

Wi-Fi Antenna Alignment & Rogue AP Detection



BERKELEY
VARITRONICS
SYSTEMS

by Herb Petrat - Sr. Software Engineer

for 802.11 b/a/n/g Networks

There are many factors associated with the deployment and maintenance of WiFi networks today. Providing an efficient and secure wireless network takes a considerable amount of time and effort.

Two unique concerns are covered in this paper. Both of these concerns require the use of directional antennas to achieve their purpose. The first is the problem of antenna alignment. A specific instance of this need is evident in WISP installations where a directional antenna provides a relay to another network which is also connected by a directional antenna. These two antennas must be aligned with one another to provide optimal signal strength and highest throughput capability.

Another area which also includes the use of a directional antenna is the need to locate rogue access points. These access points interfere with the operational network. A rogue may be interfering accidentally or purposely. It is the network administrator who must find the locations of these rogue access points so that the network maintains the highest possible efficiency level.

Berkeley Varitronics Systems, Inc. provides the 802.11 Beetle B/A/N/G optimizer. The Beetle is a robust tool which provides the ability to passively receive 802.11 b/a/n/g signals. The optional direction finding antenna along with the iPAQ-based software are effective in dealing with antenna alignment and rogue access point issues.

This paper will outline the benefits of using the Beetle to resolve these direction finding obstacles.



Figure 1
Beetle™-BANG Wi-Fi Optimizer

Executive Summary

There are many different obstacles to overcome when deploying and maintaining a wireless network. Some of these obstacles require the use of direction-finding equipment. Aligning antennas to join remote networks requires the ability to monitor the signal strength of the transmitting antenna as it is being aligned. Locating access points not intended to be a part of a WiFi network also requires the monitoring of its signal strength while scanning with a directional antenna.

Berkeley Varitronics Systems, Inc. provides a low-cost solution for the resolution of these issues. The Beetle B/A/N/G Wi-Fi optimizer is a valuable aid to the wireless network administrator. Using this tool, signal strength can be monitored while calibrating a directional antenna to align with a remote transmitter. The maximum RSSI (Received Signal Strength Indicator) value can be attained and then used to center the antenna.

Rogue access points can also be located as the Beetle is a hand-held tool with an optional direction-finding antenna. The user can simply walk around a network campus until the access point is located by monitoring the fluctuations in RSSI.

Background

A wireless network typically consists of a number of access points which are connected to a base wired network. The base wired network consists of network servers which contain information needed by a number of users. These users may also need to access resources such as printers. These servers also provide access to the internet.

Client machines allow the end user to connect to the network. Traditional clients access the network servers through wired connections. Other clients may have wireless transceivers through which they can access the network servers through wireless access points. These access points are connected via wires to the base network. They contain transceivers to communicate with any wireless clients which are within listening distance.

Wireless networks inherently have challenges not normally associated with wired networks. Whether or not there are enough access points to provide adequate coverage throughout the planned network is of concern. The possibility of the reduction of network throughput due to natural signal attenuation is an issue. Whether or not the maximum throughput is being gained through a bridge connection to another network may be a challenge. Interference from outside sources such as rogue access points and the security of the network are other issues which must be dealt with in designing and maintaining a network which can be accessed without wires.

Antenna Alignment

An issue that arises in the build-out of wireless networks is the alignment of antennas. A specific case of this is when companies (such as Wireless Internet Service Providers "WISP") are contracted to connect remote networks together through a wireless link. The connection is made through a pair of directional antennas in locations such as the tops of buildings or mountains.

By using directional antennas over a relatively large distance, the transmitted energy can be focused on the receiving antenna, and not spread throughout a 360 degree radius. Using an omnidirectional antenna would give a greater guarantee of connection, but a lot of throughput would be lost.

Being that these antennas are usually in a remote location such as building tops or mountains, the ideal situation would be to setup the antennas one time only. Having to go back up a tower or rooftop to change the

direction of the antenna results in aggravation as well as increased manpower costs. It also results in downtime for the link.

The situation is analogous to older satellite dishes that needed to be on motors to enable them to be tweaked occasionally. The use of test equipment to monitor the received signal while setting up the antenna is the preferred method of installation. Figure 2 shows an example of using the Beetle optimizer to monitor signals and align an antenna correctly the first time, saving time and effort in setting up and maintaining the link.



Figure 2 – Antenna Alignment with the Beetle B/A/N/G Optimizer

In this scenario, the Beetle would be attached to the antenna being installed. This can also be done after using an omnidirectional antenna to find the correct channel and MAC address of the transmitted signal. Once that has been determined, the Beetle can be drilled down to the antenna alignment screen (as shown back in Figure 1). The installer can start adjusting the angle of the antenna until the optimal signal strength is achieved.

The antenna can be slowly moved back and forth until the display shows the maximum RSSI received. Then the antenna can be locked in at the correct angle and inclination.

The value of the portability of the Beetle is seen here as it can be held in one hand and can be brought easily to remote sites for installations. Trying to carry a laptop or larger device would be cumbersome and detract from the ability of the installer to quickly and effectively lock in the correct position of the antenna.

Rogue Access Point Detection

An area that is of great concern to WiFi network administrators is the ability of unauthorized access points or client cards to interfere with the operation of a wireless network. These transmitting sources may be interfering accidentally, as when there is a network in the next building operating on the same channels. Another instance of an incidental transmitting source is an unauthorized laptop in someone's office or an access point that is plugged in but not part of the network.

These sources may also be within interference range with a purpose. A hacker may be sitting in a parking lot with a laptop attempting to break into the corporate network. Another instance would be a denial of service attack. In this case, an access point may be placed in a location so as to interfere with the throughput of a wireless network.

In either case it is necessary to remediate the unwanted traffic. One of the features of the Beetle is that it is a portable device which can be held in one hand.

Being a passive device, it cannot be seen from any other monitoring device. This means that a hacker would not be able to tell he/she is being watched.

To locate one of these devices quickly using the Beetle, a simple two-step procedure may be followed. First, the unit is set to scan all channels using the omnidirectional antenna. Then, when the rogue device is spotted, the user simply needs to click on the rogue MAC address and pull up the antenna alignment screen.

When attaching the optional direction-finding antenna (as shown in Figure 3), the Beetle can be used to sweep the area for these rogue devices. If the user slowly waves the Beetle, the signal can be found. Then the user can walk in the direction that shows the greatest signal. In no time, the intruding device will be spotted and appropriate measures can be taken.



Figure 3 – Rogue Access Point Detection

The portability of the Beetle and its ability to mount different antennas increases its versatility and usefulness in maintaining wireless networks. Special attention is made to the fact that the Beetle can rectify interference issues by simply using its optional direction-finding antenna and the antenna alignment screen of the associated iPAQ software.

About Berkeley Varitronics Systems, Inc.

Berkeley Varitronics Systems, Inc. is a Metuchen, NJ based wireless test equipment designer and manufacturer of hardware and software solutions. For 35 years, Berkeley Varitronics Systems has provided design and consulting services for the telecommunications industry. They provide a wide range of disciplines and client needs ranging from programming, DSP firmware, hardware production engineering to manufacturing. BVS specializes in 802.11 and WiMax based test systems as well as CDMA and other technologies.

About the Author

Herb Petrat is a senior software engineer for BVS, Inc. and has been programming for 20 years and has developed software solutions for BVS wireless test equipment since 1997, including CDMA and 802.11 WiFi. Herb has also written articles for trade magazines such as MP Digest in the past decade.