FSI WP 01

THE IMPORTANCE OF TUNING FOR PERIMETER AND DATA SECURITY SYSTEMS

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

ABSTRACT

Distributed sensors are increasingly finding wide applications in a world that is progressively more concerned about terrorism and other illegal activity. Two of the most common applications include sensing intrusions along protected perimeters and attempts to tap into fiber-optic networks.

The utility of the distributed sensor depends primarily on two key measures:

1. Sensitivity
2. False/nuisance alarm rate

Sensitivity defines the sensor's ability to detect the smallest possible disturbances while the false/nuisance alarm rate refers to the frequency with which the sensor responds to disturbances from non intruders, such as blowing dust, wind, animals, etc.

High sensitivity and low false/nuisance alarm rate are opposing goals. By tuning the sensor for maximum sensitivity one necessarily increases the likelihood of nuisance alarms from normal environmental sources.

This paper describes digital signal processing techniques for maximizing sensitivity while simultaneously holding the false/nuisance alarm rate within acceptable levels.

INTRODUCTION

In simplest terms, an intrusion sensor consists of two principal parts: a sensing element and a decision network. The sensing element applies principles of physics to produce a voltage that is, in some respect, characteristic of the intruder. The human ear/brain system is an excellent example of this sort of sensor (see Fig. 1).

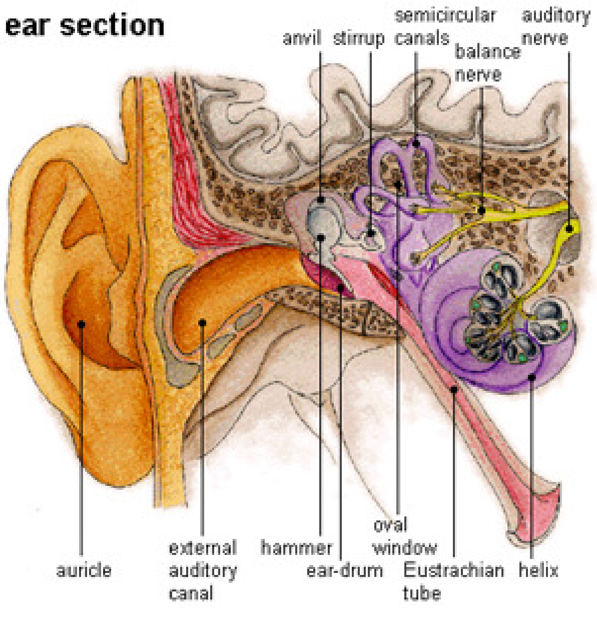


Figure 1. Diagram of the human ear (contmedia [1])

The intruder's movement causes pressure waves in the air. These pressure waves travel out in all directions from the intruder, entering the ear canal. Within the ear canal there's a thin membrane connected to a series of three tiny bones that respond sensitively to fluctuations in air pressure, converting these fluctuations into tiny electrical impulses that are then processed by the brain.

The brain's ability to detect an intruder depends on three things:

1. The ear's sensitivity to pressure fluctuations in the air, and ability to convert those pressure fluctuations into electrical signals transmitted to the brain
2. The amount of background environmental noise
3. The brain's ability to tune out noise while detecting and processing the signal of interest

For most of us, hearing is automatic, but only because we spend the first several years of life learning how to interpret the sounds we hear. This is training well spent, however. So powerful is the combination of sensitivity and tuning in the human ear that the average person can easily hear a pin drop on a hardwood floor, even when the room is filled with loud conversation.

The human ear is an example of a point sensor because the sensing element (the ear drum) has a specific, limited location. A spider web is an example of a distributed sensor because the sensing element (the web, which vibrates when disturbed) extends over a wide area and has approximately the same sensitivity over its extended area.

Many perimeters require protection. Examples include the perimeters around chemical plants, airports, rail stations, nuclear power plants, military facilities, and correctional facilities. One of the challenges for these sensors is the need to operate remotely in harsh environments with exposure to wide temperature ranges as well as rain, snow, slush, dirt and grime. Another challenge is the need to offer flat sensitivity with wide frequency range over long distances.

An ideal distributed, long-length, intrusion sensor uses optical fiber. These sensors can span tens of kilometers while maintaining optimum sensitivity along the entire length – vibrate the sensor at any point along this perimeter and it generates an alarm. Fiber optic sensors have inherent advantages in for use in these unforgiving environments. The sensor is all dielectric and passive, requiring no on-site electrical power at or near the sensing element – particularly important for facilities with highly combustible materials. Extended fiber optic sensors are also ideally suited for severe environments. Low-loss optical fibers developed for the telecommunications industry are readily available at competitive prices. These fibers are available in ruggedized cables capable of withstanding virtually any harsh environment.

The sensing mechanism uses optical interferometry in which modally dispersive coherent light traveling through the multimode fiber mixes at the fiber's terminus, resulting in a characteristic pattern of light and dark splotches called speckle. The laser speckle is stable as long as the fiber remains immobile, but flickers when the fiber is vibrated. 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. Because of the low loss of the fiber, the response of the speckle to disturbances is flat over a wide acoustic bandwidth. 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 up to several kilometers away from the processing electronics.

NOMENCLATURE

In classical electro-magnetic theory, light travels through a waveguide, such as optical fiber, in distinct modes. Mathematically, these modes correspond to solutions of Maxwell's equations, subject to the boundary conditions inherent in the design of the fiber. Each mode is characterized by a propagation constant, β, which describes the accumulation of phase as a function of propagation along the axis of the fiber. For oval-core fibers the propagation constant has been given explicitly by Shiraishi [2] as

$$\beta_{m,n}^2 = (n_0 k_0)^2 - n_0 k_0 \left[\frac{(2m+1)}{A_{gx}} + \frac{(2n+1)}{A_{gy}} \right] \tag{1}$$

where n_0 is the refractive index at the center of the core, k_0 is the wave number in vacuum, A_{gx} and A_{gy} are the normalized x- and y-directional core radii, respectively, defined by $a_x/(2\Delta)^{1/2}$ and $a_y/(2\Delta)^{1/2}$, respectively, where Δ is the relative index difference defined by $(n_0^2 - n_1^2)/2n_0^2$, where n_1 is the refractive index of the cladding.

Each mode is defined by the integers, m and n, and has the unique propagation constant defined by Eq. (1). The number of guided modes depends on the fiber construction, including parameters such as core diameter, cladding diameter, wavelength, and the index of refraction of the material used to construct the fiber. The number of modes carried by the fiber can be controlled through proper design of the fiber parameters. Generally, by increasing the diameter of the fiber core, the number of bound modes increases.

The mode numbers m and n describe the number of nulls in two orthogonal transverse directions, generally labeled "x" and "y," with "z" representing the direction of propagation. In the absence of stress each spatial mode consists of two degenerate polarization modes. The presence of bending stress causes these degenerate modes to split, with one polarization of the spatial mode having a different propagation constant than the other.

Coherent light transmitted through a multimode optical fiber randomly couples among the different modes. This modal distribution depends on the manner in which light is launched into the optical fiber, as well as how the fiber is bent and twisted. Because the propagation constants are different for the various modes, light in each of the modes accumulates different amounts of phase while propagating along the length of the fiber. Since the different modes have spatial overlap, the phase differences between the modes result in optical interference at the end of the fiber, characterized by a pattern referred to as laser speckle (see Fig. 2)

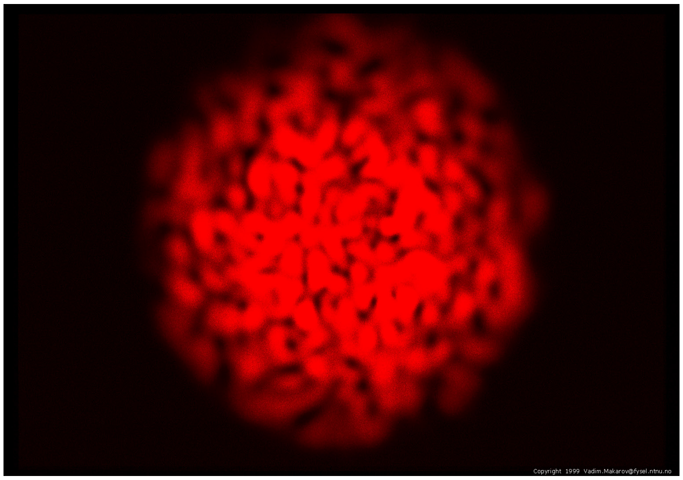


Figure 2. Example of laser speckle projected from the end of a multi-mode optical fiber, illuminated with coherent laser radiation.

Bending and longitudinal stress differentially change the propagation constants of the various spatial modes (Smith [3]), which changes the phase differences, and cause the speckle pattern to flicker. This changing speckle pattern can then be measured and used to detect vibration of the fiber, and indirectly the material to which it is mounted.

DISCUSSION

Figure 3 illustrates the basic system components required for any detection system. The signal of interest (intruder's signal, in this case) is summed with system and environmental noise in the sensor, which produces a voltage that is analyzed by a decision network. The decision network tries to distinguish between the intruder and the system/environmental noise.

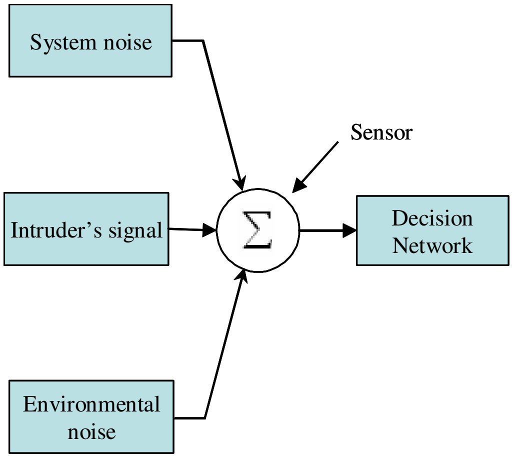


Figure 3. Basic components of an intrusion sensor

System noise arises from unwanted fluctuations (noise) in the sensor and subsequent electrical circuits. Some of this noise can be eliminated through careful design. For example, induction from 60Hz power lines can produce tiny electrical currents in a circuit, but electrical engineers can largely mitigate this source of noise by carefully shielding sensitive components. Other sources of noise are fundamental, and arise from the quantum nature of optical and electrical components. These sources of noise can be minimized through careful design, but never fully eliminated. Examples include shot noise, Johnson (thermal) noise, and 1/f noise (Dereniak, [4]).

System noise sets the limit for the smallest signal that a detector can sense. Environmental noise, however, is often the thing that effectively limits a sensor's ability to detect an intruder.

Environmental noise is particularly troublesome because it produces real signals that are much larger than the system noise. These signals, however, are not the result of an intruder. Instead, they might be the result of trucks passing on a nearby highway, airplanes taking off from a nearby airfield, or people walking near the perimeter, but not trying to actually cross it.

Imagine isolating the sensor from all possible sources of environmental noise. It may still produce alarms. We classify those alarms as "false alarms," since they originate strictly within the sensor and its associated electronics, and are the result of no actual physical (environmental) stimulus.

On the other hand, if an alarm is caused by environmental noise, we call it a "nuisance alarm." Though this distinction (between false and nuisance alarms) is often inconsequential to people who use the system, it is of utmost importance to the designer. If a system suffers from false alarms, the designer must improve the sensor and associated physics, but if the system suffers from nuisance alarms the designer must understand how to reduce the environmental noise, often by proper design and tuning of the decision network.

We define environmental noise as "statistically significant" when signals caused by the environment are larger than those cause by system noise. The only way to discriminate between statistically significant environmental noise and real intruders is to use an advanced decision-making network. This is the sort of network that your brain uses when it picks out the sound of a pin dropping onto a hardwood floor in a room full of talking people. In this example, the talking people represent environmental nose, and the sound made by the dropping pin represents the intruder. A finely tuned decision making network, such as the brain, is capable of finding small signals, even in the presence of large signals caused by environmental noise.

The simplest decision-making network is a straightforward threshold. In such a network, the system identifies an intruder whenever any part of the time-varying sensor signal level exceeds a threshold (Fig. 4 and Fig. 5). Simple threshold-based systems are susceptible to both environmental and system noise, although system noise is easier to ignore. That's because, in most systems, the system noise can be measured and characterized so that the threshold is set just low enough that no system noise exceeds the threshold. However, simple threshold-based systems are very susceptible to environmental noise whenever the strength of the environmental noise is comparable to the strength of the intruder signal.

We can deduce from the Central Limit Theorem that, in environments where there are many types of random noises, the strength of the environmental noise has a probability density function with a Gaussian (bell) shape (see Fig. 6). For example, a fence perimeter will be subject, with high probability, to gentle shaking due to breezes and local traffic. Stronger environmental signals, caused by strong winds, hurricanes, and earthquakes, will be increasingly less probable.

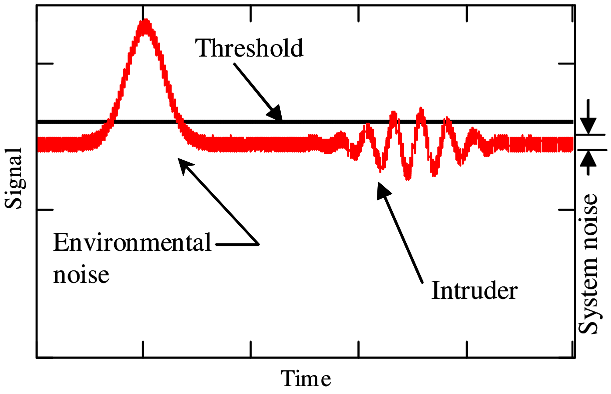


Figure 4. Simple threshold-based decision network in the presence of both system and environmental noise. In simple decision networks such as this, it's relatively easy for environmental noise to trigger an alarm. In fact, in this example, the environmental noise exceeds the threshold by a larger margin than the signal produced by the intruder.

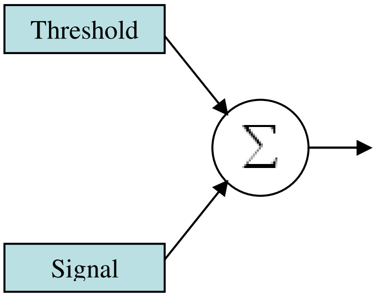


Figure 5. Inside a simple decision network.

To avoid excessive nuisance alarms in a simple threshold sensor the installer must set the threshold well above the level reached by even infrequent environmental effects, such as moderate wind. In this condition, however, the sensor will be unable to detect stealthy intruders – the sorts of intruders who might disturb the fence with less amplitude than that caused by a gentle breeze. To escape this conundrum the installer needs to have access to a tunable decision network.

A tunable decision network is one that seeks to locate small signals of interest, even in the presence of much larger environmental "noise" by applying thresholds that rely on more complex rules than those governing a simple decision network. A tunable decision network is like a neuron in a neural network. Though not nearly as complicated as your brain, it shares some basic similarities with the way your brain makes decisions.

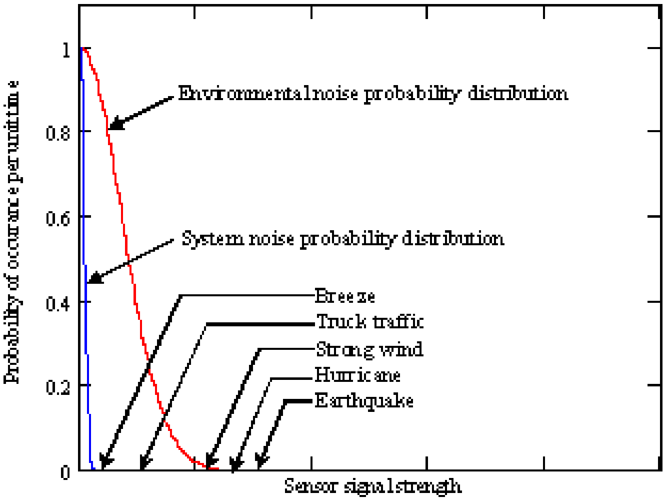


Figure 6. Environmental and system noise. The vertical axis shows the probability of occurrence, and the horizontal axis shows the signal strength. Noise with small signal strength is more likely to occur than noise with high signal strength.

Think back to how you manage to hear the pin drop on a hardwood floor, even with one person talking loudly to a second person who's sitting right next to you. The pin makes a characteristic ringing sound. Its pitch and duration are also distinctly different from that of the conversation going on around you. It's this difference in both time and frequency that allows you to make the distinction between the background conversation and the pin dropping on hardwood.

It's important to remember that a tunable decision network is still a simple threshold in the strictest sense of the word. That is, the sensor produces a signal that's compared with the threshold. If the signal is over the threshold the sensor sounds an alarm, and if it's less than the threshold the sensor doesn't sound the alarm.

The difference between a tunable decision network and a simple threshold is that the tunable decision network is a composite that looks at several effects before making a decision, and weights each contributing factor in order to produce a composite signal that's then compared with a go-no-go threshold (Fig. 7).

To better understand this distinction, let's look at an example. Suppose you are designing a visual detection system for counting alley cats. You might point your camera at a spot in the alley and then monitor the total light captured through the lens. An alley cat, upon entering the field of view, will change the amount of light captured by the lens and, if the change exceeds a threshold, the software records one alley cat.

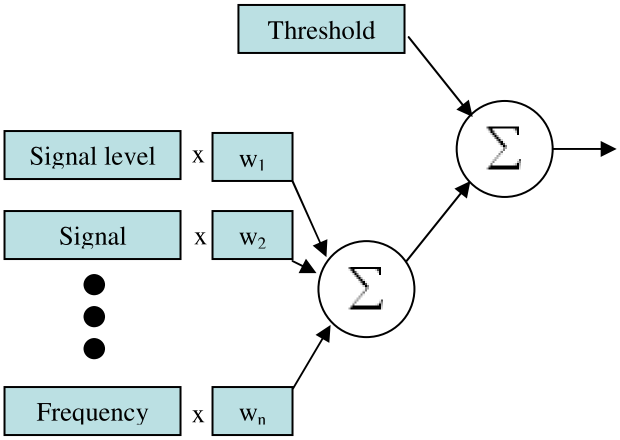


Figure 7. Tunable decision networks use apply weighting factors (w_1, w_2, … w_n) to multiple rules and then sum these to arrive at a composite "signal" that's then compared with a go-no-go threshold.

The problem with this technique is that people, birds, passing clouds, sunset/sunrise and small mammals might also change the amount of light entering the lens, and trigger a false count. To correct this problem you might look for a grouping of image pixels that suddenly change amplitude. If a group of pixels changes amplitude, and if the group corresponds to something the size of a cat, you count one alley cat. In this example the signal is no longer a change in the total light entering the lens, but rather the change from a smaller group. This compound rule (look at changes in light, from a small group of pixels) helps to eliminate the possibility of counting a person as a cat.

Of course, this still leaves the problem of how to deal with stray dogs, pigeons, blowing litter, changes in illumination, etc. To distinguish the alley cat from each of these background circumstances you could use additional rules. For example, you might add rules that look at the three-dimensional shape of groups of pixels, counting only those that have a "cat-like" appearance. You might also add rules that look at how fast the groups of pixels move, their color, etc.

From this example you can see that we never get away from a binary filter. At some point there's always a decision to either count a cat or not count a cat. Or, in the case of a perimeter detection system, there must always be some point where the system either decides to sound an alarm, or not to.

The difference in sophistication of the alarms amounts to differences in the sophistication of the rules that go into deciding where to put the threshold. The simplest rule is to sound an alarm if a voltage exceeds some level. More sophisticated systems add more sophisticated rules. These rules might involve looking at the frequency content of the intrusion, and using a frequency-domain level threshold. Additionally, more sophisticated thresholds might use correlation techniques and time-frequency methods. The more rules we build into the threshold – rules that tune it – the less likely is the system to falsely identify environmental noise as a real intruder.

One of the most powerful tools for tunable decision networks is to use both time- and frequency-domain data in the decision-making process. For example, let's look at the situation in figure 4 again. By digitizing the time-domain sensor data and taking the discrete Fourier Transform (typically using the Fast Fourier Transform (fft) algorithm) we can convert the sensor data into frequency-domain data. This allows us to more carefully analyze distinguishing characteristics of the intruder and environment, giving us a more sophisticated threshold with which to distinguish the intruder from environmental noise (see Fig. 8).

In Fig. 8 we see that the environmental noise tends to be clustered at low frequencies, while the intruder (in this example) tends to produce disturbances at mid-level frequencies. Although the environmental noise is much larger, the intruder is easily distinguished in the frequency domain by setting a dual-level threshold that requires a higher level of all signal levels below a fixed frequency before counting as an alarm.

Frequency discrimination is most useful, obviously, when the intruder acts on the sensor in a way that is fundamentally different from the way the environment acts. For example, wind on a chain link fence causes it to sway, resulting in lower-frequency vibrations. A person cutting the fence with snippers will cause higher-frequency (but lower amplitude) vibrations. By using frequency-domain tuning, it's possible to distinguish the intruder from the environmental noise.

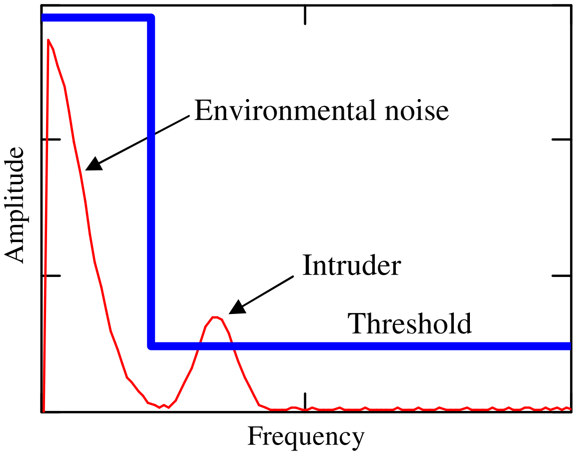


Figure 8. Fast Fourier Transform (FFT) of time-domain data shown in Fig. 4, with dual-level frequency-domain threshold (shown as blue line). Here, the intruder exceeds the threshold, while the environmental noise does not.

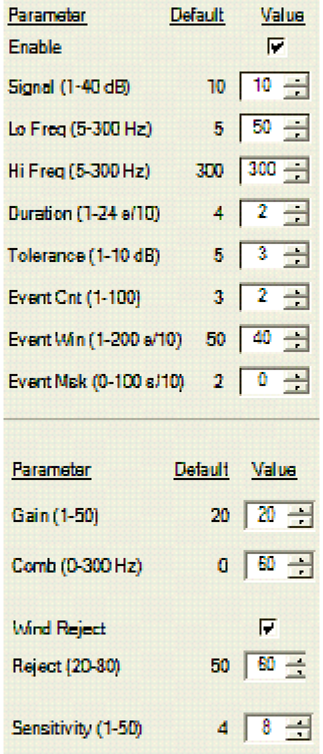
Intruders can't always be identified simply by the frequencies of the disturbances they cause. In such instances we can employ another powerful mathematical tool called time-frequency analysis. Figure 4 shows the frequency content from a single snapshot in time. Now imagine acquiring many similar snapshots in time, while looking at the frequency content of each snapshot. This would allow you to look at how frequency content evolves over time, giving you another way of distinguishing environmental noise from signals of interest.

For example, you might observe that trucks passing on a nearby road tend to produce the same sorts of frequencies as intruders trying to climb over the fence. But the trucks pass by the fence quickly, while someone trying to climb over or cut through the fence takes much longer. This distinguishing factor allows you to identify intruders by the bulk length of time that you see activity exceeding the frequency-domain threshold that you identify for climbers.

Fiber SenSys perimeter sensors use powerful, multi-parameter thresholds based on both time and frequency analysis. Figure 9 shows the user interface used to tune our point-locating SPIDeR fiber-optic perimeter sensor. These parameters allow the user wide flexibility in designing thresholds that satisfy their unique requirements, based on location and the type of material on which they mount the sensor.

Using these parameters the user can fine-tune their perimeter to reduce nuisance alarms (resulting from environmental noise) to acceptable levels while maintaining the ability to detect even stealthy attempts to violate the perimeter.

Let's look at each of these parameters in turn, see how they work, and how they might be used to distinguish environmental noise from real intruders.



Parameter	Default	Value
Enable		☑
Signal (1-40 dB)	10	10
Lo Freq (5-300 Hz)	5	50
Hi Freq (5-300 Hz)	300	300
Duration (1-24 s/10)	4	2
Tolerance (1-10 dB)	5	3
Event Cnt (1-100)	3	2
Event Win (1-200 s/10)	50	40
Event Msk (0-100 s/10)	2	0

Parameter	Default	Value
Gain (1-50)	20	20
Comb (0-300 Hz)	0	60
Wind Reject		☑
Reject (20-80)	50	60
Sensitivity (1-50)	4	8

Figure 9. User interface used to tune Fiber SenSys perimeter security products.

Signal: This parameter works with **Gain** to determine the threshold used for detecting signal between the low and high frequencies

Gain: The difference between **Gain** and **Signal** is proportional to the threshold used between the low and high frequencies

Lo Freq: The decision processor ignores signals below this frequency.

Hi Freq: The decision processor ignores signals above this frequency

Duration: This is the interval time during which the intrusion signal must exceed the threshold, in order to be counted as an event.

Tolerance: Defines exceptions to the threshold rule, for longer-lasting, but weaker signals.

Event Cnt: Shorthand for "event count." For the decision processor to sound an alarm, there must be a certain number of events that occur within the time defined by **Event Win** (shorthand for "event window"). This number is given by **Event Cnt**.

Event Win: Shorthand for "event window." The window of time where events are counted. The number of events counted in **Event Win** must be equal to (or greater than) **Event Cnt**. before the events are reported as an alarm.

Event Msk: Shorthand for event mask. Events are not counted as multiple events if they are too close together in time. After the decision processor finds an event, it ignores any other events that occur during the **Event Msk** time.

Comb: Sometimes environmental noise happens at discrete frequencies that repeat. For example, in the presence of high-current devices (like motors, or high voltage/current lines in converter stations) one often finds noise at 60Hz, 120Hz, 180Hz … The Comb function allows you to define a frequency (and its higher harmonics) where the decision processor ignores signals.

Wind Reject: Through many years of experimentation, scientists at Fiber SenSys have found characteristics of wind (environmental noise) that are fundamentally different from those of intruders. When this option is checked the decision processor uses these proprietary algorithms to automatically screen for the presence of wind, thus greatly reducing the possibility of nuisance alarms.

Sensitivity: The electrical systems in Fiber SenSys sensors have very low noise, nearly equal to the theoretical limit. This means that the signal detected by the sensors can be greatly amplified before system noise begins to cause nuisance alarms. By turning up the sensitivity the sensor can be tuned to detect very tiny disturbances. Turning it up too high, however, can result in nuisance alarms caused by environmental or even (if turned up high enough) system noise.

Let's look a little closer at the four most fundamental setup parameters, and examine a couple of hypothetical cases. The four parameters are:

G	Gain (relative, dB)
S	Signal (relative, dB)
D	Duration (1 to 100 intervals of 0.1 seconds)
T	Tolerance (relative, dB)

Increasing the gain is equivalent to making all disturbances uniformly more intense. It is analogous to turning up the volume on a radio, which has the effect of increasing the volume for all frequencies, and has the effect of making the system sensitive to smaller disturbances.

The signal, duration and tolerance parameters work together to determine how intense the disturbance must be, and how long it must last, for an event to be registered. They have the following meanings: An event will occur if the disturbance intensity (after amplification by gain) equals or exceeds S for the length of time indicated by D. Keep in mind that it takes a certain number of events to make an alarm.

A shorter disturbance won't trigger an event, no matter how intense it is. A weaker disturbance may be able to trigger an event if it lasts longer, but how much weaker or longer depends on the tolerance setting. If T is set to 3, for example, a persistent disturbance slightly more intense than 3 dB below S will trigger an event after a long time, but a signal below S by more than 3 dB will never trigger an event, no matter how long it lasts. In other words, in this example, the sensor will only tolerate disturbances weaker than S by up to 3 dB.

Note that the gain setting just increases the effective disturbance intensity that the signal processor sees. If we increase the gain and decrease the signal setting by the same amount, there is no change in how disturbances are processed.

Figure 10 is a composite showing the probability of signal levels due to system and environmental noise, as well as sensor sensitivity. The horizontal axis represents the signal (disturbance) strength that's input to the decision processor. The right horizontal axis applies to the black curve, and shows the probability of detection by the event processor, as a function of the signal strength. As the signal strength increases, the probability of detection increases. The left horizontal axis shows the noise probability density. The probability of very low noise is relatively high, and the probability decreases as the noise signal level increases.

In figure 10 there is very little overlap between the detection curve (black) and the environmental noise curve (red), so we could lower the threshold without causing false or nuisance alarms. As we lower the threshold the sensor becomes more sensitive. If we lower it too much, though, the curves will begin to overlap (Fig. 11) and this will result in more nuisance alarms.

To detect the smallest possible intrusions, we want the black curve (representative of the sensor's sensitivity) to extend far to the left (toward low signal levels). However, as we move the black curve toward smaller signal strength the black, red, and even blue curves start to overlap. The nuisance alarm rate is determined by the overlap between these curves. The more overlap we have, the greater the probability of nuisance alarms.

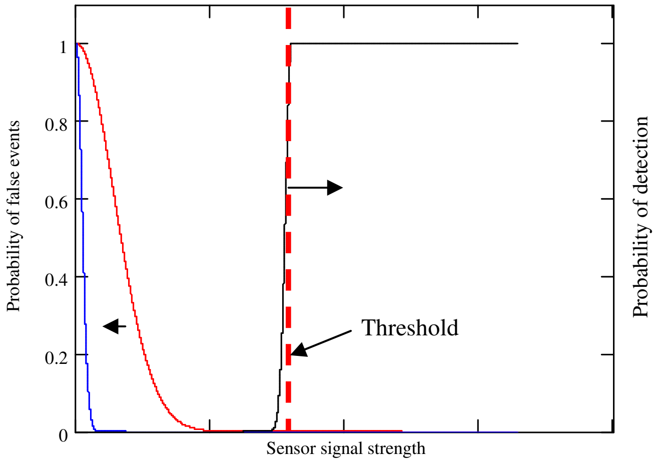


Figure 10. Noise probability density (blue and red curves) and detection probability (black curve) as a function of sensor signal strength.

This presents a fundamental dichotomy. On the one hand, we want to make the sensor as sensitive as possible. On the other hand, we need to ensure that we have as few nuisance alarms as possible.

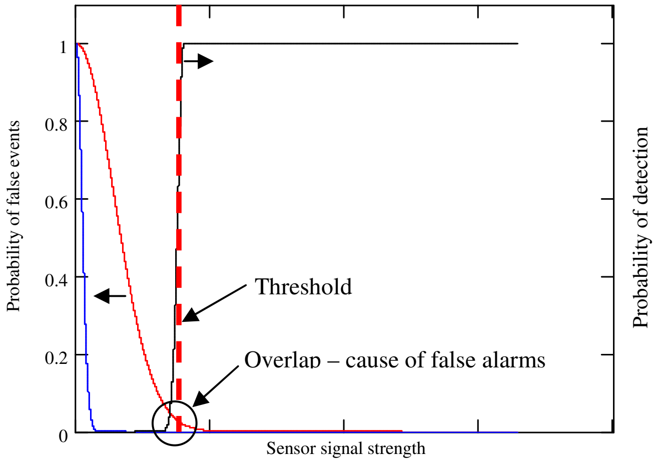


Figure 11. Moving the threshold too low causes false alarms

We address this problem with the tunable decision network. By tuning the network we greatly reduce the width of the probability curves of the system and environmental noise. To see how this works, let's digress briefly with a short discussion about probability, correlation, and random events.

Suppose you flip a penny with your thumb. What are the odds that it lands "heads up?" You probably have no difficulty answering "0.50." Now suppose you flip the penny twice. What are the odds that it lands heads up both times? Assuming the penny is fair (not biased) the probability is 0.5 that it lands heads up on the first throw, and 0.5 that it lands heads up on the second throw. So the odds of landing heads up on two throws in a row is $0.5 \cdot 0.5 = 0.25$.

This illustrates a very important characteristic of random noise; it's uncorrelated. Suppose the probability of a given level of noise, in a particular window of time, is P_{noise}, then (if the noise is random and un-correlated) the probability of two such spikes, one after the other, is equal to $(P_{noise})^2$. Since probability is always a number less than (or, at best, equal to) one, squaring the probability results in a smaller number – a smaller probability.

This is a slight simplification because most noise sources are not completely random and uncorrelated, so the effect is not quite as dramatic as described in the example above. Signal sources, on the other hand, are not random, and typically have a high degree of correlation. They have structure and the parts of that structure are correlated with each other:

> *Th t's on f t e rea ns yo can mke out the meanin of a sent ce, even with vaious pats mising; the w ds and lettes correlate with each oter, so th e's a lot of redndancy.*

You probably already understand this at an intuitive level. When you walk up to a house and knock on the door, you probably don't knock just once. A single knock could sound like someone bumping a table in the next room, or the dog's tail bumping the door. It could sound like random background noise in the house, and be ignored. Since you don't want to be ignored, chances are, when you knock on the door you knock more than once: "knock, knock, knock." The triple knock is a "signal" that is less likely to be mistaken as random background noise.

A tunable decision network applies the same sort of logic by taking advantage of the statistical differences between noise and signal by applying rules that reflect the correlated nature of the signals we are looking for. These rules narrow the probability curve of the un-correlated, random noise. In other words, since the noise is un-correlated the "AND" function in the summing node of the tunable decision network (Fig. 7) effectively raises the noise probability curve to a power greater than 1. Since the probability curve is everywhere less than 1, raising it to a higher power makes it much narrower (Fig. 12)

The "AND" function in the tunable decision network has an opposite but smaller effect on the detection curve. Here, the sloping region of the curve gets slightly broader, but the broadening effect is less pronounced in the detection curve than in the noise probability curve because, for signals of interest, the various tests that are summed together in the tunable decision network are correlated.

The overall result of these two effects is that we can lower our threshold without increasing the overlap between the detection probability curve and the noise probability density curve (Fig. 13). Looking at figure 13, we see that the tunable decision network works by effectively reducing the environmental and system noise and thus allowing us to set a lower (more sensitive) detection threshold, without incurring false/nuisance alarms.

Although extremely powerful, the tunable decision network is not a panacea. For any given decision network there will always be some disturbance that is just barely larger than the noise. Signal levels lower than this cannot be detected without high incidence of false/nuisance alarms. Though not a cure all, the tunable decision network is an extremely powerful tool that allows users to gain optimum sensitivity from their sensor without burdening them with a high false alarm rate.

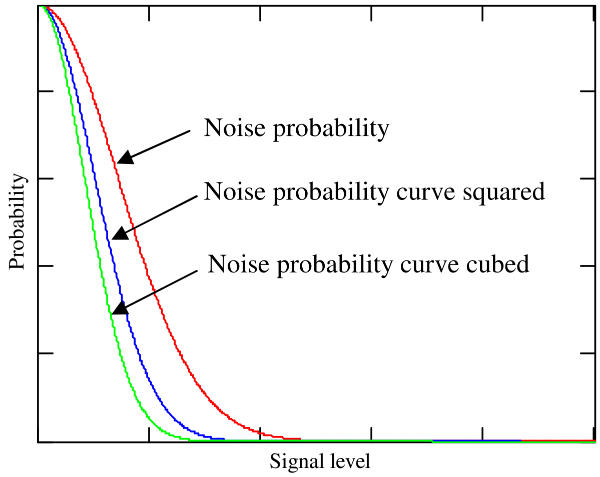


Figure 12. The probability of noise of a given signal happening in consecutive windows of time can be found by raising the noise probability curve to some power (the power used depends on the amount of correlation and the number of time windows). Since the noise probability curve is less than one, squaring and cubing it narrows the curve.

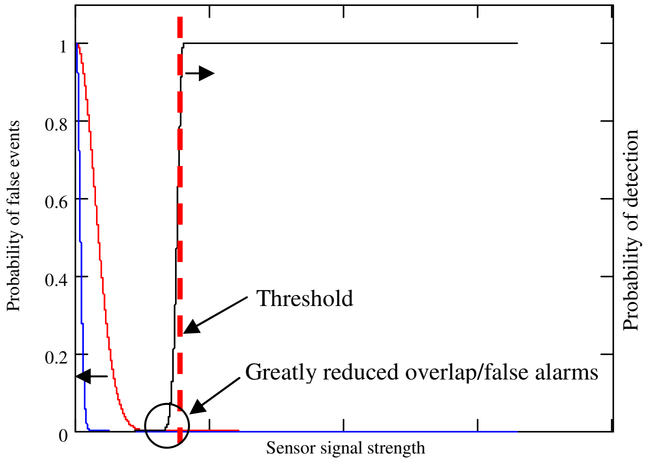


Figure 13. The tunable decision network narrows the probability distribution of the environmental noise, allowing the use of a lower threshold without incurring too many false alarms, thus expanding the system's useable sensitivity.

CONCLUSION

False/nuisance alarms are bad for several reasons. First, a system that constantly cries "wolf" when there's no danger soon loses credibility; it becomes ignored. A security sensor that's ignored isn't much different from no sensor at all. If the bogus alarms aren't ignored, then someone has to spend time and effort to investigate them. At the very least, someone is going to have to look out a window. In practice the investigation will have to be more thorough, possibly involving on-site investigation by armed security personnel – and that's expensive.

At the very least, false alarms are a nuisance and inconvenient. At worst they are expensive or result in the system being ignored and ineffective.

The cost associated with investigating nuisance alarms depends on the installation. In some cases the entire perimeter may be visible from a privileged vantage point. In other instances the perimeter can be checked using security cameras. Generally speaking, the longer the perimeter, the more difficult (and expensive) it is to check on the cause of an alarm.

This can be a real problem on very long perimeters because the probability of nuisance alarms increases as the perimeter gets longer. This is true simply because of the accumulating opportunity for some environmental nuisance to occur. For example, a 1-km perimeter has less chance of being disturbed by a deer or antelope than one that's 70 km long. Similarly, a shorter perimeter has less chance of being hit by strong winds than a very long perimeter. This holds true for all sorts of environmental disturbances such as foot traffic, minor earthquakes, nearby traffic, trains, etc.

While the probability of nuisance alarms increases with perimeter length, the cost of investigating the alarms also increases with distance. This is a worst-case scenario that can quickly get out of hand, especially when the sensor manufacturer has designed for sensitivity without also providing the ability to use a tunable decision network.

Clearly one cannot design a perimeter sensor system that focuses on just one dimension of the system's performance. Sensitivity and tunable decision networks must be designed and fully integrated in order to provide optimum detection capability without undermining effectiveness by reporting excessive nuisance alarms.

ACKNOWLEDGMENTS

The author would like to thank Dr. Peter Lovely who is the chief architect of the Fiber SenSys tunable threshold algorithms, as well as the wind algorithm that's used to automatically fine-tune the system to reject wind-generated false alarms. The author also wishes to thank Dr. Shailesh Singh and Todd Kuribayashi for their work in adapting Dr. Lovely's algorithms for use in our latest generation of point-locating fiber-optic sensor.

REFERENCES

[1]Contmedia.
http://www.contmediausa.com/shop/app/products/Human3D/human3dhumanear.html

[2] Shiraishi, K., Ogura, A., and Yoda, H., *Explicit formulas for transmission characteristics of graded-index oval core fibers*, APPLIED OPTICS / Vol. 43, No. 3 / 20 January 2004

[3] Smith, A., *Birefringence induced by bends and twists in single-mode optical fiber*, Applied Optics, vol. 19, No. 15, pp. 2060-2611, Aug. 1980.

[4] Dereniak, E.L., Crowe, D.G., *Optical Radiation Detectors*, John Wiley & Sons, 1984.