

### Data Security in Free Space Optics

MRV Communications designs, manufactures and supplies Free Space Optics (FSO) based devices for voice, video and data transmission. Our optical wireless TereScope® products can transmit and receive data at rates of up to 1 Gbps and distances up to 4 km.

FSO is technologically very similar to communication using fiber optic cables. Both use laser light to carry the 1s and 0s of digital data. But while traditional fiber optics transmits the laser light through a strand of glass, FSO sends the laser light through the air (“free space”). Since the two technologies are so similar, they share the same advantages of high data rate capacity and protocol independence. Both technologies are also very secure. This paper discusses some of the security features of FSO in detail and describes why FSO is the most secure wireless technology currently available.

Some principle attributes of FSO communication:

1. Directional transmission with an extremely narrow transmit beam for point-to-point (line of sight) connectivity
2. The absence of “side lobe” signals
3. Complete, uninterrupted links required for successful communication
4. Protocol transparent transmission
5. Physical Layer operation
6. “Plug and Play” devices

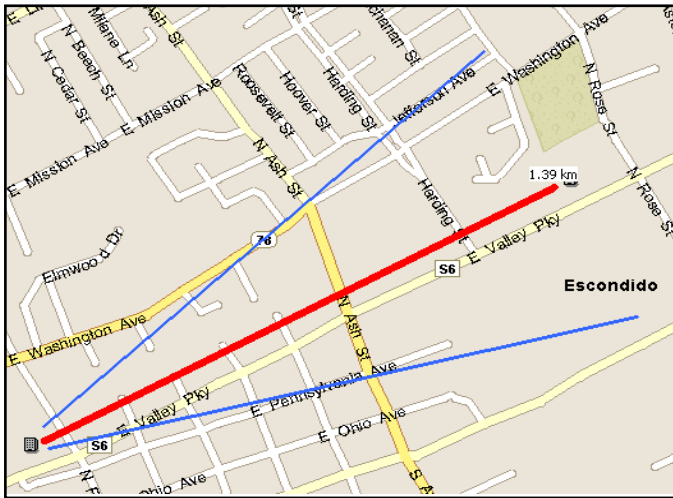
These key features allow for very secure transmission over an FSO channel. To understand why this is the case, we first need to consider what must take place to successfully steal a communication signal.

Two criteria must be satisfied for an individual to overcome the security in a network: (1) they must intercept enough of the signal to reconstruct data packets and (2) they must be able to decode that information. If these two primary requirements cannot be met, the security of the network will remain intact. Given these two conditions, we will now examine how the above attributes of FSO transmission can be used to maintain a secure data link.

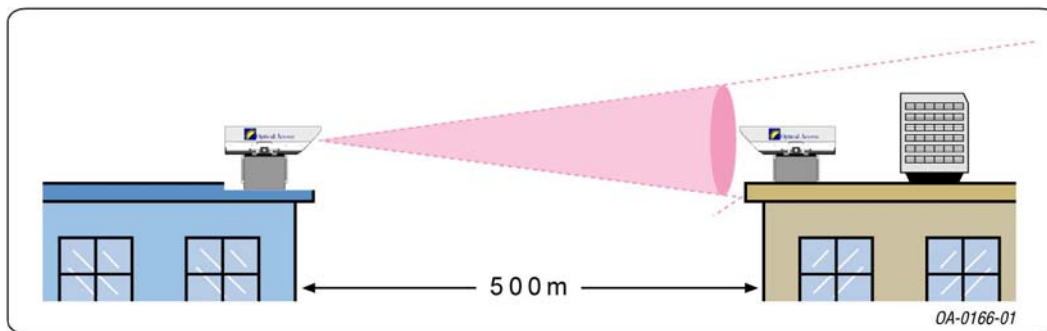
#### Preventing Interception of the Signal

##### *Directional transmission*

When considering the security of wireless data transmitted through the air, one of the most important elements is the path of the transmitted signal. Generally speaking, broader signal paths allow a greater opportunity for that signal to be intercepted. The directional nature of FSO transmission yields a tremendous security advantage here. FSO uses collimated laser light as the transmission medium; therefore, the signal is kept very narrow throughout its entire path. Figure 1 provides an illustration of the light path of an FSO beam, compared to a standard Radio Frequency (RF) signal. Figure 2 also depicts the narrow beam transmitted from an individual transceiver.



**Figure 1. Narrow divergence of the FSO** transmit path (shown in red) as compared to a typical **Radio Frequency (RF)** path (shown in blue). The tightly collimated FSO beam ensures that the signal energy is focused on the receiving unit, making interception of the beam extremely difficult.



**Figure 2.** Another view of the narrow beam divergence inherent in FSO transmission. (For clarity only one transit beam is shown.)

Table 1 illustrates the beam diameters for various TereScope products at different installed ranges. The table presents several models for transmission rates of 1 Mbps to 1.25 Gbps.

From table 1, we learn that the transmit beams of TereScopes at ranges of 300-500 meters are very narrow. This is also true of longer-range systems over 1 km- with a maximal diameter of 250 cm. Thus, whatever the application's required distance, the diameter of the beam remains very narrow, making it almost impossible to intercept.

TereScope Model	Data rate (Mbps)	Divergence (mrad)	Beam Diameter at 100 m (cm)	Beam Diameter at 300 m (cm)	Beam Diameter at 500 m (cm)	Beam Diameter at 1000 m (cm)	Transmitting Power (mW)	Transmitted Wavelength (nm)
TS2/C/E1	1.55/2.048	2.8	28	84	140	280	3.3	850
TS2/D/E1	1.55/2.048	1.8	18	54	90	180	16.5	850
TS2/E/E1	1.55/2.048	2.5	25	75	125	220	22	850
TS25/B/DST	1-25	4	40	120	200	-	2.7	850
TS25/C/DST	1-25	4	40	120	200	-	8	850
TS25/D/DST	1-25	1.8	18	54	90	180	16.5	850
TS25/E/DST	1-25	2.2	22	66	110	220	21	850
TS10/C/ETH	10	4	40	120	200	-	8	850
TS10/C/ETH	10	1.8	18	54	90	-	16.5	850
TS10/C/ETH	10	2.2	22	66	110	220	21	850
TS155/B/DSC	34-155	2.8	28	84	-	-	1.1	850
TS155/C/DSC	34-155	2.8	28	84	140	-	3.3	850
TS155/D/DSC	34-155	1.8	18	54	90	-	16.5	850
TS155/E/DSC	34-155	2.2	22	66	110	220	21	850
TS155/J/DSC	10-155	2.5	25	75	125	250	21	785
TS1000/A/DSC	1,250	2.5	25	75	125	-	9	850

**Table 1.** Beam diameter size for various TereScope operating at 1 Mbps to 1.25 Gbps.

### *The absence of side lobes*

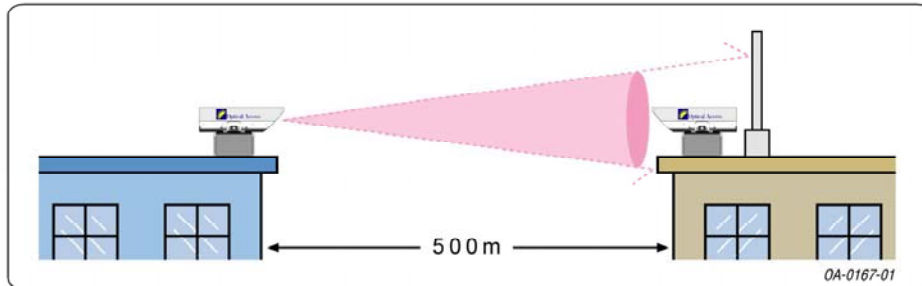
RF transmission systems are known to “spill” energy in predictable patterns on the sides and to the rear of the antenna. This lost energy is called a ‘side lobe’ and it typically carries the same signal that is being transmitted to the other end of the link. FSO systems avoid this problem since all of the beam energy is transmitted at a narrow divergence angle.

### *The need for a complete, uninterrupted link*

FSO terminals require a complete and uninterrupted link for successful operation. If someone attempts to intercept a signal by placing a detector in the path of the beam, the link will be blocked and communication will be terminated. Therefore, the only way to intercept an FSO transmission is by attempting to “pick off” the narrow beam path from a location behind the building on which the receiving unit is installed. To prevent this highly unlikely event, it is possible to shield the beam so that it does not continue beyond the point of reception.

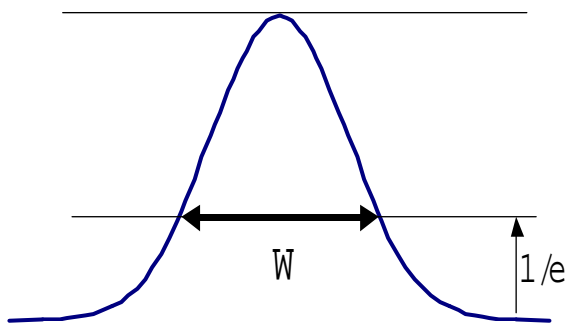
This shielding can be accomplished in two ways:

1. Install the receiver against a wall, which is twice as wide as the radius of the FSO beam, thus ensuring that the entire FSO signal will be absorbed and cannot be intercepted beyond the building.
2. If the link is installed on a rooftop or an open surface, it is possible to place a covering or shield



**Figure 3.** Beam shielded to avoid reception beyond the

behind the receiver. Figure 3 provides an example of how this can be accomplished. For the greatest security, the shield should be at least twice as large as the beam diameter at the receiver (see the explanation in Figure 4 below). This serves to block the diffusion of the beam.



**Figure 4.** In FSO transmission, the cross-sectional profile of the beam is Gaussian in shape. The width of the beam “W” is defined as the full-width at  $1/e$  of the maximum power. Beyond the defined width of the beam, there is still some laser energy, but it is much lower in strength, so it would be very difficult to “pick off” and decode the transmitted signal. However, where security is especially mission-critical, the beam width should be multiplied by 2 to ensure that all of the laser beam’s energy will be blocked. For example, the signal of the TereScope 3000 has a divergence of 2.5 mrad. At a distance of 500 m, the beam diameter is 1.25 meters (using the definition of beam diameter above). To completely block all energy past the transceiver, a screen of 1.25 m x 2 (or 2.5 meters) diameter should be placed directly behind both transceivers.

### *Chance interception impossible*

When light travels through free space, the path can sometimes be altered by heat or other factors. Someone might believe it possible to take advantage of this fact and try to “pick off” a signal through random scattering effects. However, this is practically impossible.

Over a long distance, temperature changes between pockets of air can cause an FSO beam to scatter slightly. This is known as *scintillation*. When the beam is scintillating, photons of light are temporarily steered by pockets of air in random directions. This same atmospheric effect is what causes stars to appear to ‘twinkle’ at night.

These air pockets are in permanent motion, so the boundaries between the various pockets are constantly changing. Because scintillation is caused by the laser light passing through the boundaries of neighboring air pockets, the path of these ‘twinkling’ photons is also always changing randomly. Furthermore, these changes from scintillation last for only fractions of a second. Since the angle of



## FSO Technological Paper

scintillation is random and changes are very fast, it is impossible to forecast a specific spot for intercepting the signal.

Experimental evidence of this phenomenon is contained in the article, “Characterization of an Optical Wireless Channel”. According to the experimental findings, it appears that the maximum deviation that can occur is +/- 70 mrad. This deviation is minimal and does not exceed the security range recommend for the beam.

### *Misdirection of the beam*

It is important to note that if a strong deviation of the beam path occurs unnaturally, the beam will not be received on the opposite side of the link. The networking equipment will automatically halt the transmission until the link is reestablished. Therefore, if someone intentionally aims the system in another direction in an attempt to redirect the signal, the TereScopes automatically drop the link and stop transmission.

### **Preventing Decoding of the Signal**

Because the TereScope systems operate at the physical layer and have no inherent protocol, they can be viewed as optical repeaters. With such a “bit in – bits out” design, it might seem as though an FSO signal would be easy to decode. However, because the TereScopes can passively transmit protocols, they also retain the security features of those protocols. Therefore, all switching and routing security features existing in a wire-line infrastructure can be carried over to the TereScopes.

Since the TereScope systems are also “plug and play”, encryption devices can be added to the link to offer additional security. The TereScopes passively re-transmit an encoded bit-stream, making outside signal decoding even more difficult.

### **Summary**

We have attempted to explain how the features inherent to FSO technology make outside interception and decoding practically impossible. Both theoretical and experimental arguments have been presented to demonstrate the security features of the TereScope systems.

MRV’s equipment has been used for years by the military in several countries and by other organizations in which secure information is mission-critical. The inherent features of FSO transmission have made it the most secure mode of wireless transmission current in use.

For further information, please visit us at: [www.mrv.com](http://www.mrv.com)