Reliability Issues and Improvements in Remote Monitoring Security Systems

R. Hariprakash
BIHER,Bharath Univ, Chennai-73
rhp_27@ieee.org

G. Venkat Ramu
University of Madras
Chennai-25, India
ramu_nec@yahoo.com

T. Rajakumari
Polytechnic College
Chennai, India
visa4466@hotmail.com

S. Ananthi
Univ. of Madras
Chenna-25, India
ananthibabu@yahoo.com

K. Padmanabhan
AC Tech, Anna Univ., Chennai-25,
ck_padmanabhan@rediffmail.com

***Abstract* – The paper deals with the methods of security implementation in community areas based on certain high technology sensor system and communication methods. Security systems for home or industry have a lot to perform today in terms of reliability and performance. After examining the various modes for security management, the paper describes data collection and fusion which demand careful processing and discerning of the security problem. Herein, the problem of data detection without errors becomes important to avoid falsely discerning insecurity levels. This paper examines some signal management methods for error free operation of signals from Doppler motion sensors and camera image data. Amongst them this is considered the technique for encoding data using the Hilbert Transform. This is better for motion sensors with a few extra bits of transmission enabling error free reception at the monitoring computer station. Also considered are wavelet compression and transmission for remote site image data using spread spectrum.**

Keywords*: Home security system; Hilbert Transform for data encoding; Wavelet transform; Spread spectrum.*

1. REMOTE SENSOR SURVEILLANCE-METHODS AND PROBLEMS

Now-a-days, it is common to have a central monitoring system of remote surveillance doing the job for many a home or industry floor. The monitoring system itself has to be securely located in a place difficult to identify. It deals with the problem of receiving inputs from a multitude of signal sensors, from all its customers, periodically. It has to process them despite any transmission system noise and identify events of insecurity as well as send suitable commands to take proper action [1]. In this, there are two categories of security levels: i) totally un-manned and uninhabited; ii) partially manned by sentinel.

The methodology and implementation of security monitoring systems are varied and wide. On the one hand, there are various methods of sensing the internal environment to be monitored employing whatever sensors that would fit the environment best. On the other, there are different approaches to prevent intrusion, by simulating the presence of human existence in an unmanned area. When many sensors and cameras are used for many rooms and areas, the quantity of signals become large; their continuous monitoring over extended periods of time render the data manipulation large and extensive. Among these are the several CCTV, metal detectors, burglar alarms, fire alarms, access control and so on [2].

While new techniques in sensors have brought forth more and more components for the security environment, there have also been incidents of pilferage, interference and mal-operation in many sites leading to failure of the entire monitoring system. Attacks against security have been very many. Therefore, in this write – up, we first cite the sensor techniques and then concentrate on how the sensor information is getting immense when a single monitoring station caters to many sites which have entrusted their security problems to it. With such a continuous flow of information to the processing station, data can be interrupted by hostile elements and it can gain errors. Erroneous information in security monitoring would invariably provide false alarms. So much so, it becomes necessary to confirm the validity of such communicated data while also being able to correct errors. In this context, methods conventionally available in data communication for error detection are not sufficient in this respect because none of these could provide the surety of correctness of data, though they could correct a very small percentage or errors which might be present. Particularly important are the motion sensor data with regard to error detection.

2. TYPES OF SECURITY SENSORS

Security makes use of sensors extensively. Sensors must be reliable and should not provide false alarms and must operate with low power and also from battery in order to provide security signaling even when power is purposely shut down in the area being protected. Vendors [3] supply products for real estate developers and hotel operators a cost effective and reliable way to provide their customers with total control over home or hotel rooms.

To provide security in unattended situations, simulation methods are common. The monitoring systems simulate the presence of inmates for external observers. This is by switching on and off, the several internal lights, issuing

noise akin to speech and turning on the television set at intervals, particularly during day time. This means a pre-planned appliance switching control from an external monitoring station in order, to simulate the presence of inmates in an actually vacant home or commercial site. Signal commands sent for activating these simulation systems need to be protected because if they are watched by an intruder, it makes it easy for him to intrude such a site.

Sites hired for security management by the central monitoring station may need activation and de-activation as and when needed. Current technology provides for security systems activated with one or more buttons or with a voice command key pad with select regions of security or levels. The activation can also be made from external through telephony, but this has to be handled with suitable password protection and encryption embedded in it.

There are a variety of signal sensors available in this area. The most common are the switches in the several movement paths, tampering signal detection components for lockable items, door signals, lighting signals. There are motion sensors based on the Infra-red, microwave and ultrasound reflectance principle which are capable of sensing human and only human movement. The three states of any sensor signal would be:

i) inactive
ii) active, indicating a presence of an event (closure, opening) and
iii) failed sensor.

Here again, the characteristics of sensors - the resolution, linearity, sensitivity, response time, offset, range, hysterisis, long term stability, their temporal behavior etc., need reliable proper signal hardware concepts.

For movement of humans in unexpected sites and areas, usually reflectance sensors or infra-red thermal detecting sensors are used.

The path-way switches, the door hinge switches are digital; the motion Doppler signals are analog and need processing further; the mixed signals arise from reflectance sensors with varying threshold depending on ambient lighting conditions. Most of these are available with wireless communication in built. Security monitoring based on audible signals detected through remote microphony [4] is also cited with classification techniques based algorithms for detecting non-speech and speech audio.

There are several issues relating to sensors that need to be addressed today. Sensors should be precise and should be communicative by themselves such as the radio remote transmitting door lock sensor [5]. There are also systems like the Sony's Wireless iPod Whole-House S-AIR Audio System [6]. In this paper, with respect to motion sensors, a new encoding scheme is indicated that enables data to be transmitted with error correction embedded in the method.

With Doppler signal data from sensors, the movement profile of the source, which, in our case, happens to be the possible intrusion in the monitored site, should be identified with high level of probability. The ability of the radar to reject faster than walking speed targets can also be controlled by time constants in the circuit. A typical value of radial velocity is 16 mm/s at the MID frequency of 10.687GHz and this determines the range [7].

3. SIGNAL HANDLING AT MONITORING SITE

Sensor signal processing follows sensor signal conditioning. The question as to which signal sensors would do all detection and processing at site and which ones at the remote monitoring station have to be decided first. For most sensors, it involves advanced signal processing algorithms that go far beyond sensor signal conditioning. Examples are linearization, adaptive filtering, correlation, signal transforms, signal compression, and pattern recognition. While some of these can be implemented easily with analog circuits, digital signal processing does the rest. Signals digitized can be stored for long time for comparative inferences. It is possible to send signals all collectively as and when they are sampled and communicate them remotely to the monitoring site via a communication channel. Or else, the processing can be done by local hardware and only the final components of signal complexes be transmitted to the monitoring site.

Complex systems of security levels are required in the several vulnerable locations. Once a preprocessed signal is available, it is not necessary to perform all further processing in the site itself. Doppler signal processing from at least two different motion sensors would need not merely be a signal indicating a motion that is causing a suspicion, but also the time course of the signal indicating its positive aspect of suspicion.

Image signals are also now becoming more and more important. These are usually transmitted with encryption and compression. They need to reduce the data size and increase the throughput.

4. INFORMATION FUSION FROM MULTI-SITE SENSOR COMPLEX

In areas related to industrial and military applications, there are such systems of information processing, such as the (VMMD) Vehicular Multi-Sensor Mine Detection [8]. Land mine detection sensor development and systems integration are evaluating new technologies, incrementally improving existing technologies, increasing the probability of detection, reducing the false alarm rate, and planning out usable deployment scenarios.

With all these sensors and data, one would think that a body of data would exist from which effective real time algorithms for information fusion or "detection" could be developed. The application of Dempster-Shafer evidential theory for implementing a home security system using sensor data fusion has also been considered [9].

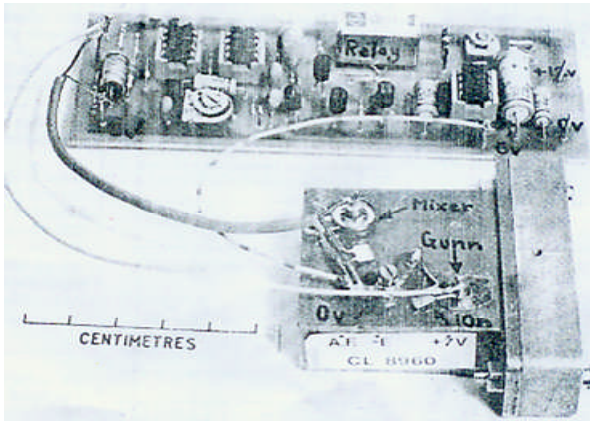

Figure 1 A early bird MID homebrew MID device using Gunn Diode and Mullard CL8960 mixer [5] .

There should be a multiplexed signal processing software, which would handle the several communicated signals from time to time from the customer sites.

Thus, 300 signal bits would need to be processed at least once a few seconds, continuously and with around 100 customers per one network that monitors its area, there would be a signal processing of 30000 bits in unit time slot.

The mathematical processing of the signals would vary from simple to mathematically time intensive approaches, such as complex Fourier transform, for the Doppler signals from motion sensors.

Then, the simulated testing of the sites are also to be included as part of the sentinel system. In this, the site would be simulated with events from a manned or automatic program of closure or opening of proximity switches, movement simulators with lights or infra red beaming lights with motion and so on. The programs for such periodical testing would be part of the maintenance routine which would be run as often as needed or requested by the customer.

So much so, a monitoring station hired to monitor surveillance activity in about 50 sites would be dealing with more than 500 signals over the whole day in sequence; this would require sufficient processing power and software management.

Consider a system with around fifty digital logic outputs from switches and proximity sensors; around a dozen motion sensor input signals processed or given in raw format with just a digitization on an 8 or 10 bit ADC. Combine this with the signals which are created to simulate human presence by the outputs to the lights, the noise speakers, the switching on and off the television or other similar simulated activity, including answering a telephone call from recorded information, all amounting to around 40 approximately.

The above will need a signal vector, which could be having a dimension that would be $50 + 12\times 2 \times 10 + 40 = 330$. The sampling time could be anywhere between hours to a few seconds, depending upon the security system's time resolution. (The Doppler signals are two in number, which are analog but converted into 10 bits digital by the ADC and hence we have $12\times2 \times 10$). This is just from a single site being monitored for security. There could be many such homes and security monitored sites contracted by the monitoring central agency, which will be therefore continuously receiving information from the several sites all through the 24 hours.

The job management and control strategy as well as emergency functions of the central monitoring system would be to analyze the above data, assuming that there is no loss or corruption in the system used for transmission or any man-made interference in the system of communication. There could also be a protocol communicated via any of the wireless or similar communication systems, including the use of the cellular phone [10].Error free transmission should be the aim, since errors in data, if not identified, will lead to false alarms and disturbances to customers.

5. ENCODING OF SIGNSALS FROM MOTION SENSOR

Motion sensors are a very important of the totality of sensors at sites.

The sensors of the motion detectors quantifies motion that can be either integrated with or connected to other devices that alert the presence of a moving object within the field of view. In Simpler systems, the motion sensors used to be connected to a burglar alarm to alert the security

station after it detects motion or the signal used to trigger a red light camera. Amongst these sensors, (PIR) Passive infrared sensors [11] look for body heat. In Some specific cases the signals are usually detected either by all of these and in addition, ultrasound or infra red sensors.

The ultrasonic active sensors send out pulses and measure the reflection off a moving object. The Doppler effect principle is used for ultrasound signal transducers to detect and determine the moving intrusion and hence it is more reliable. To avoid false alarms due to pets, the dual-technology motion detectors are used [12]. In these *PIR/*Microwave combination detectors Pet-Immune functions that allow the sensor to ignore pets that weigh up to 40 pounds or 80 pounds. The IR sensor detects movement by thermal noise from the source which varies much more than threshold with an intrusion in the region of the sensor.

This motion sensor detects IR energy changes in multiple areas and then couples them for extremely accurate detections. Quad-zone Logic provides multi-segmented detection zones over the detection area. It is designed so that a human-size target will normally fill four to eight zones [11], and this will cause an alarm to be generated. Any smaller temperature change (i.e., small to medium-size pets, rodents or moving curtains) only activates one or two zones at the same time, creating a much weaker detection signal.

Using a noise reduction current, the 40 × 40 PIR/Microwave/Pet Immunity motion detector provides high-reliability performance against outside noise, such as electromagnetic interference and especially noise from fluorescent lights, thus solving a problem common to microwave motion sensors. Its Anti-Crosstalk System prevents interference from other microwaves if you have more than one detector in the area.

In Motion artifacts, it is known that the signal at an instantaneous time is likely to be corrupted by noise bursts, such as, for instance, a lightning flash (that could also be notoriously simulated by the intruder!). Dual sensors and cumulative signal processing would enable the detection of such artifacts but at double the cost. If the motion is detected without ambiguity, then the remote monitor will call for operator intervention who would then switch on to direct video observation of the site.

With ultrasound motion sensors, we get two signals in quadrature. By taking a combination of these with the Hilbert Transform, we can detect the motion direction. Let $e_{r,}$ e_q be the real and quadrature signals. Taking the Hilbert Transform of the second, we get

$$H\{e_q\} = e_q'$$

Adding and subtracting to e_r, we get the forward and reverse direction time signals.

Therefore, we can transmit the signal e_r and $e_{q'}$ as well as the Hilbert transform of e_r and e_q to the remote monitor for evaluating the movement and assessing direction and further inferences. In this process, we can also detect errors in the signal transmission, as we shall see in the next paragraph, which is an added advantage of this technique.

But transmission of the signal through a medium, say, by some form of radio telephony, is beset with errors of PCM data en-route. Then it means much more for these motion sensors than other direct sensors. A bit error in a stream will intimate a sudden change which will be interpreted as a movement caused by Doppler shift of ultrasound reflected. That is why some form of detecting errors has also to be included.

6. ENCODING OF SIGNALS, NEW METHODS

The Signal *s(t)* that is picked from the sensor is usually digitized and the value of the same is stored in, say, *N* bits, for each sample.

The principle is to take an encoded version of the signal, which uses the signal and its past samples, while transmitting to the distant monitoring site. This encoding is very much like the encoding used for sending GSM signals with convolution encoded data. The system of motion sensor along with this convolution encoding would be built at the site, along with the hardware of the sensor electronics. An example of such encoding by convolving with delayed signal components, would have a block diagram as shown below in a simple scheme with two delays. Actually GSM uses a convolution with a larger constraint length.

The signal is $x_{n,}$ in its n^{th} sample; this is combined with x_{n-2} in order to get y_n

$$y_n = x_n \text{ EOR } x_{n-2} \qquad ...(1)$$

Another bit that is transmitted is $z_{n..}$

$$z_n = x_n \text{ EOR } x_{n-1} \text{ EOR } x_{n-2} \qquad ...(2)$$

At the receiving end the signals are combined by a simple exclusive *OR* and we get the signal $w_{n,}$ which is same as $x_{n-1.}$ Two bits are transmitted for each data bit, see Figure 2. The decoding process at the received monitor would detect and correct errors using Viterbi's algorithm [12]. It is possible to detect errors present and to some extent correct the same.

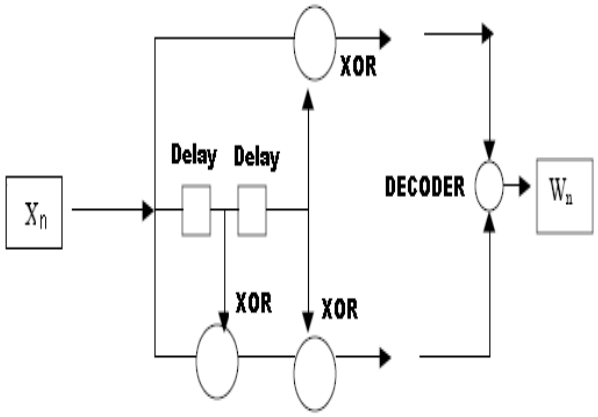

Figure 2 Sensor codes are also convolution encoded and transmitted.

The scheme works alright because only detection of errors is more important here rather than its correction.

There is yet another scheme which uses the improved (RS) Reed Solomon coding [13].This is useful for correcting bit errors in data by adding additional bits. The scheme is very complex using Galois field numbers. This has provision only for correcting a small number of bits in a total stream. If n is the data bits, *t* is the number of errors to be corrected, then *n+2t* bits will be total that would be sent by the RS encoder. Usually *t* is very small fraction of the total *n*. For example, the RS (255,235) code has 8% (20/256) of the transmitted message as redundant and it can correct ten errors. This scheme is very popular in general communications. But here, for security applications, this has one drawback. It cannot tell if the data is free from error. Though it can correct *t* errors in a total of *n+2t*, if there were more than *t*, it will give a wrong result. In security data, we can ignore a set of incorrect data rather than having it fully corrected; but we should not be informed with wrong data any time.

In the proposed method, the encoding does not suffer such a limitation. Suppose for the signal *s(t),* after digitization, its Hilbert transform is calculated, this gives the total signal as

$$s' = s_r + js_h \qquad \ldots(3)$$

Here, *s'* denotes the transmitted signal comprising of the real and imaginary parts of the signal. The imaginary part is obtained from the real part through the Hilbert Transform. The same is done using digital data with the formula given in (5). The first term in the above equation is the actual signal and the second is the Hilbert transform.

Therefore, the data bits which are transmitted will be double the actual signal data.

Thus, each bit of s_r is combined with the bit from s_j and a *dibit* is transmitted. This is having the same overhead of 1:2 like the convolutional encoder.

The property of the Hilbert transform is used at the reception data processor. If we take the Hilbert Transform of the latter signal s_j, we get the negative of the real part signal, giving

$$H\{s_j\} = - s_r \qquad \ldots(4)$$

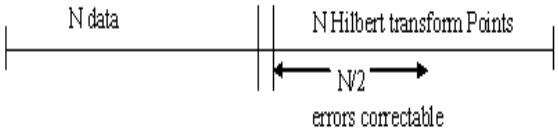

Figure 3a showing the data and parity symbols in the newly developed H.T. coding.

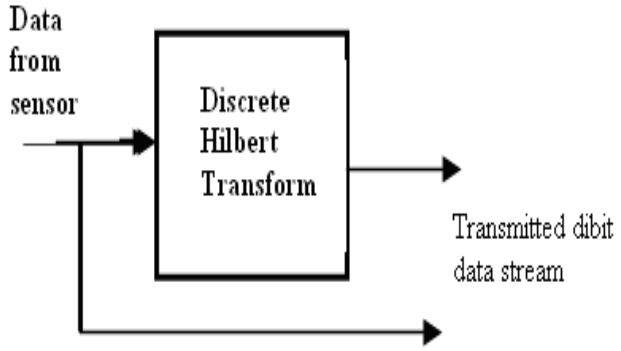

Figure 3b Hilbert transform based data encoding for motion sensors

So, after collecting the data, its Hilbert Transform is also evaluated see Figure 3b.The *N* Hilbert transform values of *N* data are calculable directly as an (FIR) Finite Impulse Response equation and the matrix of calculations for finding the transform can be shown [14] as

$$y'_n = \sum_{j=1}^{N} C_{j+n-1} y_n \qquad \ldots(5)$$

The *y* is data (discrete form) and y' the transform, while the *C* coefficients are a cyclic set of values,

Also, $H\{s_r\} = s_j \qquad \ldots(6)$

Taking for example, 256 samples of data, the same number of data which are obtained by transforming the former, will make for total data of 512 samples, which is treated as a composite data while sending through the channel. In addition, convolutional data can be used for additional basic bit error correction.

Now, channel noise and interference will produce bit errors on the data, even after correction to the extent possible. Let us illustrate a sample data stream which is just a simple continuous analog signal. The same is digitized and after combining with the Hilbert transformed bits so that the total data stream has two bits for each actual sensor data bit. Suppose, there are random locations of bit errors which cause the value to differ in the received signal at certain sample locations. The signal and its transform are shown in Figure 5 (a-e).

Thus, a check is made on the above data bits by performing digital Hilbert transform, the data part as well as both the transform parts. From this, we calculate the syndrome by the following equations.

$$[a] \rightarrow a_e$$

The data *a*, gets corrupted as wrong data set a_e.

$$[b] \rightarrow b$$

The other parity part b is the Hilbert Transform of *a*, which also gets corrupted. Denote *H* as the Hilbert transform operator,

$$\text{Evaluate } [s] = H\{H(b)\} + [a] - Mean[a]$$

This *[s]* is the syndrome of the errors received in $[a_e]$.

This is plotted in Figure 4 for this sample data set.

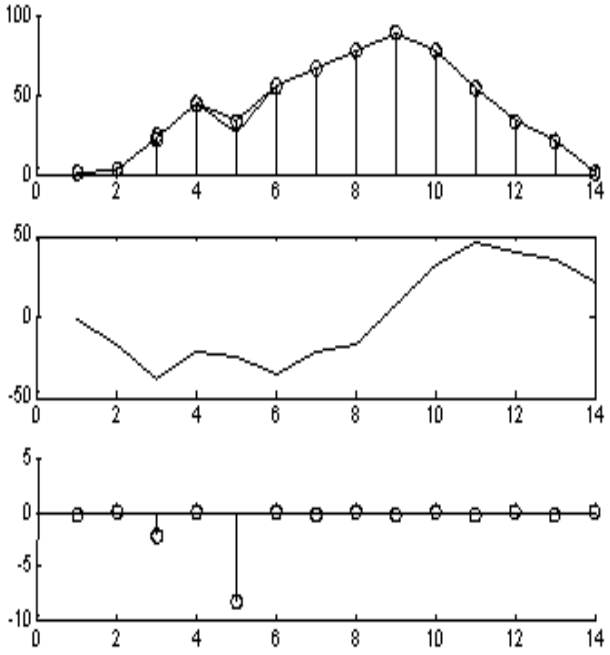

Figure 4 a) Data set plotted, showing error point at (5).
Figure 4 b) Showing Hilbert Transform of data as received.
Figure 4 c) The syndrome shows exactly where errors have occurred.

Thus, it is inferred whether the data is free from corruption in the transmission channel or not. If the equation is non-zero at certain time slots, these time slots could have erroneous data bits. Since some of the data slots are known to be erroneous, ignoring these data bits, the rest of the data is examined for a change from a previous data set for detection of real motion effect. The sensor electronics itself could be using an embedded controller, in which case, the output of the sensor could transmit a combined data set as per equation (3).

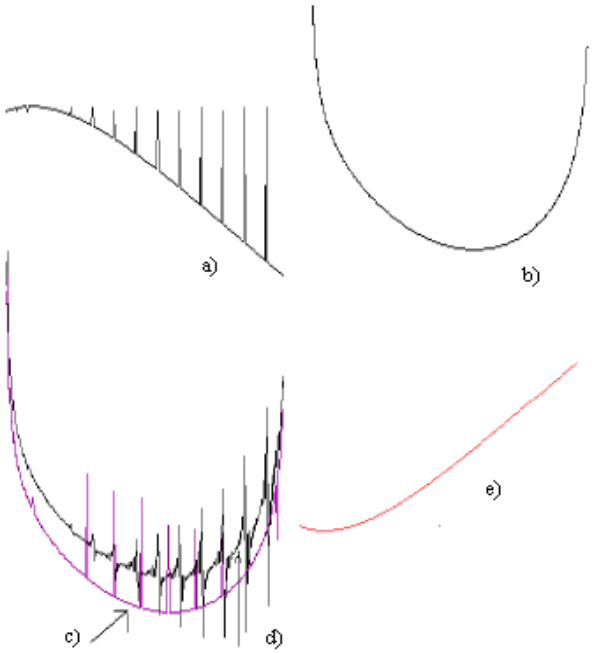

Figure 5 Showing methods of error detection and correction in the Hilbert Transform coding Scheme.
a). Sample segment of signal with bit errors.
b). Hilbert Transform of original signal, as transmitted.
c). Hilbert Transform of received signal part.
d). Hilbert Transform component of the received signal.
e). Transform of corrected Hilbert transform, the negative of signal itself.

Thus, by a suitable encoding technique, it contributes to the overall system reliability.

7. INTRUDER INTERVENTION – IMAGE DATA

Information is often transmitted with a view that security allows a transmitter to send a message to a receiver without the message being detected by an intruder or be disturbed from reception by jamming by a purposely introduced noise signal. Today, any of the mobile communication receivers can be inactivated by properly jamming the select region with high power jamming techniques [15]. A portable cell phone jammer featured by universal and handheld design, could block worldwide cell phone networks within 0.5-10meters, including

GSM900MHz, GSM1800MHz, GSM850MHz/CDMA800 Hz and also 3G networks (UMTS/W-CDMA).

We need definitely techniques to combat jamming in these security maintenance systems, because it is easy for an intruder to jam the signals passed from the monitoring station before he intrudes into the area. It would take time for the monitoring station to understand that jamming has been introduced in a particular home or location, by which time the culprit would have escaped after gaining his objective.

There is no better technique than spread spectrum communication which is proof against jamming. Among the two schemes available, the frequency hopping technique is more useful see Figure 6.

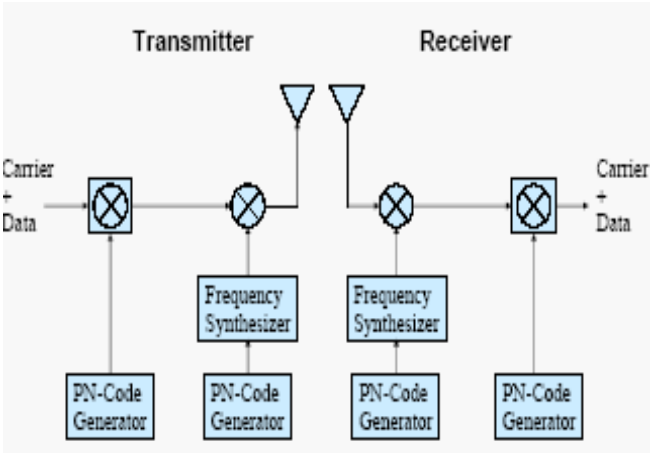

Figure 6 The principle of spread spectrum communication as useful for security monitoring systems.

While the scheme is by itself satisfactory only for en-route jamming, it is not quite satisfactory for jamming from near the site. Further techniques have been investigated by the authors for such a purpose [16].

8 WAVELET TRANSFORMED SPREADSPECTRUM

In Wavelet decomposed spread spectrum, we take the signal *s (t)* and first convert it into wavelets at different frequencies (scales) and time grids as *C (a,b)*. Then, we transmit each of these in different frequencies as a spread spectrum signal. In frequency hopping spread spectrum technique, the signal is sent at different frequency bands as decided by a random PN sequence.

Whatever are the advantages in the conventional Frequency Hopping technique, they are improved when wavelet decomposed signal packets are spread and transmitted [17].

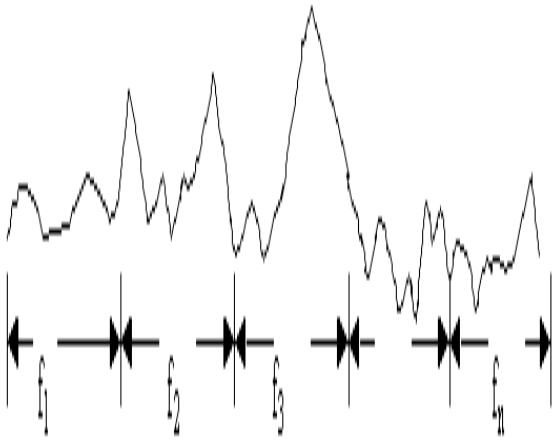

Figure 7 Spread spectrum uses hopping frequencies.

The spread spectrum signal is available at different frequency bands at all times (Figure 7).

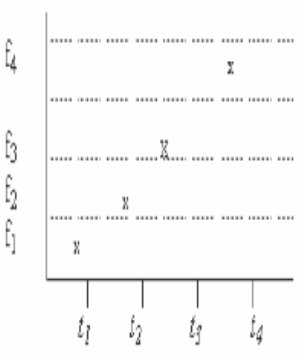

Figure 8a

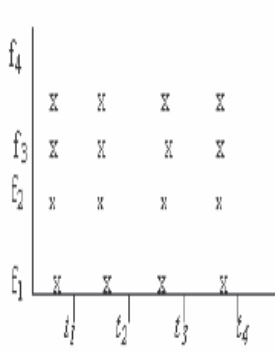

Figure 8b

Figure 8a shows the presence of signals at different frequencies at different at time slots. Figure 8b Wavelet based spreading has signals in all frequency bands at all times.

With the method of sending each wavelet scale in one frequency band, we have the signal available in all the spread frequency bands.

To retrieve the signal back in Figure 8a, we simply take the signal at different time slots, do a filtering with the PN sequence and integrate over a bit time to get the bit value.

If the signal gets jammed in one or more frequency bands, as in Figure 8c (by? code), the probability of error is high at time slots t_2, t_3.

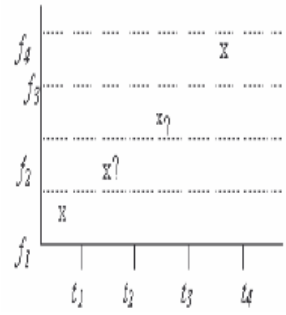

Figure 8c

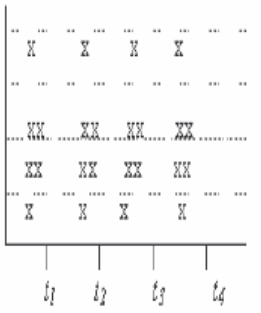

Figure 8d

In Figure 8c The time slots t_2, t_3 are noisy signals caused by jamming. In Figure 8d here, with wavelets at each band, all time slots are noisy in f_2, f_3.

But, in *(d)*, when two bands (f_1, f_2) are noisy and jammed, then at all times we get only noisy signals at the two bands f_1 and f_2.

However, the signal is only partly contained in these bands. When we do the wavelet reconstruction of the signal at the t_1 time slot, we get the erroneous output as

$$s(t)_{t_1} = \sum_{a,b} \{\mathbf{dwt}(a,b) + N(b)\}\psi(a,b) \quad \ldots (8)$$

where the *dwt* (a,b) corresponds to the (discrete wavelet decomposed) signal at the band *a* at all time slots (*b*) and N(b) denotes the noise time signal at the time slot *b*, while the function ψ(a,b) is the wavelet function chosen.

8.1 IMAGE DATA FROM LOCATION

The data of an image is coded and sent usually. There was a jamming as shown in Figure 10b, while Figure 10a shows the actual image.

In the method of wavelet based spread spectrum, the image is converted into 2-D wavelet data. The wavelet coefficients for the first level are denoted as:

Ca1, Ch1, Cv1 and Cd1.

These are the wavelet coefficients known as approximate coefficients and detailed coefficients. *Ca1* is the first level approximate coefficient.*Ch1* is the horizontal detailed coefficient; *Cv1* the vertical detailed and *CdI* the diagonal detailed coefficient.

If the image is *256× 256*, the first level coefficients above will each be of size *128 × 128.*

Then, a second level wavelet 2-D *DWT* decomposes the same into a set of further four coefficients

Ca2, Ch2, Cv2, Cd2.

Note that the Ca2 is the second level approximate Coefficient; the others are second level detailed coefficients. The Ca1 is not necessary for reconstruction, if the above four are given.

Thus, the picture or image of 2D DWT coefficients occupy a matrix of size 256 × 256 by stacking the elements of the above *7* coefficient matrices.

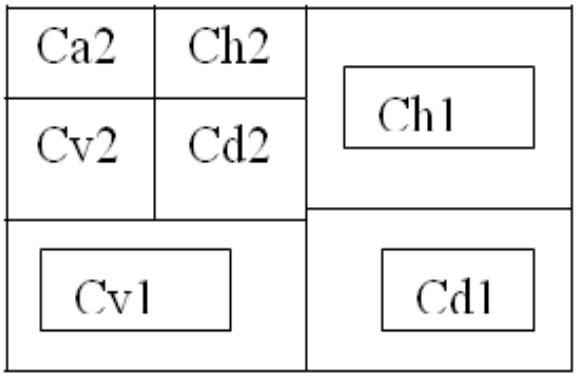

Figure 9 Wavelet coefficients for site image data shown in Segments.

The above matrix is also the same size as the original image for some of the wavelet transforms such as db1 or Haar, but its size will be slightly larger for other wavelets.

The data from the above matrix is got conveniently by tacking the row data and column data into a linear vector. This vector is *65536× 1*. This vector is what is fed to the communication receiver.

Suppose the jamming occurs in this data stream, then what would the above matrix look like (?). It will be jammed at the exact locations as shown in Figure 10b. Thus Figure 10*c* shows this.

Then, this data is used by the receiving communication system. It converts the stream of data thus jammed. Then, the image is got by an inverse 2-D DWT process by equation (8). This gives the matrix image of reconstructed data, though jammed en route.

This image is decoded and shown in Figure 9d There is evidently loss of detail due to smear visible at a few locations in this, but not so many as in the image jammed by the direct jamming as in Figure 10b.

The information as to how much improvement in the process of reconstruction against jamming is given by summing up the pixel errors for the entire image. Thus, if

the image original and the image got after jamming shown in Figure 10b is considered, we get an error. But if we do the same with the Figure 10d image, we get error less than the first one.

The ratio between the two errors is varying between 7 to 14 for several images and several kinds of patterns of jamming.

This method, therefore, combines data encryption (because wavelet information is not visible as any meaningful image) as well as error detection. If an image is in error, it might indicate an intruder for instance. Erroneous image received might be subject to false alarming. Here, we can identify errors in data clearly, while maintaining image secrecy [18].

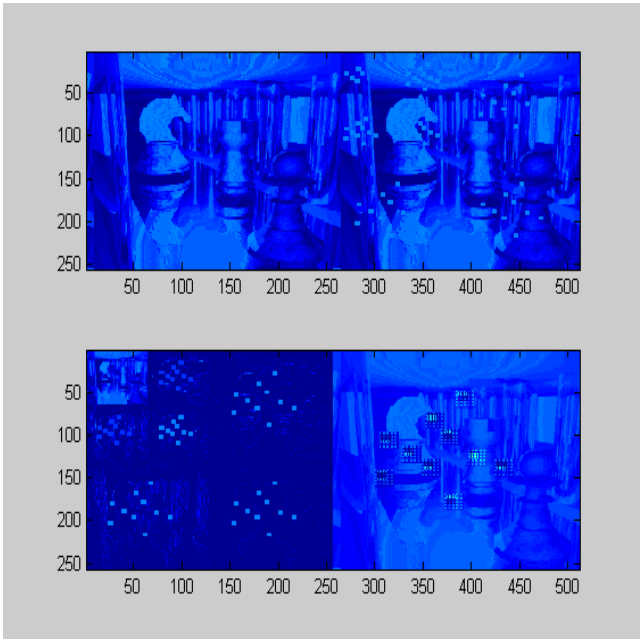

Figure 10a *(Top* left) Shows original image.
Figure 10b (Top right) Shows erroneously received image
Figure 10c (Bottom left) Wavelets
Figure 10d (Bottom right) reconstructed image, showing that data had met with errors.

9. CONCLUSION AND SUGGESTIONS

Data collection from site [19] and transmission for remote monitoring were discussed. Among the several sensors, a method for dealing with motion Doppler sensors was described.

Also, data communication with encoding using the Hilbert transform was considered for detection of errors in data. Clear detection of a motion event due to any intrusion is one of the major criteria in intruder detection. The method based on the Hilbert transform encoding was shown to be better in several respects, compared to the Reed Solomon type of encoding.

Data of images are better handled by wavelets. Spread spectrum communication which is the choice for remote security management can benefit from sending images in wavelet coefficient encoding. This not only does some compression but also provides secure image decoding and error detection.

Security system remote monitoring has been discussed in the context of protecting a living environment so far. Other environments include plant and process units in factories.

In process plant units, data management and control schemes are involved for operating the several plant items like motors, compressors, boiler, reaction vessels and so on. In mechanical plant, there would be robotic assembly lines handling jigs and fixtures. In these situations, security aspects are concerned with data mismanagement by intruders.

With computer based controls all over, the computer data are fed to process units through PLC modules to fix the set values of operating levels of each equipment. It is possible to add units for remote transmission of process variables from every such unit, such as the temperature, pressure, concentration, flow rate etc to the remote station with the plant Identifier code juxtaposed at periodic intervals.

Intrusion herein can be done with undesirable intentions to mal-operate the plant by altering the set values or process variable data. Since most plants of these kinds work under a bus scheme like the Profibus^{R}, security aspects should be incorporated in these schemes of plant control, with remote monitoring of the data. Schemes for key encrypted handling in such fieldbus control are discussed in [20]. The method uses one of the bits in the protocol to provide for such encryption.

As to the pros and cons of totally local management of security problems versus totally remote monitoring, there are several issues to be thought of. Wherever a security site is fully managed by local system, the problems of communication and jamming by intrusion is avoided. Remote monitoring helps in assessing the integrity of the security system by periodic checks on its inside hardware, which is not feasible with all local monitoring. Remote monitoring is ideal for multiple sites as the cost is distributed among them. Security of several plants located at different sites and handled by a single remotely monitored system is helpful for interactive management among the plants.

There is good scope for development of sensors with built in remote transmission through some form of RF communication with encryption. There is likewise a need for separately developing communication protocols similar to the ones employed for cellular telephony particularly for process plant management. Emphasis can be made on error free data communication even with greater redundancy than used in general communication schemes for absolute error free data collection, which is absolutely important in any security system management.

Future systems should examine and standardize sensors free from artifacts and develop methods for communication. Emphasis must be on detection of errors and possibly correcting them to the extent possible by all known methods of redundant data encoding.

References

[1]. R.Hariprakash, G.Venkat Ramu, T. Rajakumari, S. Ananthi, and K. Padmanabhan: "Some Problems & Methods for Remotely Controllable Automatic Home Security Systems" presented at ICSNC.2008.41, pp. 400-403 , 978-0-7695-3371-1/08©2008 IEEE.

[2]. Security systems and Devices ", controlelectronic.com

[3]. *x*10.com/security Systems

[4]. Abu-El-Quran, A. R., and Goubran R. A: "Security Monitoring Using Microphone Arrays and Audio Classification", Proc. IEEE Conf., IMTC 2005 pp. 1144-1148, May 2005.

[5]. www.pulseliving.com- Advanced KNX/EIB and Z-Wave automation for homes and hotels.

[6]. Sony AIR-SA20PK Wireless iPod Whole-House S-AIR Audio System smarthome.com

[7]. K. Holford, "Microwave intruder detection", Wireless World, Vol.86, pp. 34-40.

[8]. Rob Siegel, "Land mine Detection", IEEE Instrumentation and Measurement Magazine, Vol. 5(4), pp. 22-27, 2002.

[9]. B. Moshiri, A. M. Khalkhali, and H. R Momeni,: **"**Designing a home security system using sensor data fusion with DST and DSmT methods", Proc. of the 10th IEEE Conf. on Information Fusion, July 2007, pp. 1-6, ISBN: 978-0-662-45804-3**.**

[10]. "GSM phone for remote control", Elektor India, March 2002.

[11]. "Pet-Immune IR/Microwave Motion Detector Eliminates False Alarms" Optex Product No.: MX-40PI, UPC: 788924082486.

[12]. R.J.Mc. Eliece, R.B Ash and C.Ash, "Convolution encoding and Viterbi's algorithm", Chapter-6, Introduction to .Discrete Mathematic, McGraw-Hill Intl., 1989.

[13]. M. Sudan, "Decoding of Reed Solomon codes beyond the error correction bound," Jour. of Complexity, vol. 13, pp. 180–193, 1997.

[14]. Cizek.V:"Discrete Hilbert Transform", I.E.E.E. Trans. on audio and Electroacoustics", Vol.18(4),pp. 340-44, 1970.

[15]. blog.tayx.co.uk/2008/03/10/cell-phone-jammer.pp.682

[16]. T. Rajakumari, S. Ananthi and K.Visalakshi, "Use of Hilbert Transform Data encoding for spread spectrum communications", Presented at the Intl. Conference on Advanced Telecommunications , (AICT2007) Organized by IEEE at Mauritius , May 13-19, 2007

[17]. Sonia Grgic, Mislav Grgic and Branka Z-Cihlar, "Analysis of image compression using Wavelets," IEEE Trans. Indl. Elec. 48(3), 2001.

[18]. S. Ananthi, R. Hariprakash, V.Vidya Devi and K. Padmanabhan "Spread Spectrum Communication Using Wavelets of Signal for More Security", Proc. of the Advanced International conf. on Telecommunications, (AICT/ICIW2006), pp. 87,19-25 Feb' 06 at Guadelope, (0-7695-2522-9/06 © 2006 IEEE).

[19]. Texas Instruments Data manual: "Converters - Analog to Digital (ADC) 12Bit 50KSPS I2C Lo-Power 8Ch MUX Converters", SBAS181C – Nov' 01 - Revised Mar 2005.

[20]. P.Swaminathan, K.Padmanabhan, S. Ananthi and Pradeep.R: "The Secure Fieldbus (SecFB) protocol -- Network communication security for secure industrial process control", Proc. of the TENCON 2006, Hongkong, pp. 1-4, 1-4244-0548-3/06©2006IEEE.