WLAN Protocol Tester R&S®PTW70

Multimode protocol analysis in WLANs

You can find IEEE 802.11-based WLANs in all types of environments:
- in wireless home networks but also
- in company and campus networks
- or in giant hotspots for providing coverage for complete cities. As a result, the requirements placed on protocol testers are quite complex and demanding.

Designed for high performance

At first glance, the R&S®PTW70 is quite simple in design (FIG 1). The tester does not even have a display since one would be of little use for graphically displaying the results of complex protocol analysis anyway. The actual strength of the new protocol tester is its convenient and extremely powerful control software which can be installed on any PC running on Windows®. The link between the controller and the protocol tester is established via a LAN. This concept is ideal since it allows the highly versatile use of the protocol tester via remote control.

From a classic protocol tester to a general-purpose instrument

The main task of a protocol tester is to check DUTs for compliance with standard specifications (conformance tests). To ensure a uniform test procedure covering all relevant scenarios, the standardization bodies usually specify protocol conformance tests. This is mostly done in the TTCN language (TTCN = tree and tabular combined notation), which was specially developed for this purpose and is used, for example, for the 3G standards and Bluetooth®.
The IEEE 802.11a/b/g standards, however, do not use this language. Instead, golden device tests are defined to ensure interoperability. During these tests, a DUT is checked for correct operation in conjunction with several other reference units.

The drawbacks of this indeed very pragmatic approach soon become evident. The selected reference units have a significant influence on the result. A possible malfunction does not give many clues to the actual source of error since it could have also been caused by one of the reference units. Many scenarios cannot even be tested with this method. There are no invalid behavior tests at all. During these tests, the response of the DUT to malfunctions of the counterpart is examined more closely.

The Protocol Tester R&S®PTW70 of course provides all conformance test functions. But Rohde & Schwarz is known for offering devices that far exceed standard requirements: A classic protocol tester would probably not be accepted in this difficult market. The new protocol tester was meant to go far beyond these standard requirements. In addition to the defined test cases, it was supposed to be flexible enough to handle a wide variety of tasks in non-conformance testing. This included not only multimode capabilities, but also the capability to adapt the test sequence as quickly as possible and without any special knowledge of the TTCN language, for example. The R&S®PTW70 meets these demanding requirements.

Multimode capability – versatility required

Multimode capability means that all important associated standards and extensions are supported by the R&S®PTW70. This includes IEEE 802.11a/b/g in the ISM and U-NII bands but also the Japan band. The protocol tester can be operated as an access point and station. Switchover is dynamic, i.e. the stack is not reloaded.

The R&S®PTW 70 has two main operating modes: the monitor mode for passive communication sniffing on the air interface and the active mode for triggering the communication stack. You can run the protocol tester in both modes at the same time. This allows direct control at any layer (LLC, MAC, PHY). These characteristics make the R&S®PTW70 ideal for a variety of applications, e.g. retransmission tests, invalid behavior tests and stress tests.

The R&S®PTW 70 offers calibrated level measurements, a settable output level (–30 dBm to +10 dBm) and packet error ratio measurements. The high time resolution of 50 ns for recording protocol messages makes detailed problem analysis easy. You can send IP payload files through the protocol tester directly via the network interface.

Simple operation despite maximum flexibility

Even setting up a small WLAN home network can present problems, because so many parameters have to be defined. Imagine how complex a user interface for a protocol tester must be where practically every parameter down to the individual bits of a layer-1 message can be modified. Rohde & Schwarz solved this problem by using a hierarchical script user interface (FIG).

In the R&S®PTW70, scripts are not edited in text form but are created by means of a special graphical user interface. The structure is deliberately kept simple: You can program whatever you want without having to know a script language or higher programming language. Even so, this graphical user interface contains very complex functions, i.e. the timeout-controlled reception of messages, the evaluation of individual message fields and the generation of report files.

The IEEE 802.11 standard

IEEE 802.11 is an IEEE-specified family of standards for WLANS. The 802.11a/b/g standards are widely used. The 11b and 11g standards operate in the license-free ISM band at 2.4 GHz, 11a in the U-NII band at 5 GHz. The 11b standard uses DSSS modulation, whereas 11a and 11g operate with OFDM and 52 subcarriers that are modulated with BPSK, QPSK, 16QAM or 64QAM depending on the data rate. The 11g standard is backward-compatible with 11b. The 11b standard allows gross data rates up to 11 Mbit/s, 11a and 11g up to 54 Mbit/s.

Numerous expansions are available, e.g. 11e (quality of service enhancements) and 11i (security enhancements). Especially 11i uses encryption technologies other than WEP, which was originally used and was less safe.

Interestingly, the very similar European ETSI standard HiperLAN/2 basically specifies many of the subsequent 802.11 expansions. However, HiperLAN/2 could not match the 802.11 standard, which was promoted much faster.
Scripts run directly on the protocol tester and are therefore independent of the network connection or the load on the controller. A script is downloaded to the protocol tester and then compiled so quickly that you may think that the script was executed immediately. Together with the convenient test step editor, scripts can thus be modified and executed again within seconds.

Uncompromising online data analysis

The message analyzer (FIG 3) supports detailed evaluation of protocol messages. The R&S®PTW 70 has uncompromisingly been designed for online analysis and high performance. While log messages are being recorded, you can navigate through all received messages and display their hierarchical structure in a separate window in fully decoded form. You can open multiple analysis windows with different software filters.

Internal data retention is so powerful that a very large volume of messages can be managed without any loss in performance. There is also no concern about a limited data buffer, a drawback quite common in other systems.

In addition to software filters, the protocol tester also contains hardware filters for adapting the primary message stream. These hardware filters can handle layer-1 messages as standard, for example.

You can store the messages in files and reload them for offline analysis. A script command can also be used to trigger the storage of messages. This is useful with automatic test sequences, for example, when you want to store message logs generated due to errors for later troubleshooting.

Full remote control also possible

The script interface can be remote-controlled via TCP/IP. By sending the script name and the parameters as ASCII text, the corresponding script will be loaded and immediately executed. Execution confirmation and return parameters or error messages will be returned. Any script created by the user, including parameterization, will immediately be available via the remote-control interface. Remote-control is thus dynamically expanded.

The TCP service port can be selected as needed and transferred as a start parameter. Since practically any script and programming language supports TCP/IP, you can easily integrate the R&S®PTW 70 into automatic systems without any special knowledge required.

Future prospects

Further interesting applications will be opened up for WLAN in the future, e.g. unlicensed mobile access (UMA), an initiative to expand mobile radio services in license-free bands via 802.11, for example. Thus, mobile phones will also transmit voice and data services economically via WLAN and be able to handle handover between the WLAN and the corresponding mobile radio network. The universal concept of the WLAN Protocol Tester R&S®PTW 70 readily enables the instrument to meet these new application requirements. And with 802.16, which is also known as WiMAX and is based on the OFDM transmission method, the next promising standard is already on its marks.

Frank Rieder
5

Test set
Low-level scripts
High-level script
Test step editor

Analyzer window
Message sequence chart
Decoder window
Scan window

News from Rohde & Schwarz Number 188 (005/IV)