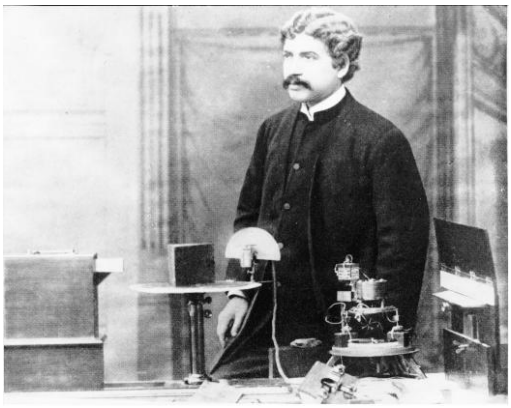
# Millimeter Radios – Clean Spectrum and Security

Millimeter Wave Frequencies

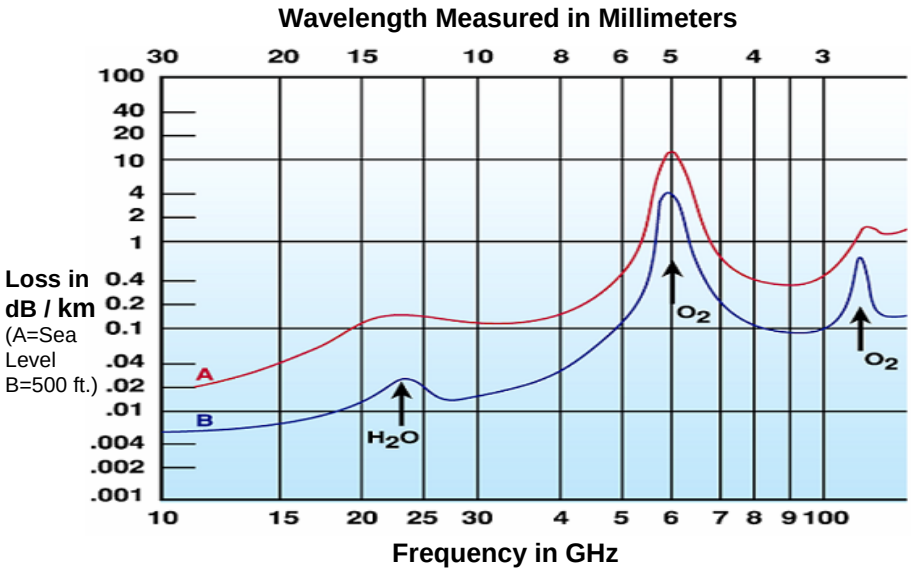
The spectrum between 20 GHz and 300 GHz is referred to as the millimeter wave band because the wavelengths for these frequencies are about one to fifteen millimeters. Old physics books refer to this frequency band as “quasi-optics”. Use and experiments in the band predate Marconi’s radio experiments but several years. In 1895 J.C. Bose gave his first public demonstration of electromagnetic waves (millimeter waves @ 60 GHz), using them to ring a bell remotely and to explode some gunpowder (see Bose in Fig. 1). It wasn’t until 1897 that Marconi made his “radio waves” demonstration on the Salisbury Plain in the UK.

Fig. 1 – J.C. Bose



In microwave systems, transmission loss is accounted for principally by the free space loss. However, in the millimeter wave bands additional loss factors come into play, such as gaseous losses ($O_2$) and rain in the transmission medium. Fig. 2 shows the loss due to atmospheric conditions by GHz frequency.

Fig. 2 – Atmospheric Loss of Millimeter Wave Frequencies



While signals at lower frequency bands can propagate for many miles and penetrate more easily through buildings, millimeter wave signals can travel several miles but do not penetrate solid materials very well. However, these characteristics of millimeter wave propagation are not necessarily disadvantageous. In fact, because microwave signals travel many miles, they are likely to interfere with each other when operated in proximity to other microwave signals. Conversely, millimeter wave signals travel much shorter distances and are able to operate in close proximity to one another without interference. Also, millimeter waves can permit more densely packed communications links, thus providing very efficient spectrum utilization, and increase security of communication transmissions.

2.4 and 5 GHz Frequency Bands

The availability of unlicensed frequencies in the 2.4 and 5 GHz bands and the price reduction of radio technology have caused wireless networks to explode across the landscape at an unprecedented pace. It is estimated (ABI Research) that there are over 500 million radio devices operating in these bands worldwide, with the lion's share in the United States. These devices range from the Bluetooth on your mobile phone to WiFi /WiMax chips embedded in laptop computers to high data rate radio systems for commercial communications.

One of the technical reasons for such success of these systems in the 2.4 and 5 GHz bands is that they can go long distances and operate in a broadcast mode (i.e. Omni -directional antennas). However with the addition of each radio device in these bands the background noise level at these frequencies increases across a large area. With over 500 million radio devices deployed, the background noise level is quite high and can severely impact the functionality of a radio system from reduced throughput to outright failure of the signal. So, to properly operate radio systems in these frequencies an increased level of engineering is required for installation along with constant monitoring and possible re-engineering.

The same characteristics of these frequencies described above also mean that these networks can be "seen" (intercepted) from long distances. The cost of interception equipment is also quite low. It can range from $29.99 to $3,000 depending on how sophisticated the intercept (see Fig. 3). In fact, a very low cost but effective interception device can be made from common household and electronic parts. Instructions are on the internet (see Fig. 4)

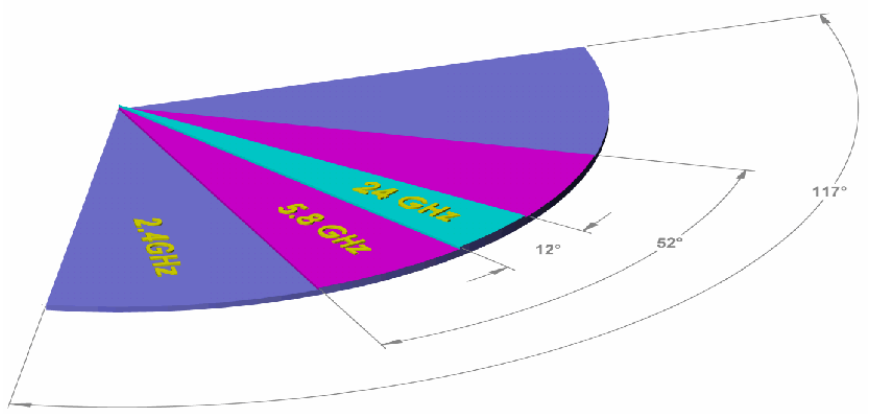
Fig. 3 - 2.4 GHz and 5 GHz Intercept Devices

Fig. 4 - Pringle's Can Intercept Device

24 GHz Unlicensed Band

There are many expensive and involved techniques, engineering schemes and alternate media's available to "get around" problems described above. However, most are marginal and require constant monitoring and adjustments. The most effective and secure technique is to operate these radio systems in the millimeter wave bands. For this discussion we will concentrate on the unlicensed 24 GHz band. 24 GHz radio signals do not go as far as the 2.4 and 5 GHz bands because there is more atmospheric attenuation at this frequency and higher attenuation due to rain as described above. Also, at this frequency the radio waves are much more directional (i.e. it has a narrower beam of energy). See Fig. 5.

Fig. 5 - Beam Widths with a 12" Antenna



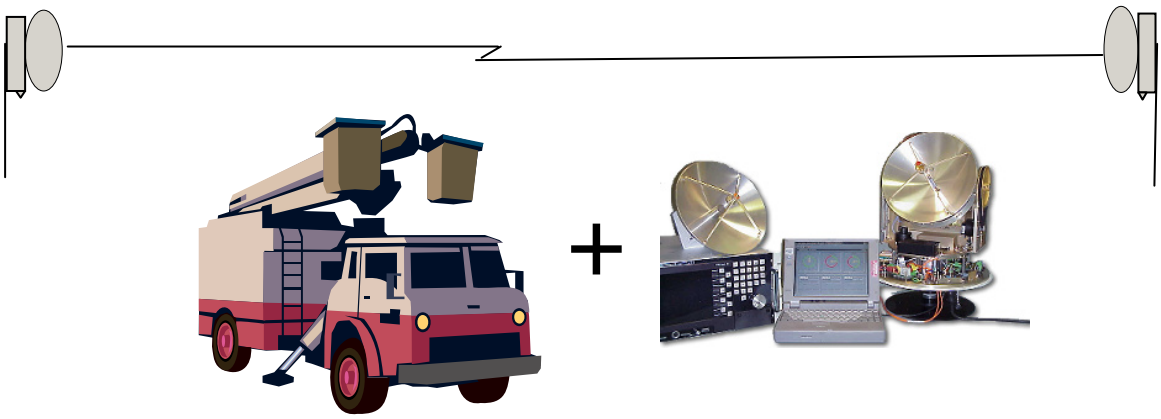

This means that signals at 24 GHz do not bounce around like the signals at 2.4 and 5 GHz to create a noisy environment. Additionally, because radios at these frequencies have traditionally been very costly and bulky, few have been deployed. This means that 24 GHz is an interference free frequency and will not suffer the degradation and difficulties of the noisy 2.4 and 5 GHz frequency bands.

One of the best advantages of the 24 GHz band is its inherent security. Unlike the 2.4 and 5 GHz bands that have low cost and easy to use "intercept" tools (See Fig. 3 and 4), the equipment and tools to "intercept" a 24 GHz signal are expensive and require very specialized engineering knowledge. In fact, the cost of such equipment is more than $300,000 and they have to be custom built for the exact frequency to be intercepted. Additionally, the expertise to use this equipment normally resided only with large government intelligence agencies (See Fig. 6). Frequency security should not be the only consideration for security of a link. Strong encryption must play a significant role in any wireless security scheme.

Fig. 6 – Specialized and Custom Equipment for 24 GHz Interception

As seen in Fig. 5, the beam width at 24 GHz is quite narrow and makes "finding" the beam that much more difficult. In fact, because of the low power requirements of radios operating in the unlicensed 24 GHz band (FCC mandated), someone trying to "intercept" the signal ("Man in the Middle") would have to literally get directly in the path of the radio with the equipment in Fig. 6 to have any hope of intercepting the signal (see Fig. 7). Because of the inherent security of the millimeter wave bands, DoD and covert operatives have used millimeter bands for years for their secure communication needs.

Fig. 7 - "Man in the Middle" needs a lift !!! Plus his stuff!!



Summary

For commercial applications of wireless radios, especially in a point to point mode, the use of millimeter bands and especially 24 GHz can offer interference free and secure links. Systems at 2.4 and 5 GHz can be quite good but suffer the problems of too many systems in the same space (frequency) and are too easily and cheaply intercepted. In the end, the customer must make their own cost / benefit analysis of which systems to use, but for customers requiring high levels of performance and security, 24 GHz systems offer a significant advantage.