDD deployments [29].

The air interface of NR is “beam-based”, which means that all the channels in NR can be beamformed for range extension and coverage enhancement. To support beam management, Channel State Information (CSI) can be acquired by means of codebook-style feedback as well as through leveraging TDD channel reciprocity. Two kinds of codebook-based CSI feedback are provided, one of which, known as Type II CSI feedback, is particularly aimed at low-rank multi-user MIMO (MU-MIMO). Type II CSI feedback provides higher precision angular-domain feedback than Type I, and recent studies (e.g. [20][21][22]) have shown that the gains from the Type II CSI over the best LTE codebooks are in the order of 25-30% in full buffer traffic depending on the scenario and array configuration.

Finally, enhancements are being introduced to support full power uplink transmission in the case of UE implementations with multiple power amplifiers.

**NR Positioning:** Precise and up-to-date location knowledge is an essential requirement for emergency calls as well as new services like IIoT.

Some methods which are available in LTE are again being introduced in NR, namely downlink-based Observed Time Difference of Arrival (OTDOA), Uplink Time Difference of Arrival (UTDOA), and Enhanced Cell ID (E-CID). Some new positioning methods are also being specified for NR: Multicell Round Trip Time (Multi-RTT), Uplink Angle of Arrival (UL-AoA) and Downlink Angle of Departure (DL-AoD).

**Sidelink communication:** sidelink feature to enable direct communication between terminals.

Unlike LTE, the NR sidelink is being specifically designed first for the requirements of Cellular V2X (C-V2X), including vehicle-to-vehicle, vehicle-to-pedestrian and vehicle-to-roadside unit (RSU) communication.

While C-V2X in LTE is primarily designed for broadcasting of basic safety messages, NR will also support more advanced use cases with lower latency, larger payloads and higher data rates, as well as both groupcast and unicast modes. These capabilities will provide the foundations for operations such as platooning and remote driving.

**NR-Light:** A version of NR known as NR-Light is planned to be introduced in Rel-17, aiming to address use cases that cannot be met by NR eMBB, URLLC or mMTC.

The feature is intended to provide low-complexity solutions to address IIoT and other verticals in both FR1 and, as one of the distinguishing features compared to NB-IoT and LTE-M, also in mmWave frequencies (FR2). NR-Light is not intended to replace the mMTC low-power wide-area use cases currently supported via LTE-M/NB-IoT but will target the following requirements:

1. higher data rate and reliability, and lower latency, than LTE-M & NB-IoT.
2. lower cost/complexity and longer battery life than eMBB.
3. wider coverage than eMBB.

Specifically, NR-Light will address the following objectives and use cases:

1. Moderate data rates up to 100 Mbps to support, for example, live video feed, visual production control and process automation.
2. Moderate latency of around 10-30 ms to support, for example, remote drone operation, cooperative farm machinery, time-critical sensing and feedback, and remote vehicle operation.
3. Low-complexity devices with module cost comparable to LTE.
4. Coverage enhancement compared to eMBB.
5. Low power consumption with longer battery life than eMBB.

**Non-Terrestrial Networks (NTN):** NTNs are the key to supplementing the coverage of terrestrial networks and extending service provision to remote areas of the Earth, for example to support global IoT and asset-tracking. The most interesting deployment modes for NTNs are expected to use Low Earth Orbit (LEO) satellites and HAPS such as balloons and airplanes.

**5G Beyond 52.6 GHz:**

The NR Rel-15 physical layer channels were designed and optimized for frequencies up to 52.6 GHz. At higher frequencies, very large spectrum allocations in both licensed and unlicensed bands are expected to become available, which will enable extremely high capacity and data rates [26]. 3GPP has already nearly completed a study of use cases, deployment scenarios and requirements for the full frequency range 52.6-114.25 GHz, and this is expected to lead to a detailed study of technical considerations in Rel-17 and specifications in Rel-18.

A number of technical challenges exist at these frequencies. Since power amplifier (PA) efficiency and linearity decreases with frequency, a more efficient modulation scheme than OFDM is beneficial, such as single carrier modulation. The key to achieving reasonable efficiency is minimizing the PA back-off necessary to operate within the linear region, and this requires analysis with realistic PA models. It is also well known that local oscillator (LO) phase noise increases with carrier frequency, and to mitigate this it is necessary to consider very large sub-carrier spacings (SCS) (e.g. 960 kHz) and a re-design of the phase tracking reference symbols (PTRS).

Finally, at high mmWave bands a greater number of antenna elements are required to compensate for the pathloss, and this results in narrower beams, higher Equivalent Isotropic Radiated Power (EIRP), and path diversity solutions to increase the availability of Line-of-Sight (LoS) channels. Therefore, enhancements to beam management and handling of path diversity are also expected to be studied in the design of NR for this frequency range.