FSI TP 02

OPTICAL FIBER SENSORS FOR PERIMETER AND IT PROTECTION

Duwayne Anderson
Engineering Manager
Fiber SenSys
2925 NW Aloclek Drive
Hillsboro, Oregon 97124
Tel: (503) 692-4430
Fax: (503) 692-4410
email: Duwayne.Anderson@FiberSenSys.com

ABSTRACT
Fiber optics revolutionized the telecommunications industry by bringing un-surpassed improvements in bandwidth and signal clarity. Some of the same characteristics that make fiber the undisputed preference in telecom also give fiber a clear advantage in long-range distributed sensing. Long-range distributed sensing applications abound, and one of the most important applications is perimeter security. Fiber-optic perimeter security sensors are able to locate the presence, and often location, of intruders as they attempt to penetrate perimeters up to tens of km long. Applications for such sensors include borders, airport perimeters, pipelines, mass transit, and chemical plants.

This technical note summarizes the science of sensing while describing the various ways for categorizing sensors based on their function and underlying physics. It then discusses perimeter security sensors in more specific detail, highlighting the specific advantages offered by fiber-optic sensors.

INTRODUCTION
Sensors are devices designed to convert energy (often very small amounts of energy) into useful information. Many times sensor designs simply detect presence, as in the case of a coyote looking for rabbits in tall grass, or a jet fighter pilot scanning his radar, looking for a MiG 31. Other times the sensor reveals detailed information, as when an expectant mother and father look at the sonogram of their unborn child, counting toes and trying to decide on blue or pink jammies.

Most sensors consist of multiple parts. All sensors have a sensing element that's actually an energy transducer, designed to convert the energy of interest into some useable form, as when an acoustic transducer converts sound waves into electric potential. There's also a decision network (Anderson [1]) for evaluating the signal from the transducer and making decisions like "there's a MiG bearing 213 degrees at 27,000 feet and mach 1.4."

Broadly speaking we can place sensors into four categories (Fig. 1):

1. Passive
2. Active
3. Point
4. Distributed

	Point		Distributed	
	Nature	Engineered	Nature	Engineered
Passive	Eyes, ears	microphone	Spider web	Fiber optic sensors
Active	Echo location (bats, dolphins)	Radar	Lateral line (fish)	Phase radar array

Figure 1. Four ways to classify sensors

Passive devices sense ambient energy reflected by the environment. Eyes are an example of passive sensors; ambient light from the environment bounces off objects, reflecting into the eye, and focusing on the retina, which sends signals to the brain for analysis and decision-making (Fig. 2).

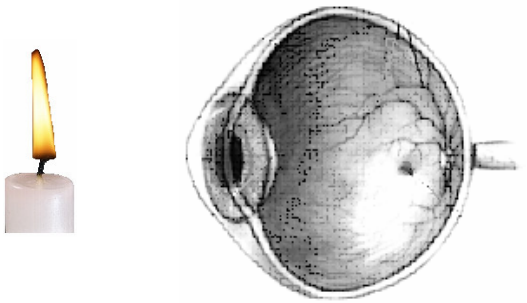

Figure 2. The eye is a passive point sensor that relies upon light emitted or reflected by an object in order to see it.

Sharks are equipped with one of the most impressive group of sensors known to science. They have a row of fluid-filled sensory canals on either side of their bodies that respond to pressure changes caused by movement in the water. This structure acts as a passive distributed sensor that lets the shark virtually feel the presence and location of moving animals in the water. Sharks can also sense electrical potential in the water. In their snouts, most sharks have small jelly-filled pits, called the ampullae of Lorenzini. Each pit contains a passive sensor able to detect electric fields as small as a hundred-millionth of a volt per centimeter. This allows the shark to detect contracting muscles (such as a heart beat) in animals, even when they are hiding under sand and gravel on the sea bottom (Bright, [2])

Active sensors emit energy and then measure the energy reflected, scattered, or otherwise modified by objects in the environment. Active sensors have at least three parts:

1. Emitter
2. Sensing element
3. Decision network

The emitter transmits energy into the environment. Some of this energy reflects off (or is absorbed and re-emitted by) surrounding matter. This energy returns to the sensing element, which converts the reflected energy into a signal for processing by the decision network. Bats, for example, emit high-pitched chirping sounds. Bats produce these pulses in their larynx (the emitter) by forcing air past a thin specialized vocal membrane. Some bats employ their tongue as the emitter, using it to make high-pitched clicks, while others emit pulses through a complex nose structure. Bats use their large ears (the sensing element) to collect the reflected acoustic energy, which produces signals for processing by the brain (the decision network). Their sonar is so precise that some species can find and catch small insects in flight.

Other animals have also evolved active sonar. Dolphins, for example, use both optical sensors (their eyes) and acoustic sonar to locate fish (Fig. 3).

Scientists have emulated many of these sensors. Eastman Kodak, for example, produced a camera that used acoustic sonar to set the autofocus in its camera (Marcus [3], Dann [4]), and radar (the equivalent of sonar, except that radar emits and detects radio waves instead of acoustic waves) was instrumental in securing an allied victory in World War II.

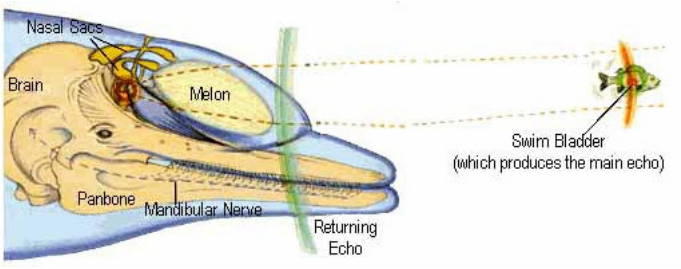

Figure 3. Dolphins use sonar. The dolphin produces clicks with its nasal sack, and focuses the acoustic energy with the melon. This is an example of an active point sensor.

Point sensors aren't really "points," at least not in a mathematical sense. In fact, some of them can be quite large. The distinguishing thing about a point sensor is that it's of limited dimension and often uses some device to focus energy on a detector. Eyes, ears, and noses are examples of point sensors. So are the nerve endings in your fingertips. The sonar in a submarine is a point sensor, as are the large parabolic dishes used to collect radar echoes.

Distributed sensors have extended dimensions and don't focus energy. A spider's web is a good example of a passive distributed sensor (Fig. 4). An insect caught anywhere on the web causes it to vibrate through its death struggle. The spider detects these vibrations using tiny hairs that grow along its legs. Some spiders can even analyze these vibrations and tell the location of the trapped insect.

Figure 4. A spider tends its web. The spider's web is an example of a distributed sensor. An insect trapped anywhere on the web causes vibrations felt by the spider. [credit Wikipedia encyclopedia]

The hair covering a tarantula (called setae) are hollow, with tiny sensory nerves in the base. These hairs are sensitive to vibration. The tarantula uses the ground (as opposed to a web) to guide vibrations to the hairs on its body. In this example, the ground acts as a distributed sensor and the hairs as the transducer. These vibrations alert the tarantula to the presence of prey as well as danger. The tarantula also has specialized hairs around its mouth that sense different chemicals.

A true distributed sensor is uniformly sensitive along its entire length. There are also quasi-distributed sensors that string together and multiplex many discrete sensors. For example, you can feel points of touch sensation along your arm because you have thousands of nerve cells (point sensors) distributed along your arm and multiplexed through your spinal column to your brain.

Many sensors act as classical wave detectors. Eyes, for example, detect electromagnetic energy. With the exception of rare cases where eyes detect single photons, we can treat this detection process accurately by modeling electromagnetic radiation as a wave phenomenon. Ears detect sound waves. The hairs on a tarantula's leg detect seismic waves in the ground. Active sonar transmits pressure waves and measures the reflected energy. Radar transmits waves of electromagnetic energy, and looks for the echo.

Any sensor can be defeated; they all have weaknesses and vulnerabilities. Let's look at a few of the vulnerabilities facing sensors in the four major categories.

Passive sensors must rely upon ambient energy, or energy emitted by the target, so being non-reflective is an obvious way to defeat a passive sensor. For example, criminals often try to avoid detection by working at night, when it's harder to see. Society tries to counter their tactic by installing lamps that illuminate streets and alleys, and by issuing night-vision devices to police, to augment the performance of their eyes in the dark.

There are two different types of night-vision devices. One type amplifies the ambient light, magnifying it millions of times. These devices rely on enough ambient light from the moon, stars, or other sources to make vision possible. The other type of night-vision device relies on the fact that all objects emit electromagnetic radiation. At room temperature these emissions happen at wavelengths of a few microns. People can be distinguished from their environment with such devices because their body temperature is typically warmer than the surrounding environment. One way to avoid detection by such infrared detectors is to hide behind a room-temperature reflector and/or attack in warm weather when the difference in emission wavelength between the environment and body is small.

Active sensors overcome problems with ambient illumination by supplying their own source of "light." Active sonar sends out pulses of acoustic energy, and measures the time (and sometimes the direction as well as phase) of the echo. Radar sends out pulses of electromagnetic energy while measuring the time, direction, and phase of the reflection.

While active sensors don't rely upon background (environmental) illumination, they make it easy for potential intruders to see the sensor, and potentially evade or destroy it. A burglar hiding in the alley is likely to see the advancing police officer's flashlight before the officer sees the burglar. This is the concept behind radar detectors. Police radar measures the velocity of a speeding car by bouncing microwaves off the vehicle and heterodyning the reflection with the local oscillator. However, the strength of the reflection is much less than the strength of the emitted microwave beam. This makes it possible for speeders to detect the emitted beam before the officer's radar gun can detect the reflection, giving the speeder time to slow to the legal limit before detection.

There's another inherent problem with active sensors. Since the intruder can often detect the sensor before the sensor can detect the intruder, the intruder may have the opportunity to preemptively disrupt or destroy the sensor. In war, one side might target enemy aircraft with radar for guiding surface-to-air missiles. At the same time, however, the targeting radar provides an ideal beacon for the aircraft to use in guiding its air-to-ground missiles to destroy the ground-based radar.

Another technique for avoiding active point sensors is to coat the intruder with a material that absorbs the emitter's energy (Carpenter [5]). Alternatively, insurgents may try to shape the intruder to deflect the emitter's energy so that none (or very little of it) is reflected back to the sensor. Radar-evading (stealthy) aircraft use special coatings to absorb radar waves, and engineers shape the aircraft so that it reflects non-absorbed radar energy off to the side, and not back toward the radar sensor (Fig. 5)

Figure 5. Stealthy aircraft designed to avoid detection by active radar. The aircraft surface has a radar-absorbing material, and it's shape is designed to scatter any remaining radar radiation so that it is not returned to the emitter.

Active point sensors can also be jammed. Flash bombs can momentarily blind a person, while the bomb's concussion saturates their hearing. Security personal can take advantage of this momentary jamming of the intruder's eyes and ears to disable him. Jamming is a common counter measure with radar, too; broadcasting a very strong radar beam designed to saturate or destroy sensitive radar receivers looking for radar reflections and/or backscatter. Of course, for every counter measure there is a counter-counter measure. For example, spread-spectrum radar systems avoid jamming by spreading the radar signal over a wide spectrum.

Point sensors (whether active or inactive) have a common weakness; except for cases of energy reflected or diffracted around obstacles, these sensors can't sense outside their "line of sight." The phrase "line of sight" means that the energy they sense (usually a wave phenomenon) travels in an approximately linear path. This is a simplification, since waves bend (diffract) around objects when those objects are of similar size to the wavelength of the energy. Diffraction, though, is often limited, and weak, allowing intruders to hide in the shadows cast by other objects.

A burglar might avoid the police officer's flashlight by crouching down behind a dumpster; a tank commander might hide behind a rocky outcrop; an intruder breaking through a perimeter may hide behind a bush. Some types of radar limit this disability by using very long wavelengths that travel through the atmosphere in a manner analogous to the way light travels through optical fiber in guided modes. Such radar systems, called "over the horizon," can see well beyond normal line of sight, but most point sensors lack this ability.

Generally, distributed sensors have comparable weaknesses as point sensors, except they can often see beyond the line of sight. This is because a distributed sensor spreads over an extended area, and the sensor itself conducts the disturbance signal back to the detector, regardless of corners, obstructions, or other interference. The table below summarizes these weaknesses and strengths:

Sensor type	Weaknesses
Passive Point	Relies upon ambient energy and/or energy emitted by intruder. Line of sight. Jamming
Active Point	Line of sight, emission gives away location. Jamming
Passive Distributed	Relies upon ambient energy and/or energy emitted by intruder. Jamming
Active Distributed	Emission gives away location. Jamming

DISCUSSION

The best sensor depends on the application. For perimeter security applications the objectives are:

1. Locate the intruder in any environment
   - Maintain optimum capability in all weather, at all times, day and night, spring and fall, summer and winter
   - Ideally, the sensor doesn't let the intruder know they've been identified
   - The sensor cannot be destroyed without the intruder being identified
   - Work 24 hours a day, never sleeping, with minimum maintenance
2. Provide security over long distance
3. Have a very low rate for false alarms (false positives)
4. Have a very high rate for true positives (correct identification)

Looking over this list it seems apparent that the best sensor for perimeter defense is a passive, distributed sensor, assuming one can always count on the intruder generating enough energy for detection.

For thousands of years perimeter security has relied upon the point sensors in the human head, in the form of posted sentries. The posted sentry is a multi-sensory solution, using the guard's eyes, ears, and nose to detect intruders. Though these sensors are extraordinarily sensitive, with high noise rejection, they have all the problems of other point sensors; namely, they interrogate only the local region around the sentry's head. Sentries are also subject to fatigue (their decision network is compromised), and, in spite of the threat, many a soldier has been disciplined for sleeping on duty.

To overcome these disadvantages the perimeter requires sentries to be located at more-or-less regular intervals, with overlapping line-of-sight, with fresh replacements on a regular basis.

Although human senses are remarkable, they are not as effective as those of other animals. If sharks were trainable, and walked on land, they'd be far more formidable than your average infantryman. Since people get tired and fatigued, they need augmentation. Augmentation is always a good idea as it improves overall security through redundancy and multiple layers of (hopefully) different but complementary sensors. To extend the sentry's effectiveness, guards often patrol in the company of dogs; though their eyesight isn't as good as mans, a dog's hearing and olfactory senses are considerably better.

Of course, the dog's sensors are point sensors (like men) and dogs get tired and sleep, too. So, although they've been used for millennia, what's needed is a replacement for the sentry: a long, linear sensor with high sensitivity, capable of detecting stealthy intruders, that never gets tired and never sleeps.

Sometimes security systems remove the sentry from the perimeter, and use cameras so the sentry can study the perimeter remotely. These cameras might even be equipped with infrared viewing capability, to maintain effectiveness at night. Even with the technological wrapping, though, this is still a sentry defense system, and, with a comfortable chair from which to view the camera images, it might be even more susceptible to the problem of concentration and fatigue by the guard.

Table 1 summarizes key examples of some of the many inventive technologies used in perimeter security. Let's look at each of these and see where their strengths and weaknesses lie.

Reflectometry

Reflectometry is a method of detecting objects and determining their position, velocity, or other characteristics by analyzing energy reflected from their surfaces. All devices that use reflectometry are active sensors.

The different types of reflectometry are characterized by the types of energy they use (Table 2). Sonar, for example, uses sound waves in air, water, or (less frequently) in the ground.

Radar uses electromagnetic radiation at radio and microwave frequencies, while laser reflectometry uses energy at optical wavelengths.

Classification	Type	Examples
Reflectometry	Active point	Radar
	Active point	Acoustic sonar
	Active point	Water sonar
	Active point	IR illumination
Field disruption	Active point	TX-RX, IR and Microwave
	Active distributed	Ported coax
	Active distributed	Capacitive wires
	Active distributed	AC wires
Emission sensing	Passive point	Camera, still
	Passive point	Camera, motion
	Passive distributed	Strain-sensitive cable
	Passive point	Geophone, Microphone
	Passive point	Taut wire
	Passive point	Optical fiber pinch
	Passive distributed	Liquid-filled pressure sensor
	Passive distributed	Optical interferometer
	Passive distributed	Metallic TDR

Table 1. Summary of types of sensors used in perimeter security

Reflectometers, like other active point locators, are limited to line of sight and dead zones caused by shadows and/or saturation caused by bright reflectors. For example, metal objects like trash containers might cause dead zone at microwave and radio frequencies. Any object that blocks optical radiation can interfere with laser reflectometers, and any object that blocks acoustic sound waves can cause problems for an acoustic reflectometer. Extreme weather conditions like rain or snowstorms can limit their detection ability and/or cause false alarms.

Name	Frequency range
Water sonar	Low freq. < 1 kHz Med. freq. 1-10 kHz High freq. 10-500 kHz
Acoustic sonar	Generally < 500 kHz
Seismic sonar	Generally < 10 kHz
Radar	50 MHz to 100+ GHz
Laser radar	> 30,000 GHz

Table 2. Types of energy used by different reflectometers

Reflectometers can look at the reflected energy in several ways. The simplest reflectometer simply illuminates the target for an imaging device. A flashlight, for example, illuminates objects so you can analyze them with your eyes. A similar, but more sophisticated, approach is to use an infrared source to illuminate objects while looking at them with a camera that's sensitive to infrared wavelengths.

Reflectometers that are more sophisticated emit pulses of energy and measure the time required for the pulse to reflect off objects and bounce back to the emitter. They measure the distance to the objects by measuring the time between emitting the pulse and detecting the echo. Some types of reflectometry measure the Doppler shift between the frequency of the emitted and reflected pulses, allowing these types of reflectometers to measure the velocity of the objects, as well as their direction. Other systems measure all three parameters: distance, velocity, and direction, giving a nearly complete description of the target's dynamics.

For perimeter applications, designers tune reflectometers to look for motions that are statistically associated with human movement. Microwave sensors, for example, look for Doppler shifts between 20 and 120 Hz.

As you would expect, reflectometers are subject to interference from devices that transmit energy at the frequency used by the reflectometer. For example, microwave sensors are susceptible to things that emit radio or microwave frequencies. This can include radio transmitters, electric motors, and generators. Sometimes microwave sensors might even misconstrue the ionization cycle from fluorescent lights, causing false alarms.

Sometimes reflectometers can pick up false/nuisance alarms by "seeing" objects they're not "supposed" to see. For example, microwave energy can transmit though the walls of structures, making it possible for movement within a protected building to cause false alarms in a perimeter security system.

Because they measure location and often velocity as well, reflectometers can provide important information about potential intruders. Reflectometers can measure and map the locations of objects in the surrounding area, identifying moving objects within the covered area before they enter a protected area. The system can then classify such objects as intruders when they move into a restricted area.

The transmitters used by all reflectometers have limited apertures and so their beams of energy exhibit diffraction effects like side lobes. Much of the work that goes into designing a good reflectometer involves controlling the side lobe pattern. Sometimes this even involves multiple emitters operating in phase (though perimeter security systems seldom use this degree of sophistication because of the cost/complexity involved). It's impossible to eliminate diffraction effects and, depending on their size and distribution, they can produce false/nuisance alarms due to objects outside the intended filed of view.

Field disruption

Closely related to reflectometry is a type of sensing based on field disruption. Reflectometry emits energy and then looks for a reflection, where the emitter and receiver are either co-located or closely located. Field disruption involves a transmitter that emits energy, and a remotely located receiver that receives the

transmitted energy. The presence of an intruder between the emitter and receiver changes the energy (usually attenuating it) detected by the receiver, thus indicating the presence of an intruder. All devices that use field disruption are active sensors.

Perhaps the simplest example of a field-disruption sensor is the one used with automatic garage door openers, designed to prevent crushing deaths by raising the door if an object (like a child) enters the area beneath the door. The object (in this case a small child) blocks the transmitted beam, preventing it from reaching the receiver on the other side of the garage door. When this happens the decision network raises the door.

As with reflectometry, field disruption can use any energy source. The most common types of field disruption sensors use infrared beams (as in the case of the garage door opener) and microwaves.

Active infrared sensors emit infrared radiation and monitor changes in the received power. This is analogous to creating a fence made of light, with infrared beams transmitted through space to a receiver. An intruder that blocks the infrared beam sets off an alarm. These sensors are susceptible to the accumulation of dirt and dust, as well as outside sources of radiation (such as infrared lights, etc.) that might cause false alarms. Blowing debris might also trigger false alarms, as well as small animals such as crows and pigeons. Snow, wind, and rain may also interfere with these sensors, and affect their sensitivity and/or false/nuisance alarm rate.

Another type of active field-disruption sensor uses ported coaxial cable (Fig. 6). Ported coaxial cable is a type of cable that's deliberately designed to be leaky (it has small holes in it). The stuff that "leaks" out of this cable is an electro-magnetic field that surrounds the coax. The installed system has a pair of ported coaxial cables, typically about five feet apart. Specially designed electronics emit pulses of RF energy through one of the cables. This energy spreads out and couples into the other cable. When an intruder enters this field they change the field configuration, producing a measurable change in signal detected by electronics attached to the cables.

Ported coax sensors can be very sensitive but severe weather conditions, including severe electrical storms and wind-blown waves on the surface of standing water, can sometimes cause false alarms. Because the sensing element is metallic, lightning ground strikes might destroy the sensor. Metallic objects can distort the electric field, necessitating their removal before installing the cables and adding to overall installation cost. Electromagnetic emissions from nearby equipment can also interfere with ported coax systems, as can nearby metallic surfaces as well as shrubbery. In addition, because the coaxial cable is "leaky" the attenuation is quite high, and this limits the length (range) of the distributed sensor to relatively modest perimeters.

"Capacitive sensing" is another technique that uses field disruption. These sensors detect changes in an electrostatic field created by an array of wires. Typically, the sensor uses three wires attached to the top of a fence using dielectric brackets. An electronics unit attached to the wires continually monitors the capacitance between the wires and the fence (ground). When an intruder approaches or touches the wire array, they alter the electrostatic field. The sensor detects this alteration and uses the change in capacitance to determine the presence of an intruder.

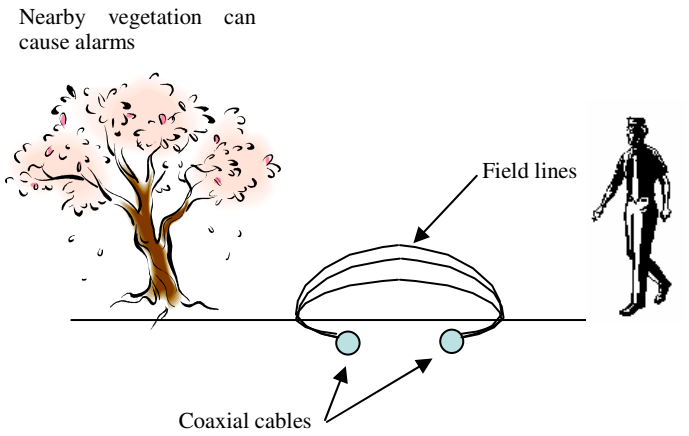

Figure 6. A pair of ported coaxial cables buried beneath the ground sets up an electromagnetic filed above the ground. Objects entering this field disrupt it and trigger an alarm.

Rather than measure the capacitance between the wires and the ground, the designer can apply an alternating current through the wires, thus generating an electric field that surrounds them. If an intruder enters this field, by either approaching the fence or touching it, they will disrupt the field, triggering an alarm from the electronics unit attached to the wires.

Capacitive and electro-magnetic field sensors detect presence and vibration. As such, they are susceptible to nuisance alarms from weather conditions and/or small animals or other non-threatening objects that vibrate the fence.

Emission sensing

All devices that use either reflectometry or field disruption are active sensors; they generate and emit energy and infer the presence of an intruder based on the intruder's interaction with the energy they transmit. Active sensors can detect the presence of an intruder that emits no energy at all.

Emission sensors, in contrast, are all passive devices. These sensors measure energy that the intruder generates or/and they rely upon the intruder's disruption of ambient energy. Your ears, for example, detect acoustic energy produced by nearby objects such as a door closing, someone walking on the sidewalk behind you, a car honking its horn, etc. Your eyes detect and classify objects based on the way they reflect ambient light. Passive sensors still use energy to operate. The distinction is that they don't broadcast energy that interacts with the objects in the environment.

Video camera systems are probably the most common example of emission sensing. These devices are like eyes. They collect

ambient light reflected off objects, use a lens to focus the light to an image, and then use computers (or human operators) to analyze the images and draw conclusions about the presence of intruders. A video system that uses only passive (ambient) lighting is a passive sensor, while a video system that uses active illumination (IR illumination, for example) is an active sensor.

Some emission sensors rely on the fact that all warm bodies emit radiation. The wavelength of this emitted radiation depends on the temperature of the body. The peak wavelength radiated by a human body, for example, is about 10 microns. Cooler objects, such as the furniture in a room, emit at longer wavelengths. Thus, a sensor tuned to measure radiation at the same wavelength as that emitted by the human body will be able to catch the intruder. In practice, these sensors may not measure the absolute (calibrated) temperature of objects. Instead, they look at temperature differences, spotting hot spots within their field of view.

Because the sensor looks at temperature differences, as the temperature of the background approaches that of the intruder it becomes harder and harder to detect intruders. Even on cool days, an intruder can mask his body temperature by hiding behind a thermally insulated shield (though a plume of hot air may still rise from behind the shield). False alarms can result from tuning the system too sensitively, so that it picks up the movements of small animals, heating vents, areas that receive extra solar heating, etc.

Intruders don't emit just infrared radiation; they also emit sound, in the form of vibrations. When they walk, intruders cause minute vibrations in the ground. When they try to climb fences they cause them to vibrate. Sensors designed and tuned to catch these vibrations can thus catch the intruder in much the same way that a Funnel Weaver spider senses the vibration of an insect crossing the web.

Vibration sensors either can be point sensors or distributed. A buried geophone is an example of a point emission sensor, designed to listen for vibrations that indicate an approaching intruder. The early Native Americans used this type of sensing when they listened to rail lines for the approach of a distant locomotive.

One type of vibration sensor, for detecting intruders walking on the ground, is the pressure line. This sensor consists of a long pliable tube filled with liquid (typically a water/antifreeze mix) connected to a pressure transducer. Sound waves in the soil couple to the fluid in the pliable tube. This modulates the pressure in the tube; sensed by the pressure transducer, which produces a modulated voltage interpreted by electronic circuits as the presence of an intruder.

Some types of emission sensors are quasi-distributed. These sensors consist of a backbone with various point sensors distributed along it. The point sensors distributed along the backbone detect the actual intrusions, and the backbone conveys this information to the decision network.

An example of this quasi-distributed sensor is the taut wire system. Taut wire sensors combine wire fencing with micro-switches that detect changes in the tension of the fence fabric. This system consists of micro switches placed about every 6 inches apart and connect to tensioned wire installed on top of the fence, or as part of the fence fabric.

The micro-switch consists of a cylindrical conductor with a moveable center rod suspended inside. In the normal, or open mode, the center rod doesn't touch the outer cylinder wall, but changing the tension (either increasing or decreasing it) which happens when someone tries to climb, spread, or cut the fence, causes the center rod to move and touch the outer cylinder wall, closing the switch and sounding an alarm.

A similar sensor consists of a fiber-optic backbone with point sensors spread long the length. These point sensors respond to vibration in the fence, and when triggered they snap shut, pinching the optical fiber and causing local bend loss. Loss through the fiber is continuously measured, and sudden increases sound an alarm.

Sensors measure loss in the fiber-optic version in two ways. The simplest way is to measure the total loss through the optical fiber by using an optical transmitter at one end of the fiber, and an optical power meter at the other end. Although relatively simple, this method doesn't allow measurement of the location of the intrusion.

The other way to detect intrusion is to use an optical time-domain reflectometer (OTDR). When designed with sufficient sensitivity such reflectometers can detect Rayleigh backscatter, and when the point detector snaps shut on the fiber it shows up as attenuation in the Rayleigh backscatter signature at the location of the intrusion (Anderson [6])

It may seem odd that we have an OTDR-based system categorized as a passive emission sensor when OTDR is, effectively, laser radar. The reason for this classification is that the sensed phenomenon is fence vibration, and the actual sensor is the mechanism that snaps shut on the fiber. The OTDR is a secondary sensor in this case. It's not used directly to sense the intrusion, but only after the fact, to find the location of where the primary sensor snapped shut on the fiber.

Strain-sensitive cables are distributed sensors with uniform sensitivity over the length of the protection zone. These sensors use specially designed cables that generate an electric potential when vibrated. When mounted on a fence, attempts to cut the fence, climb over it, or raise the fence fabric cause minute amounts of stress in the cable, producing electrical signals detected by the signal processor.

Strain-sensitive cables are very sensitive to electromagnetic interference from things like radio transmitters, power substations, etc.

Given the proper characteristics, certain conduits can support guided modes of energy at particular wavelengths. We call such conduits waveguides. Early waveguides consisted of metallic conduit that looked a bit like heating/cooling air ducts,

but with smaller dimensions; they guided microwave energy. Other waveguides use metallic coaxial cable. Metallic waveguides tend to have relatively high loss and high dispersion, which limits their ability to conduct narrow pulses over long distances. Fiber-optic cables have enormous advantages over other waveguides in terms of information bandwidth, dispersion, and loss. These all-dielectric waveguides, made of silica glass, are in worldwide use, guiding electro-magnetic energy at optical frequencies over distances exceeding 100 km and over one Tbit/sec.

Waveguides function as passive distributed sensors by placing them on perimeters (such as fences) or burying them under ground. Intruders attempting to cross the perimeter disturb the waveguide, altering slightly the waveguide's physical properties. Physical stress on metallic waveguides alters its dimensions, which changes the local impedance. When this happens, small amounts of energy traveling through the waveguide reflect back to the transmitter, forming the basis of an intruder detection system.

Time-domain reflectometers employee this principle when designed to catch intruders by looking at vibrations in a fence. To increase their sensitivity these devices use specialized cable designed for maximum impedance change when the cable is disturbed. These minute changes in impedance cause tiny reflections on the TDR trace, allowing identification and the location of the intruder.

Some perimeter intrusion sensors use optical waveguides. They have an important advantage over metallic waveguides because of their low loss and insensitivity to electromagnetic fields. While metallic waveguides are typically limited to about 1 km, optical waveguides can span tens of kilometers while maintaining optimum sensitivity along the entire length.

Often there's a requirement for the perimeter sensor to be stealthy, or undetectable by the intruder. The need for stealthy sensors reflects on the psychology of intruders. Intruders that think (or know) they've been detected might move quickly from the area, making it more difficult to intercept them. Intruders that don't know they've been detected might move slowly to prevent future detection from (yet) unknown sensors, making it easier to intercept and capture them.

If an intruder thinks (or knows) there is a sensor in the area, they will assume they've been detected, and act accordingly. Think back to the speeder. If the speeder senses police radar, they alter their behavior and slow down to avoid a ticket. They assume that, if the radar is on, they've been detected, even though the officer might be outside his car, writing someone else a ticket. On the other hand, if the speeder is using a radar detector, but the police are using laser reflectometers, there's a much better chance that someone's going to be pulled over for speeding. Clearly, there is considerable advantage in having a stealthy sensor that doesn't make its presence known to the intruder.

It's possible to detect any active sensor (reflectometers and those based on field disruption) by sensing its emissions, as in the case of radar detectors used to sense the presence of speed traps. When mounting the sensor above ground there's a possibility that it can be visually detected. Burying the detector offers the possibility that it will be undetected, but only if the sensor is non-metallic, because buried metallic sensors are easily detected using inexpensive metal sensors. For true stealth, the sensor should be a buried dielectric device, such as optical fiber.

The sensing mechanism in optical fiber uses interferometry in which coherent light travels through different optical paths and "mixes" at a sensor. One type of optical sensor uses a single optical fiber in which the two "paths" are different modes in the same fiber. The interferometric pattern from these different modes produces a characteristic pattern of light-and-dark splotches called speckle (Fig. 7). The laser speckle is stable as long as the fiber remains immobile, but flickers when vibrating the fiber. The system works by measuring the time dependence of this speckle pattern and applying digital signal processing to the fast Fourier transform (FFT) of the temporal data.

Since the sensing fiber is all dielectric, the sensor is inherently immune to electromagnetic effects that might otherwise damage it or interfere with the vibratory signal. And since optical fiber has very low loss (less than 0.2 dB/km at wavelengths of 1550 nm), the sensor can be deployed at remote locations that are many tens of kilometers away from the processing electronics.

Sensors based on optical interferometry detect vibration with very high sensitivity. Other optical sensors are designed to use optical fiber in a transmit/receive configuration. These sensors don't measure minute fluctuations, but rather the total transmission through the waveguide. As such, they are incapable of measuring vibration, and are only able to detect breaks in the optical cable and, sometimes, severe bends.

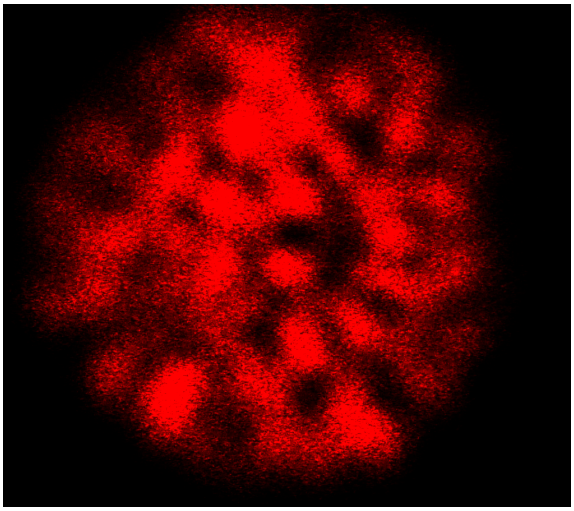

Figure 7. Example of laser speckle projected from the end of a multi-mode optical fiber, illuminated with coherent laser radiation.

To be effective, intruders must be unable to breach a perimeter without breaking the fiber. This, however, is a difficult thing to ensure. One technique is to weave a mesh out of the optical fiber and cover the fence with this fiber mesh on the

assumption that anyone trying to climb the fence will break the fibers in the mesh. However, semi-skilled intruders can dismantle the mesh (one technique is to cut/drill the mechanical connectors at the mesh nodes) on the fence, cut the fence, and walk through the perimeter undetected. Alternatively, the intruders may simply climb the fence with ladders. [These types of sensors cannot be used in buried applications except in cases designed to catch people tunneling through a protected area, where tunneling will break the optical fibers.]

The basic problem with mesh-type fiber-optic perimeter sensors is their poor sensitivity. While it's true that fiber-optic mesh sensors have a low nuisance alarm rate, this comes at the expense of sensitivity and the ability to detect stealthy intruders. The sensor designers try to overcome this poor sensitivity by making it physically impossible to climb a fence without breaking the mesh, but in practice this is a very difficult task, virtually always fails, and makes an inadequate security system for high-priority perimeters.

Optimum perimeter sensing

With this background material, we're finally ready to answer the question, "what is the best sensor solution for protecting long perimeters?" Let's begin by listing our operational requirements:

1. Catches intruders with high probability
2. Low false/nuisance alarm rate
3. Able to protect perimeters that are many km long
4. Linear (system sensitivity not distance dependent)
5. Able to withstand harsh/dangerous environments

Perimeter security systems tend to be long. Meanwhile, the units for the probability density curve for noise is $day^{-1} \bullet km^{-1}$, reflecting the fact that the likelihood of a particular level of environmental noise increases with both time and the length of the perimeter. This means that long perimeter security systems tend to be particularly susceptible to environmental noise. This, combined with the twin requirements of high probability of detection and low false/nuisance alarm rates, mandates the use of sensors that have tunable thresholds. These sensors use multiple criteria in conjunction with a tunable decision network to distinguish between environmental noise and intrusions. Without tunable thresholds, the sensor is unlikely to have the high sensitivity that's required to catch intruders, while keeping false/nuisance alarms sufficiently low.

The requirement for tuneability essentially rules out the use of quasi-distributed sensors like taut wire systems and mechanical sensors that work by tripping and pinching an optical fiber. That's because differentially tuning each of the hundreds or thousands of mechanical switches distributed along the perimeter becomes a practical impossibility. This is especially true where the tuning requirements demand a level of sophistication beyond simple thresholds.

There is another problem with quasi-distributed sensors. The problem is that the distance from the disturbance to the point sensor is a random variable that depends on where the intruder approaches the perimeter, and where the point sensors are located. If the point sensors are, for example, 10 feet apart, then the distance from the nearest point sensor to a randomly chosen point disturbance will be a random variable between 0 and 5 feet.

This presents a problem because the trigger level depends on the local strength of the disturbance at the point sensor, and the local strength depends on the distance between the point sensor and the disturbance. This means that the sensor's sensitivity cannot be uniform for any randomly chosen event along the perimeter because disturbances close to a point sensor will set off the sensor more easily than disturbances further away. This compounds the already onerous problem of how to tune the many hundreds of point sensors along the backbone.

In summary, the problems with quasi-distributed sensors are:

1. Non-uniform sensitivity
2. Difficult or impossible to achieve proper tuning for reliably detecting intruders while avoiding excessive nuisance alarms

Perimeter sensors are, by their nature, spread out over large distances. Often mounted to fences, other times buried under the ground, in all cases they extend over hundreds, if not thousands of meters. This presents another problem because lightning is more likely to strike somewhere along a very long perimeter than a shorter one. The threat of lightning strikes constitutes justifiable concern about metallic conduit sensors. Such sensors are not only susceptible to being destroyed by a lightning strike, they can also conduct high-voltage, high-current surges into the area containing the analysis software/electronics, destroying the sensing electronics and possibly other un-related electronic modules as well. The cost of such mishaps is manifest in the replacement cost of the lost electronics modules, as well as the cost of re-deploying the sensor on the perimeter. While lightning surge protectors provide a degree of protection they also add cost and are not 100% effective.

Other factors also make metallic conduit problematic. Oscillating electric fields near conductors create induced currents by electro-magnetic induction. High oscillating fields are common, especially along the lengths of extended perimeters. They can arise in proximity to high-voltage overhead lines, motors, transformers, etc. Often it is impractical or impossible to shield the sensor from these outside fields, yet failure to do so can result in the sensor producing excessive false/nuisance alarms.

Another reason to avoid the use of metallic conduits for perimeter sensors is the possibility of corrosion and failure over time. This is especially true in designs that have different metals touching each other, particularly in the presence of water.

A final reason for rejecting metallic conduits is the limited length of perimeter they can cover (due to resistive losses, dispersion, etc). While this is a more serious problem for some metallic conduits than for others, they all have much higher loss than glass (dielectric) waveguides. Some metallic conduits, like ported coax, have such high attenuation that they cannot be used effectively beyond a few hundred meters.

In summary, long distributed sensors that use metallic conduit are unsatisfactory because of:

1. Susceptibility to lightning strikes and subsequent damage to the sensor and associated/nearby electronics
2. Susceptibility to noise from induced currents resulting from nearby oscillating electric fields
3. High attenuation loss, resulting in limited range

The need to avoid using quasi-distributed sensors, and/or metallic conduit, essentially rules out using taut wire, metallic TDR, capacitive wires, AC wires, ported coax, strain-sensitive cables, and optical fiber pinch sensors.

In addition to metallic-conduit sensors, we should also eliminate optical mesh perimeter sensors because of their poor sensitivity and the comparative ease with which such sensors are defeated. Fiber optic meshes have an additional problem; it's comparatively easy to tell if you've set off an alarm. That's because the fiber responds only to tight bending (enough to cause a measurable loss in signal) and/or breaking. For example, reliably detecting a bend in single mode fiber (carrying light at 1310 nm) might require bending it to a radius tighter than about 1.5 cm, over 180 degrees. Yet the cable in fiber-optic mesh sensors can easily be handled without exceeding this bend radius, making it simple for intruders to work on the sensor while using specialized tools to separate the mesh at the nodes, and then simply walking through the sensing net, knowing that (unless they break the cable) they have not tripped an alarm.

Perimeters are seldom straight, with an un-obstructed view of the entire length. Often there are adjoining structures near the perimeter, on both the outside and inside, that create shadow regions for point sensors. Sometimes these structures are outside the perimeter, but they enclose people or machinery that might set off sensors, such as microwave, that can sense movement through walls.

Point sensors can be manual or automated. An example of a manual point sensor is a video system manned by security personnel. An automated point sensor might consist of a microwave sensor with associated electronics/software that sounds an alarm when the return signal fluctuates too much. Or, it could be a video system designed to find, track, and identify moving objects in the field of view.

Some perimeters allow public access up to the protected zone. These perimeters may be unsuited for automated point sensors if they (depending on the volume of public access) sound too many nuisance alarms from nearby traffic.

Other perimeters consist of a double barrier. This may consist of an outside fence and an inside fence. Such double perimeter systems may use automated point sensors to cover the clear area between the inside and outside perimeter, but they must be carefully mounted and installed to avoid looking beyond the outside perimeter, where they might inadvertently trigger an alarm.

Manual point sensors are essentially extensions of the ancient sentry concept, except that the sentry is remotely located. Like the sentries they emulate, these manual systems benefit from the exquisite performance of human senses and image processing, but they also suffer from failure if the sentry is inattentive, drowsy, or distracted. Very long perimeters are particularly unsuited for protection using manual point sensors because of the number of such sensors that need monitoring.

While point sensors have a legitimate use in perimeter security, they are most useful in a tiered approach, in which the point sensor is one layer of a multi-layer security system. Ideally, the primary layer of defense will be a distributed sensor, with the point sensor used to verify and/or classify alarms that are setoff by the distributed sensor.

Examples	Problems
Radar	Point
Acoustic sonar	Point
Water sonar	Point
IR illumination	Point
TX-RX, IR and Microwave	Point
Ported coax	Metallic
Capacitive wires	Metallic
AC wires	Metallic
Camera, still	Point
Camera, motion	Point
Strain-sensitive cable	Metallic
Geophone, Microphone	Point
Taut wire	Metallic, not tunable
Optical fiber pinch	Point, not tunable
Liquid-filled pressure sensor	Limited range
Optical interferometer (point-to-point or TDR)	
Metallic TDR	Metallic

Table 3. Sensor technology applicability to perimeter security. Green cells highlight sensor technology that uses point locators. Red cells highlight sensor technology that uses distributed metallic sensors. Yellow cells highlight technologies not amenable to using a tunable decision network. Each of these technologies is disadvantaged with respect to the design requirements for high-security perimeter sensors.

Table 3 shows examples from the categories and types listed in table 1, highlighted to illustrate their various weaknesses when considered for high-security perimeter applications. Point sensors are highlighted for the reasons just discussed, while all metallic sensors are highlighted because of the susceptibility to lightning strikes, high attenuation (limited range) and potential problems with corrosion. In addition, taut wire is inadvisable because of tuneability problems, as are systems that use mechanical sensors to pinch an optical fiber. Not listed are optical mesh sensors, which are inadvisable because of low sensitivity.

The only class of sensor not highlighted in table 3 is the optical interferometer (whether point-to-point or TDR). This sensor measures vibrations at the perimeter, and can be made extraordinarily sensitive. It has none of the disadvantages of sensors based on metallic conduit. It has extremely low loss, making it possible to construct uniform sensors many km long. It is all dielectric, so it will not conduct lightning strikes into the equipment rack and/or sensing electronics, and the fiber is impervious to electro-magnetic interference. Since it's a true, flexible distributed sensor, it can go wherever the perimeter goes. It can bend around corners and follow the terrain over hills and through valleys, well beyond the line of sight for point sensors. High-end systems mount the fiber inside a flexible conduit, making it impossible for the intruder to see if the fiber is vibrating (thus preventing them from knowing if they've set off the sensor, or not) and ensuring reliable operation in virtually any environment. Moreover, when buried, the sensor is undetectable without digging.

The only issue with fiber-optic interferometer sensors is one that's common to any sensor, namely tuning the sensor to catch intruders, but not to catch false/nuisance alarms. This problem isn't germane to the sensing material (the fiber-optic cable), though; it's a design problem to be solved in the decision network (Anderson [1]). Outside the decision network, the primary objective when evaluating the sensing element is to ensure that it's linear and highly sensitive. Regarding these criteria, no distributed sensors exceed the performance of optical fiber.

So far, we've considered only problems related to performance and reliability, without giving much thought to questions of cost, ease of installation, and overall reliability. In any real-world application, though, we must consider these issues carefully as they may be as important as the others may.

Some systems are complex, difficult to manufacture, made of rare/expensive materials, and time consuming and/or difficult to install. Having these attributes results in systems that are inherently costly to buy, install, and/or maintain. Technologies that are potentially susceptible to high costs include radar and microwave reflectometers, ported coax, strain-sensitive wires, fiber-optic mesh, and camera systems.

Fiber optic sensors are conspicuously absent from this list of high-cost products for several reasons. First, the raw material in optical fiber is primarily oxygen and silicon, the two most abundant materials in earth's crust. True, these materials must be extraordinarily pure when used in fiber optic sensor, but no more pure than what's used in the telecommunications industry. Telecom uses millions of km of optical fiber annually, so that ready supplies of cost-effective optical fiber are available for perimeters sensors.

Optical interferometric sensors use microscopic waveguides made of silica glass, similar to, or identical to, the fiber-optic waveguides used throughout the telecommunications industry. Since factories use the same equipment to make these waveguides as telecom fiber, they benefit from economies of scale; fiber-optic sensors tend to be among the least expensive perimeter sensors on the market.

These silica waveguides have very low loss (one of the primary reasons they are used in telecommunications) so the sensor can span very long perimeters. Moreover, because they use optical interferometry, they have better sensitivity than almost any other type of sensor. When used in conjunction with tunable threshold algorithms, these sensors are also less susceptible to false/nuisance alarms than systems that use technologies like taut wire.

Optical fiber sensors are also relatively easy to install. Compared with other technologies, installers who place distributed optical fibers around a perimeter need not have extensive training. And, unlike some technologies, such as microwave and IR, fiber sensors require no pointing alignment/re-alignment. Compared with other sensors, fiber optic perimeter sensors require very little maintenance. Microwave and IR sensors, for example, must be aligned at installation and they may require periodic maintenance to check the alignment over the course of their lifetime. These sensors are also susceptible to degradation/damage over time. Fiber optic perimeter sensors, on the other hand, require no alignment at installation or afterwards, and are practically immune to damage from environmental effects. Of all the sensors used in perimeter protection, fiber-optic sensors come closest to providing a maintenance-free solution.

The electrical systems in fiber-optic sensors tend to be sophisticated, as well as the software used in the decision network, but no more sophisticated than what's required of any other sensor system, given equal levels of performance. Overall, when considering the purchase price, installation costs, and maintenance requirements, fiber-optic perimeter sensors are the lowest-priced solution for medium- to long-length, high-security perimeters.

CONCLUSION

Distributed fiber-optic sensors are an outstanding technology for perimeter security, but as we've seen, every technology has shortfalls and determined intruders can defeat even the best of them. This is why highly secure systems always use layered sensor systems based on varied sensing phenomenology. The original perimeter sensor, the sentry, illustrates this important principle.

Imagine you're a sentry, posted on a critical perimeter with the task of catching intruders. As you scan from your post, you see something suspicious and out of the ordinary. You may do a double take, training your eye on the spot, but you'd probably also strain your ears to see if they confirmed the oddity. You'd respond in a similar manner if you heard something that startled you – turning your head to get visual confirmation of whatever made "that noise." These are two examples of ways evolution has designed organisms with layered, complimentary sensing mechanisms; eyes for visual sensing, ears for acoustic sensing, smell for chemical sensing. In addition to reducing the rate of false alarms, redundant systems also improve the probability that at least one of the sensors will catch any given intruder. It's why organizations like NASA use multiple sensors for every critical measurement on space flights.

The situation with perimeter security may not always be as critical as with the space shuttle, but it might be. A terrorist attack on an oil refinery, for example, could be nearly as expensive and have an economic ripple effect that spreads across the country. Given the importance of perimeter security, it should come as no surprise that the best solutions involve a tiered perimeter system. This might consist of microwave or IR "eyes" coupled with fiber-optic vibration sensor "ears" that surround the perimeter, listening for intruders. This may be further augmented by a visual system that automatically trains cameras on the site where the sensors identify an intruder so that the most capable sensors, and the most remarkable decision network of all – the human mind – may classify the threat, decide on necessary action, and initiate the response.

REFERENCES

[1] Anderson, Fiber SenSys Technical Note 01

[2] Bright, M., Jaws: The Natural History of Sharks, "The Natural History Museum"

[3] Marcus; Michael A., "Acoustic transducers for acoustic position sensing apparatus," United States Patent 4,494,841

[4] Dann; Lynn D., "Video camera microphone with zoom variable acoustic focus," United States Patent 4,862,278

[5] Carpenter; Harry W., "Radar absorbing coatings, United States Patent 6,909,395"

[6] Anderson, D., Johnson, L., Bell, F., "Troubleshooting Optical-fiber Networks, Elsevier," 2004, pp 63-65

[7] Anderson, D., Johnson, L., Bell, F., "Troubleshooting Optical-fiber Networks," Elsevier, 2004, p. 50