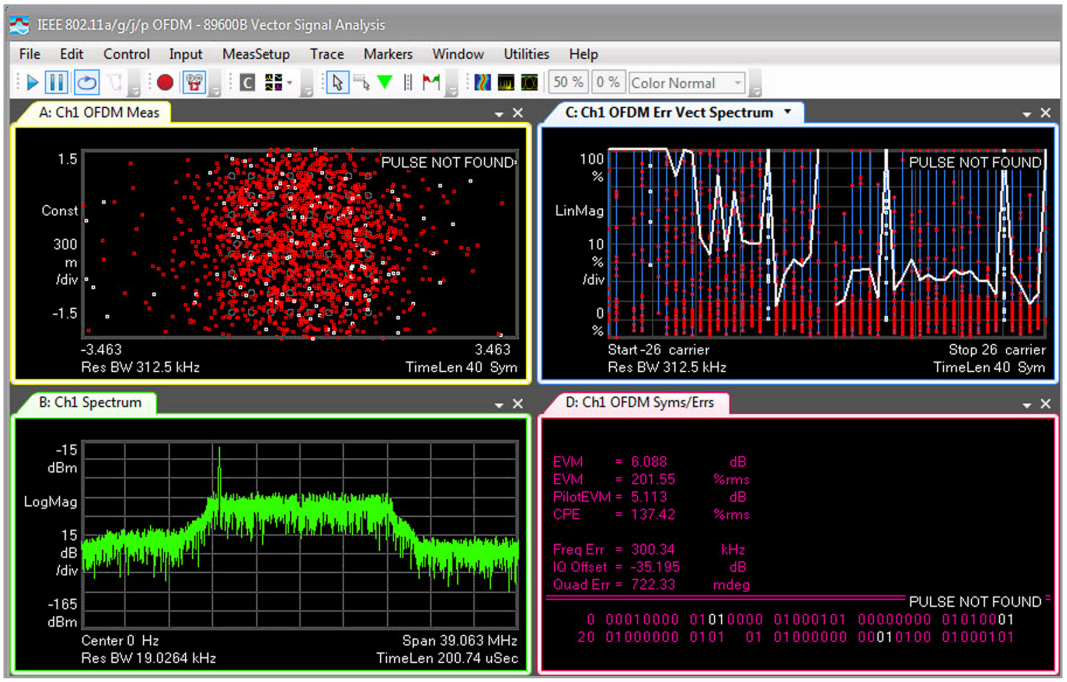
Keysight Technologies

Streaming, Analysis and Playback of RF Interference Signals in Aerospace and Defense Applications

Application Note



KEYSIGHT TECHNOLOGIES

Introduction

In a perfect world, receivers would use brick wall filters, amplifiers and mixers would never distort, command centers would always coordinate their spectrum operations, and the term “jam” would have meaning only at breakfast and during musical gatherings. Until then, there will be interference.

Interference may be either unintentional or intentional. Unintentional interference is part of the RF environment: cell phones, wireless links, cordless phones, terrestrial television, medical electronics, and more, all contribute. Intentional interference has been created to disrupt the operation of a victim receiver.

Our focus is on intentional interference and the ultimate goal of countering undesired signals. The proposed process has four steps:

- Capture the signal in the field
- Analyze it in the lab
- Simulate and playback the signal
- Develop ways to defeat it

Because this interference is intermittent and transient, capturing the signal may require seconds, minutes or hours of data. To provide a complete picture during analysis, the captured data must be gap-free.

All this can be accomplished with a system based on commercial, off-the-shelf (COTS) hardware and software elements from Keysight Technologies, Inc. and X-COM Systems. The system accelerates the process of sifting through terabytes of data and performing detailed analysis. It also retains the original signal fidelity throughout the entire process—capture, analysis, simulation and playback. Because all elements are COTS, the solution offers traceable performance and enables easy redeployment for traditional applications.

Problem

As a general problem, intentional interference is being transmitted for a specific purpose: disrupting communication, jamming a radar system, and otherwise deceiving or disrupting a victim receiver. Because such signals are at once intermittent and transient, it is often difficult to see or determine the culprit.

Within this scenario, the specific problem is capturing and analyzing a complete set of spectrum data that contains an offending signal. This often requires the acquisition of seconds, minutes or hours of spectrum data—and this can consume gigabytes or terabytes of disk space.

In most cases, storage capacity is perhaps the least challenging part of the problem. More difficult is the continuous acquisition of high-fidelity data. Once the mountain of gap-free data has been acquired and stored, the next challenge is pinpointing one or more interference events. True understanding comes with the extraction of meaningful signal information—in the time, frequency and modulation domains—from each event.

Solution

The driving idea behind our solution is "Captured interference is information." The more quickly and accurately you can extract meaningful signal information, the better you can understand its impact on the victim system and the sooner you can create and deploy countermeasures.

A block diagram of the solution is shown in Figure 1. As described earlier, the system addresses the major steps in the process: capture, analysis, simulation and playback.

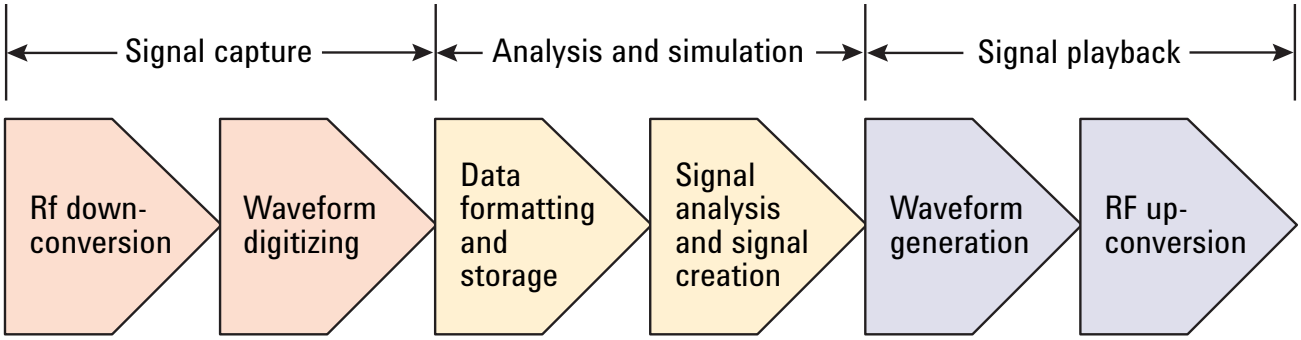


Figure 1. The flow of the system block diagram supports the conversion of captured interference into useful information

Signal capture and analysis

Signal capture and analysis utilizes three hardware elements: signal analyzer, data recorder and external datapack. These are shown on the left and center sections of Figure 2.

Keysight X-Series signal analyzer:

The diagram shows the PXA, our flagship signal analyzer. Depending on performance requirements, an MXA or EXA could also be used. Using an X-Series signal analyzer as the front-end downconverter and IF digitizer helps maximize signal fidelity from the beginning of the process.

X-COM IQC5000A data recorder:

The input to the recorder is a stream of digital I/Q samples from the signal analyzer. The IQC5000A formats the I/Q data, tags it with external marker events, and adds time and GPS stamps before sending to the datapack.

X-COM Datapack:

This unit can be configured with an internal capacity up to 2 TB or external capacities of 8 or 16 TB.

A variety of post-processing activities can be performed with the software elements of the solution.

X-COM Spectro-X signal analysis software:

Key capabilities include pre-processing of large data sets and location of suspect signals. Spectro-X includes search engines to identify and "fingerprint" waveforms as well as "clip and save" capability for replay into the 89600 vector signal analysis (VSA) software.

Keysight 89600 VSA software:

Our industry-leading vector signal analysis (VSA) software provides multiple views into highly complex signals. Its built-in capabilities support more than 70 standards and signal types, and it enables bit-level modulation analysis.

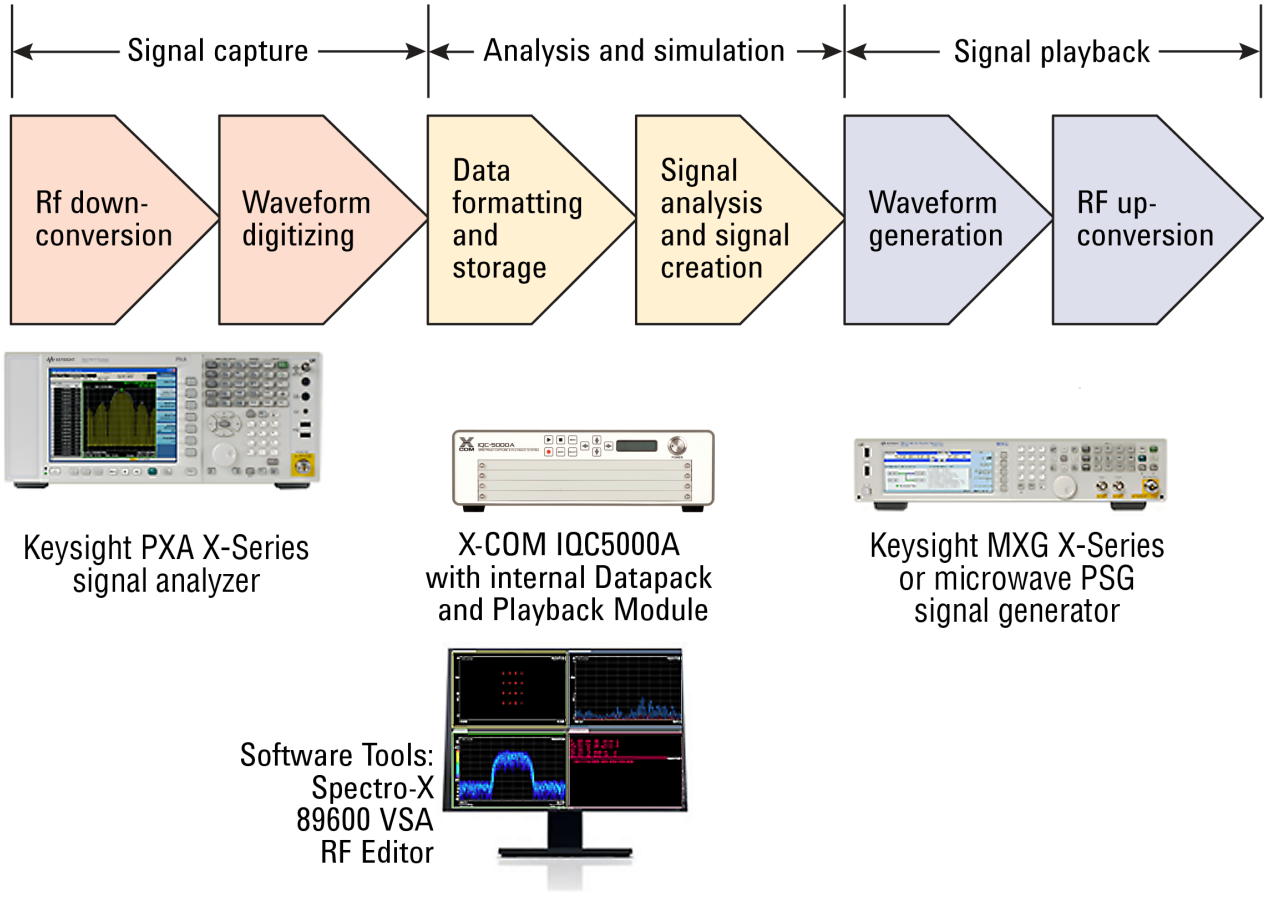


Figure 2. A combination of COTS hardware and software elements enables high-fidelity capture, analysis, simulation and playback

Signal simulation and playback

For simulation and playback, the system includes signal-creation software, a baseband generator and a vector signal generator. These are shown on the bottom and right of Figure 2.

X-COM RF Editor:

This software can be used to create signal scenarios that include the recorded files. Capabilities include clipping, stitching, translating, filtering and looping of waveforms. The resulting waveforms can be downloaded to the IQC5000A for playback.

X-COM IQC5000A playback module:

This baseband generator is used to drive the I and Q modulation inputs of the vector signal generator.

Keysight vector signal generator:

Example models include the PSG, EXG and new MXG. The vector signal generator upconverts the I/Q modulation and serves as the over-the-air signal source.

Results: Signal capture and analysis

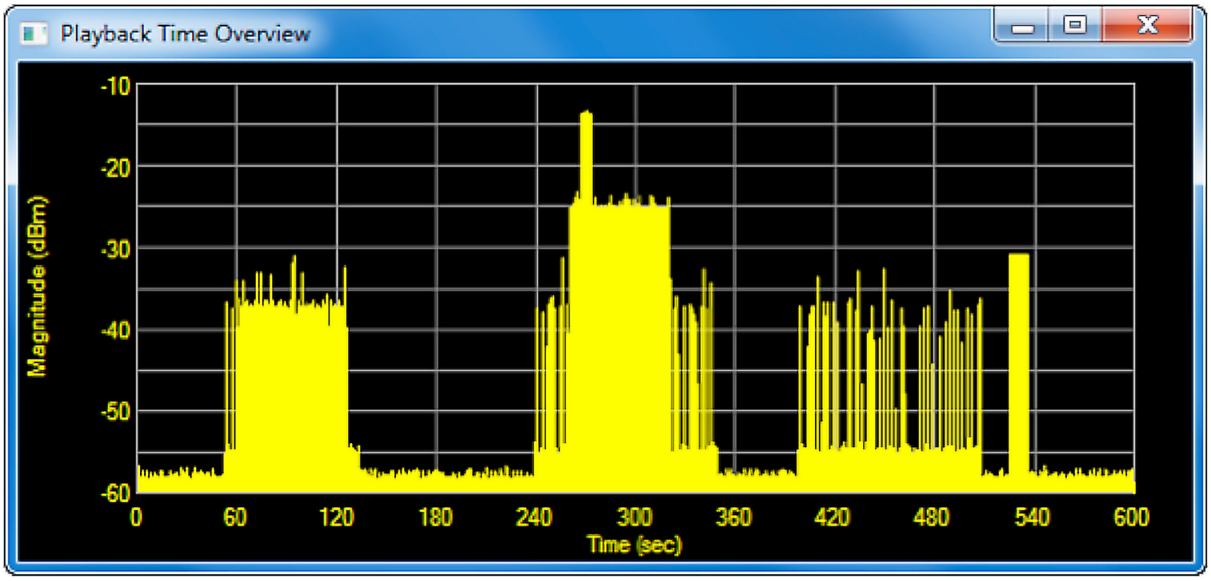


Figure 3. A visual inspection of the captured spectrum data revealed four regions of interest

A brief case study based on an actual interference scenario will illustrate the capabilities of the solution. The initial signal acquisition was performed using a PXA signal analyzer, which streamed a 40 MHz-wide capture into the IQC5000A recorder and a 2-TB data pack. The gap-free capture ran for 10 minutes and generated 120 GB of data.

Information from interference

Spectro-X was used to visually inspect the captured data for interesting interference signals. An overview measurement of magnitude versus time for the full 600-second capture revealed four distinct periods of potentially interesting activity (Figure 3).

A quick analysis of the region between approximately 400 and 500 seconds showed that the signals were 802.11b Wi-Fi transmissions. Setting that segment aside, the search tools in Spectro-X were focused on the three remaining regions of heavy activity: from 50 to 140 seconds, from 230 to 350 and from 510 to 540. Frequency-domain analysis provided the following information:

- Region 1: The span between approximately 50 and 140 seconds contained 137,000 total carrier signals.
- Region 2: During the span from approximately 230 to 350 seconds an IEEE 802.11g transmitter was operating, as was an unknown signal that is clearly visible in the overview. The unknown signal was on for approximately five seconds.
- Region 3: Within the approximately 510 to 540 second span, there were 20,000 occurrences of an arbitrary carrier signal.

Focusing on Region 2 provided interesting views in the spectrogram and persistence spectrum formats, as shown in Figure 4. In the spectrogram display (top), two bursts of the interferer intrude into the spectrum of an orderly carrier signal.

The "standard search" capability in Spectro-X was used to identify the orderly carrier, which was believed to be an 802.11g signal. As shown in Figure 5, the search parameters include a confidence limit (set to 40 percent in this case), a candidate type of standard (here set to 802.11a/g) and the time range of interest within the captured data (set to 250 to 300 seconds).

The confidence limit helps reveal signals that look similar to an idea wireless standard. This value is relative to an ideal wireless-standard signal and defines the desired level of correlation between the reference and a captured signal. Using a value of less than 100 percent provides clues into how severely the interference is affecting the victim signal.

In this case, the search found more than 92,000 instances of signals that resembled the 802.11g reference.

As expected, there were regions of severe degradation that occurred when the interference signal appeared: as shown in Figure 6, correlation dropped from 80-plus percent to less than 50 percent.

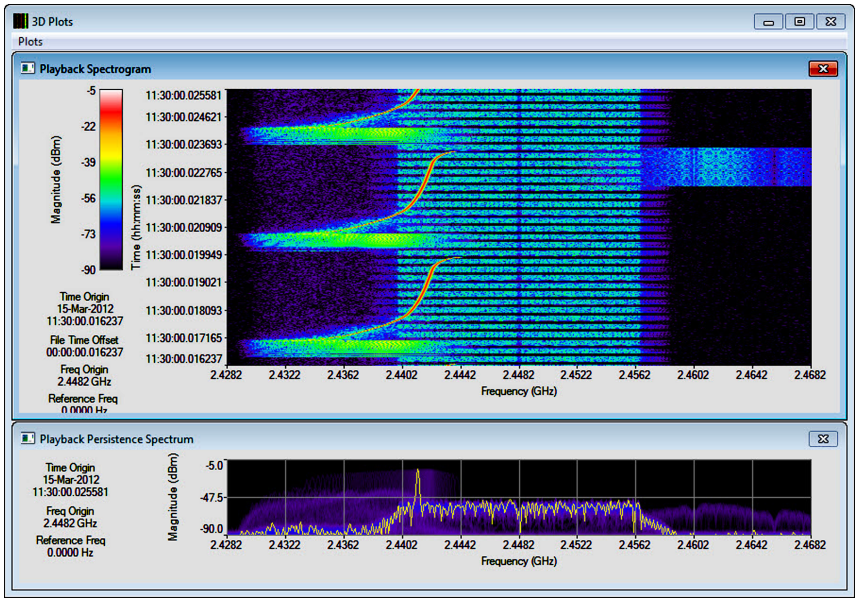


Figure 4. In the spectrogram (top), the suspected interferer intrudes into a portion of an orderly carrier signal

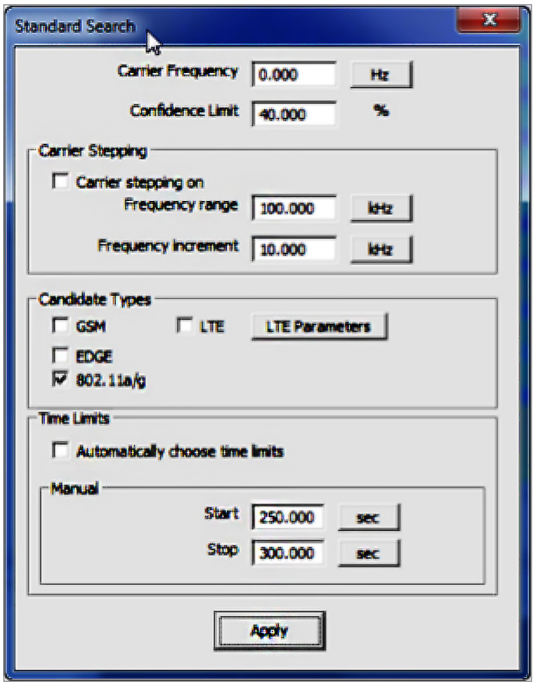


Figure 5. The "standard search" dialog box is used to select parameters such as the candidate wireless standard and the desired level of correlation

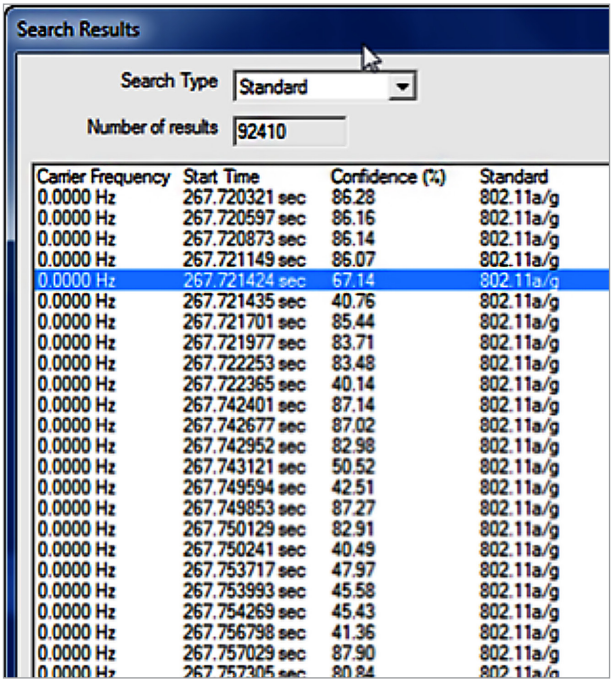


Figure 6. The search results summary reveals areas of high and low confidence

For each region of poor correlation, the results were examined using a spectrogram display (Figure 7). This pinpointed the five-second span during which the interferer was operating.

The associated I/Q data was then exported to the 89600 VSA software for detailed analysis. In the time prior to the interference, the key indicators of modulation quality were all good, as shown in Figure 8. When the interference was active, the impact was catastrophic: the pilots and payload carriers were completely disrupted as the interfering signal walked through the transmission (Figure 9).

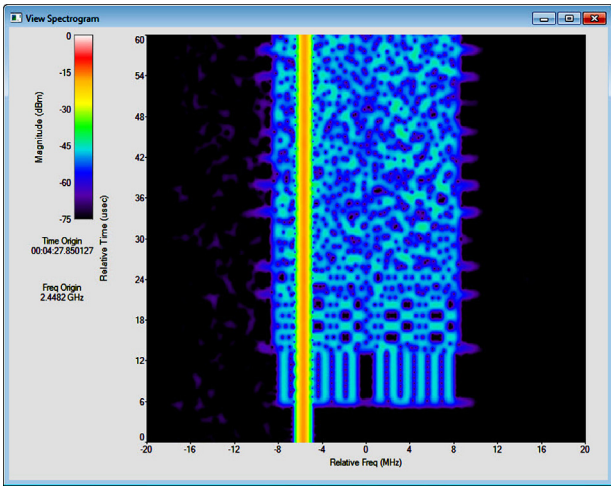


Figure 7. This 60-µs (top to bottom) spectrogram display from Spectro-X shows the interferer disrupting the reference sequence (3-11 µs) and payload (11 µs and above) of the 802.11g signal

Behind the scenario

This scenario occurred in an Internet café. The unintentional jammer was a microwave oven and it disrupted Wi-Fi connectivity every time the staff warmed a pastry or sandwich.

Even though this was a relatively benign situation, the suggested procedure works equally well in scenarios that involve interference that affects radio communications, telemetry links, flight range operations, signal intelligence (SIGINT), system interoperability, and so on. It also supports the three most common usage scenarios: record in theater and playback in the lab, record in the lab and playback in the lab, and create in the lab and playback on the range.

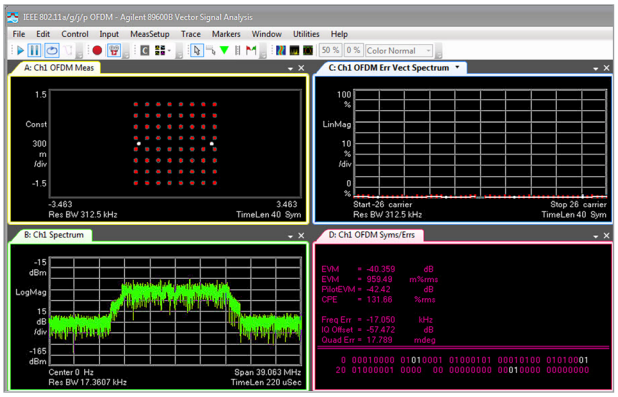


Figure 8. Prior to interference: The OFDM constellation (upper left), EVM (upper right) and spectrum (lower left) are normal

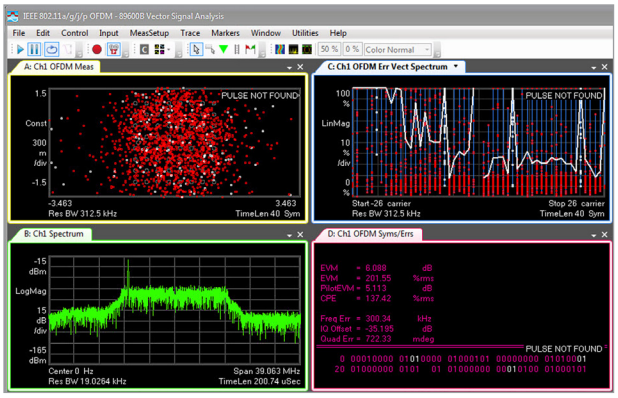


Figure 9. Interference is active: The OFDM constellation (upper left) is shattered, EVM (upper right) is erratic and a large spike is present in the frequency spectrum (lower left)

Conclusion

Various types of interference can impact critical defense systems. Thus, it's important for designers to have "RF forensic tools" that can unravel what actually happened in the electromagnetic spectrum. Extracting useful RF forensic information is the first step in developing successful mitigation strategies and solutions.

As shown here, Keysight and X-COM have teamed up to provide measurement and analysis systems that offer high signal fidelity over broad frequency ranges and long-duration captures of gap-free data. Once captured, these signals can be searched for specific types of interference and analyzed in detail. The signals can also be manipulated in software to simulate alternate interference scenarios. In addition, the recordings can be rebroadcast in their entirety for use in electromagnetic environmental (EME) simulation and interoperability testing.

Related literature

- Brochure: X-Series Signal Analysis, publication 5990-7998EN
- Brochure: PXA X-Series Signal Analyzer N9030A, publication 5990-3951EN
- Brochure: 89600 VSA Software, publication 5990-6553EN
- Solution brochure: RF Interference Troubleshooting, publication 5990-9511EN
- Solution brochure: RF Interference Analysis, publication 5990-9243EN
- Solution brochure: Spectrum Management Solution, publication 5990-9089EN
- Application note: Capturing Events of Long Duration or High Data Volume, publication 5990-7734EN
- For additional information about X-COM, Spectro-X and RF Editor, please visit www.xcomsystems.com

To learn how this solution can address your specific needs please contact Keysight's solutions partner, X-COM
www.keysight.com/find/xcom

X COM

KEYSIGHT TECHNOLOGIES

Keysight Solutions Partner Program
Keysight and its Solutions Partners work together to help customers meet their unique challenges, in design, manufacturing, installation or support. To learn more about the program, our partners and solutions go to www.keysight.com/find/solutionspartner

X-COM Systems designs RF signal recording, analysis and playback solutions for system design, signal simulation and test applications. www.xcomsystems.com

For information on Keysight Technologies' products, applications and services, go to www.keysight.com

myKeysight

myKeysight

www.keysight.com/find/mykeysight
A personalized view into the information most relevant to you.

Three-Year Warranty

www.keysight.com/find/ThreeYearWarranty
Keysight's commitment to superior product quality and lower total cost of ownership. The only test and measurement company with three-year warranty standard on all instruments, worldwide.

Keysight Assurance Plans

www.keysight.com/find/AssurancePlans
Up to five years of protection and no budgetary surprises to ensure your instruments are operating to specification so you can rely on accurate measurements.

www.keysight.com/quality
Keysight Electronic Measurement Group
DEKRA Certified ISO 9001:2008
Quality Management System

Keysight Channel Partners

www.keysight.com/find/channelpartners
Get the best of both worlds: Keysight's measurement expertise and product breadth, combined with channel partner convenience.

www.keysight.com/find/ad

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:
www.keysight.com/find/contactus

Americas

Canada	(877) 894 4414
Brazil	55 11 3351 7010
Mexico	001 800 254 2440
United States	(800) 829 4444

Asia Pacific

Australia	1 800 629 485
China	800 810 0189
Hong Kong	800 938 693
India	1 800 112 929
Japan	0120 (421) 345
Korea	080 769 0800
Malaysia	1 800 888 848
Singapore	1 800 375 8100
Taiwan	0800 047 866
Other AP Countries	(65) 6375 8100

Europe & Middle East

Austria	0800 001122
Belgium	0800 58580
Finland	0800 523252
France	0805 980333
Germany	0800 6270999
Ireland	1800 832700
Israel	1 809 343051
Italy	800 599100
Luxembourg	+32 800 58580
Netherlands	0800 0233200
Russia	8800 5009286
Spain	0800 000154
Sweden	0200 882255
Switzerland	0800 805353 Opt. 1 (DE) Opt. 2 (FR) Opt. 3 (IT)
United Kingdom	0800 0260637

For other unlisted countries:
www.keysight.com/find/contactus
(BP-06-09-14)

KEYSIGHT TECHNOLOGIES

Published in USA, August 3, 2014
5991-0768EN
www.keysight.com