



HIGHPOINT SECURITY TECHNOLOGIES Inc.

ANTENNAS FOR TECHNICAL SECURITY APPLICATIONS

By BILL CRUNKHORN

2006

Property of Highpoint Security Technologies Inc The use of this document may use the contents to recreate the design for their own non commercial use. This document shall not be reprinted in part or in whole for any commercial enterprise.

Abstract

Technical Security countermeasures includes searches for radio devices, which may be either audio or data transmission devices intended to relay sensitive information from the target's location to a listening post.

As the eavesdropper invariably wishes to make the detection of his attack as difficult to find as possible, the frequency of the radio transmission can be whatever the available technology makes possible.

Technical Security Inspections invariably include searches of the Radio Frequency Spectrum for Spatial Radio Frequency attacks, using either a Spectrum Analyser or Receiver.

This paper discusses the available antenna options for interfacing a Receiver or Analyser to the Electromagnetic universe.

The Electromagnetic Spectrum

It is widely known that Radio waves are Electromagnetic waves akin to heat and light, and differ from heat and light only in the rate at which the waves repeat themselves, or their frequency.

Effectively, the Radio Frequency spectrum is a somewhat variable part of the Electromagnetic Spectrum that tends to grow as technology find better ways make transmission at higher and higher frequencies better. At the lower end, the Radio Frequency spectrum is limited by the size of antennas required to transmit the waves.

Electromagnetic waves travel through a vacuum at 299,792,458 metres/second. The waves are neither electrical nor magnetic, but contain the characteristics of both. At the radio frequency end of the spectrum, the waves are absorbed or attenuated by various materials to differing degrees, and are reflected by metal surfaces.

Radio Frequency waves are invariably created by changing an electrical current in a wire. They are detected by placing a wire in the field, and detecting the electrical output of the wire. The wire is known as an antenna, and for a practical application can be a simple wire or a very sophisticated transducer.

The Eavesdropper's Radio Spectrum

From an eavesdropper's perspective, the radio frequency spectrum suitable for his surreptitious radio link has to fulfil a number of priorities. The most fundamental priority is that it has to work. Installing a technical attack is difficult and sometimes extremely dangerous. The technology used has to have a very high chance of working, or it is all a waste of time. Secondary considerations are difficulties in detection, especially against a technically adept defensive capability, and sometimes battery life.

If we review the Radio Frequency Spectrum from the perspective of the attacker, the spectrum can be divided as shown in the following table. Note that the band occupancy is generalised, and all sorts of other transmissions and exceptions can be found in the bands.

Band	Frequency Range	Notes
Very Low Frequency (VLF)	3 kHz - 30 kHz	Used for submarine communications, and for lineborne (carrier current or MOVA) Technical attacks
Low Frequency (LF)	30 - 300 kHz	Useful for carrier current or MOVA attacks, but not for spatial attacks as antennas are too large.
Medium Frequency (LF)	0.3 - 3 MHz	
High Frequency (HF)	3 - 30 MHz	Can be used for spatial attacks using available cabling for antennas, but as the HF spectrum is full of many high power and unpredictable communications links which may appear at any frequency at any time, the probability of a successful operation are reduced.
Very High Frequency (VHF)	30 - 300 MHz	The low end of this band, up to about 88 MHz, are used by the military, and most of the time this band will be quiet. In the middle of the band is broadcast FM radio broadcast, while the higher end includes aviation, point to point communications, and even Television. Antennas for both transmit and receive are relatively small, and the attenuation of buildings to the waves is fairly low. A very popular band for eavesdroppers.
Ultra High Frequency (UHF)	300 MHz - 3 GHz	When definition of the bands were written, this band appeared ultra high. Now it is pretty average. Broadcast television uses the lower end of the band, in the middle are cellular telephones, and wireless LANs can be found towards the top end. A very suitable frequency range for a technical attack, though as frequency increases, power requirements for the transmitter tend to increase, which may impact battery life.
Super High Frequency (SHF)	3 - 30 GHz	Historically the domain of Radars, this band is now undergoing exploitation for LANS. A very suitable part of the spectrum for a more sophisticated eavesdropper who sees his target as moderately well protected by technical security countermeasures.
Extra High Frequency (EHF)	30 - 300 GHz	At the time of writing this on 2006, this part of the spectrum is fairly low risk, as there are significant technical challenges to mounting an attack in this range. At the time of reading, the status may be different. Attacks in this range are within the grasp of most government agencies.

It can be seen that VHF and UHF part of the spectrum are the areas of most concern, with the lower part of the SHF spectrum of growing significance.

This is not to say, however, that any part of the spectrum is insignificant, dependant upon the capabilities of the attacker.

The TSCM Antenna

There are two ways to conduct a search for Radio Frequency devices, near field and far field. The near field approach uses equipments like the Shearwater Hunter, which are relatively insensitive but very wide band equipments which are used like metal detectors to identify areas of high electromagnetic field strength. The second approach uses a sensitive wide band receiver or Spectrum Analyser to study the radio frequency spectrum from a fixed location. Both approaches have major values, and both should be used for a Technical Security Inspection.

For the Receiver/Analyser approach, the interface with the Electromagnetic Spectrum is the antenna, and without a good antenna, the receiver/analyser is effectively blind.

There are a number of terms related to the antenna which are critical for TSCM work.

Bandwidth

This term refers to the frequency range at which an antenna operates. Antennas are normally either narrow band, like dipoles or whip antennas, or broad band.

Radiation Pattern

Refers to the directions which an antenna will send, or receive, its radio waves. It is often allied to antenna gain (see below).

Gain

A passive antenna (see below) with gain has physical characteristics which concentrate the antennas response in one direction. In the case of a receive antenna, this makes the antenna more sensitive in one direction.

Active and Passive

A passive antenna is a metallic structure with physical characteristics which determine the way the antenna performs. An active antenna has integral amplifiers and filters designed to improve the antenna's performance.

Polarisation

Most Electromagnetic waves have waves which are polarised in a single direction. Like polarised sunglasses, if the receive antenna does not match polarisation of the wave, the antenna will detect the signal very poorly.

The Ideal TSCM antenna

For TSCM work, the antenna needs to be as broad band as possible. For most applications, it needs to be able to receive signals from all directions at once, as the sweeper never knows where the device is planted. The antenna needs high sensitivity, to be able to detect low power devices from significant distances.

Compromises are always part of any system, and the ideal antenna has yet to be created. Technology has allowed the production of some very good antennas, however. The table below lists a few approaches ;

Antenna Type	Disadvantages	Advantages
Whip Antenna	A narrow band antenna, this antenna is absolutely useless, except for the specialist case of the Active Rod which is useful for searching the HF spectrum. One of the saddest sights in the TSCM world is an advert for a receiver touting magnificent sensitivity specs with a whip antenna stuck on top. Like sticking a lawn mover engine in a Ferrari.	Cheap.
Dipole	As above. Can be broader band, but still very limited. Polarisation sensitive.	Cheap.
Biconical	Polarised, limited bandwidth.	Receives well from all directions with very small nulls.
Log Periodic	Directional and polarised.	Quite sensitive due to its gain, and can be very broad band.
Log Spiral antennas	Directional	Quite sensitive, broad band, and receives signals in any polarisation without penalty.
Planar Log Spiral		Less sensitive as it has no gain, but receives from all directions with very small nulls, and receives signals of all polarisations without penalty.
Active Planar Log Spiral		As for Planar Log Spiral, but with the addition of sensitivity.

Conclusion

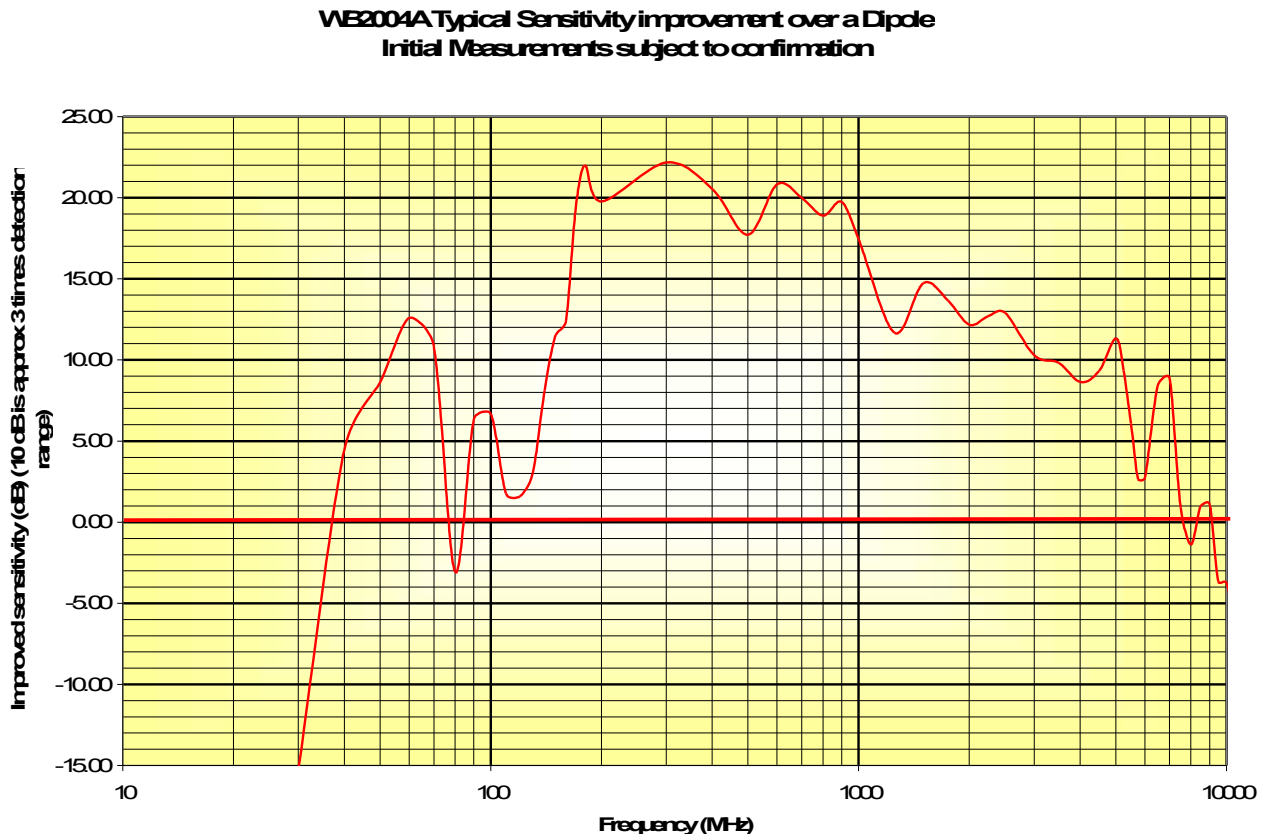
We regard the Active Planar Spiral as the best available TSCM antenna currently available. The Shearwater WB2004A is our offering in this antenna type.

Compared to competition, it has the following advantages

- Useable frequency range from 30 MHz to 9 GHz, with extremely flat response from 200 MHz to 7 GHz.
- Very high sensitivity. 20 dB better across the band than a dipole achieves at it's tuned frequency (will give a Spectrum analyser ten times the detection distance).
- Omni-directional. There is a null in response in the plane of the antenna, but it is very small.
- Polarisation Insensitive. This antenna does not care what polarisation the wave has, receives signals equally regardless of polarisation.
- Small. Antenna is a flat, thin package, easy to transport and easy to mount.

WB2004A Performance

The graph below shows the improvement in sensitivity which would be achieved if the user had a series of dipoles specifically tuned to each frequency. An impractical proposition, of course.



10 dB improvement is three times the detection range, 20 dB is ten times the detection range.