LIGHTPOINTE™

LIGHTPOINTE WHITE PAPER SERIES

Optical Wireless Security

Introduction

Network security is one of the major concerns for any business or organization transporting sensitive and confidential information over its network. Network security concerns include the base of the network model, typically referred to as the physical layer, or layer 1, as well as higher layers of networking and application protocols. Most of the interception activity by outside intruders occurs within higher protocol software layers. Password protection or data encryption are examples of counter measures to protect the network from outside and unwanted tampering. Intrusion of the physical layer itself can be another concern for network operators, although it is a far less likely target for unauthorized access to networked data. This can be a threat if information is transported over a copper based infrastructure that can be easily accessed, but optical wireless transmissions are among the most secure connectivity solutions, regarding network interception of the actual physical layer. LightPointe's optical wireless networking equipment is based on physical layer transport. This white paper discusses security aspects involving the physical layer.

Optical Wireless Systems and Network Security

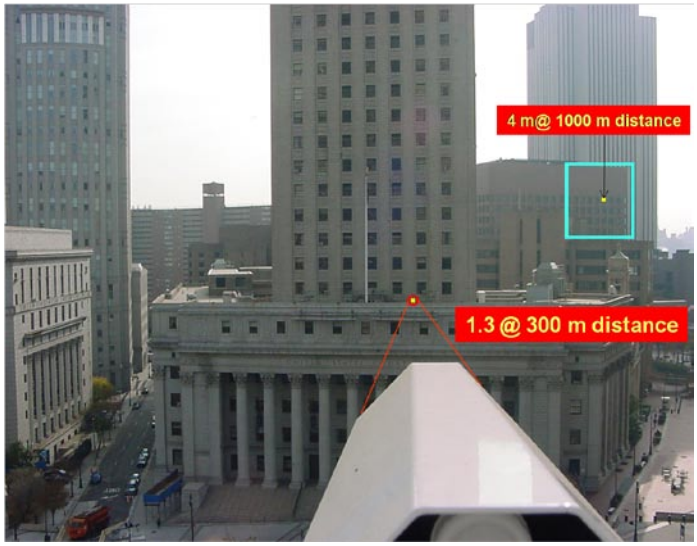
With its cost-effective and high-bandwidth qualities, optical wireless products operating in the near infrared wavelength range are an alternative transport technology to interconnect high capacity networked segments. These optical wireless products, based on free-space optics (FSO) technology, are license-free worldwide. Optical wireless system installations are very simple, and the equipment requires very little maintenance. These features make optical wireless solutions appealing to end-users and service providers globally. As a result, the number of optical wireless system installations for enterprise, cellular, and metropolitan area network traffic demands has increased significantly—even during the recent telecommunications sector slowdown.

Because optical wireless systems send and receive data through the air between remote networked locations, network operators and administrators are naturally concerned about the security aspects. Radio frequency (RF) or microwave-based communication systems have been vulnerable to security and interference problems in the past, providing cause for scrutiny. Such concerns are not valid for optical wireless systems.

Optical wireless systems operate in the near infrared wavelength range, slightly above the visible spectrum. Therefore, the human eye cannot visibly see the transmission beam. The wavelength range around 1 micrometer that is used in optical wireless transmission systems is actually the same wavelength range used in fiber-optic transmission systems. The wavelength range around 1 micrometer translates into frequencies of several hundred terahertz (THz). These frequencies are significantly (roughly three to four orders of magnitude) higher than the highest frequencies used in commercially available microwave communications systems operating around 40 GHz. This difference in frequency of operation is one of the main reasons why optical wireless systems belong in the equipment category of optical communication systems first rather than wireless, RF or microwave,

transmission solutions. While typical RF and microwave antennas used to interconnect two remote networking locations in a point-to-point architecture spread out the radiation over angles between 5 and 25 degrees, optical wireless systems use very narrow beams that are typically less than 0.5 degrees. For example, a radial beam pattern of 10 degrees roughly corresponds to a beam diameter of 175 meters at a distance of 1 kilometer from the originating source, whereas a beam of 0.3 degrees divergence angle typically used in optical wireless systems corresponds to a beam diameter of 5 meters at the same distance[1]. This wide spreading of the beam in microwave systems, combined with the fact that microwave antennas launch very high power level is the primary reason for security concerns. An outside intruder can easily intercept the beam or power reflected from the target location and pick up sensitive network information by using a "spectral scanner" tuned to the specific RF or microwave transmission frequency. To overcome these security concerns, the microwave industry uses wireless encryption protocols (WEP) to protect the transmission path from being intercepted. The 128 and/or 256 AES Rijndael encryption algorithm has become very popular over the past few years. Although it is extremely unlikely that it is possible to break into a more sophisticated encryption code, there is always the concern that it can be done.

The interception of optical wireless systems operating with narrow beams in the infrared spectral wavelength range is far more difficult. In fact, military organizations or government entities that rely heavily on extremely secure transmission technologies were among the earliest users of optical wireless communication systems as a way to avoid signal interception. Therefore, it is understandable why the study of FSO technology in military labs and security agencies dates back several decades. In the early days of FSO development, the ability to transmit information at high data rates was actually a less important factor than the fact that FSO technologies offered one of the easiest and most secure ways to exchange information between remote locations.



The small diameter of the beam at the target location, typically only a few meters in diameter, is one of the reasons why it is extremely difficult to intercept the communication path of an FSO-based optical wireless system: The intruder must know the exact origination or target location of the (invisible) infrared beam and can only intercept the beam within the very narrow angle of beam propagation. Even more difficult: the intruder must have free and undisturbed access to the installation location of the optical wireless transceiver and be able to install electronic equipment without being observed.

Fig. 1: Example of beam spot diameters at various distances for a beam divergence angle of 4 mrad.

[1] Due to the fact that the beam divergence angles in optical wireless systems are very narrow, the FSO community typically uses milliradiant as measure for beam divergence. 1 Radiant (rad)=57.3 degrees or 1 milli radiant (mrad)=0.0573 degrees. In other words, the divergence angle in mrad roughly corresponds to the beam diameter at a distance of 1 kilometer from the originating source.

Most often, the installation location does not allow free access to a potential intruder because the installation location is part of the customer premises, such as the roof or an office (when optical wireless equipment is installed behind windows). Fig. 1 shows an example of a 4 milliradian (mrad) beam projected onto the target location where the opposite terminal is located. At a distance of 300 meters the beam diameter is about 1.3 meters, while at a distance of 1 kilometer the beam expands to 4 meters. The photo clearly shows how extremely difficult it is for an intruder to intercept the beam.

The direct interception of an optical wireless beam between the two remote networking locations is typically impossible because the beam typically passes through the air at an elevation well above ground level. Due to the fact that the transmission beam is invisible and that any attempts to block the beam would occur near the optical wireless equipment terminus points, the transmission process imposes another obstacle. Picking up the signal from a location that is not directly located within the light path by using light photons scattered from aerosol, fog, or rain particles that might be present in the atmosphere is also virtually impossible due to the extremely low infrared power levels used in the optical wireless transmission process. The main reason for excluding this possibility of intrusion is the fact that light is scattered isotropically and statistically in different directions from the original propagation path. This specific scattering mechanism keeps the total number of photons, or the amount of radiation that can potentially be collected onto a detector that is not directly placed into the beam path, well beyond the detector noise level (Figure 2).

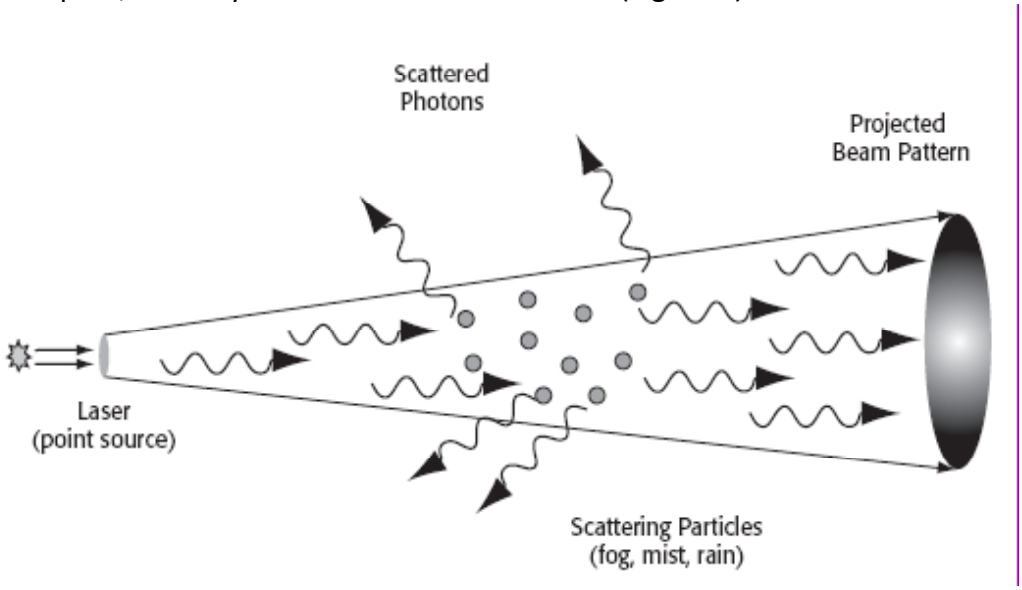


Fig. 2: Illustration of the physics of the light scattering mechanism while the light beam travels from the originating laser sources (left) to the receiver at the opposite communication location. Placing a receiver not directly within the beam propagation path will not allow for collecting a significant amount to photons to intercept the network traffic.

Summary

Optical wireless communication systems are among the most secure networking transmission technologies. Unlike microwave systems, it is extremely difficult to intercept the optical wireless light beam carrying network data because the information is not spread out in space but rather kept in a very narrow cone of light. To intercept this invisible light beam, the intruder must be able to obtain direct access to the light beam. Due to the very narrow beam diameter, interception of the beam can virtually only be accomplished at the customer premise where the system is installed. At that point, it would be certainly easier for an intruder to plug directly into the network by using the existing copper-based infrastructure (e.g. tapping into a CAT 5 networking cable). Scattered light cannot be used as a method of interception. Moreover, higher protocol layers can be used in conjunction with layer one optical wireless physical transport technology to encrypt sensitive network information and provide additional network security

About LightPointe

LightPointe was founded in 1998 and has become the global market leader for high capacity wireless outdoor bridges with over 5000 systems deployed in over 60 countries worldwide and in vertical markets such as Health Care, Education, Military & Government networks, large and small campus enterprise networks, Wireline and Wireless Service Provider networks. Over the last 10 years the company has established a unique diversified product portfolio based on high capacity Free Space Optics (FSO) and Millimeter Wave (MMW) technology. With more than 10 patents granted in the FSO, RF/MMW and in the hybrid bridging solution space LightPointe has established a strong IP and patent portfolio position manifesting the company's technology leadership position.

LightPointe has a long list of global customers including but not limited to Wal-Mart, DHL, Sturm Foods, Siemens, Sprint, AOL, FedEx, BMW, Lockheed Martin, Dain Rauscher, Barclays, Nokia, Deutsche Bank, IBM, Corning, Cisco, Huawei just to mentioned a few. For more information please visit the Lightpointe website at www.lightpointe.com