

Jammer

Hochauflösende Spektrogrammanalyse zur Aufklärung und Optimierung von Jamming-Systemen für CDMA-, TETRA-, GSM-, UMTS- und LTE-Mobilfunk

Nach den internationalen Fernmeldeverträgen ist es weltweit verboten, Funkverbindungen zu stören oder zu unterdrücken. Dennoch gibt es Ausnahmen, die jedoch immer der Zustimmung der nationalen Fernmeldebehörde bedürfen. Beispiele sind Strafvollzugsanstalten und Gerichtssäle, um verbotene Kontaktaufnahmen zu unterbinden, oder Konzertsäle, Kirchen usw., um störende Telefonate zu vermeiden.

Die vorliegende Applikationsschrift beschäftigt sich mit dem wirkungsvollen legalen Einsatz von Jammern – zu Deutsch Störsendern – am Beispiel einer GSM-Verbindung. Die Resultate geben ebenso Anhaltspunkte für das Aufspüren illegaler Jammer.



Beim legalen Einsatz von Jammern besteht die Problematik darin,
1. den Funkverkehr in allen drei Dimensionen Frequenz, Raum und Zeit lückenlos zu unterdrücken und
2. gleichzeitig zu verhindern, dass in anderen Bereichen Störungen auftreten.

Man wird deshalb immer bestrebt sein, in ein zu schützendes Objekt hinein zu strahlen, wobei eine lückenlose Abdeckung immensen Aufwand verlangt. Antennen im Gebäude sind vorteilhaft.

Bei Mobilfunk bietet es sich an, den Empfang des Downlinks zu unterbinden, da zum einen Empfangssignale am Handy einen relativ niedrigen Pegel aufweisen und zum anderen die Handys somit weitgehend deaktiviert werden können.

Breitbandige Störer arbeiten u.a. mit FM- oder OFDM-modulierten Signalen. Wirksam werden diese nur, wenn sie lange genug verweilen, so dass auch die Fehlerkorrektur der Kommunikationskanäle – die mittlerweile eine hohe Leistungsfähigkeit bietet – die Informationsverluste nicht mehr ausgleichen kann.

Das Jamming-Signal

Der Störer stellt sich wie in Bild 1 als Überhöhung im Rauschteppich dar. Das Signal kann mit OFDM-Technik oder mit breitbandiger Pseudo-Noise-Modulation erzeugt werden. Der Rauschteppich beginnt etwas unterhalb des Downlink-Bandes (925 – 960 MHz) und ist dort auch leichter zu finden, da hier kaum Nutzsignale überlagert sind.

Bild 2 zeigt eine FM-Aussendung, die auch etwas über die Obergrenze des Downlink-Bereichs hinausgeht.

Beide Bilder sind Beispiele, wie sich ein Störer in schneller Übersichtsmessung außerhalb eines geschützten Bereichs zeigen kann.

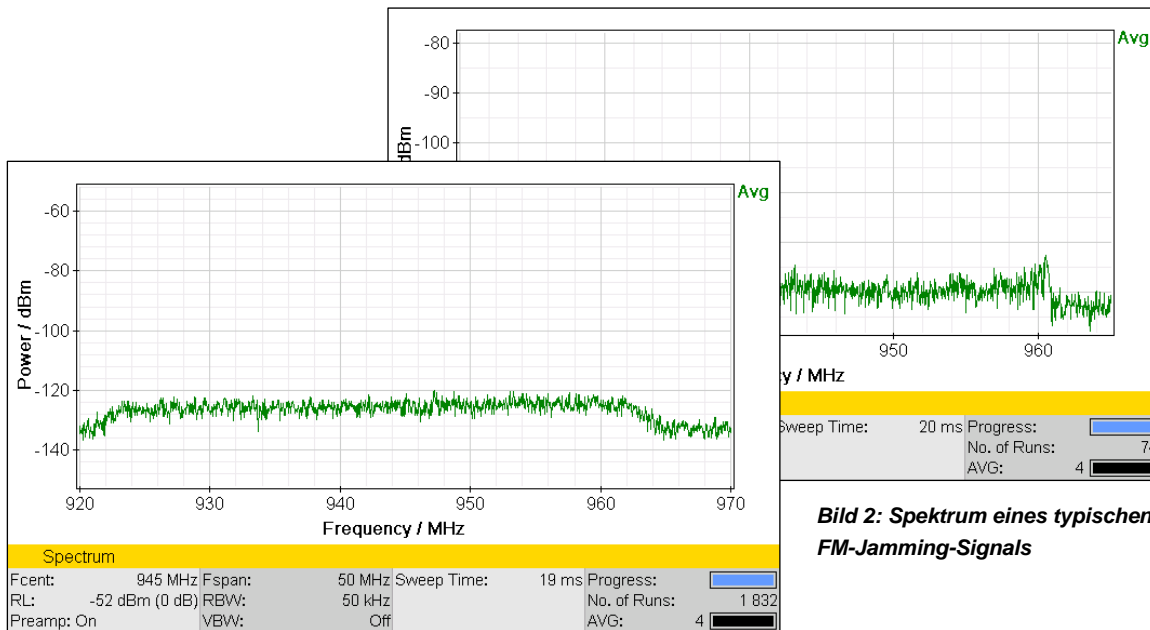


Bild 2: Spektrum eines typischen FM-Jamming-Signals

Bild1: Unterdrückung des Downlinks durch Erhöhung des Rauschteppichs

Störer und Nutzsignale im Spektrogramm

Das konventionelle Spektrogramm – basierend auf nur einzelnen Sweeps – zeigt einen Jammer, der etwas unterhalb von 925 MHz beginnt und sich im 50-kHz-Raster über den gesamten dargestellten Frequenzbereich erstreckt. Von der 9. – 15. Sekunde wurde der Jammer zu Anschauungszwecken ausgetastet.

Ein solches Bild zeigt sich regelmäßig bei Messungen außerhalb des bestrahlten Bereichs. Der Jammer ist ins Gebäude gerichtet und wird nach außen durch die Bausubstanz abgeschirmt. So ist er relativ wirkungsvoll, aber unauffällig.

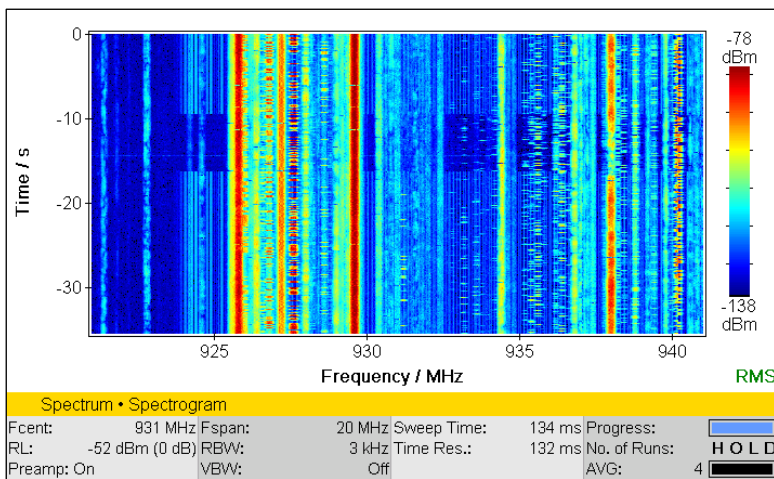


Bild 3 Jammer in konventioneller Spektrogramm-Darstellung

Störer und Nutzsignale im hochauflösenden Spektrogramm

Das hochauflösende Spektrogramm (HiRes Spectrogram) ermöglicht eine zeitlich lückenlose Erfassung und Darstellung. Bild 4 zeigt einen Frequenzbereich von 1,6 MHz. Die zeitliche Darstellung ist von 125 ms auf 16 ms gezoomt. Die Messung fand außerhalb des Gebäudes statt. Zwar sind die Störlinien deutlich sichtbar, ihr Pegel reicht aber nicht aus, um die GSM-Verbindung zu unterdrücken.

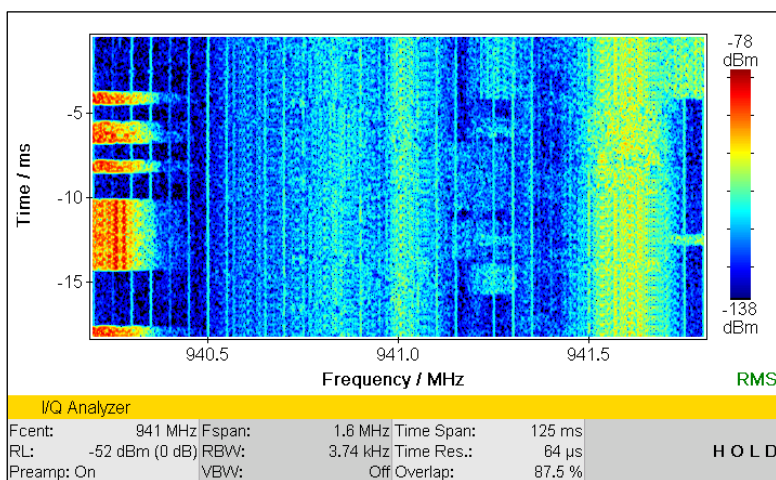


Bild 4: Lückenloses Spektrogramm. Feldstärkemessungen vor dem Gebäude in Zoom-Darstellung

Innerhalb des Gebäudes wird der Pegel des Downlink-Signals stark abnehmen und der Pegel des (Inhouse-)Jammers etwa im gleichen Maß ansteigen. Die Darstellung in Bild 5 entspricht dem vorherigen Bild, zeigt aber die gesamten 125 ms.

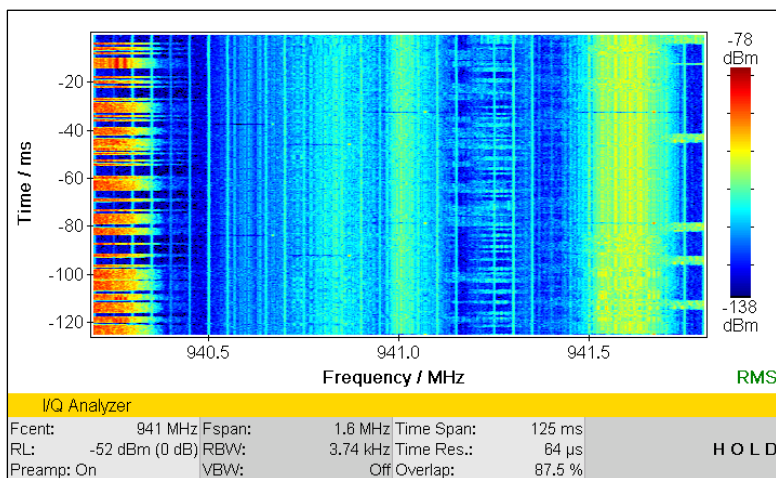


Bild 5: Lückenloses Spektrogramm. Feldstärkemessungen im Gebäude, nicht gezoomt

Das Persistence- oder Leuchtdichte-Diagramm in Bild 6 zeigt zusätzlich zur Amplitude über der Frequenz auch die Häufigkeit, mit der die jeweiligen Pegel auftreten. Durch diese Häufigkeitsdarstellung werden auch Inbandstörer sichtbar. Hier liegt derselbe Datensatz wie derjenige in Bild 5 zugrunde. Der Interference and Direction Analyzer IDA 2 kann aus denselben Datensätzen alle Darstellungen errechnen, was dem Spezialisten entscheidende zeitkorrelative Analysen bietet.

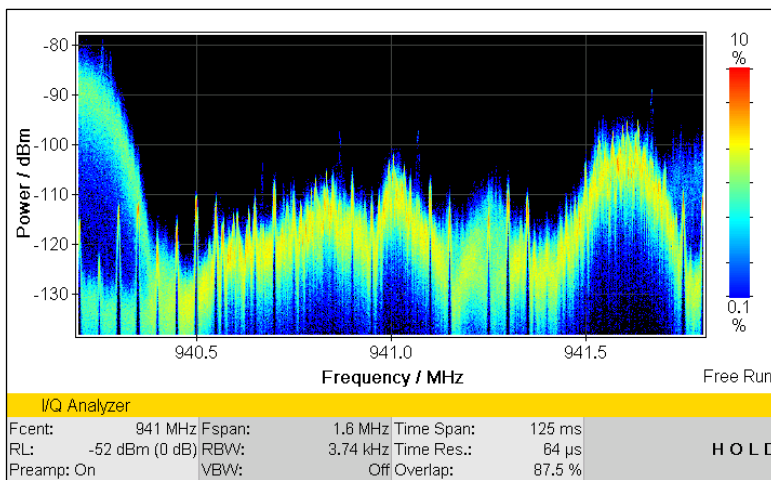


Bild 6: Erkennen von Inband-Störern durch Persistence-Darstellung

Prüfen der Wirksamkeit einer Jamming-Anlage

In den meisten Fällen reicht ein einziger Jammer nicht aus. In jedem Raum gibt es Stehwellen und Abschattungen, die sich obendrein je nach Raumbelastung ändern. Dazu reicht es, Metallgegenstände, Musikinstrumente, Transportkörbe usw. zu verschieben, einzubringen oder zu entfernen.

Hier einige Punkte:

- Am Empfangsort ist die erforderliche Störleistung minimal - daher wird man bei GSM auf den Downlink-Frequenzen arbeiten.
- Die Polarisation des Störers orientiert sich am Nutzsignal. Bei GSM wäre eine Kreuzpolarisation sinnvoll.
- Räumliche Lücken kann man durch Ausleuchtung aus verschiedenen Richtungen und/oder durch Antennen-Diversity minimieren, d.h. gleiches Signal auf versetzte Antennen geben.

Eine einfache Prüfung mit einem Handy zeigt nur ein sehr unvollständiges Bild. In sicherheitsrelevanten Anwendungen müssen Frequenzen, Ort, Signalamplitude und Zeit zusammenpassen. Zu diesem Zweck eignen sich FFT-Analysatoren mit einer breiten Erfassungsweite (FFT-Span). Dank lückenloser und überlappender FFT-Fensterkalkulation gehen keine Signalanteile verloren.

Der Spektrogramm-Algorithmus konventioneller Spektrum-Analysatoren arbeitet sukzessiv: d. h. es wird akquiriert, gerechnet und angezeigt. Dadurch entstehen erhebliche Darstellungslücken zwischen einzelnen Spektren, da die Sweeps (Traces) bzw. FFT-Blöcke singular aneinander gereiht werden.

Die Blockakquisition von 250.000 I/Q-Datenpaaren im HiRes-Mode des IDA 2 erfasst dagegen einen zusammenhängenden Datensatz aus dem demodulierten Basisband mit bis zu 22 MHz Breite. Dabei reicht die Aufzeichnungszeit in diesem Beispiel über 7,8 ms, also mehr als einen GSM-Frame. Das Bild ist schnell aufgebaut und kann so die relevanten oder ungünstigsten Punkte eines zu schützenden Gebäude oder Raumes direkt darstellen.

Wichtig ist es, die GSM-Aussendungen regelmäßig auf Änderungen zu prüfen. Diese können dauerhaft, aber auch zu bestimmten Tageszeiten stattfinden. Dazu reicht meist eine Messung an einigen Referenzpunkten: ein Raum, Ecken eines Gebäudes usw.

Bei Aussendungen wie GSM ist die lückenlose Spektrogramm-Darstellung dem Deltaspektrum deshalb überlegen, weil sie alle Ereignisse detailliert im Zeitzusammenhang zeigt.

Beispiele für die Wirksamkeitsprüfung eines Jammers bieten die Bilder 7 und 8. Beide Bilder zeigen ein Störsignal von ca. 20 MHz Bandbreite. Das lückenlose Spektrogramm Bild 7 und das Persistence-Diagramm Bild 8 sind aus demselben Datensatz erzeugt. Auf einen Blick erkennt man, dass die Wirkung des Jammers mindestens bei 925,7, 927,5, 929,6 und 938 MHz zu bezweifeln ist.

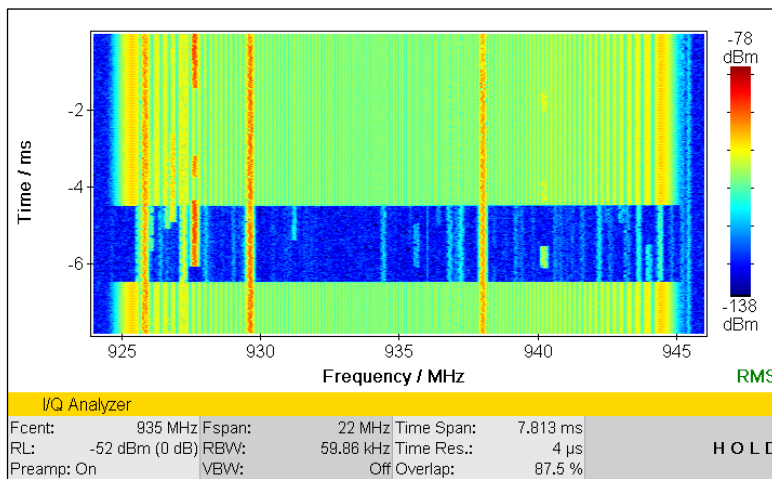


Bild 7: Lückenloses Spektrogramm.
In der künstlich erzeugten Austastlücke des Jammers sind auch die schwachen Signale zu sehen

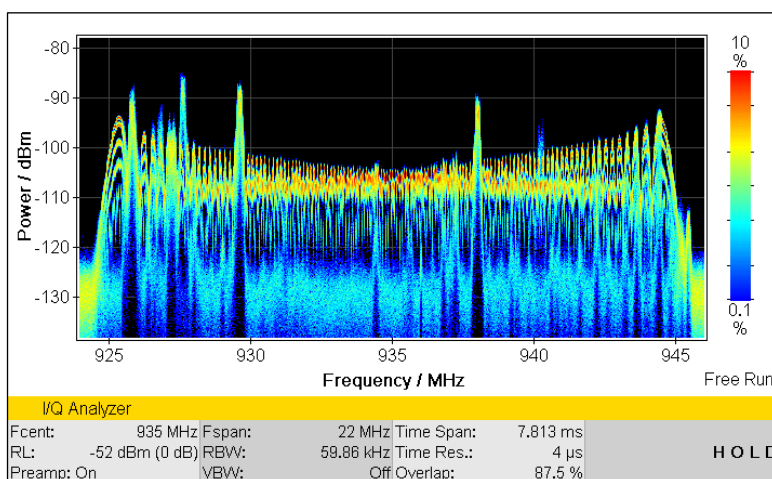


Bild 8: Persistence-Darstellung.
Hier sind die schwachen Signale auch ohne Austasten des Jammers erkennbar

Alle HiRes-Darstellungen haben ihre Stärken. Da man den zugrunde liegenden Datensatz leicht ablegen kann, kann man auch noch später alle HiRes-Darstellarten wieder erzeugen und auch nachträglich im Spektrogramm detailliert zoomen.

Narda Safety Test Solutions GmbH

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

www.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

® Namen und Logo sind eingetragene Warenzeichen der Narda Safety Test Solutions GmbH – Handelsnamen sind Warenzeichen der jeweiligen Eigentümer.