narda
Safety Test Solutions

Jammers

High-resolution spectrogram analysis for reconnaissance and optimization of jamming systems for CDMA, TETRA, GSM, UMTS and LTE Services.

According to international telephony agreements, interfering with or suppressing wireless links is prohibited globally. There are, however, exceptions to this general rule, which nevertheless always require the official consent of the national telecom authorities. Examples include inside prisons and courtrooms, to prevent any prohibited communication, or within concert halls and other locations to avoid interruptions from disruptive telephone calls.

This Application Note looks at the effective legal application of jammers using a GSM link as an example. The results also give some indication of how to trace illegal jammers.

When jammers are used legally, the problem is basically to ensure that:
1 Wireless traffic is suppressed completely in all the three dimensions of frequency, time and space, and
2 Interference does not affect other areas at the same time.

Because of this, the aim will always be to radiate signals into the building to be protected, although this requires immense effort to ensure complete coverage. Having antennas within the building is advantageous.

When suppressing mobile communications, preventing reception of the downlink is a good idea, since the signals received by cell phones are at a relatively low level, and doing this effectively disables the phones.

Wideband jammers use FM or OFDM modulated signals, among others. These are only effective if they linger long enough to ensure that the now extremely powerful error correction of the communications channel is unable to compensate for the loss of information.

The jamming signal

The jamming signal shows up as an exaggeration in the noise floor, as depicted in figure 1. The signal can be generated using OFDM or using wideband pseudo-noise modulation. The noise floor starts just below the downlink band (925 – 960 MHz) and is easier to see because there are very few information signals superimposed on it there.

Figure 2 shows an FM emission that also overlaps the upper limit of the downlink range to some extent.

Both these images are examples of how a jammer can appear in a quick overview measurement outside a protected range.

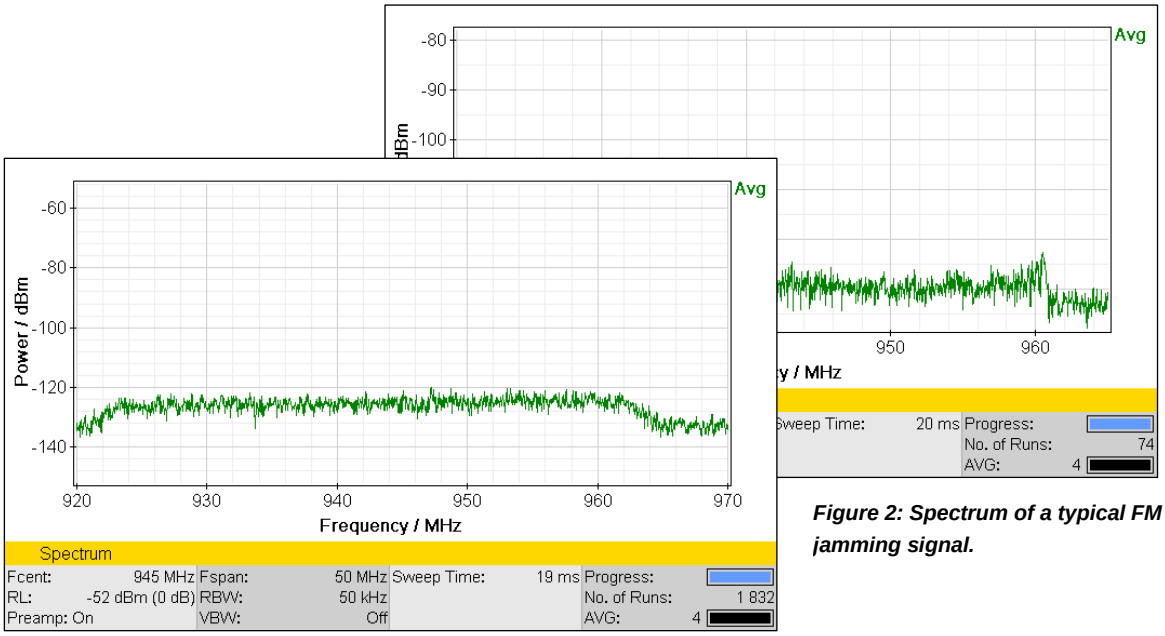

Figure 1: Downlink suppression by increasing the noise floor.

Figure 2: Spectrum of a typical FM jamming signal.

Interference and information signals in spectrograms

The conventional spectrogram based on just a few sweeps shows a jammer signal that starts just below 925 MHz and stretches across the entire displayed frequency range at intervals of 50 kHz. The jammer signal is blanked from the 9th to the 15th second for demonstration purposes.

A similar picture is seen regularly when measurements are made outside the irradiated area. The jammer is positioned inside the building, so it is screened from the outside by the structure itself. It is thus relatively effective but unobtrusive.

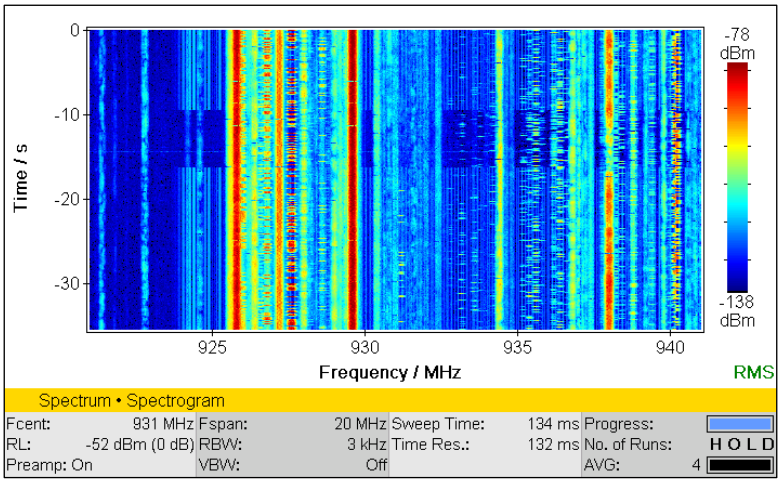

Figure 3 Jammer signal shown as a conventional spectrogram.

Interference and information signals in high-resolution spectrograms

The high-resolution spectrogram (HiRes Spectrogram) allows capture and display without any time gaps. Figure 4 shows a frequency range of 1.6 MHz. The time display range is zoomed in from 125 ms to 16 ms. The measurement was made outside the building. Although the interference lines from the jammer can be seen, their level is not high enough to suppress the GSM link.

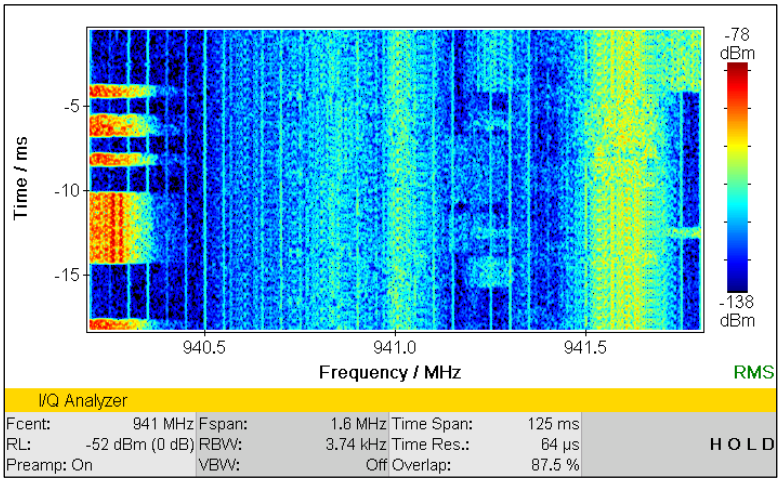

Figure 4: Gapless spectrogram. Zoomed display of field strength measurements made in front of the building.

The downlink signal level drops strongly and the level of the in-house jammer rises as strongly inside the building. Figure 5 corresponds to the previous image but shows the entire 125 ms.

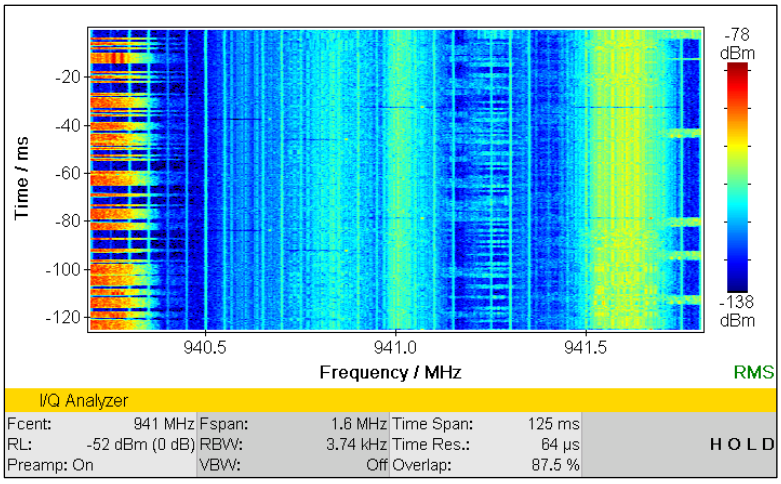

Figure 5: Gapless spectrogram. Field strength measurement inside the building, not zoomed.

In addition to the amplitude versus frequency, the persistence spectrum or luminance diagram shown in figure 6 also indicates the frequency with which each particular level occurs. This incidence display makes it possible to also see in-band interference signals. This is the same data set as was used for figure 5. The Interference and Direction Analyzer IDA 2 can produce all these different displays from the same data sets, allowing specialists to make crucial time correlative analysis.

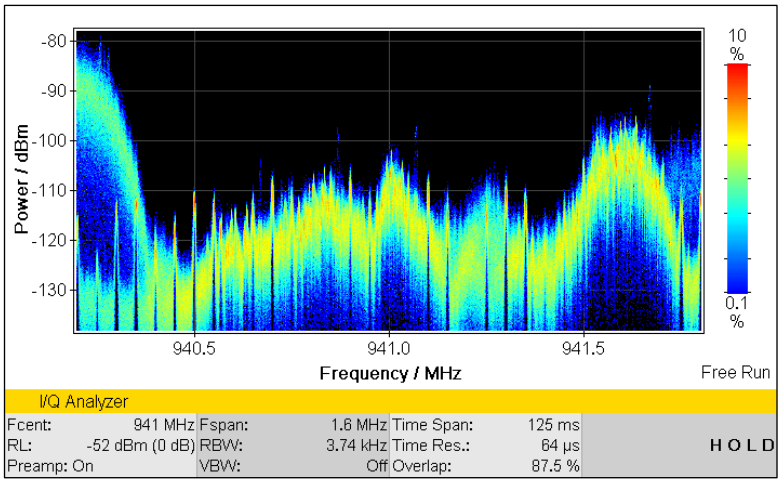

Figure 6: In-band interference detection by means of persistence display.

Checking the effectiveness of a jammer

A single jammer is not enough in most cases. Standing waves and shadowing occur in every room, and these also change according to the occupancy of the room. Such alterations are simply caused by moving, inserting or removing objects such as metallic items, musical instruments, containers, and the like.

A few main points:

- The required jamming power is least at the point of reception, so the downlink frequency is used for GSM.
- The jammer polarization is aligned to the information signal. Cross polarization is expedient for GSM.
- Spatial gaps can be minimized by radiating from different directions and / or by antenna diversity, i.e. by feeding the same signal to offset antennas.

A simple test using a cell phone merely shows a very incomplete picture. Where security is paramount, the frequency, location, signal amplitude and time must all correlate. FFT analyzers with a broad capture range (FFT span) are useful for this. No part of the signal is missed, thanks to gapless and overlapping FFT window computation.

The spectrogram algorithm of conventional spectrum analyzers is successive, i.e. the signal is acquired, processed, and displayed. This causes significant gaps in the display between the individual spectrums, because the sweeps (traces) or FFT blocks are arrayed one at a time.

In contrast, the block acquisition of 250,000 I/Q data pairs in HiRes mode of the IDA 2 captures a continuous data set from the demodulated base band with a width of up to 22 MHz. The recording time for this in this example stretches over 7.8 ms, which is more than one GSM frame. The display builds up quickly, so it can be used to directly show the relevant or worst covered points in the building or room that is to be protected.

It is important to check the GSM emissions regularly for any changes. This can be done continuously or at specific times of the day. It is usually enough to make a measurement at a few reference points such as in a particular room or at the corners of the building.

The gapless spectrogram display is better than the delta spectrum for emissions such as GSM because it shows all events in detail in their chronological relation.

Figures 7 and 8 are examples of an effectiveness test of a jammer. Both show an interference signal of about 20 MHz bandwidth. The same data set was used to generate the gapless spectrogram in figure 7 and the persistence diagram in figure 8. You can see at a glance that the effectiveness of the jammer is questionable at least at 925.7, 927.5, 929.6 and 938 MHz.

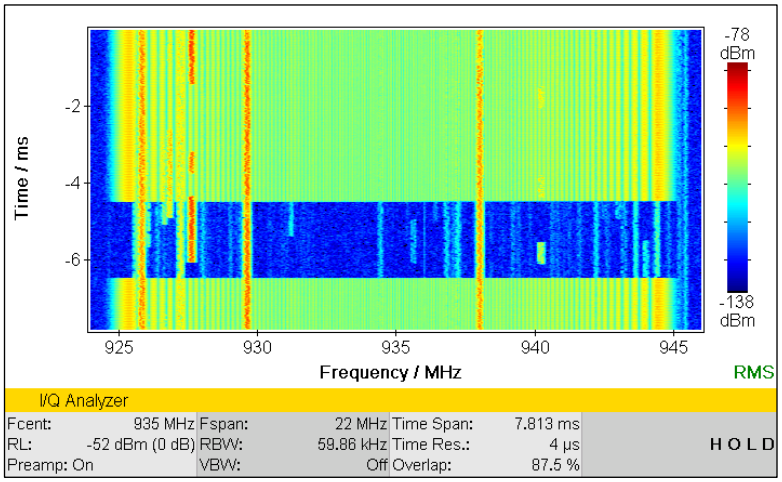

Figure 7: Gapless spectrogram. The weak signals can also be seen in the artificially generated blanking gaps in the jammer signal.

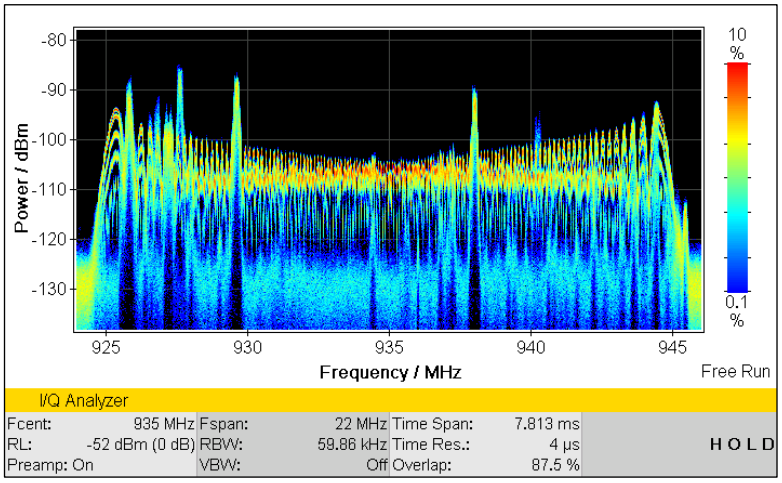

Figure 8: Persistence display. The weak signals can be seen here even without blanking the jammer.

All HiRes displays have their advantages. Since it is easy to save the data set on which they are based, they can all be regenerated and the spectrogram zoomed in detail at a later time.

Narda Safety Test Solutions GmbH
Sandwiesenstrasse 7
72793 Pfullingen, Germany
Phone +49 7121 97 32 0
info@narda-sts.com

Narda Safety Test Solutions
North America Representative Office
435 Moreland Road
Hauppauge, NY11788, USA
Phone +1 631 231 1700
info@narda-sts.com

Narda Safety Test Solutions GmbH
Beijing Representative Office
Xiyuan Hotel, No. 1 Sanlihe Road, Haidian
100044 Beijing, China
Phone +86 10 6830 5870
support@narda-sts.cn

www.narda-sts.com