Agilent
Techniques and Trends in Signal Monitoring, Frequency Management and Geolocation of Wireless Emitters

Application Note

Monitoring RF signals in a wireless environment is often required by a variety of wireless equipment operators, facility and test managers and government agencies. Signal monitoring applications can range from compliance of carrier-specific transmissions to the discovery and location of unknown or illegal transmitters. Traditional methods for signal monitoring rely on high performance spectrum analyzers and digitizers often operating as a standalone system. With the current widespread availability of broadband connectivity, signal monitoring systems have evolved into cooperative networks of low-cost sensors that collectively monitor the wireless spectrum over a large geographic area. This application note reviews various issues, techniques and associated equipment required for signal monitoring and frequency management of RF spectrum in the VHF/UHF frequency range. The goals and automation requirements for various monitoring applications will be discussed and the concepts of implementing a distributed sensor network for determining the geolocation of a wireless "emitter" will be introduced.

Agilent Technologies

Introduction

Monitoring the frequency spectrum in a wireless environment for known and unknown RF signals is required by a variety of equipment operators and government agencies. Applications can range from carrier-specific measurements to wide bandwidth spectrum searching and data logging. In all cases, the spectrum or signal monitoring equipment requires several basic characteristics such as a broad range of frequency coverage, high-speed channel scanning, high frequency resolution and dynamic range, data storage and some level of system automation for determining a course of action when a signal of interest is detected. In some applications, spectrum monitoring is required to ensure compliance with local regulatory requirements while other applications require discovery of unknown transmitters or "emitters". The discovery process may involve uncovering the type of signal including duration of transmission, number of occurrences, carrier frequency, bandwidth, and modulation type and emitter geolocation. Figure 1 shows a typical monitoring system that may contain fixed, stationary and mobile receivers placed throughout a geographic area. Several receivers may be networked together to improve the performance and localization accuracy of the overall system.

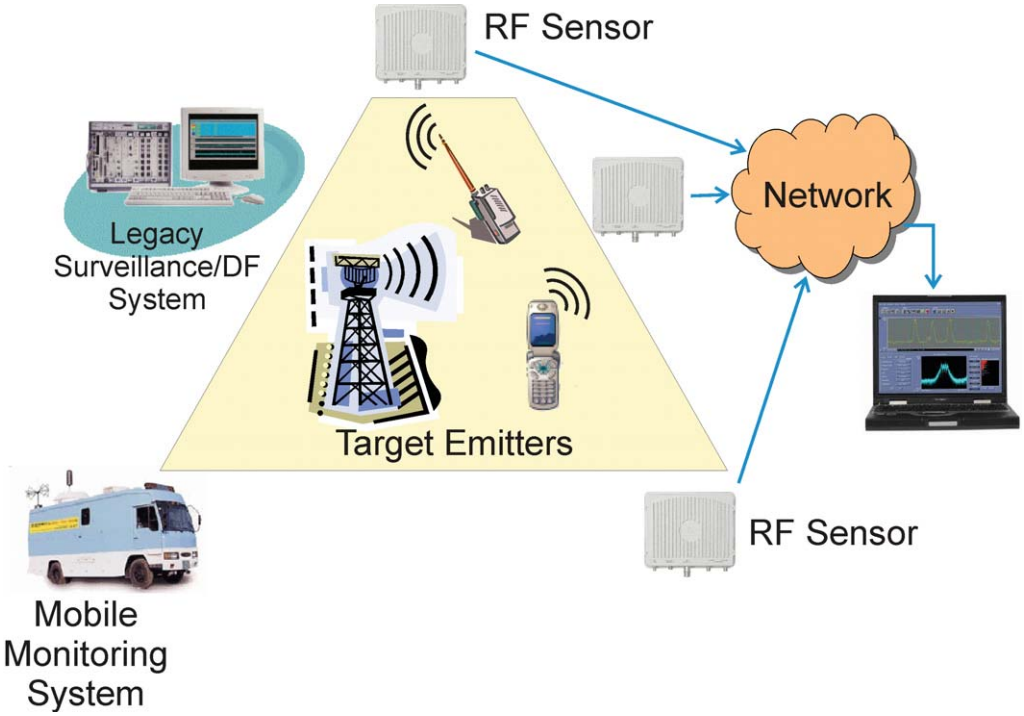


Figure 1. Signal monitoring and surveillance system

Frequency Management

Signal monitoring systems configured for the frequency management of licensed or unlicensed spectrum typically operate over a known set of RF carrier frequencies and modulation characteristics. These systems are used to verify compliance and coexistence with other wireless systems. Typical users interested in frequency management include government agencies, wireless service providers including cellular operators, broadcasters, first responders, transportation agencies for navigation and communication, and military installations. In addition, regulatory agencies that manage spectrum utilization, licensing and coordination of spectrum allocation across national and international regions often establish a network of monitoring stations that cover highly-populated areas. Agencies such as the International Telecommunication Union (ITU) have designated the ITU Radiotelecommunications (ITU-R) organization to manage the RF spectrum and satellite transmission at a global level. National/provincial regulatory agencies, such as the FCC, NTIA, OFCOM, SRRC, and ANFR, manage spectrum utilization at the national level. These agencies need a good understanding of spectrum utilization as license revenue may be lost and they need to uncover and mitigate potential system-to-system interference.

Surveillance

Signal monitoring systems configured for the surveillance of unknown or unfriendly transmissions require measurements of signals that occur sporadically over short periods of time and often require extraction of the intelligence contained within the transmission. Surveillance of wireless signals is rapidly expanding in the areas of law enforcement and correctional facility administration, boarder and coastal security and military intelligence. In many applications, eavesdropping in the form of signal demodulation is required to extract vital intelligence information for use by the military, national security agencies and law enforcement. These types of systems monitor signals originating from both indoor and outdoor locations. Direction Finding (DF) and geolocation are usually associated with these types of systems as signal recovery and knowledge of the emitter location is desirable. In the government and military areas, these transmissions are often characterized in a category called Signals Intelligence (SIGINT).

Interference Management

Signal monitoring systems configured for the interference management of known and potentially harmful signals require specific measurements for a variety of different applications. Some applications require signal monitoring over a large geographic area while some may be limited to the confines of a building or individual room. For example, in test ranges where complex systems, such as aircraft, can be studied for EMI and EMC, signal monitoring equipment may be used to understand potential interference emanating from the aircraft as different subsystems are activated. In some applications, where wireless signals are generally known to cause interference to sensitive equipment, such as specialized instruments installed within a hospital or testing facility, signal monitoring becomes very important to the proper operation of the equipment. For example, healthcare administrators often impose restrictions on the use of cellular handsets within their emergency and intensive care facilities. Studies have shown that transmission from cellular devices in close proximity to sensitive equipment can obstruct the proper operation of equipment such as an electroencephalogram (EEG) monitor [1, 2]. As it is difficult to prevent mobile handsets from being carried into these specialized facilities, it may be necessary to monitor the RF cellular spectrum and trigger an alarm when an undesired signal transmission is discovered.

Emitter Geolocation

Identifying the location of a target emitter is highly desirable especially in surveillance and interference management applications. Direction Finding (DF) and geolocation methods are traditionally based on receivers attached to highly directional antennas. Received signal strength, triangulation and/or angle of arrival (AOA) techniques can be used to accurately locate a transmitter in two and possibly three dimensional space. Increased accuracy can be achieved by increasing the number of monitoring receivers and adding GPS-assisted sample timing and positioning of the receivers. Other geolocation techniques include time difference of arrival (TDOA) and correlation based methods that use digital processing of signals that are simultaneously captured by multiple receivers. The timing among the multiple receivers in these systems can be coordinated using GPS assistance or the IEEE 1588-based network timing protocol pioneered by Agilent and approved by the IEEE in 1992.

The challenge in any signal monitoring system is to quickly detect, identify and possibly locate a distant non-cooperative signal which may be intermittent, be of short duration, and/or have low received power. The trend in wireless communications is toward digital modulation schemes, higher carrier frequencies and wider signal bandwidths. The higher carrier frequency results in larger path loss between the target emitter and the monitoring system making it more difficult to recover the desired signal due to lower signal to noise ratio (SNR) at the receiver. In addition, wider signal bandwidths will result in lower power spectral density at the receiver again making it difficult to detect the desired signal. In many cases, signal monitoring systems based on a single measurement point within a wireless environment may be inadequate for these emerging technologies and proper signal recovery may require the coordinated effort of multiple receivers or sensors being repositioned closer to the target emitter.

Equipment and methods for signal monitoring

The most basic configuration for a signal monitoring system includes a receiver, antenna, low noise amplifier, output display, and possibly, some level of software automation for signal searching and data storage. A traditional swept-tuned spectrum analyzer can provide a minimum set of requirements for the monitoring receiver. The spectrum analyzer is a very flexible platform with a broad frequency range, high dynamic range and graphical display with limit line capability for setting amplitude level detection thresholds. Typically a low noise amplifier (LNA) is placed between the antenna and analyzer to improve the sensitivity of the spectrum analyzer which increases the signal amplitude and lowers the noise figure of the measurement system. Most high performance spectrum analyzers, such as the Agilent PSA and MXA series analyzers, have options for an internal LNA. Many spectrum analyzers have built-in analog demodulation capability but often their use requires the re-tuning of the analyzer's center frequency and span to match the signal of interest. When changing the analyzer's frequency settings it is important that the instrument can rapidly tune the instrument's internal local oscillators (LO) otherwise the probability of intercepting an intermittent signal of short duration may be reduced. Other types of receivers designed specifically for signal monitoring applications may use fast tuning LOs and high-speed digitizers to rapidly measure the frequency content using FFT signal processing. For example, the Agilent E3238S is configured with up to six dedicated FFT processors operating in parallel to achieve exceptionally fast spectral survey rates. When selecting the receiver architecture for surveillance and signal monitoring it is often necessary to examine the features and the performance of the measurement system for the proposed application. Table 1 shows many of the important characteristics required for a basic monitoring receiver.

Table 1. Desired characteristic for a basic signal monitoring receiver

Characteristic	Function
Broad frequency range	Start and stop RF frequency range
Fast survey rates	Fast tuning local oscillators and FFT processing for narrow RBWs
High sensitivity	LNA and narrow RBW settings
Good selectivity	RBW shape
IF output and/or video output	Downconverted and/or detected analog output with wide instantaneous bandwidth. Useful for handoff receiver applications
Graphical display	Visual aid in signal identification. Limit line capability.
Local or remote computer control	Programmable control. Connectivity through LAN, USB, IEEE-488

There are numerous receiver architectures that can be used to achieve the characteristics described in table 1. For example, figure 2 shows the block diagram of a super-heterodyne architecture found in many traditional spectrum analyzers. The input RF signal is filtered and downconverted to an intermediate frequency (IF) using a mixer and local oscillator (LO). A broad range of RF frequencies can be measured by sweeping the LO and measuring the signal amplitude after the IF filter (also known as the RBW filter) in a spectrum analyzer. In signal monitoring applications, it is desired to quickly sweep the receiver's LO in order to capture intermittent signals and increase the probability of intercept (POI). When resolution and sensitivity requires the use of a narrow RBW, the sweep time proportionally increases resulting in a potentially reduced POI. To overcome this sweep time limitation, many receiver architectures use a digital IF and perform IF filtering in the digital domain. Digital filtering can offer a large improvement in sweep time when compared to their analog counterparts. Digital signal processing (DSP) at the IF also provides a convenient path to flexible demodulation capabilities should the measured signals require additional analysis and identification. Figure 2 also shows a separate IF path through an analog-to-digital (ADC) converter where the signal amplitude is detected and processed using DSP techniques.

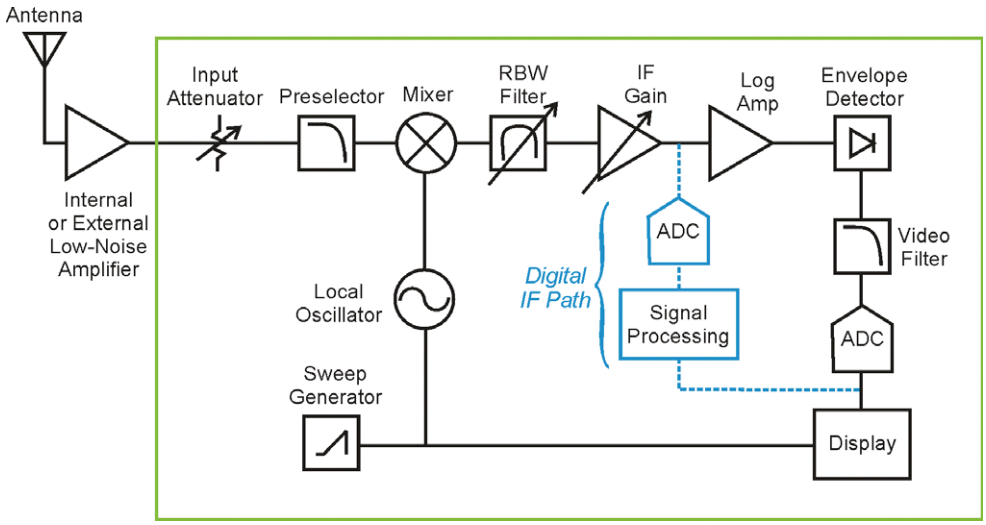


Figure 2. Block diagram of a super-heterodyne receiver

In systems requiring demodulation of the measured signals, the instantaneous bandwidth of the IF must be wider than the modulation bandwidth of the signal otherwise a portion of the occupied spectrum will be attenuated. In traditional AM and FM analog communication systems, the signal's instantaneous bandwidth were typically much less than 200 kHz. In this case, an IF filter approximately matched to the channel spacing of the analog modulated system, such as 30 kHz, would properly pass the desired signal and provide good receiver sensitivity due to the relatively narrow IF bandwidth. With the desire for higher data rates and the introduction of digital modulation schemes, the signal's instantaneous bandwidth increases to 5-20MHz for many emerging wireless systems such as WiMAX™[1] and 3GPP LTE. As the instantaneous bandwidth increases, the receiver's IF filter bandwidth also needs to increase if the signal is to be properly demodulated and identified. Unfortunately, the wider IF bandwidth results in a proportionally reduced SNR into the demodulator. To overcome the SNR limitations, the monitoring system can be modified to increase the signal level into the receiver by increasing the preamplifier gain, increasing the antenna gain or positioning the monitoring system in closer proximity to the emitter. In practice, these techniques have limitations of their own. For example, increasing the preamplifier gain may introduce undesired intermodulation distortion (IMD) products when the receiver is operated in the presence of other signals with higher amplitudes. Antenna gain can be increased resulting in a highly directional antenna with an increase in the antenna's physical size and a potential reduction in operating bandwidth. Physically positioning the monitoring system closer to the emitter may not be practical for a number of reasons including conditions when the emitter's location is unknown over a large geographic area. Consequently increasing the number of receivers in the surrounding environment will tend to increase the total system cost unless a set of low-cost sensors can be placed at a higher density to alleviate many of the SNR issues when monitoring wideband, high-carrier frequency signals.

A traditional rack-mounted surveillance system, configured around a conventional spectrum analyzer or VXI-based receiver, is typically installed in a weatherproof shelter or building and interconnected to rooftop antennas through low-loss coaxial cables. These typically standalone systems may also contain several handoff receivers for demodulation and data storage of specific signals of interest. The handoff receiver takes the downconverted analog IF, and working in parallel with the primary receiver, demodulates the AM or FM signal of interest while not interrupting the search function of the primary receiver. For signal monitoring over a large frequency range, various antenna types may be required to cover the complete range of interest. In this case, an RF multiplexer is connected to the receiver and switched between one of several antennas externally mounted to the facility or vehicle.

In contrast to the traditional approach, a lower-cost network-ready receiver, also referred to as an "RF sensor", can be used as a downconverter and signal acquisition system capable of transferring sampled IQ data over a wired network to a remote system controller for signal processing, data archiving and demodulation. A typical low-cost RF sensor, such as the Agilent N6841A, is a small self-contained weatherproof receiver that can be easily pole-mounted, rack-mounted, vehicle-mounted or configured into a man-portable system. To increase receiver flexibility, the RF sensor is typically configured with "software defined" functionality and a wideband digital IF architecture. Figure 3 shows a simplified block diagram of the Agilent N6841A RF sensor. The sensor has two antenna inputs for local connection to broadband and/or diversity antennas. The system also includes a set of banded pre-selection filters.

1. *("WiMAX," "Fixed WiMAX," "Mobile WiMAX," "WiMAX Forum," the WiMAX Forum logo, "WiMAX Forum Certified," and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum. All other trademarks are the properties of their respective owners)*

These selectable filters are useful when searching for small signals in the presence of high power transmissions and designed to reduce sensor cost and improve reliability. Downconversion to IF is performed using tuner architecture similar to a traditional spectrum analyzer. The digitized IF implements a digital downconverter (DDC) for processing the sampled IF down to baseband. The completely digital IF of the N6841A has a variable bandwidth up to 20MHz to accommodate a variety of wireless technologies and modulation types. Embedded software controls the receiver's triggering, FFT operations and memory capture. Sampled time-stamped data is transferred over the network to a remote server where signal identification and data logging is performed. The receiver's internal clocks can be controlled by the IEEE 1588 network timing or optional GPS. The general concept for implementing a distributed signal monitoring system is to deploy a higher density of low-cost RF sensors placed physically closer to the intended emitters and to have all the advanced signal processing functions operate on the sampled data at a common, centrally located server.

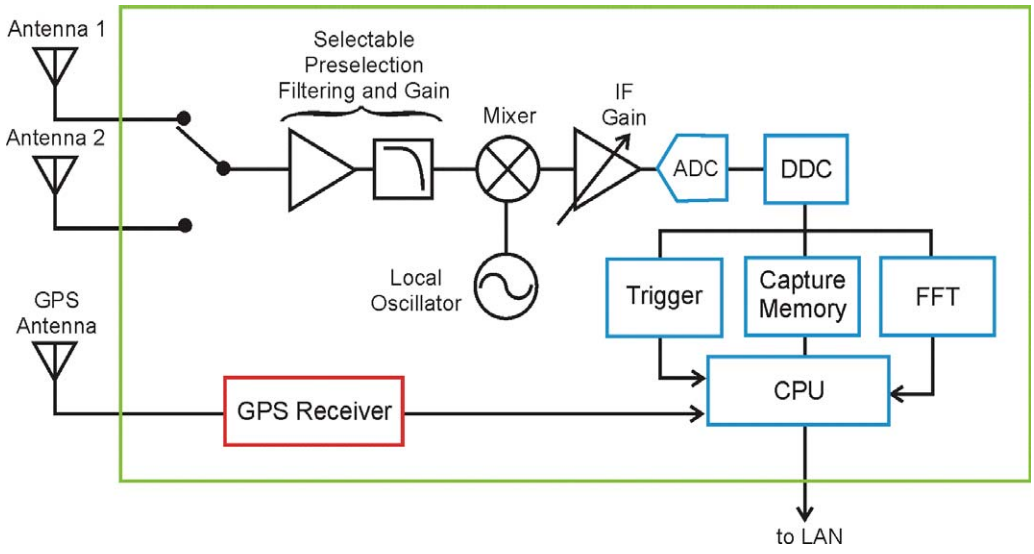


Figure 3. The N6841A RF Sensor block diagram combines a VHF/UHF Receiver with software-defined signal processing

Receiver Location and Proximity Gain

The location of the signal monitoring equipment and the associated antenna(s) will have a great effect on the overall system performance. Attenuation of the propagating signal, also referred as path loss, and nearby interference can impact the receiver's ability to detect the energy from a target emitter. Path loss is a function of the RF carrier frequency and the relative distance between the emitter and the receiver. At higher carrier frequencies, the path loss increases and it may be necessary to locate the receiver in close proximity to the emitter. Interference from the surrounding environment may also influence the receiver's performance. For example, when a receiver is placed in close proximity to a television broadcast station, cellular base station and/or radar system, significant interference can be induced from spurious emissions, harmonics and intermodulation distortion [3]. These effects may also include receiver front-end overload produced from these nearby high power transmitters. It is important to initially monitor the spectrum around the proposed vicinity of the receiver to quantify the influence that these interferers and high power systems may have on receiver performance.

The receive antennas in a signal monitoring system are typically placed high on towers, buildings or hills to reduce the multipath effects introduced by the surrounding environment [4]. Ideally, antennas should be separated from surrounding metallic objects by a distance of several wavelengths otherwise the expected antenna pattern may become distorted [3]. Even the metallic mast that the antenna is attached can greatly influence the gain pattern [5]. Also other antennas in the nearby vicinity can alter the antenna pattern and reduce system performance in unexpected ways. Proper placement of the antenna is crucial to the overall performance of the monitoring system especially in applications where a limited number of high performance receivers are located over a wide geographic area. On the other hand, systems based on low-cost RF sensors allow relaxed antenna requirements resulting from the proximity gains achieved using a higher density of receivers. Figure 4 shows a roof-mounted RF sensor connected to a broadband antenna with a second antenna placed on a separate mast. The sensor is placed relatively close to the antennas to reduce cable loss that could degrade the noise figure of the system.

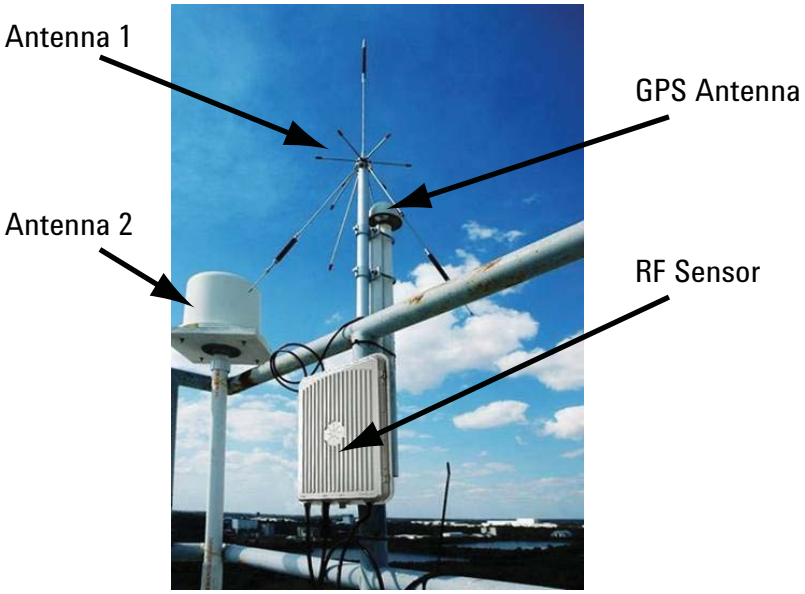


Figure 4. RF sensor and antennas configured on a rooftop installation

Receiver Location and Proximity Gain (continued)

When the emitter location is unknown, it is desirable to use antennas with omni-directional patterns for terrestrial applications. Unfortunately omni-directional antennas have low gain, approximately 0dBi, and do not help to improve the receiver's SNR. Increasing antenna gain may improve the SNR but the resulting antenna pattern will favor signal reception into a particular direction. Unless a highly directional (high gain) antenna is physically or electronically scanned into the direction of the emitter, it is possible that an unknown emitter may be missed due to low receive SNR.

Higher RF carrier frequencies often used in modern wireless communications such as cellular and WLAN, result in an increase in the free space loss when compared to similar systems operating at lower VHF/UHF frequencies. At these higher carrier frequencies, it may be necessary to locate the monitoring antenna/receiver closer to the emitter in order to maintain a reasonable level of SNR. The signal improvement achieved when reducing the separation between the emitter and the receiver is referred to as "proximity gain". For example, assume that two communication systems are operating over the same distance between the emitter antenna and the signal monitoring antenna. One system is operating with a RF carrier frequency of 100MHz with a 20 kHz modulation bandwidth. The second system is operating at 2.4 GHz with a 20 MHz modulation bandwidth. What is the measured SNR for each system assuming identical transmit power, antenna gains, cable loss and receiver noise figure? What are the main contributors to the SNR difference? In order to answer these questions and to estimate the performance of each system, the SNR is calculated using the following equation (1).

$$SNR = [P_T + G_T - P_L + G_R - C_L] - [-174 + NF + 10\log_{10}(BW)] \quad (1)$$

where

SNR = Signal to Noise at Receiver (dBm)

PT = Transmitter Power (dBm)

GT = Transmitter Antenna Gain (dB)

PL = Path Loss (dB)

GR = Receiver Antenna Gain (dB)

CL = Cable Losses between antenna and receiver (dB)

NF = Receiver Noise Figure (dB)

BW = Receiver Bandwidth (Hz)

The path loss, PL, is a function of the RF carrier frequency and the distance between the emitter and receiver antennas. The path loss increases at higher frequencies and larger distances. The path loss is calculated (in dB) using the following equation (2) [6].

$$PL = K + 20\log_{10}(f) + 20\log_{10}(R) \quad (2)$$

where

f = frequency (MHz)

R = distance (km)

K = 32.45 (for R in km)

As an example, assume that an emitter is transmitting a signal with +20dBm (100 mW) from a distance of 5 km to the monitoring system. Using antenna gains of 0dBi, cable losses of 0dB and receiver noise figure of 14dB, the signal transmission at 100MHz with a 20 kHz BW has a calculated SNR of approximately +51dB. For the signal operating at 2.4GHz with a 20MHz bandwidth, the calculated SNR is -7dB. Under these conditions, it would be easy to measure the 100MHz signal but very difficult to measure the signal operating at 2.4 GHz. Table 2 summarizes the path loss and SNR performance for these two systems. The difference in SNR between these two systems is directly related to the carrier frequency and modulation BW. For this example, the relative SNR for the 2.4GHz system is reduced by 28dB due to the increased path loss resulting from the higher carrier frequency and reduced by 30dB due to the increase in the noise power resulting from the wider modulation bandwidth. As it may be difficult in practice to greatly improve the receiver's noise figure and/or increase the receiver's antenna gain, SNR improvement for systems operating at high carrier frequencies would require a smaller separation between the emitter and receiver. The proximity gain would overcome the excessive path loss introduced by RF signal transmission at higher carrier frequencies. Continuing with the above example, if the minimum required SNR is 10dB, the proximity gain needs to increase the SNR from the original -7 dB to the required +10 dB or a total gain of 17 dB. In this case, the distance between the emitter and receiver for the 2.4GHz system would need to be reduced from original 5 km to less than 0.7 km. It is important to note that in order to keep the same monitoring coverage over the same geographic area it will be necessary to increase the density of receivers when operating at higher RF carrier frequencies.

Table 2. Calculated link budget for two types of wireless systems

Basic Parameters

P_T = +20dBm
G_T = 0 dB
G_R = 0 dB
C_L = 0 dB
N_F = 14 dB
R=5km

	System 1	System 1
Freq (MHz) BW (MHz)	100 MHz 20 kHz	2400 MHz 20 MHz
Calculated Path Loss (dB)	86	114
Calculated SNR (dB)	51	-7

The path loss calculations shown above were made for an ideal line of sight (LOS) condition without the ill effects of multipath fading and/or shadowing. Multipath can create additional signal loss at the receiver and is often stated in terms of fading depth. There have been numerous studies for estimating and modeling multipath fading in various terrains but in general, systems operating in the VHF/UHF frequency range have been shown to experience fading depths of 5 to 40 dB when operating in urban and rural areas [7, 8, 9]. The additional amplitude loss at the receiver must be considered when estimating the overall link budget and placement of the signal monitoring equipment especially in narrow bandwidth systems.

Receiver Location and Proximity Gain (continued)

Increasing proximity gain is only one of several techniques to combat the detrimental effects of multipath. Another relatively simple technique using a second antenna can potentially improve the fading characteristic through the application of spatial or polarization diversity. It is know that two antennas either separated by a distance of greater than ¼ wavelength or positioned in a cross-polarized orientation will have uncorrelated multipath characteristics. It becomes possible that when one antenna experiences a deep multipath fade, the second antenna could be receiving a signal with a reasonable power level. The monitoring system would scan between the two antennas looking for the largest signals for analysis. Most signal monitoring systems are equipped with RF multiplexing circuits to add additional antennas as required by the operating environment. For example, the Agilent N6841A has three antenna ports, two for antenna multiplexing and one for the optional GPS subsystem. The two antenna multiplexing ports can be used for spatial and/or polarization diversity to combat multipath fading or configured to extend the measured frequency range when narrow-bandwidth antennas are used. Understanding the effects of multipath on system performance has created a need for advanced measurement tools specifically designed for simulating multipath conditions on the bench. For those interested in additional details on the characteristics of multipath, multiple antenna systems and techniques for simulating multipath channels, Agilent has published a detailed application note on the subject which includes numerous measurement examples using the Agilent PXB N5106A MIMO channel simulator [10].

Goals and methods for signal identification

As previously mentioned, the challenge for any signal monitoring system is to have the performance and speed to quickly detect, identify and potentially locate the transmissions of wireless signals which may be intermittent, be of short duration, or be wideband with low SNR. The signals of interest may include transmission from multimedia broadcast systems, wide area network (WAN) communications including cellular handset and basestation transmissions, wireless local area network (WLAN) communications, point to point microwave links including satellite uplinks and downlinks, and radio frequency identification (RFID) reader/tag communications including active and passive tag technologies. At any one time, a measurement over a wide frequency range will contain many of these signal types and it is the function of the signal monitoring system to sift through the numerous signals to identify and analyze only those signals of interest.

Efficiently sorting through the spectrum data may not be an easy task for a human operator using a standalone spectrum analyzer. Automating the process of signal searching and identification is better handled with software tools such as the Agilent N6820E Signal Surveyor analysis tool. When the signal survey tool is configured with a high performance receiver, such as the E3238S VXI-based receiver or the N6841A RF sensor, the process for automatic signal detection can be accomplished through the use of thresholds, and software alarms that can be set to trigger a system response when the measured signal power exceeds a pre-determined amplitude. A typical configuration of a RF sensor connected over a network to the signal survey software is shown in figure 5. The RF sensor can continuously stream data when the IF bandwidth is configured for 200 kHz or less. Due to latencies in the 10/100 TCP/IP network protocol, signals with wider IF bandwidths, up to 20MHz, requires data to be transferred in time-coded blocks. The survey software processes the sampled data for signals of interest. The software may also be configured to automatically identify modulation type (option MR1) or configured to store the time series or frequency data. Archived data can later be post-processed using a variety of commercial and custom software tools.

As shown in figure 5, the Agilent 89601A software can be used to demodulate the captured analog or digitally modulated waveforms, or the Agilent N6829A software player can be used for listening to the recovered audio.

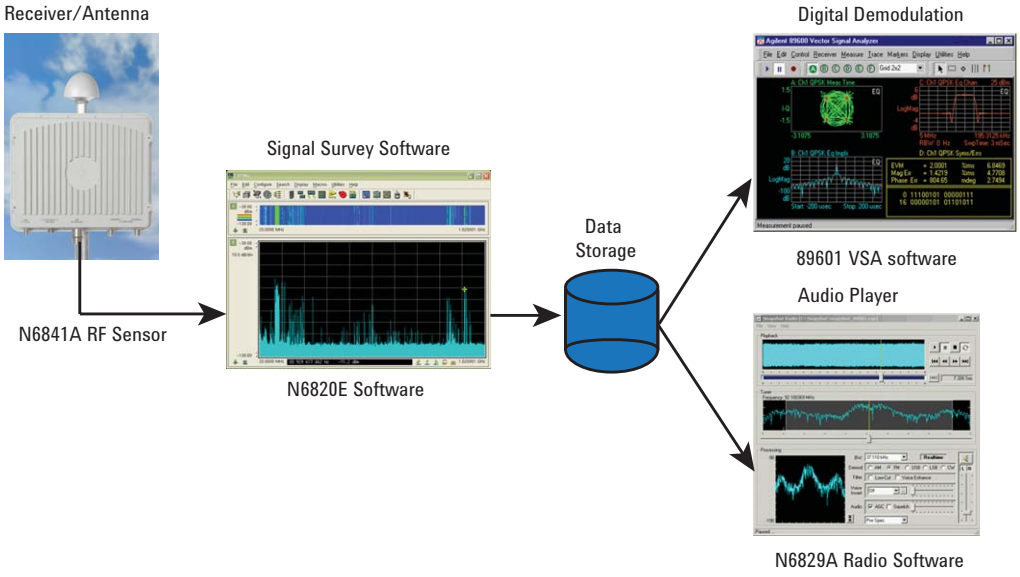


Figure 5. Signal monitoring automation software collecting time series data from receiver and data storage for post-processing

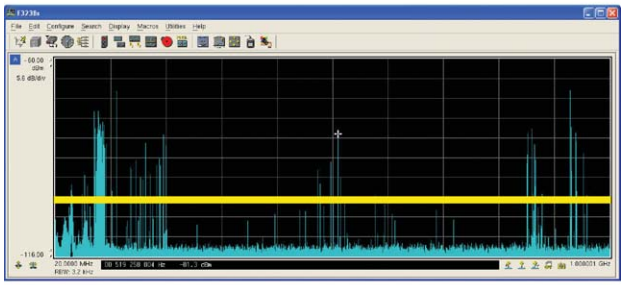
Limit lines and other software alarms is an important feature for any signal monitoring system. These alarms can be configured to automate the discovery process for unknown emitters as well as confirm spectrum compliance for known transmissions. Threshold levels can be determined using either measurement from the baseline RF environment, automatically configured by the system, or defined by the user. For example, figure 6 shows three types of threshold techniques available using the N6820E signal survey software. The upper plot shows the "level threshold" that has a similar function to a limit line in a spectrum analyzer. The level threshold works well when the noise floor is flat and unchanging, as it often is in VHF/UHF and microwave spectrums. The center plot displays the "auto threshold" technique that shapes itself to the noise floor. This is especially important when the noise floor is not flat, such as in the HF range, and/or changes with the time of day and year. The lower plot shows the "environmental threshold" that uses a snapshot of the current spectrum, including any existing signals, and then uses this shape as the threshold for subsequent measurements.

Another option for automatically identifying signals of interest is with the use of "universal signal detection" software. This type of specialized software, such as the Agilent N6820E option USD, automatically identifies signals by operating on the characteristics of RF transmissions. The universal signal detectors include bandwidth and shape filters, frequency plans, wideband detectors, and narrowband confirmers. The combination of wideband and narrowband technologies efficiently sifts through the crowded spectrum and significantly increases the probability of intercept. The wideband search processes all signals in the RF environment and uses signal detection tools to filter out all but the signals of interest. Once the signals of interest are identified, only that data is collected and recorded for additional analysis. As new signals are detected, an energy history log can be updated.

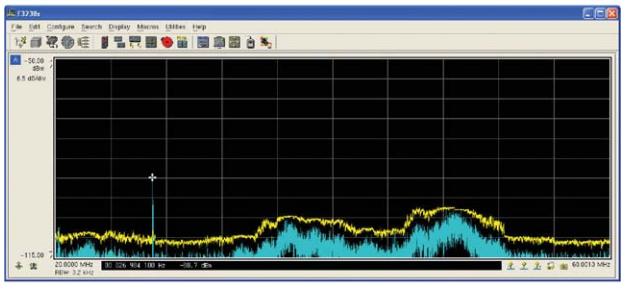
The energy history log automatically stores the parameters of all energy above the threshold on every sweep. The following list shows typical parameters that would be stored to the energy history log file. These parameters can also be used as alarm conditions for triggering a system response.

- Frequency
- Bandwidth
- Percent Occupancy
- Date and Time of first intercept
- Date and Time of last intercept
- Amplitude Statistics
- Duration

(a) Level



(b) Auto



(c) Environmental

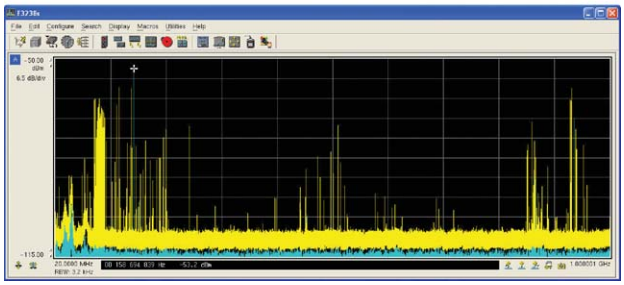


Figure 6. Energy detection threshold techniques

Sensor networks and geolocation

The trend for modern communication systems toward higher carrier frequencies and wider bandwidths will result in higher path loss and receiver noise. As previously shown, the detection probability of known and unknown signals is directly related to the emitter's RF carrier frequency and the modulation bandwidth. There is also a trend in the wireless industry, especially in emerging cellular systems such as 3G and 4G, toward implementing a higher density of basestations. Numerous industry and academic studies are examining picocell and femtocell topologies for higher frequency reuse and lower transmit power levels [11, 12]. The combination of higher path loss and lower transmit power levels will reduce the probability of detecting signals operating with wider instantaneous bandwidths. To overcome these difficulties, a signal monitoring system can improve system performance by increasing the proximity gain of the receiver, or in other words, place the monitoring system physically closer to the emitter. Increased proximity gain does not come without a cost. If the distance between the emitter and receiver is required to be halved for adequate SNR then the equivalent coverage area drops to ¼ of the original. In order to maintain adequate probability of detection levels, mobile and/or portable receivers can be moved into the geographic areas where emitters are expected to be operating. Alternatively, a higher density of monitoring receivers, including fixed low-cost RF sensors, can be placed throughout the environment and networked together for an improvement in overall system performance. This network of sensors can also be used to estimate the location of an emitter in a process also referred to as geolocation.

Sensor networks have been studied and implemented in recent years for a variety of applications including environmental sensing, asset tracking and manufacturing process flow but the concept of extending this technology to signal monitoring and frequency management is relatively new to this industry. An RF sensor network for signal monitoring will implement either non-coherent or coherent detection of measurements from distributed receivers connected over a wired backhaul network. Receivers in a sensor network using non-coherent detection will provide faster detection speed due to reduced signal processing requirements and backhaul network loading. However, non-coherent detection may result in the inability of the system to separate the signal from the noise as noise biases the power measurements and obscures low-level signals. In this case, a positive SNR is required for increased PoD using non-coherent detection. On the other hand, RF sensor networks using coherent detection combine signals captured from multiple receivers resulting in a large improvement in the PoD when compared to non-coherent methods. One method of coherent processing uses the cross-correlation function. In this case, measurements of the same transmitted signal from two separate sensors are cross-correlated resulting in a suppression of the independent noise characteristics. In the theoretical limit of long cross-correlation times, the receiver and environmental noise is not a factor and the system's detection performance becomes less limited by the receiver's performance including its noise figure. Even when the signal is of short duration, coherent detection using multiple sensors provides additional benefits relative to non-coherent detection schemes.

As a comparison of the PoD performance between receivers using non-coherent detection and a networked system using coherent detection, figure 7 shows the PoD contours for three RF sensors operating using traditional and cross-correlation techniques. In this figure, areas shown in blue have an 80% or higher probability of detecting a 1.6GHz signal transmitted at 300mW and having 200 kHz bandwidth. Areas shaded in red have a lower than 20% PoD. As shown in figure 7a, sensors that independently monitor signal level have a very small area of high PoD. For this traditional non-coherent scheme, the detection performance is limited by the performance of the receiver and the proximity gain.

Alternatively, figure 7b shows the PoD performance for the same sensors using the same measurements but now coherently combined. As shown in the figure, the areas of high PoD are greatly improved when compared to those using the traditional methods. The sensor network approach to signal detection allows lower-cost receivers, or RF sensors, with "just enough" performance while providing a scalable system that is remotely managed.

Another benefit to the RF sensor approach is the potential for geolocation of emitters in the surrounding environment. Finding the location of indoor and/or outdoor wireless transmitters has many applications including search and rescue, tracking high-valued equipment and finding illegal or interfering transmitters to name just a few. Many different technologies have been developed to locate wireless emitters including received signal strength (RSS), angle of arrival (AOA), time of arrival (TOA) and time difference of arrival (TDOA). Most of these approaches require measurements to be taken from three or more separate locations. Whether the measurements involve power level, time of flight or some other parameter, or combinations of these, the emitter's geolocation is typically determined by mathematical triangulation of the received signals. Coherent processing of signals measured using an RF sensor network is ideally suited for geolocation. For this application, the cross-correlation properties previously discussed also yields the time difference of arrival between pairs of sensors. Having the TDOA between three or more pairs of RF sensors can be used to triangulate the location of an unknown emitter in relation to the sensors locations. For example, figure 8 shows the measured cross-correlations between two pairs of sensors. In this figure, the cross correlation between measurements taken from sensor 1 and sensor 2 is shown in blue, and the cross-correlation between sensors 2 and 3 is shown in yellow. The correlation between sensors 1 and 3 is not shown but required for determining emitter location. The peak in the cross-correlation corresponds to the relative timing between the signals measured at that associated receiver pair. All correlation measurements in this figure are coming from a single emitter transmitting a broadband CDMA signal. An estimate of the emitter's location is calculated using the timing differences between the peaks in the cross-correlation responses. In this example, the time difference, Δt, between the correlation peaks of 1-2 and 2-3 is approximately 10 microseconds. Using the time differences between the peaks for 1-2/1-3 and 2-3/1-3 sensor pairs, the location of the emitter can be triangulated. It should be understood that using additional sensors can greatly improve the geolocation accuracy especially in high multipath environments.

(a) Traditional non coherent dection (b) Sensor-based coherent detection

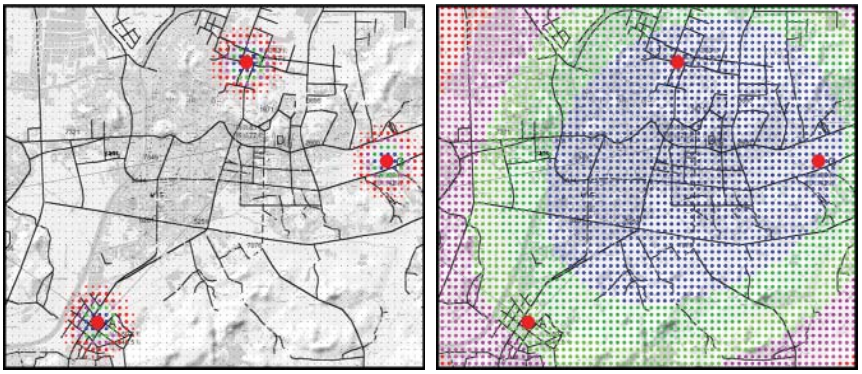


Figure 7. Probability of detection using non-coherent and coherent detection schemes

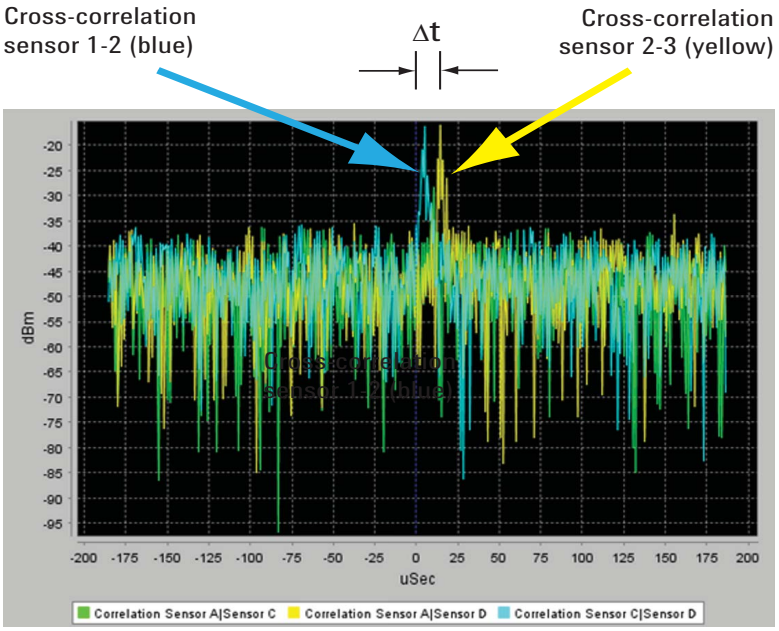


Figure 8. Cross-correlation responses between multiple RF sensors

Conclusion

This application note has described the techniques, goals and trends in signal monitoring and frequency management of RF spectrum. New technologies based on distributed low-cost RF sensors have been shown to improve the detection capabilities of monitoring systems and a method for determining the geolocation of wireless emitters has been introduced.

References

[1] E.D. Nanoun, V.G. Tsiafakis, E.S. Kapareliotis, A.I. Sotiriou, C.N. Capsalis, "Electromagnetic compatibility between GSM base station and EEG signal,"

IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications 2005, vol. 1, pp 535 – 538, Aug. 2005.

[2] J.L. Silberberg, "Achieving medical device EMC: the role of regulations, standards, guidelines and publications," IEEE International Symposium on Electromagnetic Compatibility, 2001, vol. 2, pp. 1298 – 1303, Aug. 2001.

[3] International Telecommunications Union Radiocommunication Sector (ITU-R), Supplement to Handbook on Spectrum Monitoring, 2008.

[4] A.G. Kanatas, , N. Papadakis, P. Constantinou, "An empirical model for high elevation angle land-mobile satellite channels at urban environment," IEEE Communications Letters, vol., issue 4, pp 92-93, April 1998.

[5] M. Albani, P. Focardi, A. Freni, S. Maci, "Pattern distortion for corrugat horns open-ended on a finite ground plane," IEEE Antennas and Propagation Society International Symposium, 1999, vol. 4, pp 2272-2275, July 1999.

[6] Modern Antenna Design, Thomas A. Milligan, Wiley Interscience, 2nd edition, 2005.

[7] K.H. Loso, W.T. Barnett, A. Vigants, F.G.; Inserra, J.R.; Brockel, "US Army tactical LOS radio propagation reliability," Proceedings of the Tactical Communications Conference, 1992. Vol. 1 Tactical Communications: Technology in Transition, pp 109-117, April 1992.

[8] T.S. Seidel, S.Y. Rappaport, "Simulation of UHF indoor radio channels for open-plan building environments, IEEE 40th Vehicular Technology Conference, pp 597-602, May 1990.

[9] H. Suzuki, "A Statistical Model for Urban Radio Propogation, H. Suzuki," IEEE Transactions on Communications, vol. 25, issue 7, pp 673-680, Jul. 1977.

[10] Agilent Application Note "MIMO Channel Modeling and Emulation Test Challenges," lit. number 5989-8973EN, Oct. 2008.

[11] C. Edwards, "The future is femto, " Engineering & Technology, vol.3, issue 15, pp 70-73, Sept. 2008.

[12] D. Das, V. Ramaswamy, "On the Reverse Link Capacity of a CDMA Network of Femto-cells," IEEE Sarnoff Symposium, 2008, pp 1-5, April 2008.

www.agilent.com
www.agilent.com/find/ad

Agilent Email Updates

www.agilent.com/find/emailupdates
Get the latest information on the products and applications you select.

Agilent Direct

www.agilent.com/find/agilentdirect
Quickly choose and use your test equipment solutions with confidence.

LXI

www.lxistandard.org
LXI is the LAN-based successor to GPIB, providing faster, more efficient connectivity. Agilent is a founding member of the LXI consortium.

Remove all doubt

Our repair and calibration services will get your equipment back to you, performing like new, when promised. You will get full value out of your Agilent equipment throughout its lifetime. Your equipment will be serviced by Agilent-trained technicians using the latest factory calibration procedures, automated repair diagnostics and genuine parts. You will always have the utmost confidence in your measurements. For information regarding self maintenance of this product, please contact your Agilent office.

Agilent offers a wide range of additional expert test and measurement services for your equipment, including initial start-up assistance, onsite education and training, as well as design, system integration, and project management.

For more information on repair and calibration services, go to:

www.agilent.com/find/removealldoubt

Product specifications and descriptions in this document subject to change without notice.

For more information on Agilent Technologies' products, applications or services, please contact your local Agilent office. The complete list is available at:

www.agilent.com/find/contactus

Americas

Canada	(877) 894-4414
Latin America	305 269 7500
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
Thailand	1 800 226 008

Europe & Middle East

Austria	01 36027 71571
Belgium	32 (0) 2 404 93 40
Denmark	45 70 13 15 15
Finland	358 (0) 10 855 2100
France	0825 010 700*
	*0.125 €/minute
Germany	07031 464 6333
Ireland	1890 924 204
Israel	972-3-9288-504/544
Italy	39 02 92 60 8484
Netherlands	31 (0) 20 547 2111
Spain	34 (91) 631 3300
Sweden	0200-88 22 55
Switzerland	0800 80 53 53
United Kingdom	44 (0) 118 9276201

Other European Countries:
www.agilent.com/find/contactus

Revised: March 24, 2009

Printed in USA, April 27, 2009
5990-3861EN

Agilent Technologies