WLAN traffic offload – bypass for crowded mobile networks

WLAN traffic offload – the rerouting of mobile data traffic to WLAN networks – is an interesting alternative for network operators to cope with the constantly growing data volume. Now that the specification has been completed, test operation for the new feature is the next major obstacle to be taken prior to the official launch. The test systems play a key role, since they have to ensure smooth interoperation of a wide variety of different components used in these complex systems.

It is foreseeable that even the most advanced mobile networks will reach their capacity limits before long. This is mainly due to the increasing consumption of videos via smartphones and tablets. Since the lion's share of the resultant data volume is generated inside buildings, WLANs can be used as economical alternatives and addition to mobile networks, provided that access points are available. The two types of network ideally complement each other. While mobile networks provide comprehensive coverage for mobile services, broadband WLANs reduce the load on mobile networks for indoor applications.

The underlying technology is referred to as WLAN traffic offload; it basically works in combination with any mobile communications standard (GSM, WCDMA, CDMA2000®, LTE, etc.).

The advantages for network operators are obvious. Almost all modern mobile devices have a WLAN interface. The acquisition costs for access points (WLAN access points – WLAN AP) are relatively low. What is more, WLANs use two license-free frequency blocks at 2.4 GHz and 5 GHz within the ISM bands that lie outside those assigned to cellular standards.

Before the launch of WLAN traffic offload, the standardization bodies of 3GPP and IEEE had to expand a number of standardized protocols and procedures.In the following, we will focus on how this feature works with LTE.

Authentication and authorization

When gaining access to the core network of a mobile network operator via WLAN, it must be ensured that access is authorized. As with the cellular standards, this is verified using the SIM card in the mobile device. To avoid having to enter the password and to facilitate a seamless transition, the same procedure is applied as would be used with a secure WLAN AP. A number of protocols has been defined to enable the SIM card data to be automatically compared via WLAN on the network operator's authentication server (extensible authentication protocols – EAP) and incorporated into the diverse cellular standards.

Policy – the rules of the network operators

Network operators can balance the load on their networks using a set of rules, known as policy. For this purpose, mobile devices are for instance informed what WLAN APs are available where and when for the offloading of what data services (audio or video telephony, Internet services, etc.). This makes it easier especially in metropolitan areas to find WLAN APs that are suitable for offloading, and helps smartphones save energy at the same time. The policy is distributed to the mobile devices by the access network discovery and selection function (ANDSF) server via Open Mobile Alliance (OMA) device management, and the subscribers can query the information where necessary. The signal field strength at the WLAN AP is also a key criterion for the use of LTE-to-WLAN traffic offload. The mere presence of a WLAN AP is not sufficient; a specified minimum field strength must be available (Fig. 1). If the required field strength is no longer present, the connection is terminated and the device returns to LTE.

LTE or WLAN?

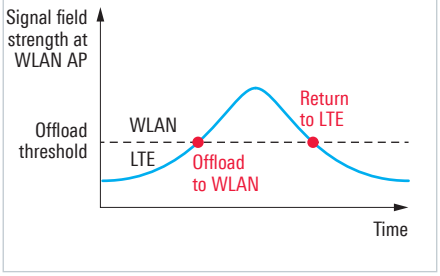


Fig. 1: WLAN traffic offload takes place only if a minimum signal field strength is present at the WLAN access point.

Encryption

Protection against eavesdropping is also required. Let us assume that a mobile subscriber makes a video telephone call with a subscriber in the LTE network via a freely accessible WLAN AP. To ensure data protection, additional encryption is provided by establishing an IPsec tunnel to the smartphone via the WLAN AP starting from the firewall in the LTE core network (Fig. 2).

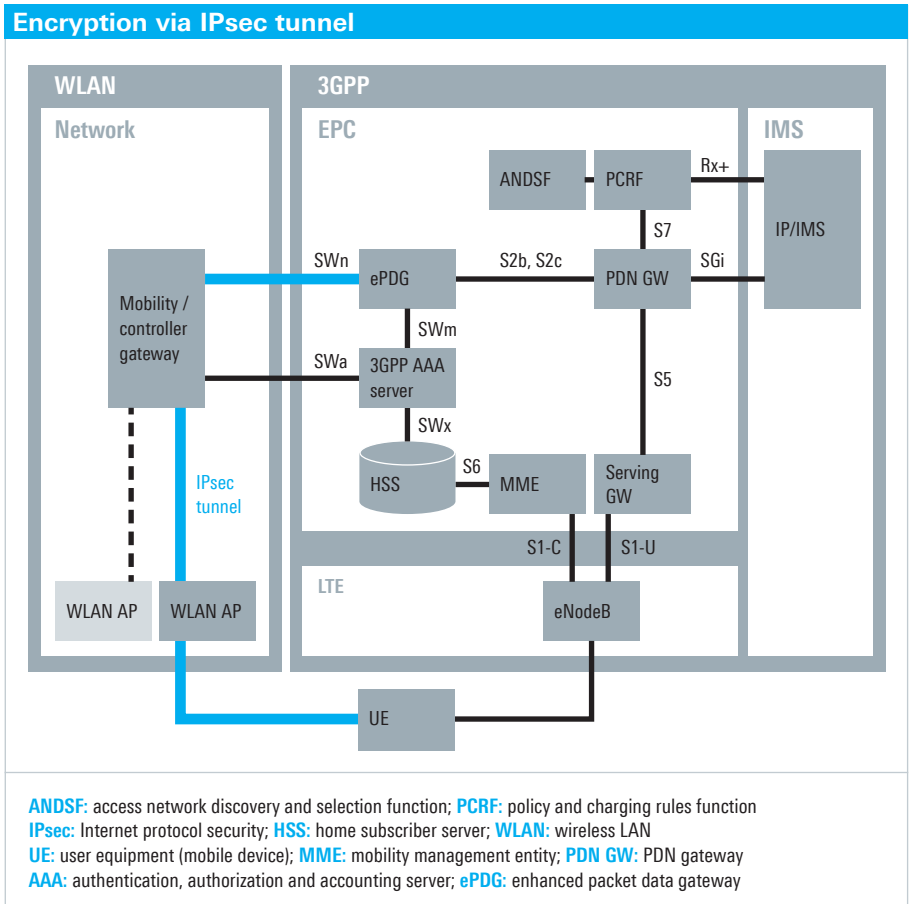


Fig. 2: Protecting communications from unauthorized access: Additional encryption is provided by establishing an IPsec tunnel to the smartphone via the WLAN AP starting from the firewall in the LTE core network.

Automated and accelerated WLAN access

The IEEE 802.11 standardization group has expanded the WLAN access protocol in a new version (Amendment IEEE 802.11u) to include the access network query protocol (ANQP). This protocol automates and accelerates the WLAN access of smartphones to the mobile network. Even before the actual connection with the WLAN AP is made, the smartphone receives information about 3GPP mobile networks or roaming consortia that are accessible via the WLAN AP. The Wi-Fi Alliance issues a certificate (Wi-Fi Hotspot 2.0, also known as Passpoint™) to ensure uniform implementation of the new standard and a maximum degree of interoperability for certified WLAN components.

The IEEE 802.11u amendment added further information to the beacons that a WLAN AP transmits every 100 ms (Fig. 3). Before the connection with the WLAN AP is actually established, which takes place after an authentication and association procedure, the smartphone can use the ANQP to determine via the new generic advertisement service (GAS) whether a WLAN AP can be used for an offload.

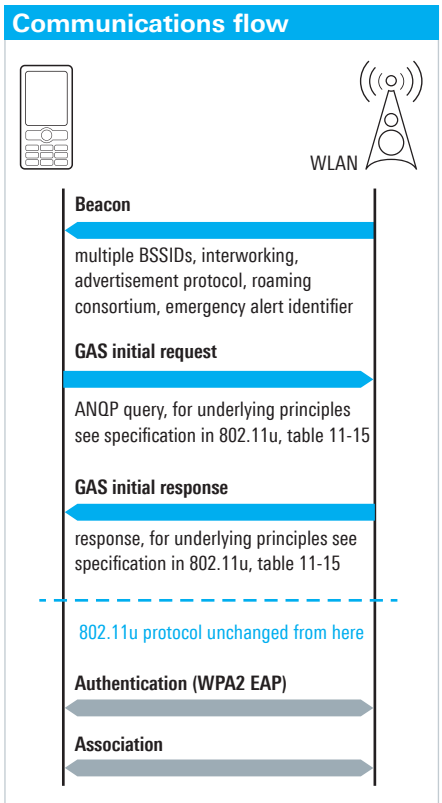


Fig. 3: Additional information in the beacons provides the smartphones with criteria as to whether a WLAN access point is suitable for traffic offload.

Network change – ideally unnoticed by subscriber

An important precondition for the acceptance of WLAN traffic offload is an uninterrupted transition between a mobile network and a WLAN. No interaction or entry should be needed on the part of the subscriber; in the ideal case, the subscriber should not notice the transition at all.

Interruption-free continuation of IP-based services after a mobile cell change or change of the radio access technology (RAT) calls for IP flow mobility. In a world in which communications are based on a client/server architecture, this requires intelligent address management with dynamic IP address assignment. This has been achieved with a number of protocol amendments by 3GPP and enhanced IP addressing.

High demands placed on verification test systems

Comprehensive tests need to be carried out to ensure that all system components are implemented uniformly and in conformity with the standards. The tests focus above all on the mobile device as the pivotal element of the standard amendment. The device under test (DUT), with its particularly critical interface to the user, takes on vital significance in this scenario. In the tests, the DUT is connected with the test setup via both WLAN and LTE.

The test setup for LTE-to-WLAN traffic offload includes the following main components:

- Emulation of an LTE base station, including the LTE core network
- Emulation of a WLAN AP (HotSpot 2.0 or Passpoint)
- Gateway / firewall at the entrance to the LTE core network from the WLAN end
- IMS server for implementing real-world applications such as video or speech telephony
- Message analyzer for recording all protocol messages between the DUT and the WLAN AP and the LTE base station

The individual components are either networked to form a test system or, as with the R&S®CMW500 wideband radio communication tester (Fig. 4), are integrated into a single device. As a general rule, to ensure that tests are reproducible, professional instruments should be used and the number of commercial system components reduced to a minimum.

Fig. 4: The R&S®CMW500 offers, in a single box, all that is needed to carry out the tests required to verify LTE-to-WLAN traffic offload functionality.

Custom solutions for every test requirement

For the integration of the LTE and the WLAN protocol stacks, tests on the lower protocol layers are needed in an early development phase. The required signaling tests can be performed with the R&S®CMW500 and suitable medium level application programming interface (MLAPI) test scenarios.

The R&S®CMW-KF650 option contains a package with roughly 50 test scenarios. They range from establishing a connection with the gateway of the LTE core network (ePDG) to authentication and to changing the IP service from LTE to WLAN and back. The appropriate source code and interface description are also provided, allowing test scenarios to be adapted to individual test requirements.

Using the MLAPI test scenarios offers a very wide range of testing options for the lower protocol layers, but requires expert programming knowledge. An alternative is R&S®CMWcards (R&S®CMW-KT022), a graphical user interface that resembles a card game. This tool makes it possible to compile signaling tests without requiring any specific programming skills (Fig. 5).

To be able to ensure smooth communications in their networks, network operators specify test cases that all devices wishing to use their services must pass. For a number of network operators, Rohde & Schwarz offers options to verify LTE-to-WLAN traffic offload functionality, e.g. R&S®CMW-KO576 and R&S®CMW-KO569.

The R&S®CMW500 can be used as a callbox for the development and verification of the WLAN traffic offload feature. In this case, tests range from verifying the DUT's RF characteristics to functional tests, including analysis of the LTE and WLAN protocol messages.

Protocol analysis

The possibility to record LTE and WLAN protocol sequences at the same time is a major bonus when it comes to

Fig. 5: The R&S®CMWcards graphical user interface for the R&S®CMW500 makes it very easy to compile signaling tests in line with the specification.

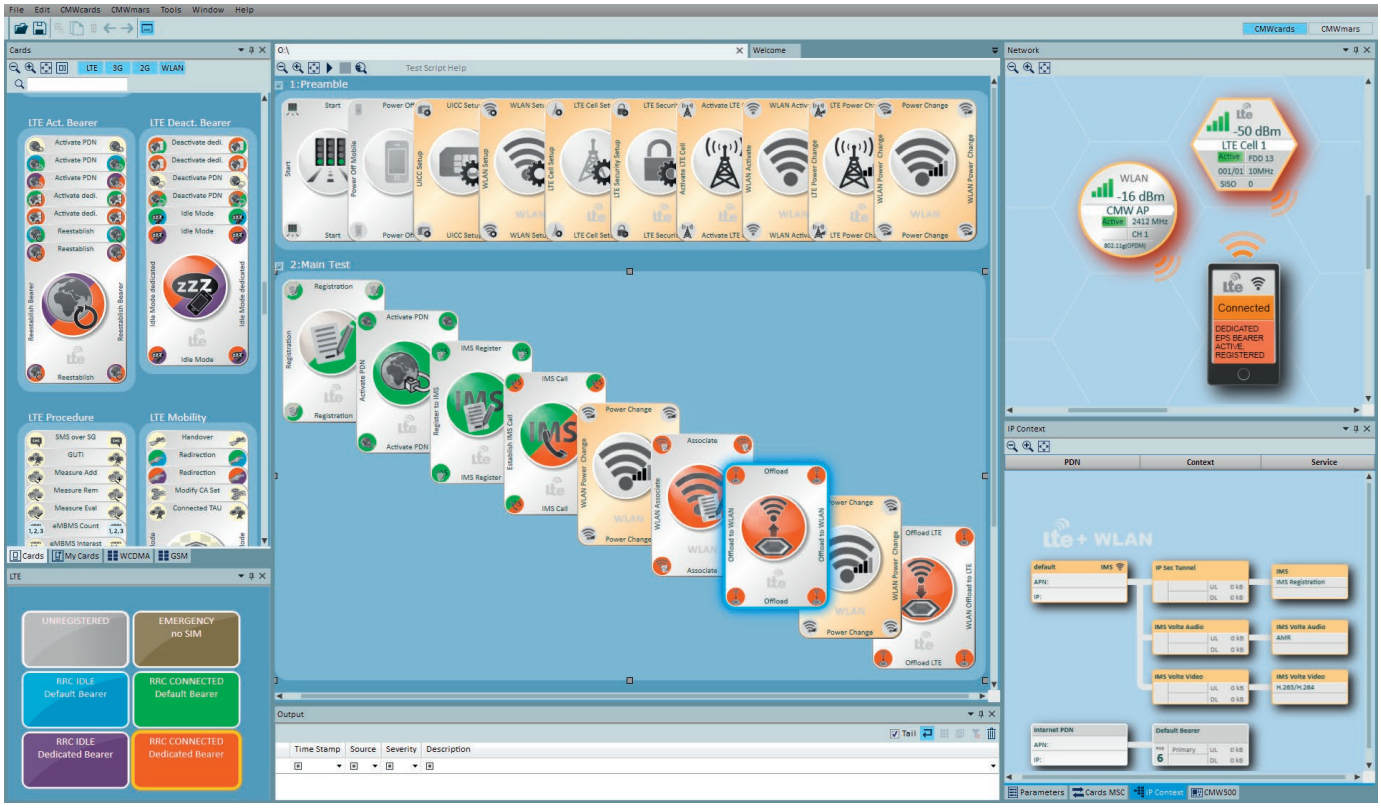
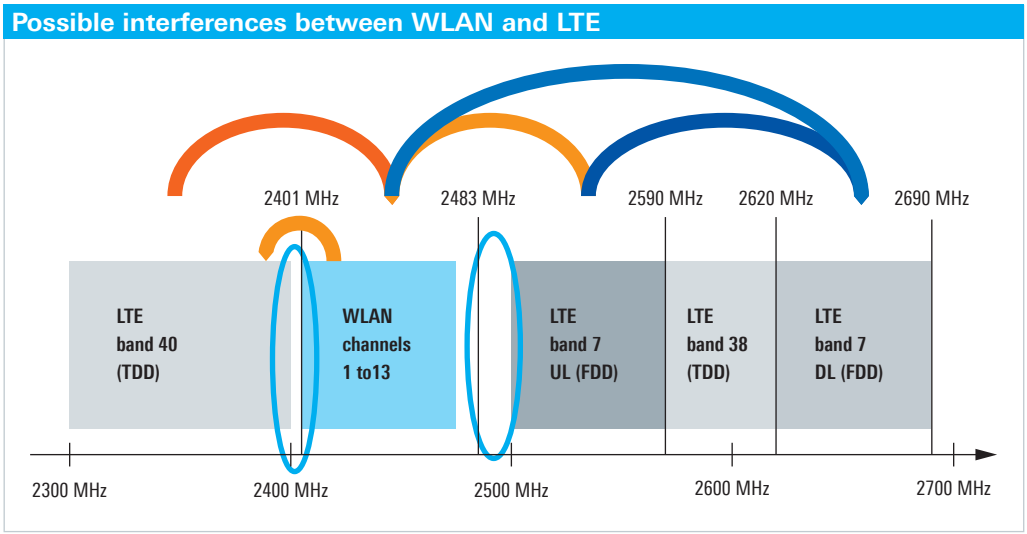


Fig. 6: Mutual interference between WLAN in the 2.4 GHz ISM band and the LTE bands 7 and 40 is particularly critical.



verifying whether the process is operating according to standard, discovering any errors or optimizing the process. The R&S®CMWmars message analyzer can be used, for example, to verify whether a smartphone has established a Hotspot 2.0 compliant connection with a WLAN AP. The message analyzer records data messages and protocol information across several layers of the ISO OSI model. Filters can be set to record precisely what is required.

Packet loss and performance test

The change of a data service, such as a video telephone call, from LTE to WLAN should take place without interruption wherever possible and with no data packet loss. In addition to a visual check, this can be verified in detail using the message analyzer, which is also a valuable tool for error correction. Moreover, for data services, the minimum requirements as to the stipulated data transmission rates are to be verified under a variety of conditions and operating modes. In general terms, such quality of service (QoS) criteria, including round trip time, form part of comprehensive IP data analyses.

In-device coexistence test

Ensuring operation in conformity with the standards is not the only vital issue when testing WLAN traffic offload functionality. Another focus is on determining interference between two radio standards used at the same time within a mobile device and avoiding this interference as far as possible. In-device coexistence tests are performed to measure interference caused by the LTE transmitter to the WLAN receiver as well as interference caused by the WLAN transmitter to the LTE receiver within a smartphone. To this end, for instance, a smartphone could transmit a video on LTE band 7, while a receiver quality test (PER measurement) is carried out at the same time on WLAN channel 13, which is only 17 MHz away. In the ideal case, no interactions will be detected here, and the PER measurement will provide the same result as would be obtained without an LTE transmission. As can be seen in Fig. 6, possible mutual interference between WLAN in the 2.4 GHz ISM band and the LTE frequency bands 7 and 40 is particularly critical. While mutual interference between LTE band 40 and the WLAN channels needs to be investigated, it can be presumed that the interference caused by the transmission from LTE band 7 only affects WLAN reception.

Summary

Even if full use is made of the data transmission rates that are theoretically possible according to Shannon in today's mobile networks, it is only a matter of time before available capacities are no longer able to meet increased data throughput requirements. Alternative solutions need to be found. WLAN traffic offload is a promising technology that can significantly reduce the load on mobile networks. Following specification and standardization, there will now be a test phase prior to rollout. During this phase, suitable test systems will be needed above all. The R&S®CMW500 makes it possible to realistically simulate the entire system and to carry out all relevant tests.

Thomas A. Kneidel