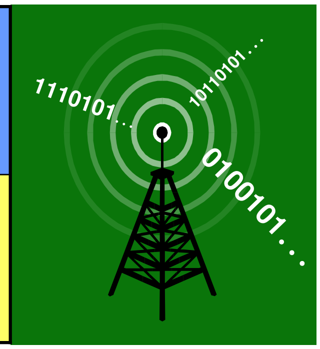
Modern radios are more efficient than their predecessors making the signals they transmit harder to detect using traditional approaches. This is especially true in urban areas where the RF environment is crowded, and signal propagation is complex. This paper explores the use and performance of RF sensor networks for improved detection, identification, and geolocation of modern signals using coherent detection, proximity gain, and time-difference of arrival.

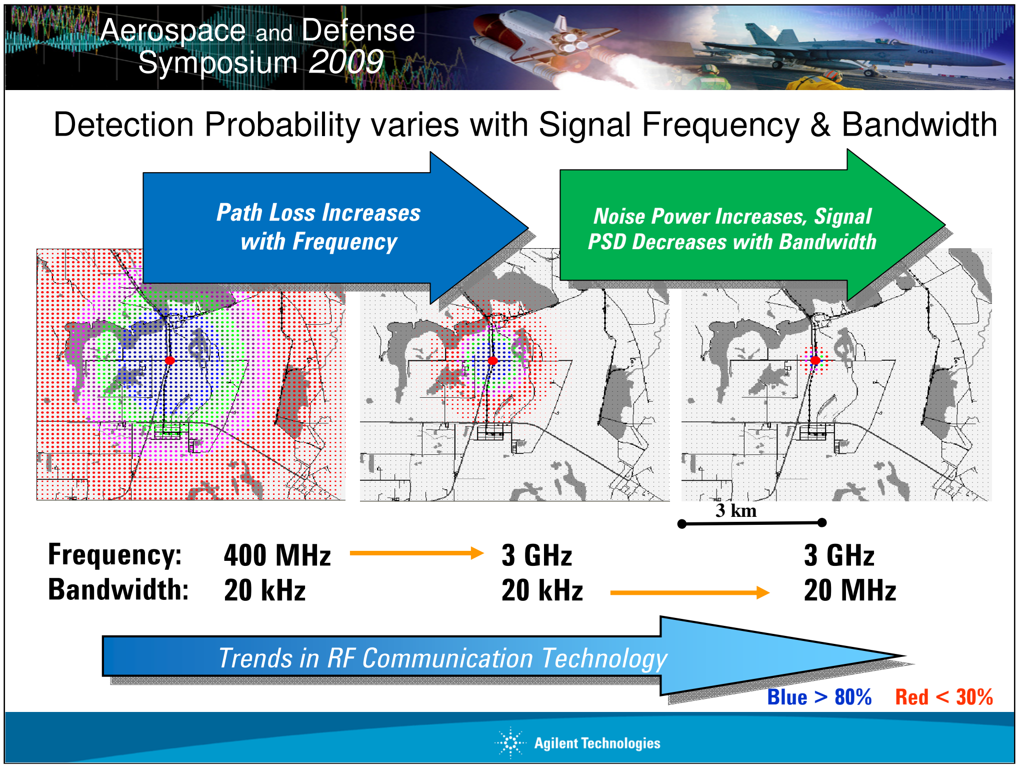
Trends in RF Technology

- *The Challenge:*
- *Quickly detect and locate non-cooperative modern signals which may be intermittent, be of short duration, spread spectrum, have low power and/or low energy.*

Frequencies and Bandwidths Increasing	***Signal Complexity Increasing***
Number of Transmitters Increasing	***Increasing Dependence on RF Technology***



Signal complexity – improve spectrum efficiency; # tx – how many in your pocket; dependence, susceptible (airports, GPS, etc)

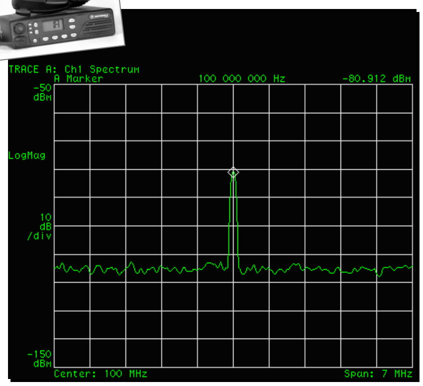


Looking at increasing freq trend; what's the implication… suppose we have a spec an….

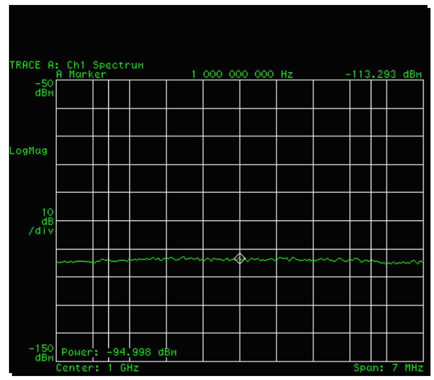
Aerospace and Defense Symposium 2009

SNR Decreases With Frequency & Bandwidth

Power Spectral Density (PSD) decreases by $10\log_{10}(BW)$ and greater than $20\log_{10}(f)$



Narrowband Signal at 100 MHz



5 MHz Wideband signal at 1 GHz (same power)

Agilent Technologies

This measurement is typical of a narrowband VHF signal. This 100 MHz signal is easily detected and is well above the noise floor.

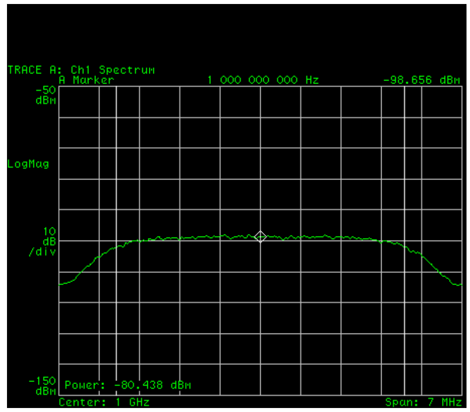
Aerospace and Defense Symposium 2009

One Solution is Proximity Gain

With modern signals we need more sensitivity than can be practically provided by improvements in receiver and antenna specifications.

Can't buy a receiver with 20 dB better noise figure performance, for example.

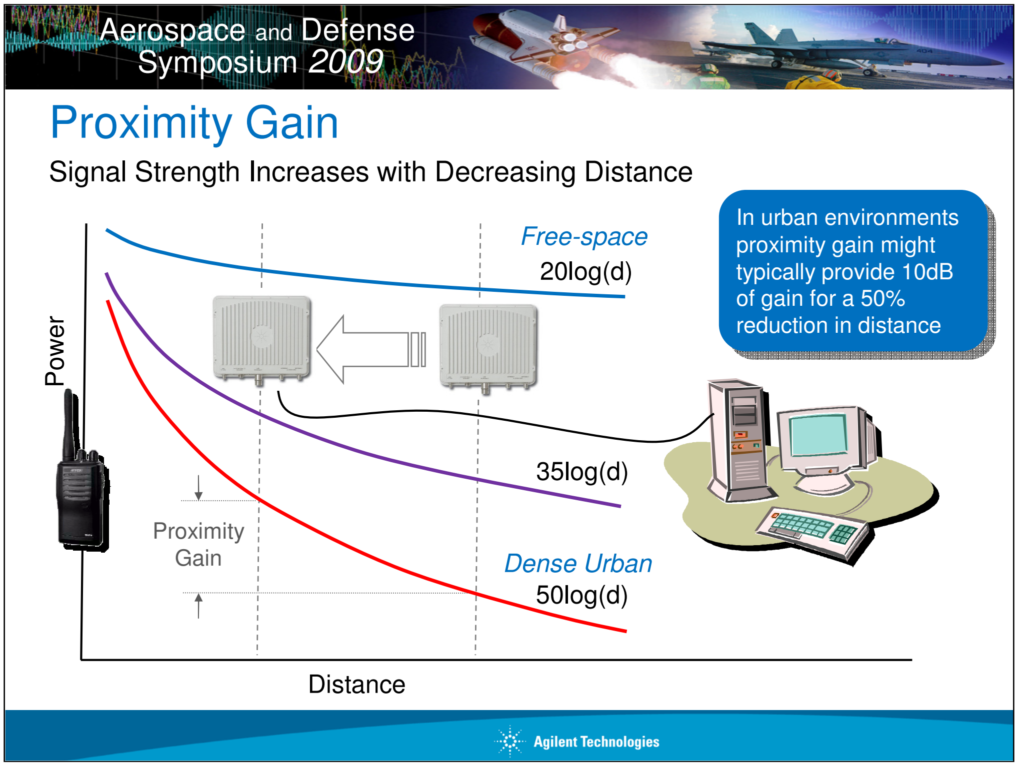
$$\text{FSPL(dB)} = 20\log_{10}(d) + 20\log_{10}(f) + 32.44$$



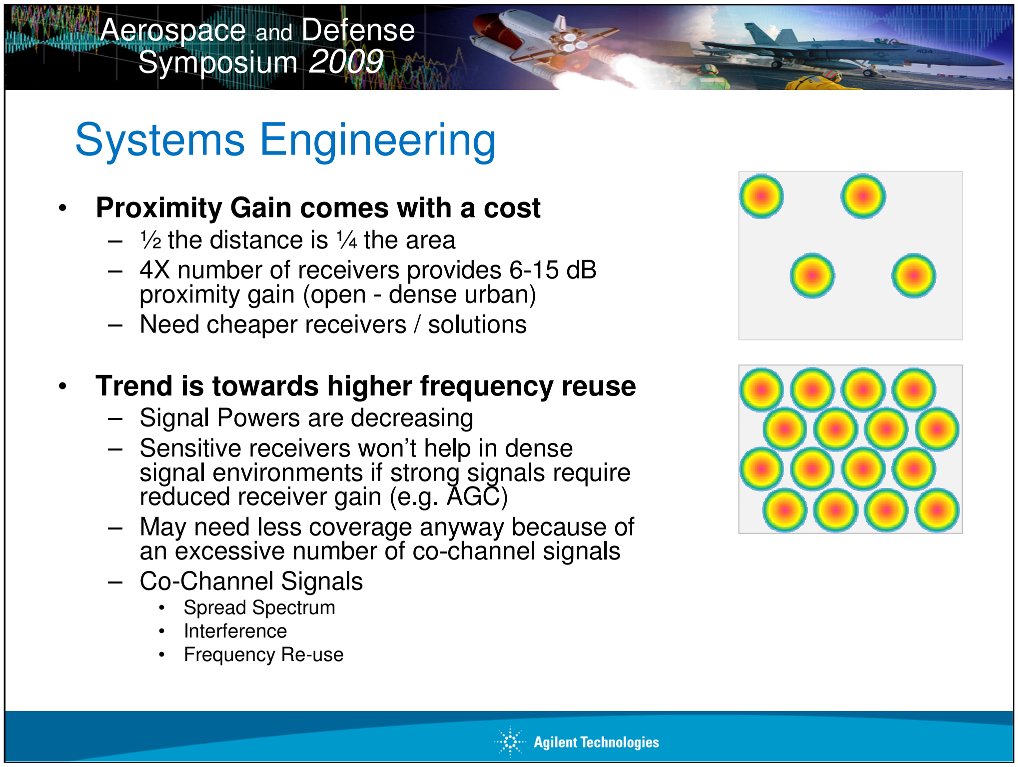
5 MHz Wideband signal at 1 GHz (same power)
Now at 1/10 the free-space distance

Agilent Technologies

Looking again at the free-space path loss equation we also see a term relating to distance. In practice this term can range from 20log(d) in free-space to more than 50log(d) in dense urban environments. We can turn this loss into a gain by moving the monitoring receiver closer to the transmitter. I call this "proximity gain". The proximity gain in free-space is 20log(d1/d2) where d1 and d2 are the two distances. He we simulate an increase in power obtained by reducing the distance between the transmitter and monitoring receiver by a factor of 10.



The simulation

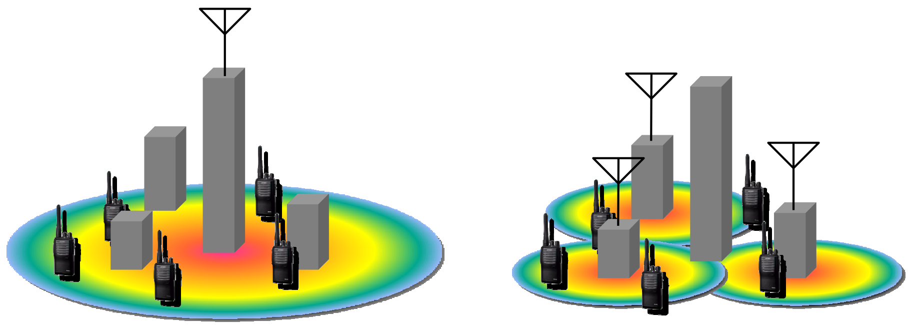


Nothing comes for free. Getting closer to the transmitter requires either mobile receivers, more many more fixed-site receivers. Moderate reductions in distance can provide significant proximity gain. Decreasing the distance by half can provide as much as 15 dB of proximity gain in dense urban environments.

While it may be possible to trade off receiver performance with coverage area, modern signals with high frequency reuse (e.g. cellular and fixed wireless) may have too many co-channel signals to monitor from widely spaced monitoring sites. Also, with greater signal density the full receiver sensitivity may not be usable without overloading the receiver's front end.

Cellular systems provide a good example of how system performance can be improved using small cells with lower performance, and less expensive base stations. Radio monitoring systems may need to take a similar approach in dealing with modern and evolving signals.

Which is Better?

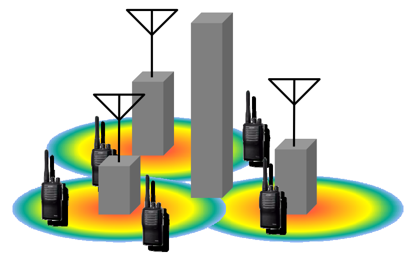


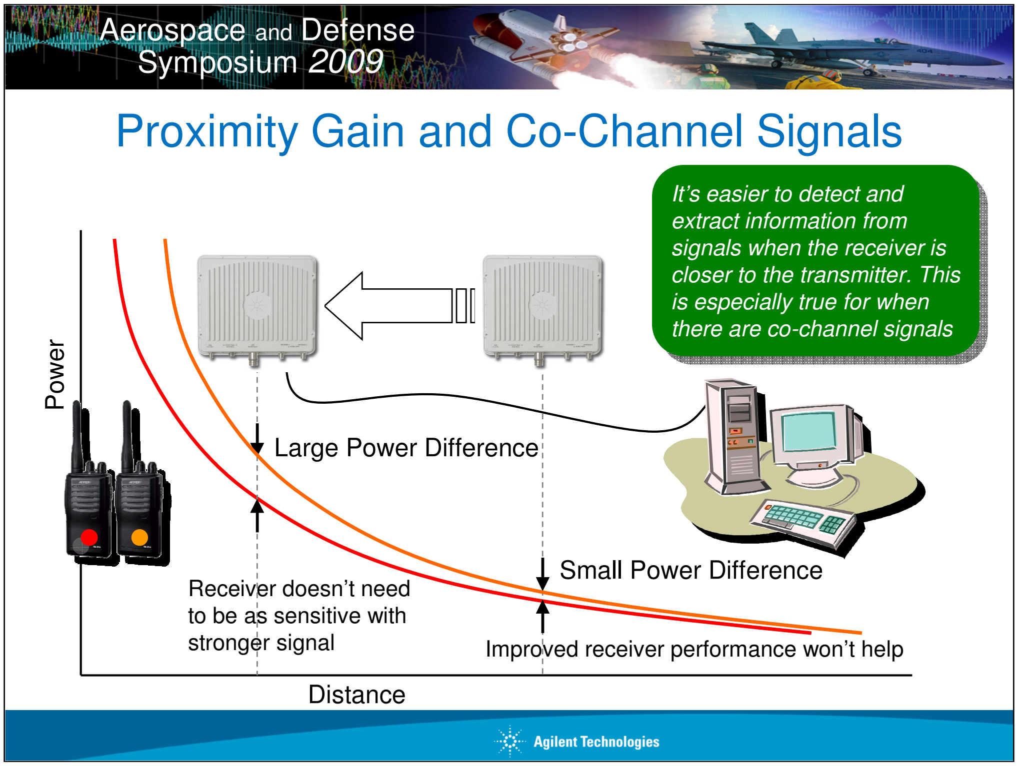
A: Small number of high-performance receivers at the highest elevations?

B: Multiple lower-performance receivers each with reduced coverage?

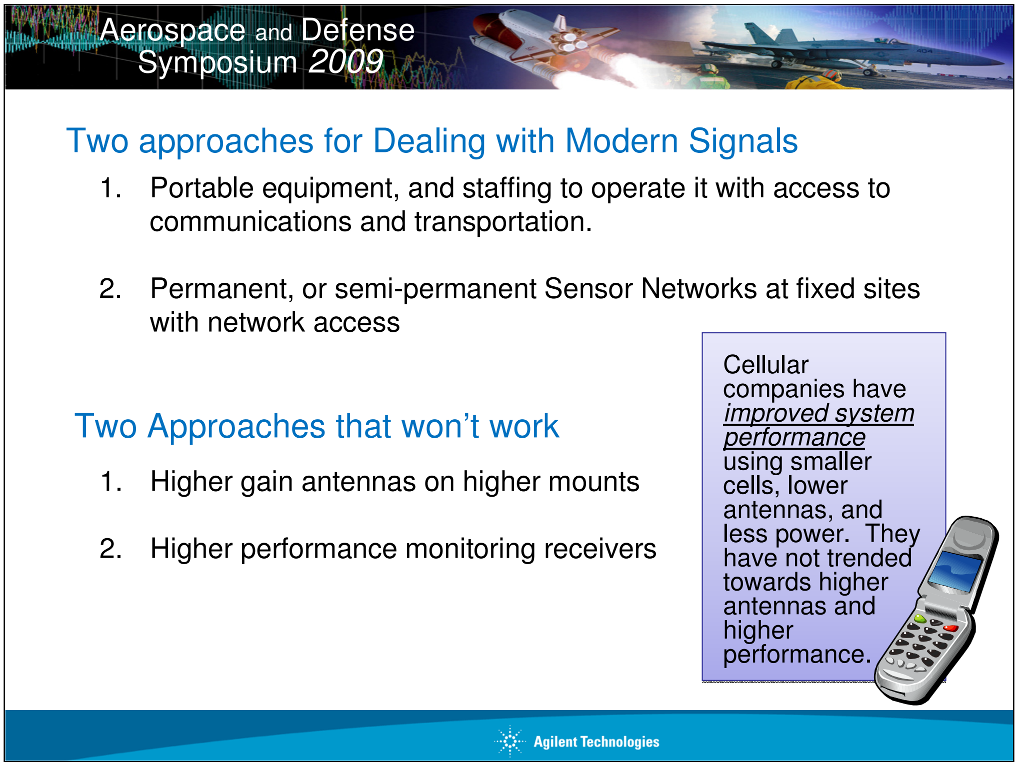
For modern signals and signal-rich environments, the answer is **B**

- A sensitive receiver with wide-area coverage is more susceptible to front-end overload without using pre-selection filters and AGC to reduce receiver sensitivity,
- Taller sites (mountains, buildings, etc) are more likely to have co-located transmitters with greater potential for intermod distortion.
- With high frequency reuse, a single receiver will see multiple co-channel signals making it difficult to extract information from any one transmitter
- Harder to do geolocation with small number of receivers



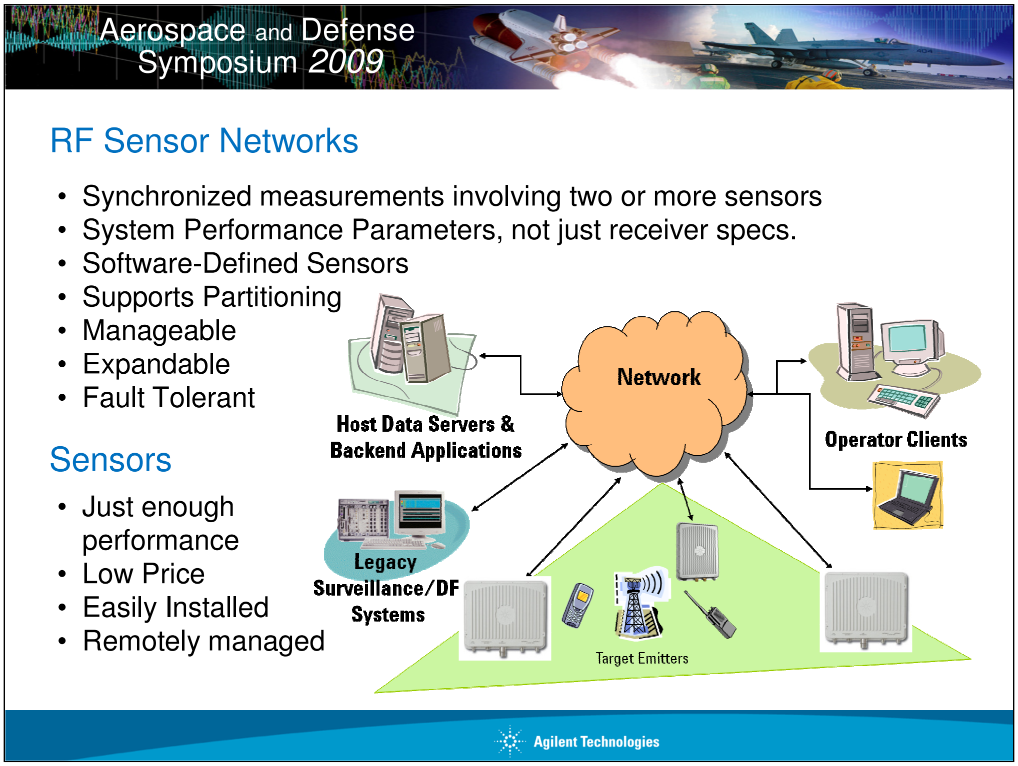


With modern signals, there are many situations where receiver performance isn't the issue, and better receiver performance won't solve the problem. Today's signals often share spectrum, whether through high frequency re-use, or through the use of spread-spectrum techniques. As the ratio



Staffing to carry around hand-held or vehicle-mounted equipment is expensive. Also, efficiency can be low because of commute times to and from area of interest. 24x7 monitoring also harder to accomplish.

Bigger antennas and higher performance receivers won't work in crowded signal environments with co-channel signals. Receiver sensitivity can only be increased so far, and is often unusable because of front-end distortion in the presence of strong signals.



A sensor network is more than a network of receivers. It also encompasses the idea of multiple receivers participating in the same measurement. This requires time synchronization, as well as system level measurement science.

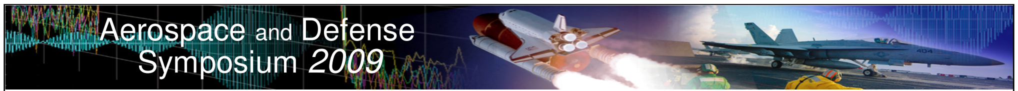
While the performance of a receiver in a system is a factor, it's important to focus on system performance parameters instead of the performance of individual components in the system.

Networks grow over time, so they need to support multiple simultaneous uses. They also need to adapt to support new requirements defined long after the sensor network was installed. They also need to be expandable, which means supporting a hetrogeneous collection of sensors.

Even if a sensor never fails, the communications links to the sensor probably will. Sensor networks need to automatically adapt to the presence or absence of a sensor so that they continue to function without manual reconfiguration.

RF Sensor Networks

- *Potentially better at detecting and locating* ***modern*** *signals*
  - **Lower power/energy, higher bandwidths, higher frequencies**
  - **More complicated modulations schemes**
  - **Multiple synchronized spatially-separated views of same signal**
- *Takes advantage of advances in networking*
  - **Capacity, Speed, Accessibility**
  - **Optical, Wired, Wireless**
- *Configurable*
  - **New tasks, New requirements, New signals**
  - **Multi-tasking (part of a sensor network is doing something different)**
  - **Expandable (new sensors), Dynamic (sensors can move)**
  - **Robust (system still works if part of the sensor network goes off-line).**
  - **Integrate and complement existing monitoring assets**
- *Ease of installation*
  - **Large directional antennas not required**
  - **Broad frequency range with inexpensive antenna**
  - **Smaller footprint – proximity to emitters**



Benefits of Precise Measurement Synchronization

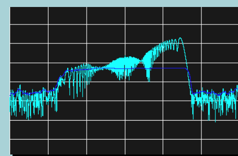
•Time-selectivity in crowded signal environments (e.g. TDD, FHSS, Shared Spectrum)

•Better comparative measurements of power and spectral shapes on modulated and dynamic waveforms

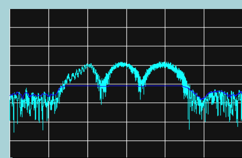
•Processing gain for better sensitivity (coherent detection).

•Geolocation

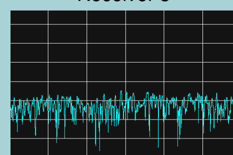
Receiver 1



Receiver 2



Receiver 3



Without accurate time synchronization, the following questions cannot be answered:

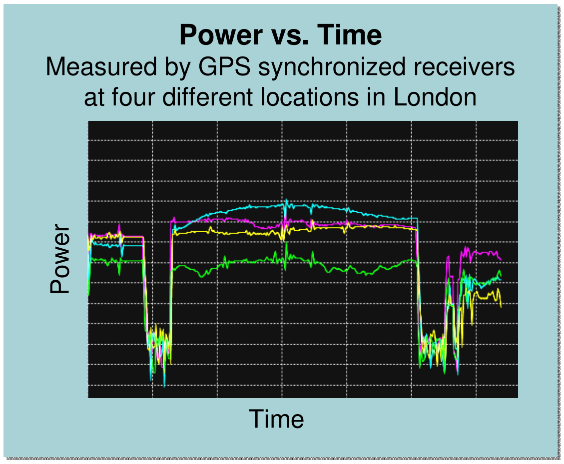
1.Are the RX1 and RX2 spectrums from the same transmitter?

2.If so, is the transmitter signal stronger at RX1, or did the TX power change over time?

3.Is transmitter energy reaching Receiver 3?

4.Where is the transmitter located?

GPS Synchronization



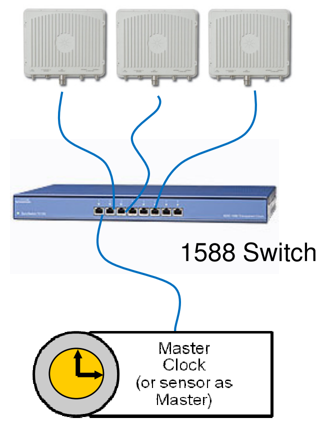
This over-the-air measurement clearly shows three different time slots. From this plot we observe:

1. The relative powers change from slot-to-slot indicating three different transmitters. For example blue is higher than yellow in the second slot, and lower in the first.

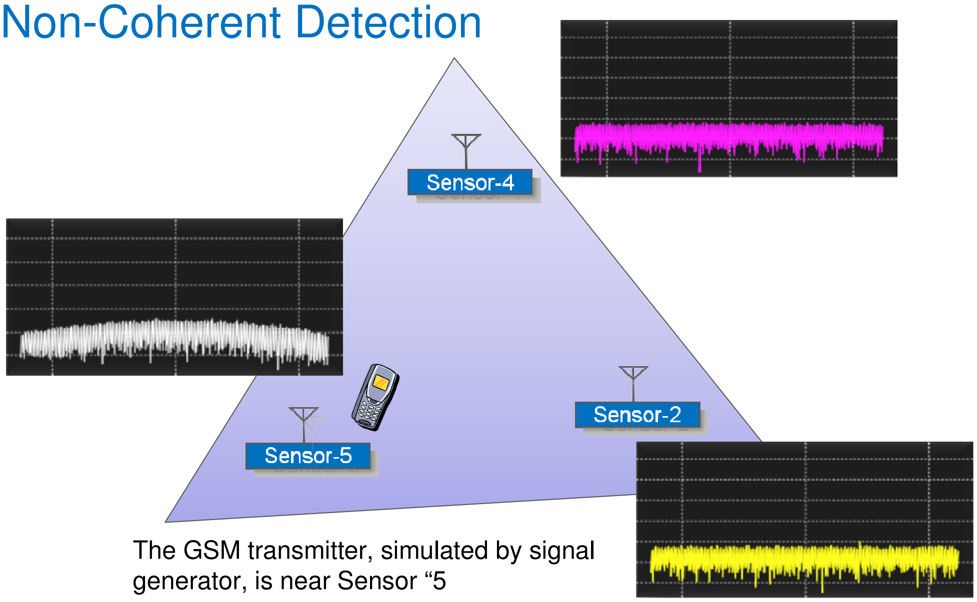
2. The power is fluctuating differently at each receiver for the middle slot. Power fluctuation is probably caused by fading from a moving transmitter.

IEEE-1588 Network Based Time Synchronization

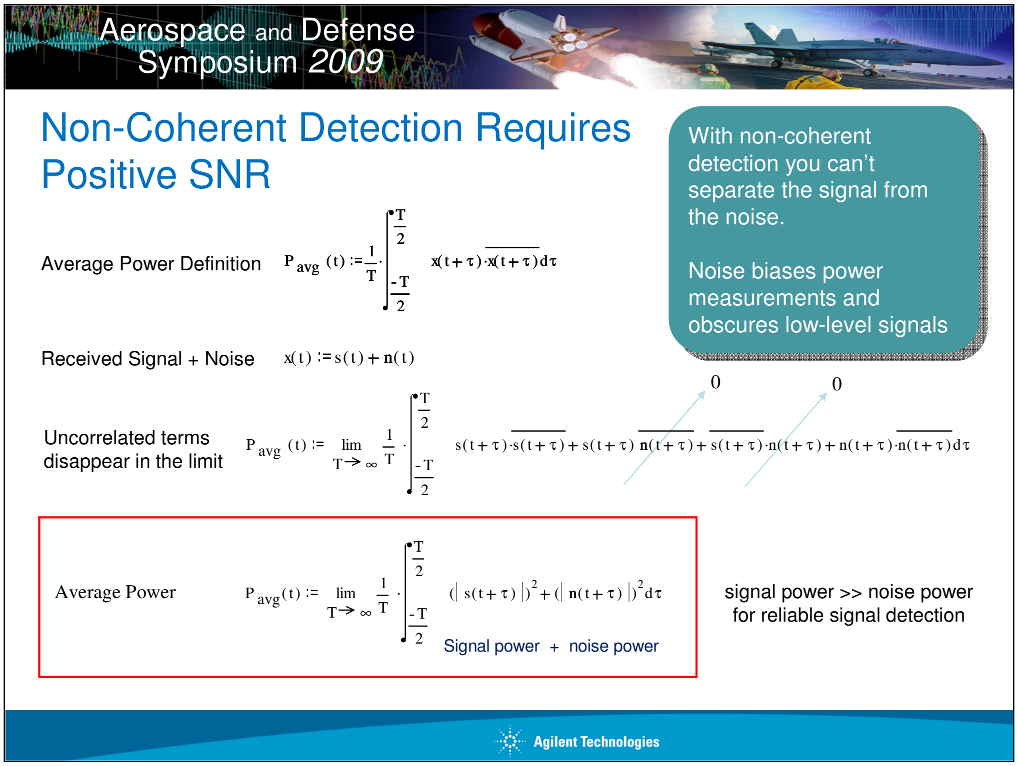
- Invented by Agilent
- Implemented in N6841A RF Sensors
- Provides alternate method of synchronization when GPS can't be used
  - Indoor Environments
  - GPS frequency monitoring
  - GPS jamming
- Time accuracies similar to GPS (10's of nsec or better)
- 1588 Boundary- and Transparent-clock switches available from several vendors



Non-Coherent Detection



The GSM transmitter, simulated by signal generator, is near Sensor "5



Let's start with a time-domain view of the problem.

At a receiver we get the signal of interest s(t) and noise n(t). With non-coherent detection, the power that's actually detected is the signal power plus the noise power. If a signal has the same power level as the noise, 0 dB SNR, then the detected power will only rise by 3dB over the noise power alone.

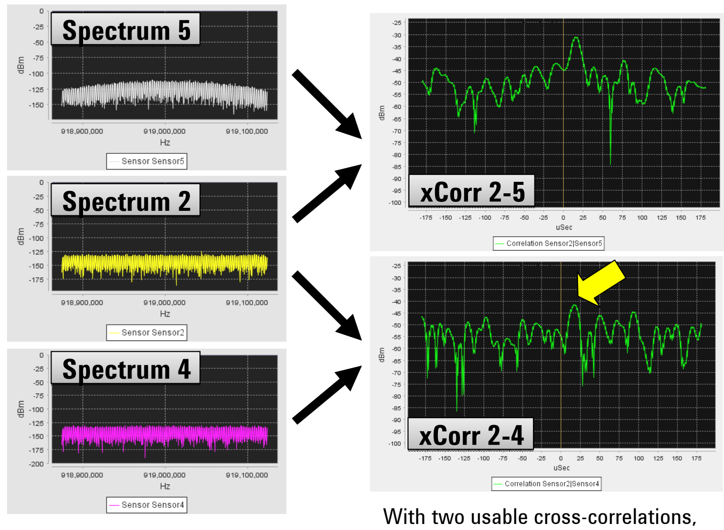
This is fine, but what is the noise power?

Coherent Signal Detection using Cross-Correlations

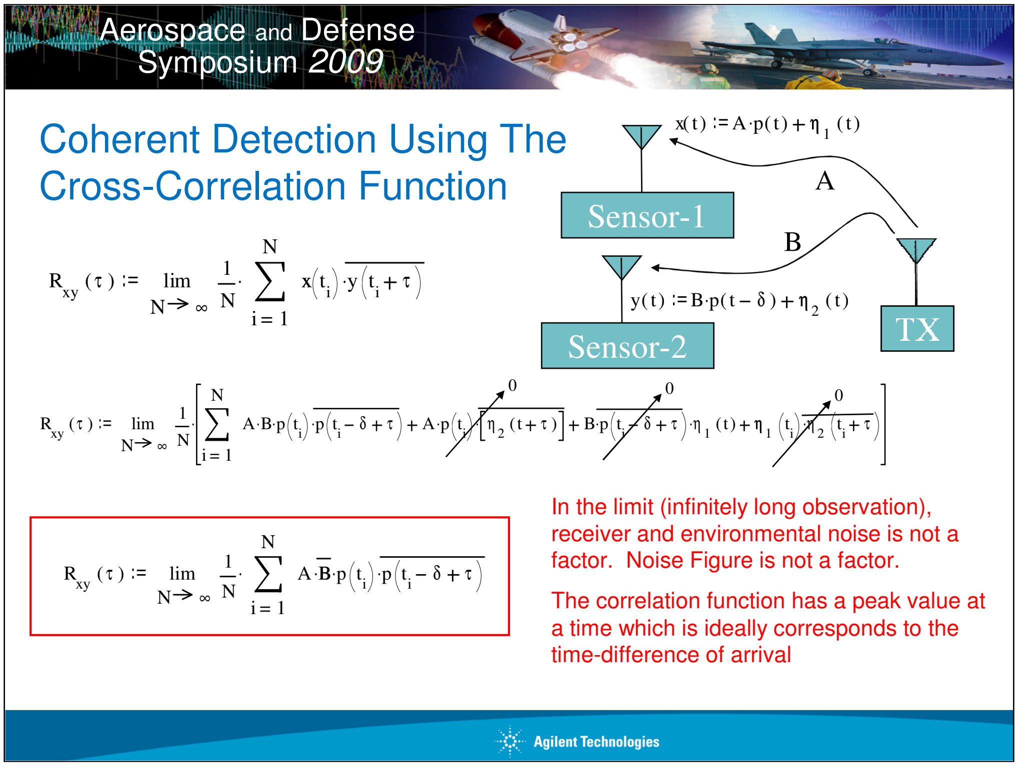
A GSM signal is visible in the sensor 5 spectrum, but not in the spectrums for sensors 2 and 4.

Even without a visible signal in the spectrums for sensors 2 and 4, the cross-correlation between data from these two sensors produces a clear correlation peak.

With the GSM signal clearly visible in the spectrum for sensor 5, it's expected that the sensor 2-5 cross correlation would have a stronger peak.



With two usable cross-correlations, this signal can be located



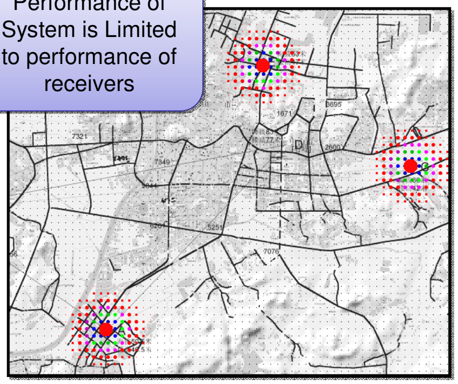
With two receivers, we can define a signal x(t) and y(t) as a scaled version of the transmit signal p(t) plus two independent noise sources. Note p(t) is the same as s(t) in the previous slide.

In this form of the equation where we're computing cross-power, the expected value of the noise is zero and in the limit we're left with a scaled version of the transmit signal's autocorrelation function.

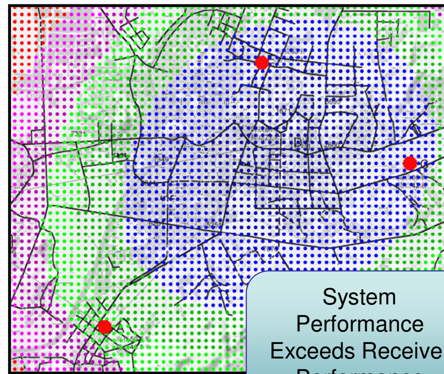
Coherent vs. Non-coherent Detection

Traditional Monitoring Stations using Non-Coherent Detection

Performance of System is Limited to performance of receivers



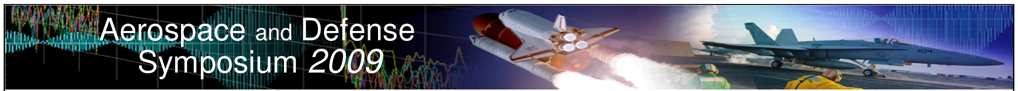
Synchronized Receivers using Coherent Detection



System Performance Exceeds Receiver Performance

1.6 GHz, 200 kHz BW, 300mW

Probability of Signal Detection: Blue > 80% Red < 30%



Another Detection Example

- Two Measurements (32k samples from each sensor)
- Four Sensors (producing 6 cross-sensor pairings)
- Same data processed twice using coherent and non-coherent algorithms

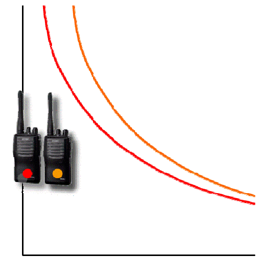
	Non-Coherent				Coherent					
Transmitter	Sensor3	Sensor2	Sensor4	Sensor5	Sensor3-Sensor2	Sensor3-Sensor4	Sensor3-Sensor5	Sensor2-Sensor4	Sensor2-Sensor5	Sensor4-Sensor5
ON	-99.6	-97.5	-102.9	-96.6	-109.2	-117.6	-104.7	-118.9	-106.9	-115.2
OFF	-100.9	-97.6	-103.0	-99.1	-120.0	-124.0	-121.7	-123.5	-115.5	-122.3
Δ dB	1.3	0.1	0.1	2.6	10.7	6.4	17.0	4.6	8.5	7.1

Hard to Detect
Traditional Approach
Requires positive SNR

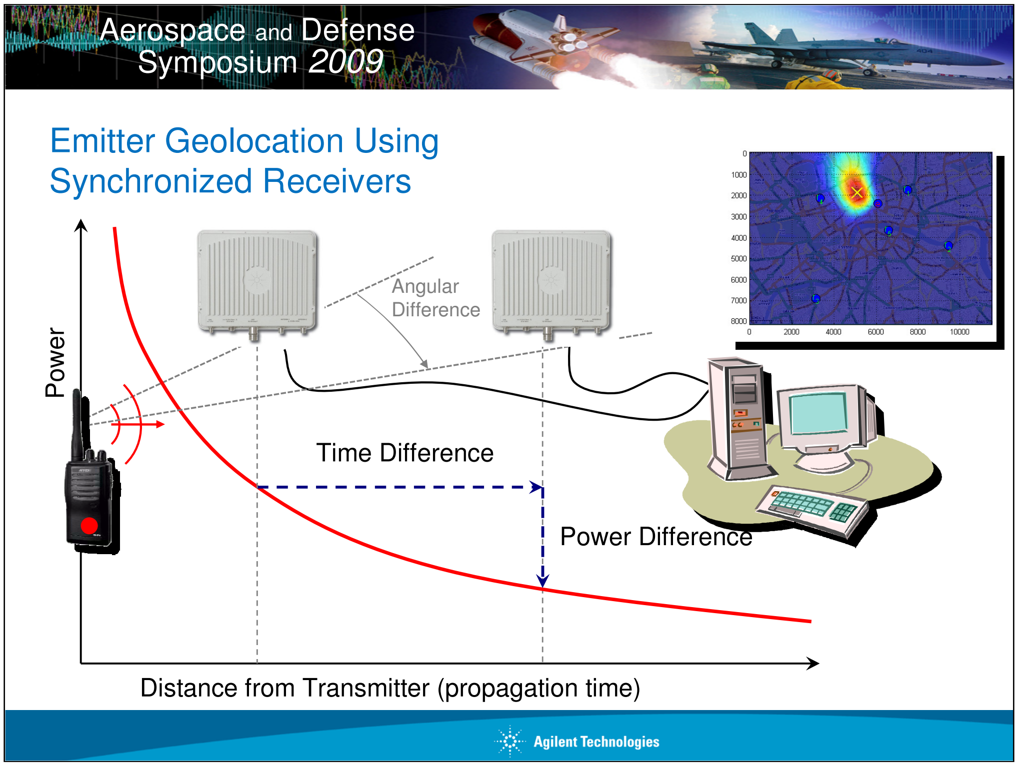
Easy to Detect
Using Correlation

Sensor System Performance Factors

- Sensor Density (receiver spacing)
  - Co-channel Signals
  - Number of sensors detecting energy
  - Cross Sensor Power
- Timing Accuracy
  - Geolocation accuracy TDOA
  - Amplitude Ratio accuracy on modulated signals
- Network Bandwidth and Reliability
- Receiver Performance (e.g. Noise Figure)
  - Important, but not the limiting factor in many instances.
  - Balance RF performance, cost, and sensor density



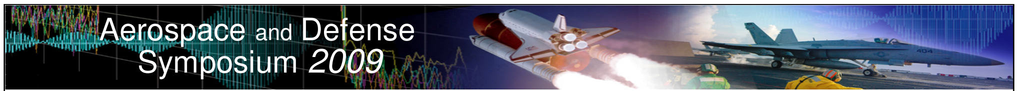
$$R_{xy}(\tau) := \lim_{N \to \infty} \frac{1}{N} \cdot \sum_{i=1}^{N} A \cdot \overline{B} \cdot p(t_i) \cdot \overline{p(t_i - \delta + \tau)}$$



With two receivers, synchronized in time, we can measure both time differences, and power differences. Note that neither sensor has enough information to do anything useful.

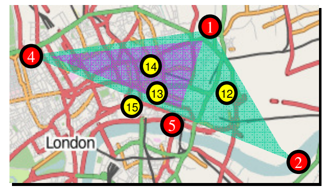
With multiple spatially separated receivers, we can also get an angular difference. We won't talk about DF here except to say that

1. It's more expensive.
    1. Antennas are more expensive, and harder to site (or hide)
2. It's mature technology, very well suited to narrowband emitters with positive SNR.
3. Doesn't work as well with modern signals with low PSD in high-multipath environments.

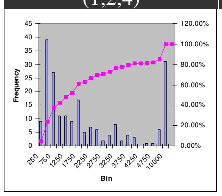


Geolocation Accuracy Improves with Sensor Count

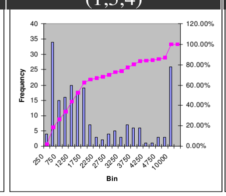
Three sensor minimum for TDOA, but overall results improve dramatically with 4 and 5 sensors. This data is from a trial in downtown London (very dense urban)



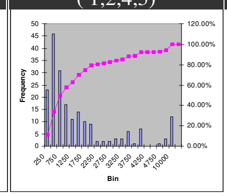
3 Sensors (1,2,4)



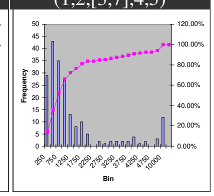
3 Sensors (1,5,4)



4 Sensors (1,2,4,5)



5 Sensors (1,2,[3,7],4,5)



Bin	Frequency	1-2-4 %
250	9	4.43%
500	39	23.65%
750	27	36.95%
1000	11	42.36%
1250	11	47.78%
1500	9	52.22%
1750	17	60.59%
2000	5	63.05%
2250	7	66.50%

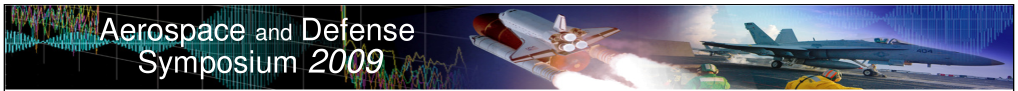
Bin	Frequency	1-5-4 %
250	4	1.97%
500	34	18.72%
750	15	26.11%
1000	16	33.99%
1250	20	43.84%
1500	18	52.71%
1750	19	62.07%
2000	7	65.52%
2250	3	67.00%

Bin	Frequency	1-2-4-5 %
250	23	11.33%
500	46	33.99%
750	31	49.26%
1000	17	57.64%
1250	11	63.05%
1500	14	69.95%
1750	10	74.88%
2000	9	79.31%
2250	2	80.30%

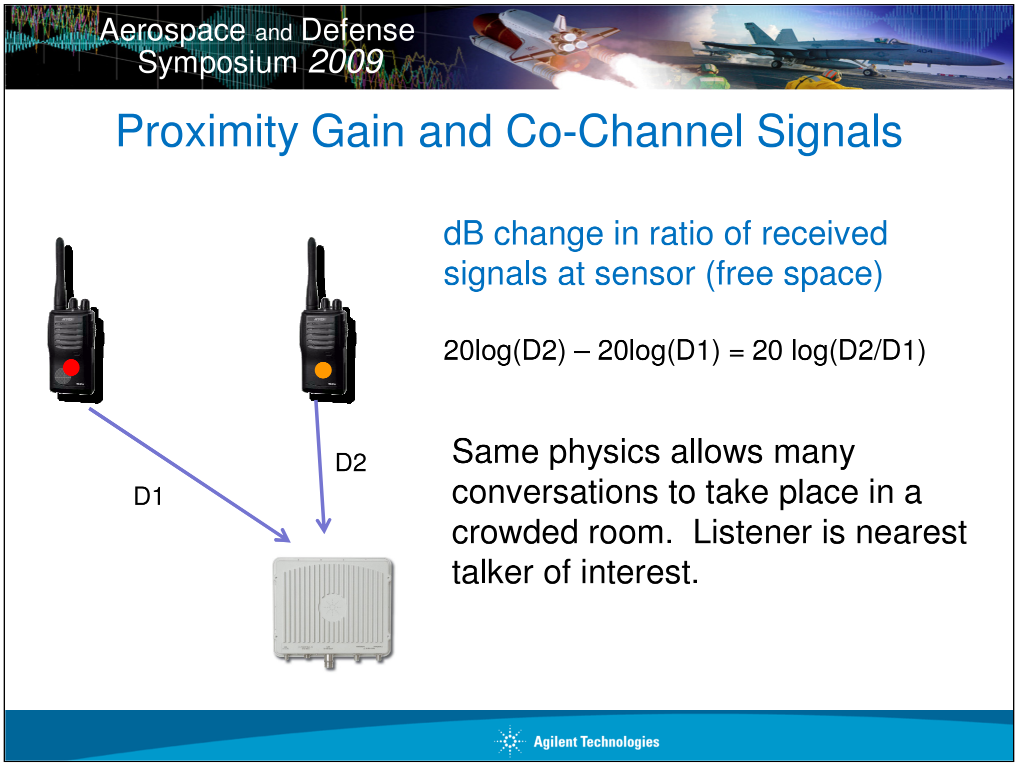
Bin	Frequency	All Avail %
250	29	14.29%
500	43	35.47%
750	35	52.71%
1000	27	66.01%
1250	13	72.41%
1500	8	76.35%
1750	10	81.28%
2000	5	83.74%
2250	0	83.74%

Summary

- RF Trends Drive paradigm shift in monitoring
  - Can't buy/build receivers with enough performance
  - Receiver performance can't solve co-channel signal problems
- Network Trends support paradigm shift
  - Transfer data to common processing point for processing gain
- Synchronization
  - Required because of dynamic signal environment
  - Required for geolocation
- Focus on system price/performance
  - Sensor density is important
  - Trade off density with price/performance of individual receivers



Backup Slides



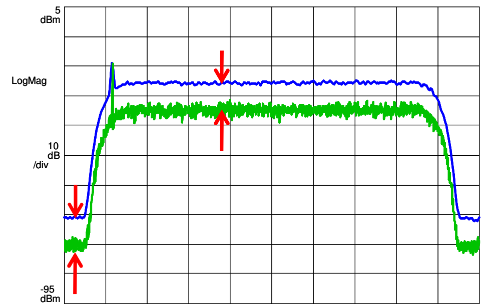
With modern signals, there are many situations where receiver performance isn't the issue, and better receiver performance won't solve the problem. Today's signals often share spectrum, whether through high frequency re-use, or through the use of spread-spectrum techniques. As the ratio

Aerospace and Defense Symposium *2009*

Reducing RBW…

Doesn't work with Most Modern Signals!

- In the DTV Signal on the right the same signal is shown measured with two different RBW's. The pilot stays at the same amplitude while the rest of the signal, and the adjacent noise appears to have lower power.
- The signal power hasn't changed.
- When we reduce the RBW, we are simply dividing the power into smaller pieces. Summed together, those smaller pieces still add up to the same total power.



For signals that are narrower than the RBW, like the pilot, decreasing the RBW will not indicate a change in power. This "trick" is used to pull periodic signals out of the noise. For most modern signals and noise, there is no periodic component, so the trick doesn't work.

Agilent Technologies

With modern signals, you usually can't increase the dynamic range of a spectrum measurement by decreasing the RBW. The DTV signal shown is a bit of an exception because of the pilot (carrier). While the pilot level remains the same as the RBW decreases, the modulated portion of the signal and the adjacent noise both decrease at the same rate so there's no perceived change in SNR. To deal with modern signals and noise, we can talk about the total power, for example the transmit power, or the noise power, and we can talk about the power spectral density. PSD is especially useful for noise signals with uniform densities as a function of frequency.