

Intruder Alert! Recognizing WLAN Attacks and Locating the Culprits

During the exponential growth of wireless networks over the past few years, certain issues have become fairly obvious. The absolute need for network security, the detection of network intruders (hackers), and the importance of site analysis in network security issues.

Standard local area networks (LAN's) will always have one security feature that will never be afforded wireless local area networks (WLAN's). In order to break into a LAN, one must be physically connected to the network via a wire or cable. LAN security in the past was maintained with relative ease as the network was usually contained within the confines of a single building or campus.

After the growth of the internet had connected LAN's with each other throughout the globe, a different security issue arose. Anyone with a computer which had access to the internet had the potential of accessing any other computer on the internet. This led to securing corporate gateways with levels of roadblocks known as firewalls. These firewalls would prevent hackers from gaining access to enterprise critical data.

With the advent of WLAN's, a new and more challenging security obstacle appeared. Users of a WLAN connect to a network through an access point (AP), which routes information to the correct destination. Anyone with a laptop computer and a wireless network card can try to access the network. You could be sitting in a car across the street from a building and attempt to access the network. If there is no encryption or security on the network, it is relatively easy to simply log on to the network.

WLAN's use the 802.11 protocol standard written by the Institute of Electrical and Electronics Engineers, Inc. (IEEE). Part of this standard allows for the use of Wired Equivalent Privacy (WEP). This is an attempt to secure WLAN's by the use of encryption and decryption schemes. There is also the base authentication algorithms that have a user authenticate before being allowed to access the network.

Companies and their network administrators need not only ways to prevent unauthorized access to networks, but need tools to monitor and detect potential and real threats to the network.

Berkeley Varitronics Systems, Inc. (BVS) has a variety of 802.11 tools which monitor and analyze WLAN's. The focus of this paper is based on an 802.11b network.



Figure 1 – BVS Hornet™ Monitoring System Main Screen

The BVS Hornet Monitoring System (as shown in Figure 1) is a stand-alone monitor that can be placed anywhere. It stores Medium Access Control (MAC) address lists created using the Hornet™ PC Interface (as shown in Figure 2). Each AP and/or Client has a unique MAC address that is used for identification. The first 6 hexadecimal digits of the MAC address are a unique identifier for the manufacturer of the AP and/or client.

An authorized list is created and sent to the Hornet™ to identify those MAC addresses that are valid for the network in question. MAC addresses put in the lists can be linked with alias names to identify the individual AP/Client. The PC interface also will show the manufacturer of the MAC addresses (as shown in Figure 3). The Hornet will also accept a 'Watch List'. The Hornet will then flag any occurrence of any MAC address in the watch list. The Hornet will also report back any MAC addresses it sees overall in the 'On-Air' return list.



Figure 2 – BVS Hornet PC Interface

The Hornet will use these lists to create an alarm log. This log contains a combination of authorized list violations, watch list sightings, and authentication failures. The authentication failure alarm is a powerful feature that detects when a client has failed to authenticate correctly into the network. This shows possible intrusion attempts.

It can also signal a 'denial of service' attack. This type of attack tries to bog down a network by flooding it with authentication requests. The network uses so many resources to handle the requests that the throughput of the system is jeopardized.

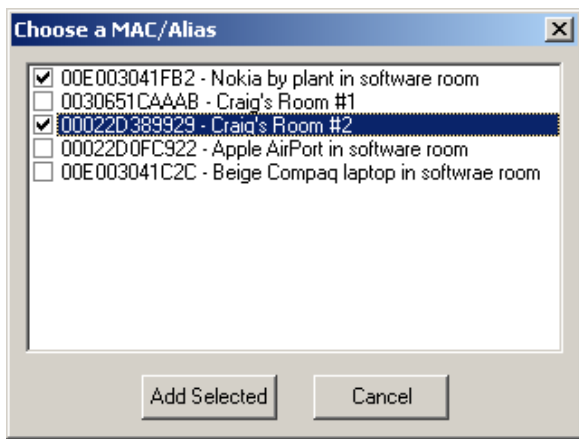


Figure 3 – MAC Aliases and Manufacturers

The log is downloaded from the Hornet to the PC for inspection and reporting. The records in the log file are time-stamped and contain Received Signal Strength Indicator (RSSI) values. Now the user knows when the alarms occurred and the strength of the signal. The strength of the signal helps in determining how close the AP/Client may be to the Hornet™. A sample Hornet™ log dump can be seen in Figure 4.

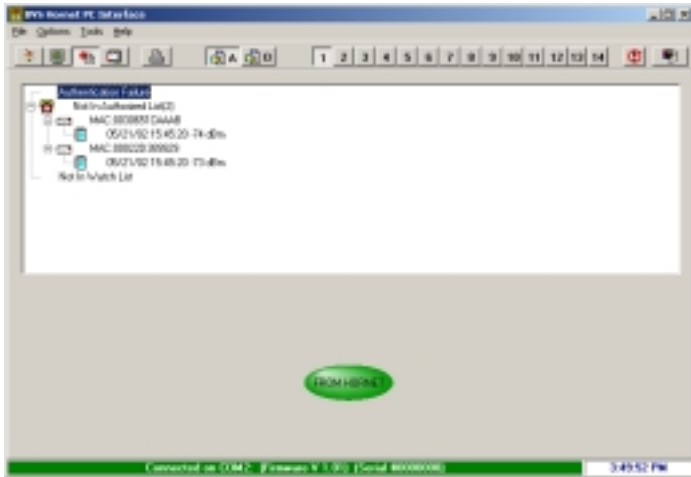


Figure 4 – BVS Hornet Log Dump

After potential intruders have been identified with the Hornet™, the BVS Yellow Jacket™ can go on "search and destroy" mission. The Yellow Jacket™ is a hand-held custom receiver that is coupled to a Pocket PC running Yellow Jacket™ software (Figure 5 shown with a directional antenna).



Figure 5 – BVS Yellow Jacket

It has a number of features that include spectrum analysis, AP/Client lists, channel utilization, network usage, multi-path/RSSI/PER/Data Rate Usage (as seen in Figure 6a). Data can be logged to the onboard memory for a later transfer to a PC through the IR,USB, or RS-232 link.

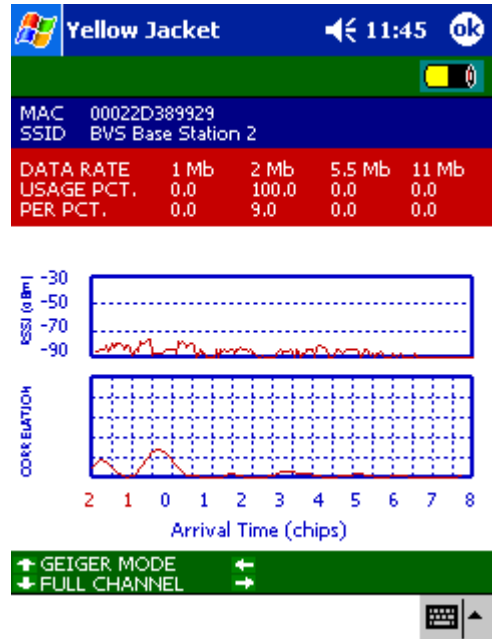


Figure 6a – BVS Yellow Jacket (RSSI/Multipath)

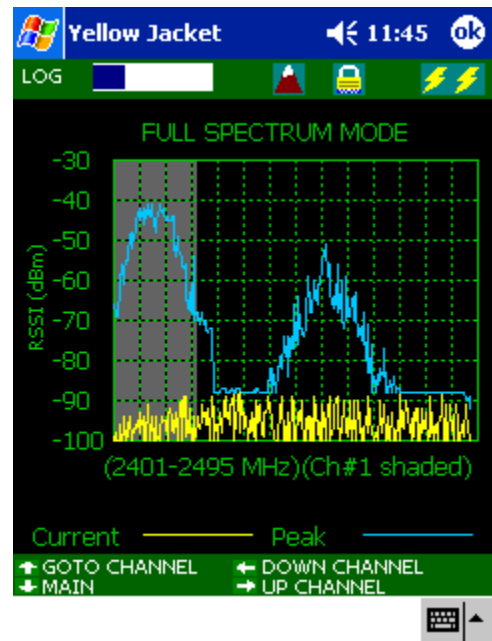


Figure 6b – BVS Yellow Jacket (Spectrum)

Using the Yellow Jacket™, a specific MAC address can be sought out. Using the multi-path screen or "Geiger screen" (Figure 8), visual and audio aides notify the user of a change in distance from the particular AP/Client.

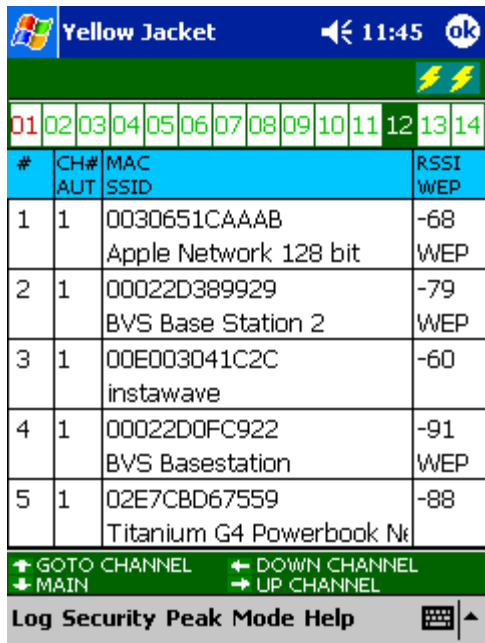


Figure 7 – BVS Yellow Jacket™ AP/Client Screen

Also, using the spectrum analysis mode, RF interference can be detected. If the network throughput is down and the packets are only being sent at 1 or 2MB/s, then interference may be the cause. In the spectrum analysis screen, you may see high levels of RF energy on certain channels where you would expect to see AP/Client traffic. This interference may be due to innocent items such as a microwave oven. But RF interference from intentional sources would also be seen in this screen.

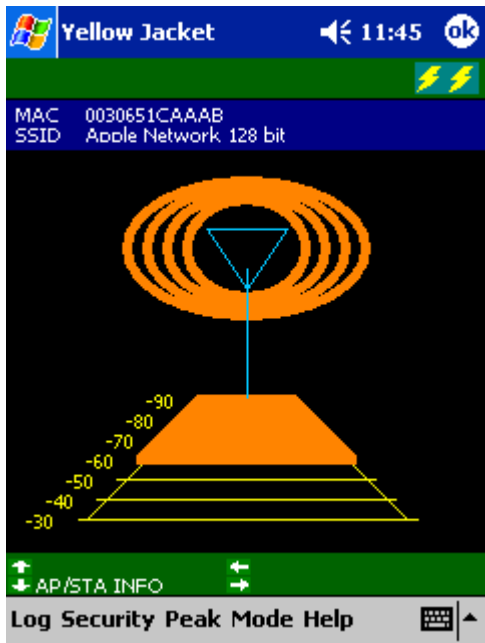


Figure 8 – BVS Yellow Jacket™ " Geiger Screen"

BVS Bird's Eye™ site survey and analysis system can be used to get a visual feel of where intruders may be lurking. The Bird's Eye™ system allows a user to create or import a site, which can be a building or other type of

campus. Using the Bird's Eye™ software on the Yellow Jacket, points are recorded with a full 14-channel analysis. The resulting data is then taken into the analysis program back on the PC.

The PC analysis program can then show a coverage analysis using the data from the Yellow Jacket™. The resulting colored site can then reveal where an intruder may be hiding.



Figure 9 – BVS Bird's Eye Analysis for WLAN

These monitoring devices are invaluable tools in the fight against possible breaches to network security. The logging and display capabilities of key parameters can help network managers maintain a secure network, free of intruders and RF interference.

References:

International Standard ISO/IEC 8802-11 ANSI/IEEE Std 802.11, The Institute of Electrical and Electronics Engineers, Inc., 1999.

O'Hara, Bob and Petrick, Al, 802.11 Handbook - A Designer's Companion, Standards Information Network, IEEE Press, The Institute of Electrical and Electronics Engineers, Inc., 1999.