Cognitive radio enhances WLANs

By Nestor Fesas and Bob Mayer, Network World, 11/14/05

The explosive growth of wireless technologies has created managerial challenges for those who oversee wireless networks. With wireless intrusion threatening security and radio frequency interference impeding performance, IT managers need an up-to-date, detailed understanding of the RF environment to make informed decisions about how to solve these problems.

Cognitive radio technology enables a radio device and its antenna to sense its RF environment and adapt its spectrum use as needed to avoid interference. Integrated software and silicon solutions enable cognitive radio to be built into enterprise-class wireless LAN (WLAN) access points to boost security and optimize performance. Access points with this feature are expected to be available next year.

Wireless intrusion occurs when unauthorized WLAN users gain access to a secured network. Causes include hackers creating ad hoc networks with WLAN clients or a rogue access point connected to a wired network without proper security levels. In either case, the keys to prevention are quick identification, containment and defensive action.

The first step in preventing wireless intrusion is identifying the intrusion point. Because WLANs are fixed to a specific WLAN channel during operation, they cannot simultaneously detect intrusion points on other WLAN channels. Relying on a single-radio access point to provide access and security is insufficient. Network managers must be able to monitor the full WLAN frequency range to be able to reliably detect and identify intrusion points.

Cognitive radio for WLANs provides a means to observe the RF environment in the 2.4-GHz and 5-GHz frequency bands within which IEEE 802.11 WLANs operate without disrupting normal wireless VoIP and data traffic. Continuous scanning of both bands for 802.11 and non-802.11 devices allows for timely detection of intruders.

With detailed information from multiple cognitive radios within a WLAN, administrators can take preventive action.

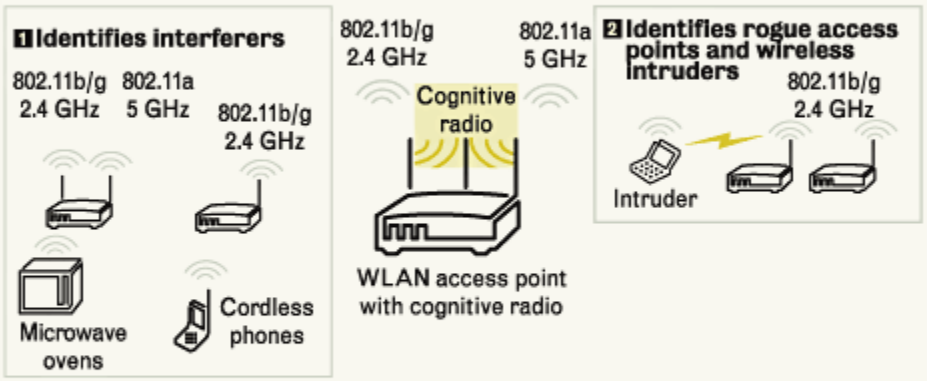
Cognitive radio can detect non-802.11 devices. This is important because interference, regardless of source, lowers effective data throughput and overall network performance. IEEE 802.11-based WLANs operate within the unlicensed radio spectrums around 2.4GHz (802.11b and 802.11g) and 5GHz (802.11a). Other wireless connectivity standards, such as Bluetooth and HomeRF, operate in the same unlicensed radio spectrums. Microwave ovens, cordless phones and industrial equipment can generate noise in these bands.

This technology allows a network to detect, identify and avoid these noise sources. Proactive behavior allows a network to be established on clearer channels during initial deployment. Ongoing monitoring allows network administrators to take rapid corrective action against RF noise. This affords the optimal network performance that WLAN users expect.

Integrated software and silicon solutions enable access points to be developed to provide simultaneous WLAN access in the 2.4-GHz and 5-GHz bands while providing integrated cognitive radio functionality that ensures security and performance for enterprise wireless networks.

HOW IT WORKS: Cognitive radio for WLANs

Implemented in the access point, cognitive radio continually scans both wireless LAN frequency bands, providing a comprehensive, up-to-date understanding of the RF environment.



1 Upon initial deployment of the access point, the cognitive radio performs a full scan of the RF environment detecting both 802.11 and non-802.11 interference. The access point selects the WLAN channels with the least interference to maximize performance.

2 Continual scanning of all WLAN access channels in both frequency bands enables the system to identify rogue access points and wireless intruders so policy-based action may be taken quickly.

Fesas is vice president of systems engineering, and Mayer is vice president of marketing for Bandspeed. They can be reached at nfesas@bandspeed.com and bmayer@ bandspeed.com.