

## 802.11a Measurement Techniques and Network Issues

by Herb Petrat, Senior Software Engineer, Berkeley Varitronics Systems, Inc.

In the continuously changing world of wireless networks, new standards for 802.11 are constantly evolving. The most popular standards currently are 802.11a, 802.11b, and 802.11g.

Each technology has its own pros and cons in regards to successful network deployment. **Table 1** shows a summary of these pros and cons. Rows marked with a \* rank the technologies from 1-3, 1 being the best. 802.11a and 802.11g both have a 5 to 1 edge in maximum throughput with the ability to transmit up to 54 Mb/s. 802.11b tops out at 11 Mb/s.

802.11a has an advantage of operating in the cleaner 5 GHz band which contains less RF interference than the heavily trafficked 2.4 GHz band. 802.11b and 802.11g operate in this band, which contains interference from microwave ovens, cordless phones, BLUETOOTH™ devices, etc. Some newer cordless phones work up in the 5 GHz band.

Also, the RF sensitivity for 802.11b is approximately 9 dB better than for 802.11a receivers.

802.11b equipment, being on the market the longest, is the most inexpensive of the trio. 802.11g and 802.11a equipment escalate up the price scale from the base of 802.11b. A main reason is that there is much more competition from 802.11b equipment manufacturers, thereby lowering the cost to the consumers.

802.11a equipment cost is high for a couple of reasons. First, the actual equipment is higher-priced on the market. Secondly, due to the smaller coverage distance for 802.11a propagation, more access points would be required over the same area than for another technology.

Of course, for a home office network, usually only one access point is needed to acceptably cover the average size home.

802.11b and 802.11g access points cover a greater area than 802.11a AP's.

802.11a and 802.11g allow more users to access the network than 802.11b at the same time. Finally, 802.11a does not penetrate clutter (such as office walls) as well as 802.11b and 802.11g due to the higher frequency band in which it operates.

These are some of the major comparisons used by network administrators to make the decision on which technology to use when deploying a wireless interface into the network architecture.

This discussion will focus on the 802.11a technology and measurement techniques to verify network availability, security, and throughput. When deploying a wireless network and later maintaining it during use, several factors must be taken into account. These include such factors as:

1. The network must have complete coverage over the intended client domain.
2. The network must be at least as secure as an equivalent wired network.
3. The network must process transactions in a timely manner such that it maintains a data rate that is satisfactory to meet productivity goals.

In order to meet these requirements, a wireless network test tool is very useful in becoming a network administrator's aide in detecting and troubleshooting various problem areas.

This tool will be needed over the lifetime of the wireless network. The reason for this is that there will be constant changes in the RF environment over time. These changes are not seen in a wired network (with the exception of network load) because

the environment is contained within wires and (hopefully) contains a firewall. This firewall protects against external anomalies (such as viruses) and intruders.

The RF environment WILL change, however, due to such actions as:

1. Building construction (more cubicles, less walls, etc.)
2. Cordless phone usage
3. Microwave oven usage
4. Other new sources of interference

This is where the correct test equipment becomes extremely important. The test tool we will use for reference in this discussion is the new Berkeley Varitronics Systems, Inc. YellowJacket™ 802.11a tool. This tool contains a proprietary 802.11a RF module (high-speed I&Q A/D converters, DSP, memory, and I/O) that connects to an iPAQ™ display and user-input device through the CF serial input.

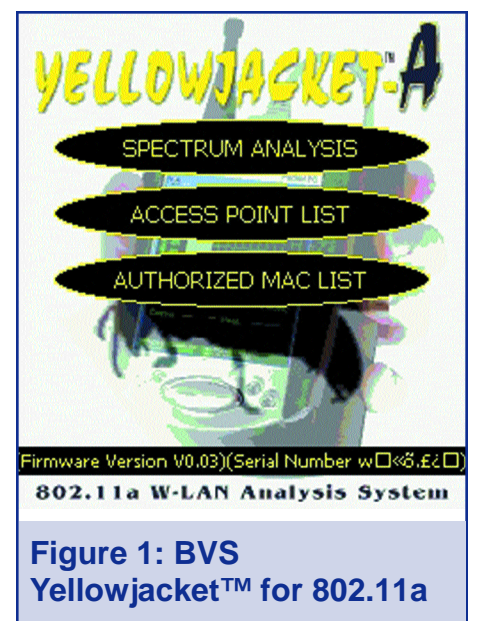


Figure 1: BVS Yellowjacket™ for 802.11a

One important feature of this tool, which other test tools do not have, is the ability to do a spectrum analysis on the RF environment. It is as necessary to be able to see non 802.11a traffic in the 5GHz band to determine if the network is being compromised by interference.

Using a directional antenna, one could determine the actual direction of the interfering party. A directional antenna is also useful in detecting the location of unauthorized MAC (Media Access Control) addresses that are interfering with the network.

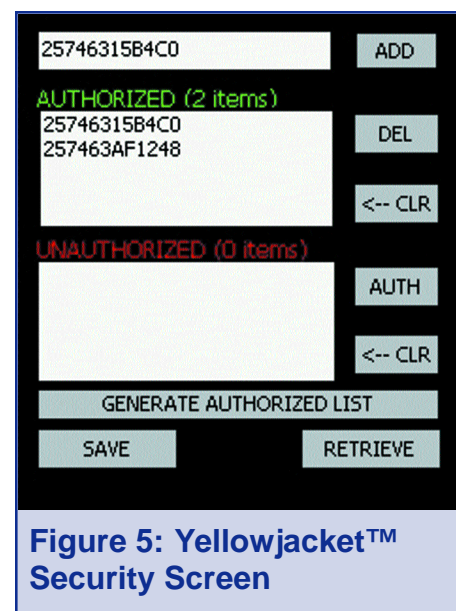
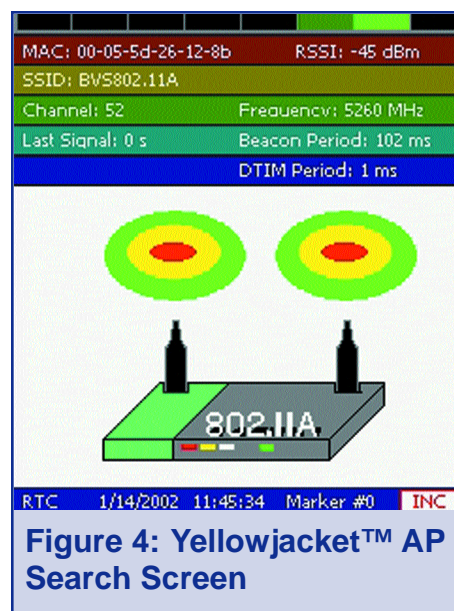
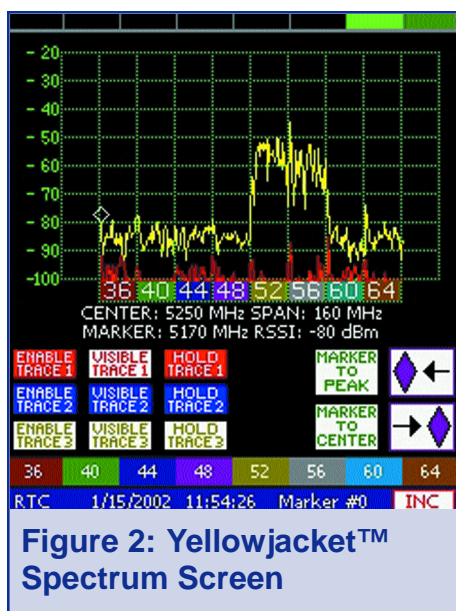
The unauthorized MAC addresses of a network may be trying to attack the network with a denial of service attack. This is an attack where the unauthorized addresses log into the network illegally and then create a lot of unnecessary traffic to bring down the throughput of the network.

Using the YellowJacket, a list can be set up using the MAC addresses of authorized access points and clients on the network. When the YellowJacket sees a MAC address that is not authorized, an alarm is set off, warning of a potential intruder and threat to the

**BVS, Con't on pg 57**

	802.11a	802.11b	802.11g
Maximum Data Rate	54 Mb/s	11 Mb/s	54 Mb/s
Frequency Band	5 GHz	2.4 GHz	2.4 GHz
RF Interference Concerns *	1	3	3
Modulation	OFDM	DSSS	OFDM
Equipment Cost	High	Low	Medium
Coverage Distance *	3	1	1
Clutter Interference Concerns *	3	1	1
Number of Users *	1	3	1

Table 1: 802.11 Technology Summary



**BVS, Con't from pg 48**

security of the network. Going into the AP Search screen, the unauthorized intruder can be located with the directional antenna. By fanning the antenna back and forth, the unauthorized MAC address would have a stronger RSSI value when in the direct path of the antenna. Once the direction is found, proceeding towards the MAC address would produce even higher readings until the user is right on top of the intruder. A game that the network hackers play is another denial-of service attack. Two clients set up within range of the network in question. They log

into their own network. They transfer high amounts of data as quickly as they can. This interferes and reduces throughput of any legal network traffic in the same area. These culprits can be found in the same manner as the other ones. Use a directional antenna and the AP search screen to zero in on the intruder. Performing site surveys is another important step in maintaining a wireless network. An associated software package that is an option with the YellowJacket is BirdsEye Site Initiator, Site Supervisor, and Site Investigator. This application package performs site sur-

veys and analyzes coverage issues in current network environments. The result is a printable color report of site coverage and interference. There are three applications associated with the BirdsEye™ package. The first is the Site Initiator application which runs on any Windows desktop or laptop. This program imports bitmapped floor plans for use in the site survey. Associated landmarks may be added to the drawing. These landmarks include AP's, cordless phones, microwaves, and text messages for different areas of the floor plan. The finished site is saved and

imported into the Site Supervisor application. This application runs on the iPAQ Pocket PC that controls the YellowJacket hardware. The site is pulled up on the iPAQ. Then the user walks around the site, tapping the current point in the floor plan with the attached stylus. The YellowJacket performs a quick scan of all 8 channels at each point, recording any access points that are found. The user only has to make sure that enough sample points are taken throughout the site. A good rule of thumb is taking a point every 40-60 square feet. After the survey has been completed

## BVS, Con't from pg 57

TYPE	MAC ADDRESS	RSSI
AP	36 004033CDE603	- 99
AP	52 458033AF4451	- 64
AP	36 004456AFF501	- 67
AP	64 004033CDE33A	- 43
AP	56 0040339ABF50	- 53
AP	56 456033AFF501	- 94
AP	36 004033AFFAFF	- 36

Figure 6: YellowJacket™ Access Point MAC List

ed, the resulting data is transferred off of the iPAQ back onto the desktop or laptop. Here is where Site Investigator is used. This application will plot out the data from the Site Survey and prepare a visual and/or printed report of the coverage for the site in question. In the figure shown for Site Investigator, a typical analysis is shown. The different colors represent different access points.

As you can see from the diagram, access point markers were placed on the site using Site Initiator. The colors for the RSSI (Received Signal Strength Indicator) data for the associated access points get noticeably darker as they get closer to the markers of the actual location of the access points. The shade of the colors will get darker as the RSSI values increase. For example, a value of -40 dBm will result in a darker shade than a value of -80 dBm.

BirdsEye™ software with YellowJacket™ hardware combines to provide a network administrator with a tool to constantly monitor the wireless network environment. Coverage holes would show up in the resulting reports as colorless (white). Then the

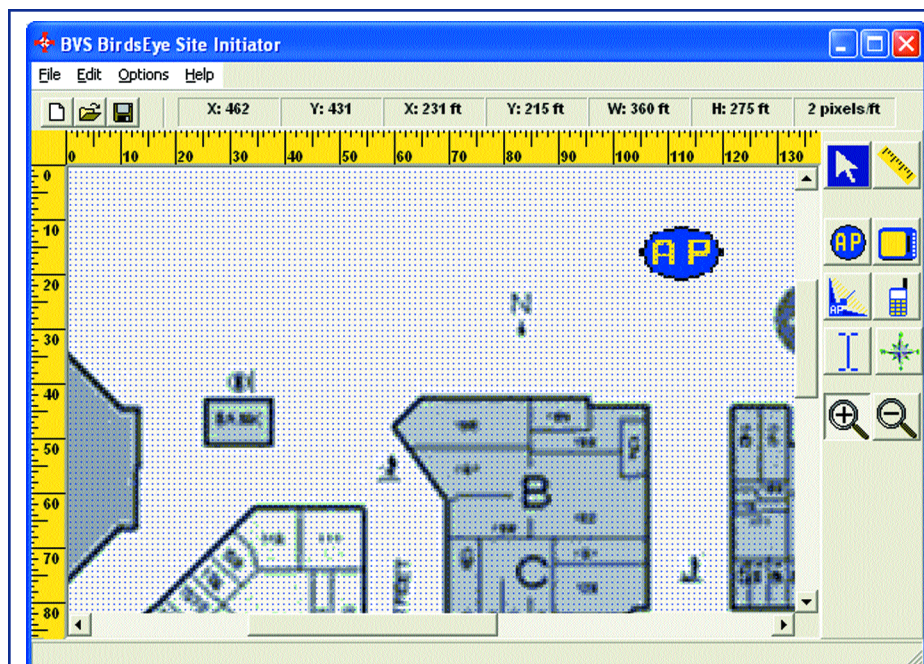


Figure 7: Birdseye™ Site Initiator

user could turn around and use the YellowJacket™ to determine why there is a network hole.

There could simply be a need for another access point. If it seems that a nearby access point should have covered the hole, outside RF interference could be the culprit. The user can take the YellowJacket™ spectrum screen to see if that is indeed the case.

There could be co-channel interference. BirdsEye™ can map the area by channel and it can be seen whether or not there are two adjoining access points that are using the same channel.

It could also be that certain clutter is preventing an access point signal from reaching the designated area. Clutter such as copper-lined walls could cause a signal to not propagate and simply reflect.

Combining BirdsEye™ with the

YellowJacket™ is one of the more effective tools in the battle against constantly changing RF environments for 802.11a networks.

There are a number of issues that must be considered when deciding how and when to deploy an 802.11a wireless network for home or corporate use. A test tool such as the YellowJacket™ is extremely useful in network setup and troubleshooting and can make an IT manager's daily work less strenuous as well provide a baseline archive of a wireless network's performance.

The key is being able to maintain your wireless network amidst constantly evolving security and environmental concerns. The right test tool helps reduce the amount of labor cost involved with network maintenance.

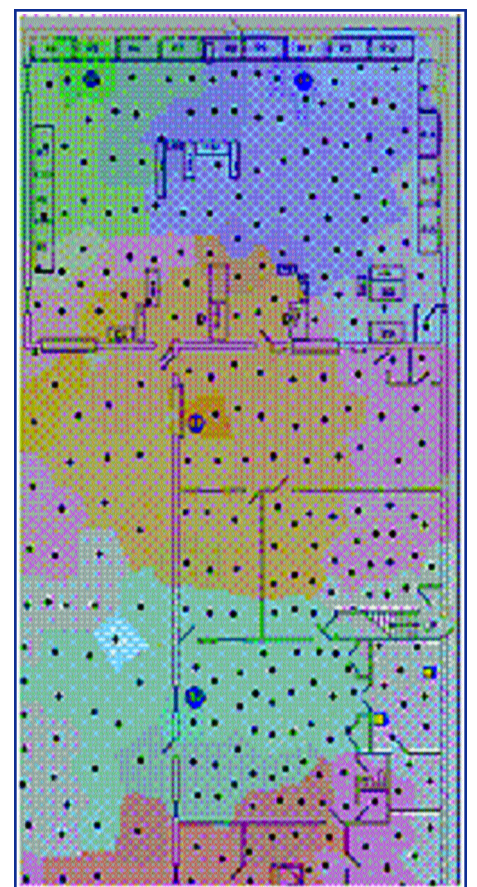


Figure 8: Birdseye™ Site Investigator

1. BLUETOOTH is a trademark owned by Telefonaktiebolaget L M Ericsson, Sweden.
2. YellowJacket and BirdsEye are trademarks of Berkeley Varitronics Systems, Inc. of Metuchen, NJ 732-548-3737 [www.bvsystems.com](http://www.bvsystems.com)
3. iPAQ is a trademark of Compaq Corporation