Understanding Spectrum Intelligence

Introduction

While many bands of the radio frequency (RF) spectrum have a dedicated purpose, Wi-Fi operates in an unlicensed band of RF spectrum carved out by the Federal Communications Commission (FCC), with few rules other than limiting the amount of transmit power, and encouraging the use of spread-spectrum technology.

On the positive side, the freedom of the unlicensed band has enabled a tremendous level of wireless innovation. These innovations include devices using standardized protocols such as Wi-Fi, Bluetooth, and Zigbee, as well as devices using proprietary protocols such as cordless phones, wireless cameras, wireless bridges, game devices, and so on. As evidenced by the unprecedented variety and number of wireless devices and applications being sold, one thing is clear: people want mobility.

The downside of the freedom has been that with so many devices sharing the same spectrum, interference can easily occur. And while the first wireless devices may have been used in casual ways, the evolution of the market has made wireless and mobility mission-critical components of today’s business networks. In fact, businesses have begun to view the wireless spectrum as a strategic corporate asset.

The main challenge for users of the unlicensed band has been the limited visibility into spectrum competition between incompatible devices. This spectrum competition can lead to impaired coverage, impaired quality-of-service (QoS), and reduced security, which, in turn, can lead to decreased network capacity and an increase in support calls, as well as more network downtime, rising operational costs, and more potential security vulnerabilities.

What Is Spectrum Intelligence?

Spectrum intelligence is technology designed to proactively manage the challenges of a shared wireless spectrum. Fundamentally, spectrum intelligence provides you with visibility into all the users of the shared spectrum, both native devices and foreign interferers. Spectrum intelligence makes this information actionable, whether the action is manual (for example, removing an interfering device) or automated (for example, having the system change the channel away from the interference).

For every device operating in the unlicensed band, spectrum intelligence tells you:

- What is it?
- Where is it?
- How is it impacting your Wi-Fi network?
- What should you and/or your network do about it?

To put it simply, spectrum intelligence makes RF easy for you, so you don’t have to be an RF expert. It is like turning the lights on and finally seeing who is in the room with you.

Why Does Spectrum Intelligence Matter?

Spectrum intelligence enables a superior mobility experience through enhanced performance, reliability, and security of wireless networks.

Performance and Reliability

The first Wi-Fi networks deployed in enterprises were convenience networks, used for example, for web surfing in the lobby or conference rooms. For these applications, a best-effort level of performance was acceptable.

But Wi-Fi has reached a maturity where it is being deployed for many mission- or business-critical applications. For example, hospitals use Wi-Fi for access to patient data, and even remote monitoring of secondary bedside systems. In retail and manufacturing applications, Wi-Fi is used for logistics and business transactions. Small branch offices are beginning to use Wi-Fi as the exclusive network access method, forgoing wired connections. And increasingly, Wi-Fi is being used to carry QoS- sensitive traffic, such as voice and video, which are very sensitive to the impacts of interference on throughput, latency, and jitter. These are all examples of systems that are expected to run with very high reliability. For this reason, it’s no longer acceptable for these Wi-Fi systems to have unexpected downtime due to interference issues.

True Wireless Security

Ultimately, spectrum intelligence is not just about performance; it’s also about security. There has been a good level of industry focus on how rogue Wi-Fi access points can open up security holes in an enterprise network. Wireless intrusion detection systems and intrusion prevention systems (IDS/IPS) have been designed to address this issue. But current IDS and IPS solutions have significant blind spots that cannot be addressed without the addition of spectrum intelligence.

First, current IDS/IPS systems generally cannot detect Wi-Fi access points running with proprietary extensions such as Super G (from Atheros) or 125 High Speed Mode (from Broadcom). So there is a class of easily available devices that may go undetected. Additionally, it’s possible for a hacker to take standard Wi-Fi equipment (for example, running Linux) and modify it to operate on nonstandard channels or with other nonstandard modulation schemes. These extended or modified devices can be detected only if you analyze the RF physical layer.

And beyond Wi-Fi devices, there are many other types of non-Wi-Fi equipment—including Bluetooth access points, access points running older standards such as 802.11FH, and proprietary wireless bridges—that can also be used to open up holes in the network. In the case of bridges, these devices could be sending data to an attacker who is miles from your building! Again, these types of devices can be detected only if you analyze all the devices that are present in your spectrum.

In addition to the rogue threat, there is always the threat that someone malicious will try to disable your Wi-Fi network with an RF denial of service (DoS) attack. Although IDS/IPS systems monitor for many “protocol-layer” DoS attacks, they do not detect RF layer DoS attacks that can be implemented through use of a jammer device or a Wi-Fi device that has been set in a diagnostic jamming mode. In addition to purposeful attacks, some simple devices like wireless video cameras or analog cordless phones can accidentally cause a total jamming of your network. Spectrum intelligence is the only solution for identifying these types of RF-level DoS security threats.

How Is Spectrum Intelligence Implemented?

Before we discuss any specific solutions, it’s worth noting that at a fundamental level, a standard Wi-Fi chipset has very limited ability to implement spectrum intelligence. The reason is that Wi-Fi chipsets were specifically designed to receive Wi-Fi signals only—they do not recognize other types of signals (with the exception of DFS radar). And the chipsets were not even designed to pass up enough information for spectrum intelligence to occur at higher levels of software.

To be specific, when a standard Wi-Fi chipset sees a transmission burst that cannot be understood, it typically is able to report only a few things: 1) that an incomprehensible burst has occurred; 2) the power level of the burst; and 3) the start and stop time of the burst. Note that the burst may actually have been from a Wi-Fi device on another channel or on the same channel, but too far away to be properly received. Or the burst may have been from a non-Wi-Fi device. Detailed information about the modulation type of the burst, where it occurred within the channel, and so on, is typically not available. And there is no ability for software to access the actual data received from the burst for further analysis.

Despite these limitations, it is possible using a Wi-Fi chip to add up all the unidentified bursts, and to calculate a total amount of interference, as well as the average strength of that interference. This information can be useful to tell you that interference exists, but unfortunately it doesn’t provide the necessary information to actually solve the problem. For example, the “total interference” approach can’t tell you:

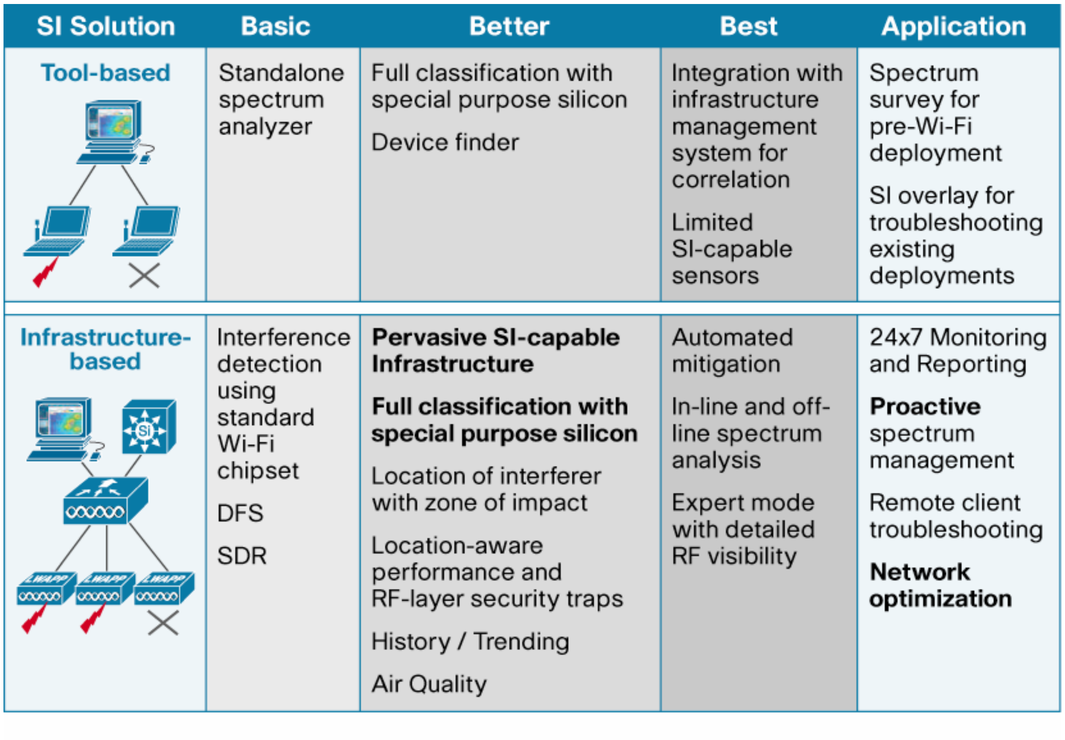
- The specific type of the interference
- Whether the interference is coming from one source or many
- Where the interference might be located

As this list suggests, the level of spectrum intelligence that can be accomplished with a standard Wi-Fi chipset is limited.

Because of these limitations, a good spectrum intelligence system requires special silicon and software solutions that have been specifically designed to analyze and classify RF activity. These solutions are designed to pass up enough information about all received data so that it can be analyzed at the software level. The analysis can include simple power versus frequency analysis, similar to a spectrum analyzer. But the most sophisticated levels of analysis include a fingerprinting capability that matches the activity in the band to specific sources of interference.

Fingerprint analysis looks at both the timing and frequency of interference bursts, and also looks at the low-level data in the bursts to discover deep attributes like the modulation type of the burst, identifying sync words, and so on. This information is then used to separate and distinguish one device from another. Such a “soft radio” analysis of the received data is what provides the powerful features of spectrum intelligence: telling you the specific source of the interference where it is located, and how it can be mitigated.

Hierarchy of Spectrum Intelligence Solutions



SI Solution	Basic	Better	Best	Application
Tool-based	Standalone spectrum analyzer	Full classification with special purpose silicon Device finder	Integration with infrastructure management system for correlation Limited SI-capable sensors	Spectrum survey for pre-Wi-Fi deployment SI overlay for troubleshooting existing deployments
Infrastructure-based	Interference detection using standard Wi-Fi chipset DFS SDR	**Pervasive SI-capable Infrastructure** **Full classification with special purpose silicon** Location of interferer with zone of impact Location-aware performance and RF-layer security traps History / Trending Air Quality	Automated mitigation In-line and off-line spectrum analysis Expert mode with detailed RF visibility	24x7 Monitoring and Reporting **Proactive** spectrum management Remote client troubleshooting **Network optimization**

Spectrum intelligence can be acquired in two basic forms: tool-based solutions and infrastructure-based solutions.

Tool-Based Solutions

The advantage of tool-based spectrum intelligence solutions is that they can be used prior to deployment of a network, and can be used with existing deployments that don’t have integrated spectrum intelligence. In some cases, tool-based solutions may be lower cost than fully integrated solutions, but this is not always the case. We will divide tool-based solutions into three categories: basic, better, and best.

Basic Spectrum Intelligence Tool

The most basic spectrum intelligence tool is the standalone spectrum analyzer. Using a spectrum analyzer, you are able to see where activity is occurring in your frequency band. Unfortunately, a spectrum analyzer, which simply provides raw data, requires a good deal of RF knowledge to use and interpret. This type of expertise is not available in many enterprise environments. (And it’s worth noting that even if you have an expert, this raw data can be difficult to interpret when there are many devices active simultaneously in the spectrum.)

The traditional spectrum analyzer is also a large, expensive item to purchase, and is designed more for the laboratory than for field use. Fortunately, a number of lower-cost and more portable spectrum analyzers have been made available for support of Wi-Fi networks. The best of these solutions work as a peripheral to an IT managers’ laptop, with intuitive Windows-based interfaces.

When you select a basic spectrum analyzer tool, important factors to look at include:

- **Level of calibration:** You want a tool that is accurate to within a few dB.
- **Spectrum resolution:** You want a tool that can view down to a resolution bandwidth of a few hundred kHz, in order to see a variety of signal types.

- **Spectrum coverage:** You want a tool that is able to see all the bands in which your network can operate. Beware of simple tools that only cover the 2.4- GHz band and leave you blind in the 5-GHz band, where interference can still occur.
- **Wi-Fi awareness:** A basic tool should understand Wi-Fi channel spacing to make it easier for you to interpret which signals are impacting specific channels.

Better Spectrum Intelligence Tool

Beyond the basic level of raw spectrum analysis, a better spectrum intelligence tool is one that provides built-in analysis so that you don't have to be an RF expert.

The most critical feature to look for here is whether the tool is capable of automatically classifying specific devices that are operating in your spectrum. A full suite of classifiers should be implemented, not just a few common devices. The list of classifiers should be expandable over time as new types of devices are introduced into the market. Also, the classification system should be able to distinguish devices in cases where different kinds of interference are occurring at the same time, and multiple devices of the same type are being used at the same time. For each device that is classified, the tool should be able to tell you what channels are affected by the device, and how severe the interference created by the device is.

And, of course, once the devices have all been classified, a better spectrum intelligence tool should allow you to lock on to a particular device and find the device (typically using a Geiger counter approach). Using a tool in the way, it's possible to find the location of the device, even in cases where the device has been purposefully hidden. This is critical, because in many cases the best response will be to remove the device or shield the device. None of this is possible if you can't find the device.

A second feature that better spectrum intelligence tools should provide is some level of analysis on the impact of interference on your Wi-Fi network. This type of analysis can be in the form of channel statistics that indicate how Wi-Fi channels you are using are impacted overall by interference. In cases where interference cannot be removed, this type of analysis can help you choose a channel that is the least impaired for operation of your network.

Best Spectrum Intelligence Tool

The best spectrum intelligence tool should go beyond being a standalone tool—it should offer some level of integration with your network management system.

One advantage of this integration is that data measured by the tool can be fed into your network management system for storage over time. This allows for a range of functions that are beyond what can be done with a tool by itself, including:

- Trend analysis
- Integrated reporting
- Non-Wi-Fi interference alarms
- Streamlined searches of interfering devices
- Correlation of interference data with actual network performance data

A second advantage is that integration with your infrastructure management system makes it possible to visualize approximately where interference is occurring in your network, and therefore understand what access points and clients are most likely to be affected by the interference. This feature would typically be implemented by visualizing the location of the tool on your location system maps, along with an indication of the zone that is being monitored by the tool.

Infrastructure Spectrum Intelligence Solutions

Although there will always be a role for tool-based spectrum intelligence solution, infrastructure-based spectrum intelligence solutions have compelling advantages. In an infrastructure-based solution, the spectrum intelligence analysis is built directly into the Wi-Fi access points, and spectrum intelligence information is fully integrated into the network architecture and management systems.

The biggest advantage of infrastructure-based solutions is that they operate 24/7, constantly monitoring for interference and air quality issues. This allows you to take a more proactive approach to spectrum management. Instead of waiting for interference to be reported by an end user (in the form of a trouble ticket) and then dispatching a tool to analyze the problem, you can spot interference as soon as it occurs, and take immediate action. Having a 24/7 history also lets you look back in time through an event window to see what happened after the fact. And using the historical data collected, you can perform valuable analyses of trends over time.

A second advantage of infrastructure-based solutions is that they can be operated remotely. For many Wi-Fi deployments, the IT staff at one location manages equipment at multiple locations, and it can be difficult to physically take a tool to these remotely managed sites. This is particularly true for deployments with many branch offices. By having spectrum intelligence integrated into the infrastructure, IT is able to remotely view interference conditions anywhere on the network.

Another advantage of infrastructure-based solutions is that the higher density of access points than in tool-based solutions means that it’s likely that multiple access points will observe the same device causing interference. This makes it possible to pinpoint the exact location of the device, similar to the way that infrastructure systems are currently able to locate Wi-Fi clients and tags.

And perhaps the biggest advantage of infrastructure-based spectrum intelligence is that the 24/7 spectrum intelligence data becomes available to the system, where it can be used by sophisticated client troubleshooting utilities and to implement automated mitigation of interference. In this way, it’s possible to tune the network to automatically work around many types of interference.

Basic Spectrum Intelligence Infrastructure

Although the level of spectrum intelligence that can be implemented with a standard Wi-Fi chipset is fairly crude, it’s important to understand what the basic level provides.

A basic spectrum intelligence infrastructure system should analyze the duty cycle (percentage of time) and power level (dBm) of interference, and report this on a per-channel basis. This provides you with the first level of spectrum intelligence, which is to detect when interference is occurring. Ideally, these basic interference statistics should be captured periodically, so you can run trending analyses and reports to see if the level of interference in your environment is increasing. And there should be a facility for generating alerts if the level of interference exceeds a threshold.

With this basic level of spectrum intelligence, the infrastructure will not be able to tell you the exact source of the interference or where the interference device is located. But a basic system can be combined with a more sophisticated spectrum intelligence tool to form a complete solution. First, the spectrum intelligence infrastructure can generate an alert to say that interference exists. Then you can dispatch the spectrum intelligence tool to diagnose the actual cause of the interference.

In addition to reporting, a basic spectrum intelligence infrastructure solution should also consider interference measurements when performing automated management functions, such as automated channel planning. For example, channels with excessive amounts of interference should be avoided. And since you need the flexibility to choose channels that have low interference, it's desirable for basic spectrum intelligence infrastructure to support as many channels as possible. In the 5-GHz band, having support for the latest dynamic frequency selection (DFS) requirements enables access to the greatest number of possible channels. In addition, infrastructure that has been qualified by the FCC under the Software Defined Radio (SDR) model can add additional channels if they are opened up by the regulatory bodies over time.

Better Spectrum Intelligence Infrastructure

First and foremost, a better spectrum intelligence infrastructure solution should have the ability to classify and identify specific interference devices. As with better tool-based solutions, a full suite of classifiers should be provided, not just classifiers for common devices.

Classifying signals requires special hardware, not just a standard Wi-Fi chipset. When you shop for an integrated spectrum intelligence solution, keep in mind that it's highly desirable for all of your access points to be spectrum intelligence-capable, with the ability to enable spectrum intelligence as a software feature. If spectrum intelligence is a separate add-on hardware feature, it can be challenging for the user to determine ahead of time where spectrum intelligence functionality will be needed and where it won't be. For example, for cost reasons, you might choose to purchase spectrum intelligence hardware for only one out of every five access points—but which ones should have it? Over time, it's likely that you will want to deploy spectrum intelligence pervasively. If all the hardware is spectrum intelligence-capable, you have the ability to simply turn on the software feature at a later date, with no need to change out or upgrade hardware.

In a better spectrum intelligence infrastructure solution, devices that have been analyzed and detected should also be integrated with the visual mapping displays provided by the Wi-Fi management system. In other words, in addition to seeing access points and clients on a map, you should be able to track where interference devices exist on the same map. In terms of performance, the ability to see interference devices on the map (as well as their zone of impact) lets you determine what access points, clients, and areas of your floor space are impacted.

From a security perspective, tracking devices on a map lets you know immediately where to dispatch your security personnel. As described previously, there are a number of threats to your network that are invisible to traditional IDS/IPS systems—that is, threats that can only be detected at the RF level. These threats include Bluetooth access points, proprietary wireless bridges, and older standards such as 802.11FH that may represent intrusion points on your network. These threats also include malicious Wi-Fi devices that operate on nonstandard operating frequencies or that use nonstandard modulation. And of course, there are always denial-of-service type attacks that can occur from jamming devices.

In addition to viewing these security devices on a map, the system should be capable of generating alerts on the presence of these devices. These alerts should ideally be customizable by location – for example a specific floor of your building. The reason is that certain devices may be considered a threat in certain areas of your building (for example, trading wing), but not if they are detected in other areas, such as the lobby of the building.

A better spectrum intelligence infrastructure solution should use this detailed device information to formulate easy to use metrics such as channel-level and floor-level air quality (AQ). This concept is similar to the interference duty cycle and power measurements in the basic spectrum intelligence infrastructure solution, but is more accurate because the sources of interference are better understood. AQ measurements are useful to provide a quick summary view of where interference problems are impacting the network. The system should also be capable of generating AQ alerts, so that you can be automatically notified when AQ falls below a threshold value.

Best Spectrum Intelligence Infrastructure

The best spectrum intelligence infrastructure solutions should offer flexibility of deployment. There are two models of how spectrum intelligence can be integrated into access points. In the first model, the spectrum-intelligence-capable access points are the same ones that carry Wi-Fi data traffic. In the second model, spectrum intelligence is implemented in separate monitoring access points dedicated as full-time sensors. These two approaches directly mirror the approaches taken by IDS/IPS systems. In general, when deployed in an access point that is also carrying data traffic, the spectrum intelligence should detect any interference that occurs on the operating channel of the access point. When deployed on a separate sensor access point, the spectrum intelligence should detect interference on all channels.

Although it is more expensive and therefore less popular, the best performance is generally provided by a combination of these two models—deploying an overlay of sensors in addition to using the traffic-carrying access points to monitor the spectrum. A solution that offers both types of monitoring (shared and separate sensors) also provides full flexibility. For example, in highly secure environments, it may be necessary to deploy separate sensors in order to meet strict detection requirements. But in other cases, cost may be the driving factor.

In addition to flexible deployment, the best spectrum intelligence infrastructure solutions should offer advanced automated response to interference. There is a wide range of automated responses that can be implemented, so you should investigate the level of sophistication in the algorithms. For example, responses may be as simple as dynamically changing channels of an access point that is experiencing interference. More complex responses factor in the type of interference and how long it is likely to remain in the area. In the most sophisticated cases, automated responses can be as complicated as determining which clients are impacted by a specific interference device and tuning the operating parameters that the access point uses when communicating with that particular client. Parameters that can be tuned include transmit data rate, packet fragmentation, and antenna steering.

Although in many cases, the best response to interference is for the administrator to manually move, remove, replace, quarantine, or shield the interfering device, automated response is highly desirable to maintain short-term performance until other actions can be taken. And in certain cases, it may not be possible to ever remove the source of interference (for example, if it comes from outside the building).

Finally, the best spectrum intelligence infrastructure solutions should offer an “expert” view of low-level spectrum analysis data similar to that offered by spectrum analyzer tools. Although it is true that the system should provide higher-level analysis including classified devices and easy-to-use concepts like AQ, there will always be cases where it is helpful to look at the raw spectrum data itself in real time. Even if you don’t have an RF expert on staff, these facilities can be useful if you bring in an expert to help with a particularly difficult-to-diagnose problem.

Conclusions

Because Wi-Fi operates in a shared unlicensed band, spectrum intelligence is a “must have” to enable a high level of performance, security, and reliability in your Wi-Fi network. Spectrum intelligence is critical for providing a rich and dependable mobility experience to end users for business-critical applications.

The best spectrum intelligence solutions provide analysis that doesn’t require you to be an RF expert. These systems go beyond what can be done with a standard Wi-Fi chipset, and use custom spectrum processing chips and software for their analysis. These systems classify and locate individual sources of interference and tell you how these devices are impacting the performance or security of your network.

Spectrum intelligence can be acquired in the form of tools, which are useful in the pre-deployment phase, when adding to existing deployments, or when finding a hidden device. For new deployments, the best solutions have spectrum intelligence integrated directly with the infrastructure. These integrated solutions provide 24/7 proactive responses to interference, as well as remote management and automated mitigation when possible.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-482837-00 06/08