

Mobile Network Testing of 5G NR FR1 and FR2 Networks: Challenges and Solutions

Christoph Hausl, Julian Emmert, Manuel Mielke, Benjamin Mehlhorn and Corbett Rowell Rohde & Schwarz, Munich, Germany

This article describes a mobile network testing approach for 5G new radio (NR) using a passive scanner, which measures synchronization signal (SS)/physical broadcast channel (PBCH) blocks, or SSBs, broadcast from 5G NR base stations. It starts with relevant background information about 5G NR and mobile network testing, followed by a description of a typical measurement methodology for the frequency ranges one (FR1) and two (FR2). Next, it addresses two typical challenges: 1) finding carrier frequencies with SSBs and 2) network synchronization. A solution is proposed for each.

5G wireless radio access technology, known as NR, contains more flexibility to address different usage scenarios.^{1,2,3} The 5G NR specification allows optimization to reduce the latency and to significantly increase the data rate. These optimizations require many new technology components, including new frequency bands, beamforming support for synchronization and broadcast and multi-connectivity to enable the combination of 5G network elements with LTE. 5G NR supports operation in two frequency ranges: FR1 below 7,125 MHz⁴ and mmWave bands (FR2) between 24.25 and 52.6 GHz.⁵

Throughout the entire chain

of laboratory testing, field trials, network rollout, optimization and benchmarking, measurement tools for mobile network testing (MNT) are required to characterize the conditions of the wireless channel and network coverage in the field.^{6,7} For example, measurements of received power enable verification of 5G NR cell beamforming and its impact on the coverage area. Measurements of the channel impulse response result in deeper knowledge about the propagation of wireless signals in different environments, i.e., reflection, absorption and scattering in urban versus rural areas. Measurements of arrival times enable verification of network synchronization aspects.⁸

5G and associated technologies such as beamforming and frequencies above 3 GHz have raised potential health concerns due to the human exposure to the electromagnetic field of base stations. Consequently, 5G base station deployment requires that the electrical field strength (V/m) is below the specific threshold for each country. Frequency selective measurement methods of exposure to 5G base stations have been described,^{9,10} emphasizing the need for code selective measurement methods, especially in networks with several base stations and with data traffic.

A mobile network operator must evaluate the quality of the network to investigate network problems,

unwanted interference or assessment of new base stations. While it is possible to evaluate the performance of the network using a mobile phone, the disadvantage is measurement variation, as results vary depending on the chip set or installed software. Therefore, a reference measurement device such as a receiver or scanner is required, which provides a common ground for comparison.

With the use of non-standalone (NSA) and dynamic spectrum sharing, the 5G NR FR1 and corresponding LTE channel must be measured at the same time to ensure that both network links work as expected. Detection and measurement of these base station cells is challenging because the measurement must achieve a high sensitivity while avoiding false alarms that result in detecting non-existing cells (i.e., ghost codes).

Measurement of the carrier frequencies of a mobile network enables independent characterization of the network and, together with a wideband passive receiver, enables benchmarking of different networks—even networks that are completely unknown—removing the influence of the mobile phone. As this measurement approach is completely passive, all public and private networks, such as campus networks, can be detected and measured.

BACKGROUND

5G NR Synchronization Signal/PBCH Blocks (SSBs)

5G NR technology uses orthogonal frequency division multiplexing (OFDM)² for downlink transmission. A band dependent table^{4,5} defines whether time division duplexing (TDD) or frequency division duplexing is used to divide the downlink

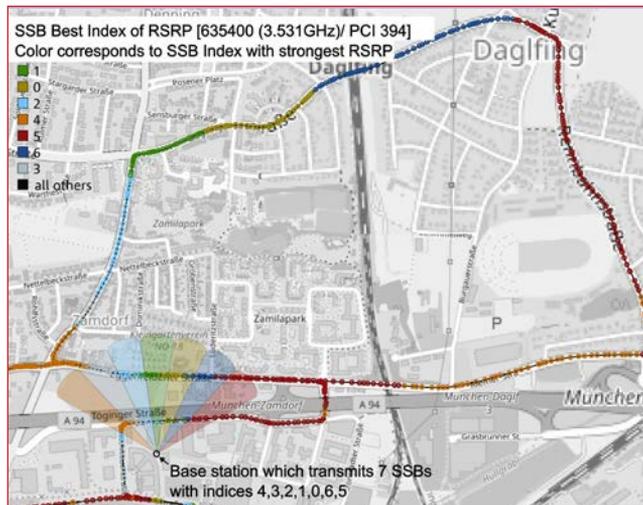


Fig. 1 Transmission direction of seven SSBs of one cell estimated by comparing the measured received power for all SSBs during a drive test. The color of the route corresponds to the SSB with the strongest receive power.⁷

(DL) and uplink (UL). A 5G NR cell broadcasts SSBs to enable cell search and initial access. One SSB is mapped to four OFDM symbols and 240 subcarriers (SC).

The SSB consists of one PBCH block, a primary and a secondary synchronization signal (PSS and SSS). There are different SC spacings (SCS) defined: from 15 kHz for Case A in FR1 to 240 kHz for Case E in FR2.¹¹ Therefore, the bandwidth of one SSB is between 3.6 and 57.6 MHz. Correspondingly, the SSB duration is between 285 and 18 μ s, enabling flexibility to use 5G NR in different frequency ranges and use cases.¹

One cell transmits up to 64 SSBs within a 5 ms window (i.e., up to four or eight SSBs for SCS of 15/30 kHz). Each of these SSBs has a specific index, which is encoded beside the cell-specific physical cell identity (PCI) into the SSB-signal. The start time of a SSB within the 5 ms window depends on the index, as defined by the 3GPP technical specification.¹¹ The cells broadcast these 5 ms windows periodically, with the default period 20 ms.

Typically, a cell uses beamforming to transmit the SSBs in different directions (i.e., beam sweeping) and, consequently, the SSBs are also referred to as beams. These beams can be considered as micro sectors that further split the macro sector of the complete cell—typically 120-degree azimuth coverage—

into smaller angular portions.⁶ **Figure 1** illustrates the main transmission direction of seven SSBs of one cell on a map. The use of beamforming for synchronization signals and PBCH provides better overall coverage. Note that the direction of the beams can be two-dimensional in the sense that each SSB transmits into a specific azimuth and tilt angle.

Mobile Network Testing

Figure 1 also shows the route of a drive test, a method often used for MNT. The aim of the drive test is to measure the reception quality of the base station cells and their SSBs to determine network quality and coverage. The drive tests are also used to find interference, either from other cells or unlicensed deployments. Variations of conventional drive tests are walk tests, bike tests and drone tests, the latter requiring small passive receivers with low power consumption because of limited battery capacity.

MEASUREMENT SETUP

Sub-6 GHz Measurement Setup

Figure 2 shows the proposed measurement setup with a passive receiver or scanner, such as the R&S TSME6 mobile network scanner. Fed by an external antenna, the scanner measures the wireless signal from 5G FR1 and LTE cells, converts this signal into a digital baseband signal of I/Q symbols and sends it to a connected laptop for demodulation, analysis and presentation. The scanner contains an internal global navigation satellite system (GNSS) receiver to measure its geographical position, as well as receiving date and time information. For security reasons, the scanner itself is a passive receiver with no transmission capability. It can measure a baseband signal with a bandwidth of 20 MHz between 350 MHz and 6 GHz, the frequency range controlled by the measurement software on the laptop. The measurement software can be based on R&S ViCom, an open application programming interface, which enables custom scanner applications. Alternatively, ready-to-use software such as R&S Romes can be used.

FR2 Measurement Setup

The carrier aggregation framework in 5G NR allows complementary operation in FR2 with an FR1 carrier to ensure good coverage,¹ requiring simultaneous SSB measurements in FR1 and FR2. **Figure 3** shows the measurement setup for FR2. It requires a down-converter which converts the mmWave signal to an intermediate frequency below 6 GHz, so a single scanner with dedicated antennas can support simultaneous measurements in FR1 and FR2. One single scanner with one down-converter supports SSB measurements in FR2, and it is possible to connect several scanners with one down-converter, extending the baseband bandwidth to 100 MHz; however, this is not necessary for current applications.

CHALLENGE 1: HOW TO ANALYZE THE 5G NR SSBs?

Accessing or measuring a 5G NR carrier starts with discovering the center frequencies of the SSBs. In LTE, the PSS/SSS and PBCH signals are always transmitted around the center frequency of the carrier with fixed periodicity, making it possible to manually detect them in the power spectral density measured with a receiver. In 5G NR, however, the transmission characteristics of the SSBs are more flexible, creating new challenges to configuring a 5G NR receiver/scanner.

The most challenging problem is the flexibility regarding the SSB center frequency (SSRef). The 3GPP standard defines a frequency raster for the appearance of SSBs,^{4,5} but the raster is narrow with hundreds of possibilities within a 5G NR carrier. Further, a single SSB only appears for a short time, so it is difficult to detect the SSB with a traditional swept-tuned spectrum analyzer; the SSB periodicity is flexible with the frame starting point and its corresponding period: 5, 10, 20, 40, 80 or 160 ms.¹²

To avoid time consuming spectrum scans, wrong scanner configuration or simply guessing the correct SSB center frequency, the proposed receiver/scanner solution is detecting the SSRef using an algorithm called Automatic Channel Detec-

tion (ACD). ACD can search quickly through large frequency ranges, where it runs an internal spectrum scan and searches for SSBs.¹³ ACD delivers the correct SSRefs within seconds, enabling the scanner to analyze both in-band and out-of-band, i.e., competitor networks where the cellular network parameters are completely unknown.

The ACD algorithm first provides a list of the SSB center frequencies; then, the scanner starts the SSB measurement algorithm (SSBmeas) for these frequencies. ACD can run in the background of the baseband processing, continuously searching for new SSB center frequencies. As soon as the scanner receives the signal of a base station cell strong enough for ACD sensitivity during a measurement, the corresponding SSRef will be scanned with the more sensitive SSBmeas for the remaining portion of the measurement. The ACD algorithm expects a 3GPP compliant 5G NR SSB transmitted on frames with an increasing system frame number. Internally, it uses the 3GPP band table to select the SSB transmission case for the selected frequency bands. This accelerates the ACD algorithm and avoids

checking for unnecessary cases (e.g., Case E for band n1). From the SSB measurement, many network features can be obtained to assess network quality, such as synchronization signal signal-to-interference-plus-noise ratio (SS-SINR) and synchronization signal reference signal received power (SS-RSRP).¹⁴ It is also possible to extract the cell identity (PCI), the SSB index, the channel impulse response and the arrival time for all detected cells and beams. SSB de-

tection includes a decoding of the PBCH, preventing ghost codes, as the PBCH payload contains a cyclic redundancy check for error detection.

Figure 4 illustrates the measured arrival times of peaks of the channel impulse response for SSB-indices 0 and 2 of two cells (PCI 75 and PCI 362) at SSRef 3,574.56 MHz (Case C). The measurement is primarily interested in the arrival time difference to the first measured peak to measure the delay spread. The measurement confirms the expectation¹¹ that the SSB with index 2 is transmitted 500 μ s later than SSB with index 0. From **Figure 4**, the distribution of the peaks indicates how much reflection and scattering occurred with higher delay spread for index 0. The signal of the cell with PCI 362 arrives approximately 2 μ s later than the one from the other cell with PCI 75, which is mainly caused by the larger cell-to-receiver distance for PCI 362.

CHALLENGE 2: NETWORK SYNCHRONIZATION MEASUREMENTS

Ensuring base station synchronization is a critical component for

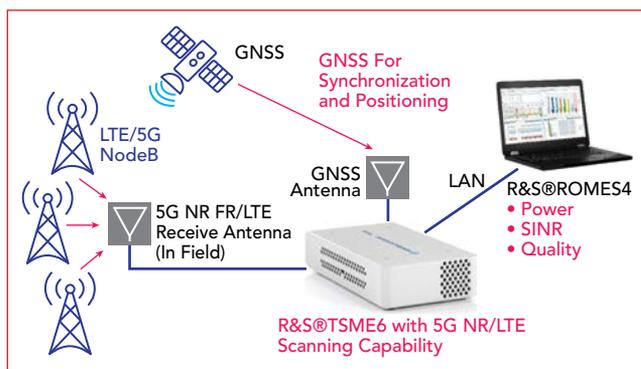


Fig. 2 Setup for sub-6 GHz measurements of 5G NR FR1 and LTE signals.

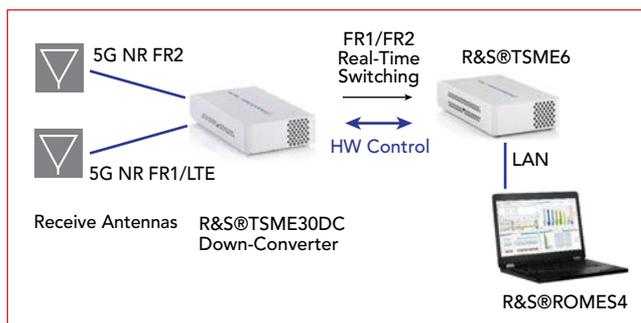


Fig. 3 Setup with mmWave antenna and down-converter for simultaneous 5G NR FR2 and sub-6 GHz measurements.

successful network deployment. If a base station is out of sync, the handover of active connections will fail, leading to dropped calls for the user and a poor user experience. For TDD, the synchronization requirement is particularly crucial, as a time offset can lead to an overlap of uplink and downlink time slots, im-

pairing base station performance and interfering with correctly synchronized neighboring base stations (see **Figure 5**).

The allowed time alignment error is specified by the 3GPP (Release 15, Section 6.5.3). To ensure proper synchronization, the cells receive their reference time from the network or via a connected GNSS receiver.⁸ Networks of different operators must be synchronized to avoid interference due to intermodulation products between networks on neighboring frequencies. This enables all operators to minimize interference.

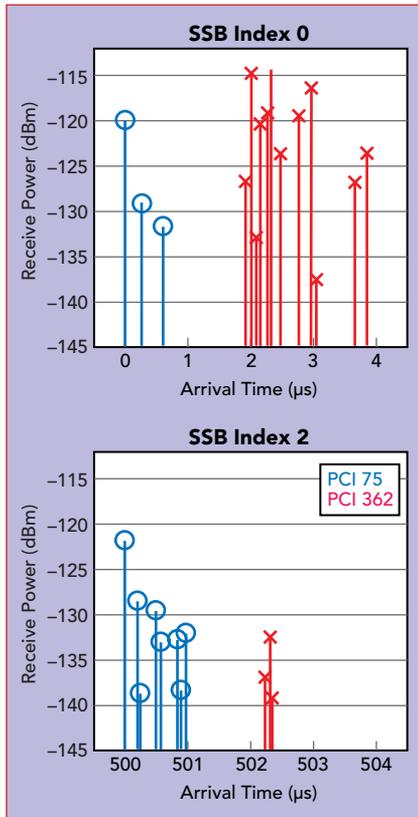
Previously, these timing measurements were performed with a spectrum analyzer and special test ports on the base station, requiring cabled measurements. In 5G NR, the common deployment of remote radio heads and active antenna systems without special test ports makes conventional timing measurements difficult and requires over-the-air timing measurements.

To verify the time synchronization of a network, the proposed scanner uses two possible measurements of varying precision: 1) a time of arrival (ToA) measurement of the received SSBs and 2) a time alignment error (TAE) measurement of the received SSBs. The ToA measurement provides a time stamp for the received SSB. This provides a good indication whether a certain base station cell is out of sync compared to other base stations received. The ToA measurement pro-

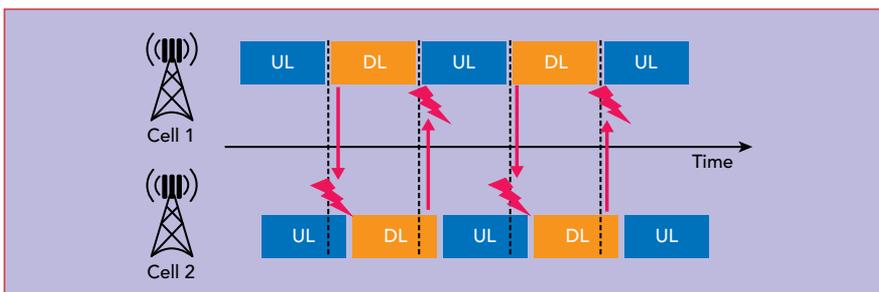
vides a precision of about 400 ns. To achieve higher precision and fulfill the coordinated universal time (UTC) second synchronicity requirement, a TAE measurement is used.

For the TAE measurement, line-of-sight (LoS) to the cell is required where the distance between measurement antenna and cell antenna is known—which can be measured with a laser range finder—together with good GPS reception or an external time base as the time reference. The receiver/scanner can calculate the UTC transmission time of every received SSB as well as the frequency error of the cell (see **Figure 6**). Measurement precision is then dependent on the provided reference of the integrated GNSS receiver. Good GPS reception yields a time accuracy below 30 ns. From the known distance between measurement position and base station, the transmit time can be calculated, identifying timing issues rooted in the setup of the base station. Experimentally, it has been verified that the following conditions need to be fulfilled to enable such a precise measurement:

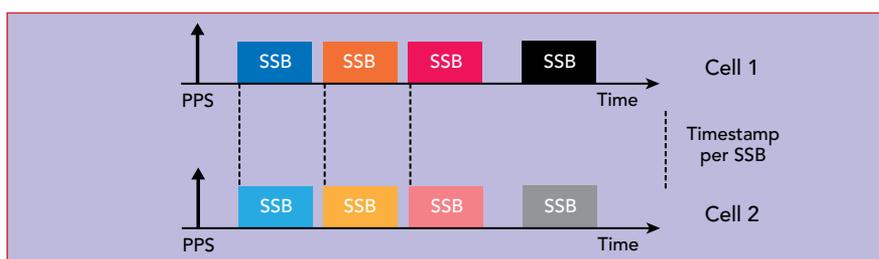
- The signal from the measured base station must have a SINR above 15 dB
- The delay spread needs to be below 17 ns, which is used as indicator for LoS
- To obtain best performance with a GNSS receiver, movement faster than 30 kmph is recommended to remove reflections from the received signals.
- A high accuracy pulse per second (PPS) signal must be available, either from the GNSS receiver or an external connection
- The PPS signal needs to provide higher accuracy than the internal time base
- The GNSS receiver must report a valid UTC time synchronization.



▲ Fig. 4 Measured arrival times and channel impulse response of SSB indices 0 and 2 for two cells.



▲ Fig. 5 Interference between two cells.



▲ Fig. 6 UTC synchronized base stations.

CONCLUSION

This article demonstrated how to use a passive scanner for measurements in 5G NR networks, with special attention to network synchronization in both the FR1 and FR2 bands. Methods for the measurement of network coverage, network synchronization and channel impulse response were proposed and

are straightforward to implement. An approach for ACD to find the relevant carrier frequencies for 5G MNT in networks with an unknown configuration was presented. Finally, the proposed methods were applied for deployed 5G networks to demonstrate effectiveness.

References

1. X. Lin, J. Li, R. Baldemair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grövlén and K. Werner, "5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology," *IEEE Communications Standards Magazine*, Vol. 3, No. 3, September 2019, pp. 30-37.
2. S. Ahmadi, "5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards," *Academic Press*, 2019.
3. M. Kottkamp, A. Pandey, D. Raddino, A. Roessler and R. Stuhlfauth, "5G New Radio: Fundamentals, Procedures, Testing Aspects," Rohde & Schwarz, 2019.
4. "3GPP Technical Specification TS 38.101-1, NR; User Equipment (UE) Radio Transmission and Reception; Part 1: Range 1 Standalone," 3GPP, V16.8.0, June 2021.
5. "3GPP technical specification TS 38.101-2, NR; User Equipment (UE) Radio Transmission and Reception; Part 2: Range 2 Standalone," 3GPP, V16.8.0, June 2021.
6. A. Sibila, "5G NR Network Rollout is Now – Let's Test!" *Microwave Engineering Europe*, July 2019.
7. M. Mielke and M. Hysten, "5G NR Network Measurements using Network Scanners and Advanced Data Analytics," Rohde & Schwarz, Version 3.0, April 2019.
8. S. Rufini, M. Johansson, B. Pohlman and M. Sandgren, "5G Synchronization Requirements and Solutions," *Ericsson Technology Review*, January 2021.
9. S. Aerts, K. Deprez, D. Colombi, M. Van den Bossche, L. Verloock, L. Martens, C. Törnevik and W. Joseph, "In-Situ Measurement Methodology for the Assessment of 5G NR Massive MIMO Base Station Exposure at Sub-6 GHz Frequencies," *IEEE Access*, Vol. 7, December 2019, pp. 184658-184667.
10. C. Bornkessel, T. Kopacz, A. M. Schiffarth, D. Heberling and M. A. Hein, "Determination of Instantaneous and Maximal Human Exposure to 5G Massive-MIMO Base Stations," 15th European Conference on Antennas and Propagation, 2021.
11. "3GPP technical specification TS 38.213, NR; Physical layer procedures for control," 3GPP, V16.6.0, June 2021.
12. "3GPP technical specification TS 38.331, NR; Radio Resource Control (RRC) protocol specification," 3GPP V16.3.1, January 2021.
13. O. Wanierke, "Method and System for Channel Detection," U.S. Patent No. 10,833,800. U. S. Patent and Trademark Office, 2020, Web: <https://patents.justia.com/patent/10833800>.
14. "3GPP Technical Specification TS 38.215, NR; Physical Layer Measurements," 3GPP, V16.4.0, December 2020.