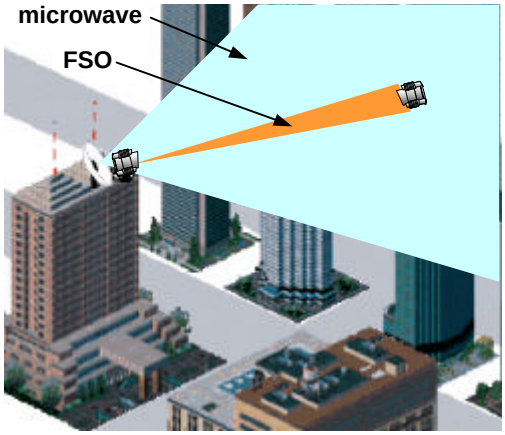
Application Note - Security of a Free Space Optical Transmission

The low-security characteristics of RF systems have led many people to wrongly conclude that all wireless transmissions are highly vulnerable to interception. What can you do to protect your data while still enjoying the benefits of high-speed wireless connectivity?

Your answer for exceptional wireless transmission security is SONAbeam™ Free-Space Optical communications.

SONAbeam™ Free-Space Optics (FSO) technology is among the most secure of all wide-area connectivity solutions due to its inherently low probability of intercept (LPI) and anti-jam (AJ) characteristics. Eavesdropping and physical interception are extremely difficult and the chance of an attempted intercept being discovered is very high. For these reasons government and military organizations that value security, including the Pentagon, have deployed FSO systems for voice, video and broadband data communications.



Traditional Wireless Security

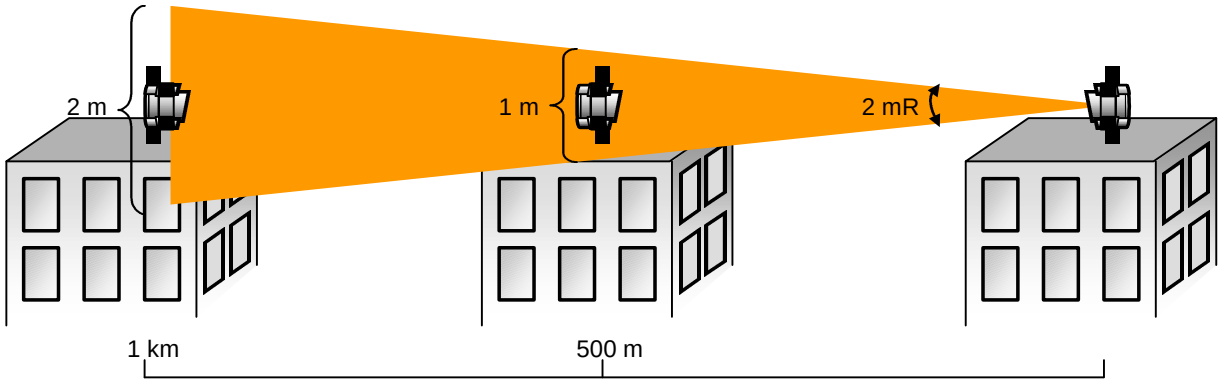
Many RF systems, like cellular phones, police radios, and wireless LANs intentionally radiate signals in all directions making the signal accessible to anyone with a receiver. Instead of radiating in all directions, point-to-point (PTP) microwave systems transmit a highly directional cone-shaped beam that minimizes off-axis radiation, thereby reducing the potential for security breaches. However, the divergent transmit beam is still vulnerable to interception and jamming within a fairly wide footprint - from the side of a building to an entire city block.

PTP microwave and RF systems also have sidelobes and a backlobes radiating off-axis energy that are vulnerable to interception. In addition, reflected energy from buildings within or near the fresnel zone can be exploited. As a result, an unauthorized receiver can be located well off-axis to the main beam and be quite discreet.

None of these issues apply to an FSO communication link. There is no fresnel zone and no sidelobes or backlobes involved, and the extremely narrow beamwidth of the transmission makes interception a significant challenge. In fact, there are a number of features that make FSO transmission, and in particular SONAbeam technology, the most secure wireless communication solution available today…

Narrow Beamwidth

In order to intercept a communications link, an intruder must intercept a portion of the transmitted beam, without exposing himself or his equipment. The narrow beamwidth of an FSO transmission (sometimes referred to as a “pencil beam”) forces a would-be intruder to get within inches of a terminal or the line-of-sight itself. Because the transceivers are normally installed high above street level, such efforts are extraordinarily difficult and the chance of being discovered is very high. The figure below shows the basic geometry involved with the SONAbeam’s 2-milliradian beam …



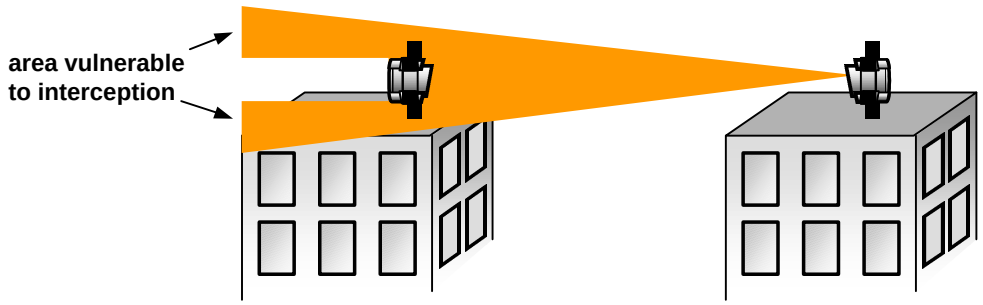
Detector Challenges

Intercepting a communication signal is not very useful if the intruder is detected in the act. Although it is possible to intercept the FSO beam without bringing down the link, any attempt would be discerned as an anomalous power loss at the receiver, which in turn would send an alarm to the user via network management software. Moreover, it is not enough to simply place an antenna in or around the beam as with an analog RF signal. The detector must be specifically designed to interpret a digital transmission on 1550nm light. Such a device, especially if it were small and stealthy, would have extremely poor sensitivity and would be useful in only the most powerful sections of the beam (near the center of the actual line-of-sight, or near the terminal itself). Consequently, the options for an intruder are even more limited.

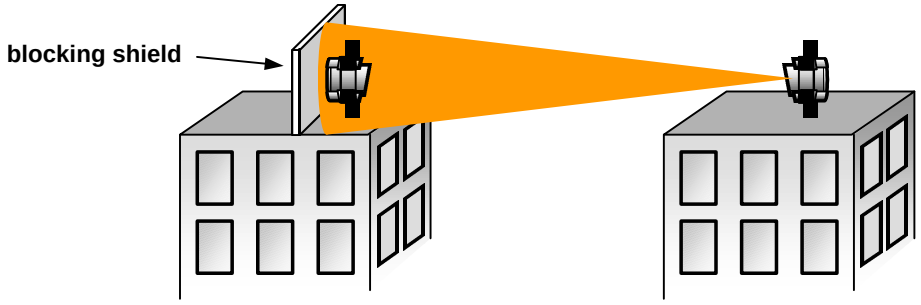
FSO transmission is not only difficult to access physically but is in fact nearly impossible to detect in the first place. 1550nm light is invisible to the naked eye and standard photography and video cameras. Unlike other systems that transmit at 800-900 nm, the SONAbeam transmission is also invisible to standard night-vision equipment.

Interception Behind the Terminal

The most vulnerable area of potential interception in an FSO link is behind the communication terminal itself. Because the incident beam of light has a larger cross-section than the terminal itself, some of the light overshoots the terminal and continues to propagate behind it for some distance (depending the atmospheric conditions). An intruder could conceivably mount an unauthorized receiver in this area, as shown below.



The simplest way solve this problem is to place a blocking shield behind the terminal (or mount the terminal against an existing wall), as shown below. This eliminates an overshoot and effectively limits the transmission signal to the immediate vicinity of the terminal itself.



For those cases in which a blocking shield is not feasible, the transmission is vulnerable to interception for a limited distance behind the terminal. At some point the light is attenuated in the atmosphere to the point where any signal is undetectable. At first glance, the exceptionally high transmit power of the SONAbeam would seem to be a disadvantage, as it would result in further propagation of the overshoot signal beyond the terminal. However, the Active Power Control (APC) feature of the SONAbeam actually uses the system's wide dynamic range to the advantage of transmission security.

The APC feature maintains optimum transmit power for the current weather and link conditions, increasing power when needed and reducing it when not needed. Consequently, the transmission power is never greater than necessary to keep the link active, with a certain amount of margin. This limits the overshoot distance beyond the terminal, as well as any opportunity for a would-be intruder.

We can loosely estimate how far the detectable overshoot distance will be for a typical application. Let us consider a 1km link on a clear day, in which the atmospheric attenuation is about 3 dB/km. Let us further assume for this example that both the FSO terminal and an unauthorized detection device have receiver sensitivities of –35 dBm. If APC maintains a power level such that the link margin is always 5 dB, than the signal level at the terminal is –30 dBm.

As the beam continues propagating beyond the terminal, it becomes more attenuated in the atmosphere at a rate of 3 dB/km. Also, because of the 2mR beam divergence, the power density falls by another 3 dB between the 1st and 2nd kilometre marks. Consequently, the signal falls to –35 dB (the sensitivity of the detector) approximately 800 meters behind the terminal. This is the furthest away that the intruder could position his/her equipment. Under more typical weather conditions, in which the atmospheric attenuation is about 7 db/km, this maximum distance is reduced to 500 meters.

In reality, an unauthorized detection device would not have the same sensitivity or collecting aperture as a SONAbeam terminal. The device would also be collecting light toward the fringes of the beam, in which the power density is lower than it is in the center of the beam. If we take these more realistic assumptions into account, the maximum detection distance is significantly reduced.

Encryption

An added layer of security may of course be applied to the data itself by utilizing an encryption scheme. Because the SONAbeam is effectively a passive layer-one transport and does not manipulate the data bits directly, the system is transparent to any encryption or coding algorithm that the user cares to employ. This includes such specialized encryption schemes as the Fastlane KG-189, Taclane KG-75/175 (NSA, Type 1), and all AES and Triple DES encryption systems.

fSONA Communications Corporation

#140 - 11120 Horseshoe Way,
Richmond, B.C. Canada, V7A 5H7
info@fSONA.com
www.fSONA.com

United States and Canada: 877.Go.fSONA (463-7662)
International: 877.2.Go.fSONA (463-7662)
Telephone: 604.273.6333
Fascimile: 604.273.6391

Please contact your sales representative for further information.