Final Technical Report

Project Title: Low-Cost, Robust, Threat-Aware Wireless Sensor Network for Assuring the Nation's Energy Infrastructure

Covering Period: October 1, 2004 through March 31, 2007

Report Type: Final Scientific/Technical Report
Date of Report: June 27, 2007

Recipient: Eaton Corporation
Innovation Center
4201 N. 27th Street
Milwaukee, WI 53216

Award Number: DE-FC26-04NT42071

Subcontractors: Oak Ridge National Laboratory (ORNL) Wayne Manges
Electric Power Research Institute (EPRI) Dr. Ramesh Shankar

Contact(s):

Principal Investigator:	Carlos H. Rentel CarlosHRentel@eaton.com
Eaton Project Leader:	Peter J. Marshall PeterJMarshall@eaton.com
DOE- Project Manager	Robert Reed robert.reed@netl.doe.gov

Abstract: The objective of this project was to create a low-cost, robust anticipatory wireless sensor network (A-WSN) to ensure the security and reliability of the United States' energy infrastructure. This project has shown the feasibility of an intelligent wireless sensor network for the protection of electrical infrastructure.

DISCLAIMER

1. EXECUTIVE SUMMARY

Eaton, in partnership with Oak Ridge National Laboratory and the Electric Power Research Institute (EPRI) has completed a project that applies a combination of wireless sensor network (WSN) technology, anticipatory theory, and a near-term value proposition based on diagnostics and process uptime to ensure the security and reliability of critical electrical power infrastructure.

Representatives of several Eaton business units have been engaged to ensure a viable commercialization plan. Tennessee Valley Authority (TVA), American Electric Power (AEP), PEPCO, and Commonwealth Edison were recruited as partners to confirm and refine the requirements definition from the perspective of the utilities that actually operate the facilities to be protected. Those utilities have cooperated with on-site field tests as the project proceeds.

Accomplishments of this project included: (1) the design, modeling, and simulation of the anticipatory wireless sensor network (A-WSN) that will be used to gather field information for the anticipatory application, (2) the design and implementation of hardware and software prototypes for laboratory and field experimentation, (3) stack and application integration, (4) develop installation and test plan, and (5) refinement of the commercialization plan.

2. INTRODUCTION

Maintaining and upgrading the security and reliability of the Nation's critical infrastructure is of utmost importance for the defense and economic security of the United States. In particular, we must provide physical security for the energy system and energy supply as these form the fundamental critical infrastructure of this system. Recent terrorist attacks have increased concerns about willful attacks on the Nation's critical infrastructure. The importance of protecting the energy infrastructure comes from the fact that it serves as the foundation for all other infrastructures e.g. manufacturing, industrial, and services. *"The U.S. energy infrastructure is complex, aging, taxed almost beyond capacity, and vulnerable to acts of terrorism*. Our Nation's energy infrastructure consists of a diverse set of highly vulnerable systems. The U.S. Power grid has more than 200,000 miles of transmission lines served by four regional grids located across North America. The grid is divided into Electricity Generation, Transmission, and Distribution Sectors. These sectors contain a nationwide network of power plants fueled by natural gas, nuclear energy, oil, and coal, as well as a physical network of gas pipelines, refineries, communication systems, and substations. Each system and region has specific vulnerabilities and single points of failure, open to either a physical or electronic attack.

To address this national urgency, this project will create a low-cost, robust, Wireless Sensor Network (WSN) incorporating Anticipatory Technology to enable pervasive, real-time threat sensing as well as assessment and evaluation of the physical security of the Nation's critical energy infrastructure. The system will implement a threat-aware, self-configuring wireless network based on Low-Rate Wireless Personal Area Network (LR-WPAN) technology with a reasoning system capable of interpreting and integrating spatially and temporally distributed, multi-spectral data and asynchronous information while postulating assertions about threats using Anticipatory theory. The system will plan and execute reasoning profiles to support its hypothesis in a distributed fashion. The proposed multi-phase project plan uses modeling and simulation to deliver to the DOE quantifiable metrics for the network's performance including measures of robustness and effectiveness. The proposed technology will offer demonstrably superior performance to wired and other wireless alternatives while not adding any new vulnerability to the physical security of the energy infrastructure. Wireless sensor network technology fundamentally transforms the architecture of physical security systems by allowing ubiquitous distributed sensors to be cost effectively deployed throughout environment of the critical infrastructure. Advanced distributed algorithms using Anticipatory technology adaptively determine vulnerabilities and failure modes of the security system. Alternative, centralized intelligent systems are untenable due to the amount of processing power required and the variable system delays existing in geographically large areas. The Low-Rate Wireless Personal Area Network (LR-WPAN) is a new technology emerging from the communications revolution in commercial and industrial wireless sensor networks. Unlike Wireless LANs (WLANs), LR-WPAN is designed to convey information without requiring pre-established network setup. Self-configuration and multi-hop capabilities are key attributes of LR-WPAN that enable large scale, mesh type networks to be formed to cover long distances and provide redundant paths within large

facilities. LR-WPAN is ideally suited to perform sensing and serve as a platform for assessing and evaluating threats by incorporating anticipatory technology.

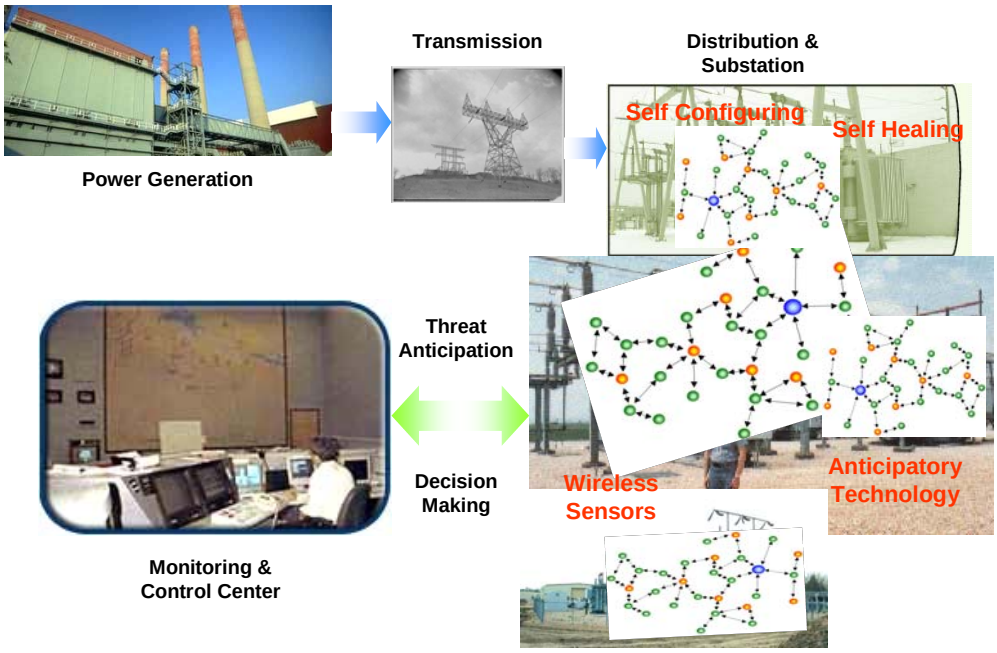
Wired solutions are not practical due to the large cost associated with deployment and maintenance. For example the cost of installing wires in a nuclear facility can be as high as $2000/ft. In a similar manner, non-LR-WPAN wireless technologies require large installation costs due to required configuration (by specialized personnel) and the need frequent maintenance. On the other hand, LR-WPAN technology was specifically designed for operation in industrial environments with enough features to allow for the creation of self-configuring mesh networks with a minimal cost on a per node basis and focus on enabling WSNs. IEEE 802.15.4 LR-WPANs use direct sequence spread-spectrum techniques to mitigate the effect of jamming and improve wireless communications reliability.

Anticipatory technology does not depend on repeating or preprogrammed patterns. Current pattern recognition technology does not work well since by definition terrorism is unpredictable. Anticipation, modeled after the human's intuition to reason, enables the system to begin to react even before the event starts to unfold.

Potential impact of the project: Current communications technology requires expensive and labor intensive approaches to assure integrity. Emerging technologies in communications offer the opportunity to protect without huge capital investment and impact on the supply conduits being protected (easily retrofitted). It has separate reporting channels, does not impact existing networks (already overloaded), can be deployed in a non-invasive way and could be used for other emergency situations. Self-configuring, self-healing LR-WPAN technology will allow retrofitting the Nation's critical energy infrastructure with a scalable and pervasive physical security sensor fabric that has the ability to detect threats in real-time. Eaton's Innovation Center (EIC) and Eaton Electrical (EE) Group expect to implement this technology broadly across non-nuclear electrical delivery assets as well as fuel processing and storage assets and delivery systems.

3. ANTICIPATORY THEORY - BACKGROUND

Intelligence is exhibited by a biological organism through its self-consistent reasoning mechanism that allows it to extract context- and environment-specific motive and intent. Similarly, within a collaborating system of intelligent agents each is self-aware and understands the local context within which it exists, the global implications of its actions, and its obligations as a member of the collaborative system. These cognitive abilities are an essential component and developing them for threat-evaluation applications is one of the basic goals of the proposed research. Reasoning abilities include the decision-making in a dynamic environment to be able to make informed reliable real-time decisions in the face of a dynamically changing process environment along with autonomous behavior to make decisions on its own or as part of a larger aggregate system.

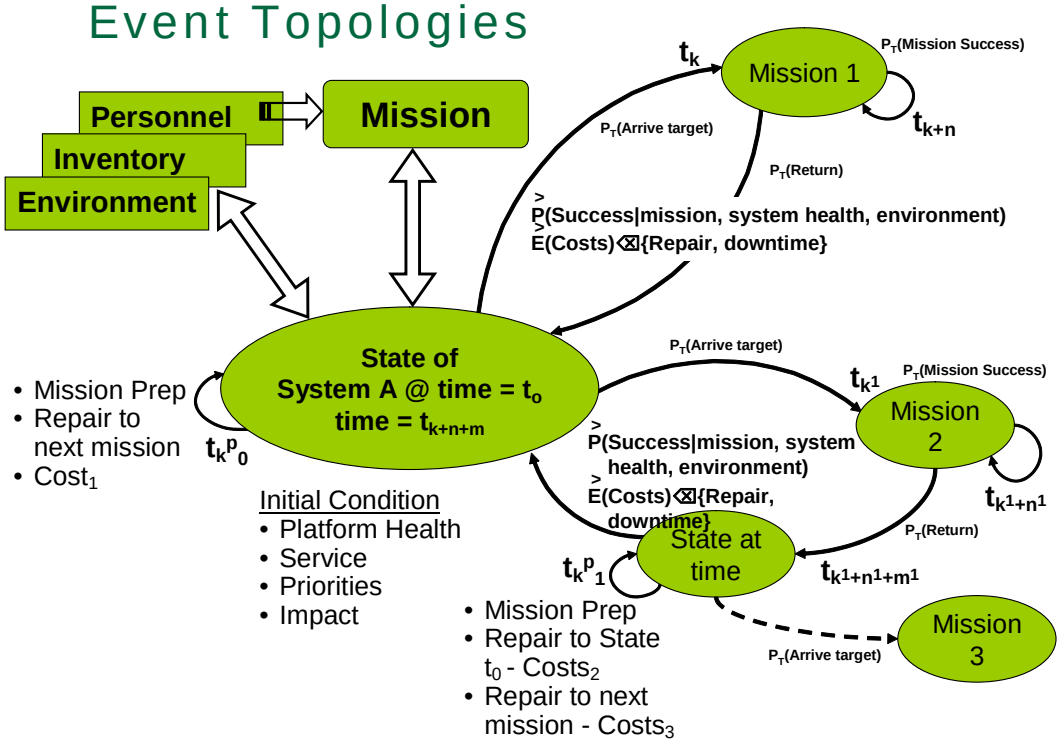


The above figure shows the process flow in the energy infrastructure and respective areas of the proposed technology implementation. The event topology is mapped in order to develop the anticipatory reasoning construct. This event topology must be at a level where aggregated behavior can be anticipated and analyzed in terms of threat prediction and risk assessment. The behavioral level system architecture is shown below:

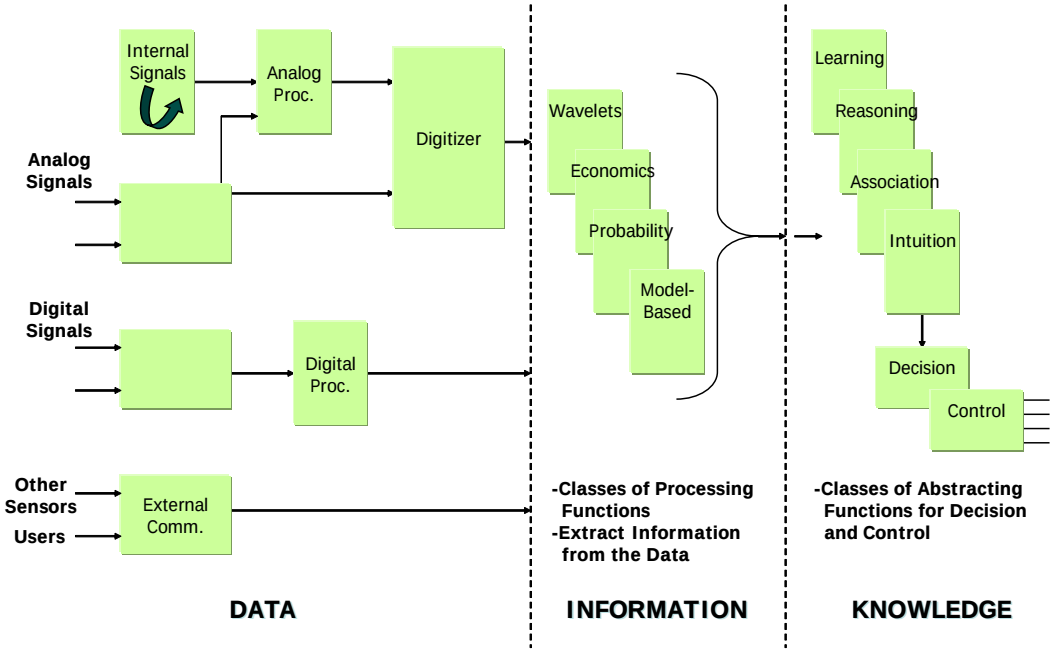
Decision Framework
Information Extraction from Sensors
Wireless Network

Conceptually, any reasoning system intended for use with network-centric information grids must have three key features. These are (1) cognitive software for aggregating and intelligently processing network-centric data to formulating hypothesis concerning threats, (2) supporting software to proactively acquire and preprocess network-centric data, and (3) an intelligent communications infrastructure to dynamically manage an ad-hoc network of geographically-disbursed non-homogenous information sources to obtain optimum stability regardless of traffic volume. Additionally, it would have to be formulated as a dissipative system; that is, be able to recover from anomalies and disturbances without impacting reasoning and confidence in any hypothesis or assertion. The information abstraction in any such network is illustrated in the following figure.

Event Topologies



Embedding Classes of Functions for Information Abstraction



4. RF SITE SURVEY OF ROANE COUNTY SUBSTATION

The purpose of this radio frequency (RF) survey is to empirically analyze the RF environment in the Roane County Substation and study the propagation characteristics by observing the received signal strength levels. The three different frequency bands chosen mainly are 902-928MHz, 2.4-2.4835GHz and 5.725-5.875GHz. These frequency bands correspond to the unlicensed Industrial, Scientific and Medical (ISM) bands, commonly used in current wireless networking technologies. The collected data will help understand the background interference and noise levels before the deployment of the desired wireless network and also help predict signal strength and related propagation issues.

Figure 1 shows the aerial map of the substation and the location of each of the measurement points. The measurement points are limited by the availability of working power outlets. The substation currently does not have any wireless sensor network installed but planned in the near future. The substation has antennae on top of its control room which appeared to be a microwave link to other TVA facilities. The details of the transmissions done over this links will be provided to the team shortly. Two calibrated test antenna, an Electro-Metrics rod/discone antenna and an EMCO horn antenna are used for recording the signals. These antennas were mounted on separate tripods and elevated. These antennas were then connected to the Aeroflex CS65040 Broadband Signal Recorder and Generator (hereafter referred to as the CS65040) and a Rohde & Schwarz FSH3 spectrum analyzer (hereafter referred to as the spectrum analyzer) that was controlled with LabView software. Losses of the test cables were measured prior to the tests.

While reviewing these results, it is important to keep the ISM frequency bands in mind, they are

- 902–928 MHz
- 2400–2482.5 MHz
- 5725–5875 MHz

We look for signals specifically in these bands and have marked their approximate locations on the plots provided as appropriate.

Notes About the Plots

The CS65040 plots provided are the result of replaying the signals that were recorded during the test. During the replay, interesting segments were captured for the report with a screen capture and inserted here as graphics. The plots provided show the spectrum along with a display of time recent to that spectrum. The spectrum is 130 MHz wide in all cases unless noted otherwise. This span, along with the center frequency and Resolution Bandwidth (RBW) is noted at the bottom of each plot.

Figure 1: Aerial View of the Roane Substation with the Locations Marked

The CS65040 analyzer has an anomaly that can be seen as two CW signals, one at –15 MHz from center and the other at +5 MHz from center. The signal at –15 MHz pulses; the one at +5 MHz is constant. They are present at these frequency offsets in all plots, in all frequency bands. These signals should be ignored.

The CS65040 spectrum plots provided show the instantaneous signal (in yellow) along with the result of a maximum hold (in green). Each sample taken with the CS65040 analyzer was the result of 400 million samples per second and was recorded for the duration of the memory limit of the analyzer which is 2.6 s.

The Rhode & Schwartz FSH3 spectrum analyzer is controlled by a laptop running LabView software. A customized script was used to scan the spectrum in five different bands for a total of 3 min per band. The bands are 150 KHz to 30 MHz, 30 MHz to 500 MHz, 500 MHz to 1 GHz, 1 GHz to 2 GHz, and 2 GHz to 3 GHz. This results in a complete scan from 150 KHz to 3 GHz over a 15-min scan window. The laptop records the frequency and power level at designated increments and records the maximum signal presented during the 3-min scan. The RBW is 100 KHz.

4.1 CS65040 Results

Signals captured with e CS65040 analyzer are shown in the figures 2 thru 14. Notes are included on each plot and items of interest are highlighted. At the end of the section, a summary table is provided to summarize these highlights.

Location 1: **In Front of the Control Room**
Elevation: 803.5 ft
N 35° 56.660'
W 84° 23.337'
Figure 2 shows a significant activity in 500MHz band and looked like a paging system in two channels at ~ 460 MHz. The noise floor in this band is about -70dB. Figure 3 shows the 900MHz band. This appears to be clean in the ISM band. It could be a good choice for wireless network considering the better propagation in this band. Figures 4 and 5 show the band of interest, 2.4 GHz, with a resolution bandwidth of 20KHz and 100KHz respectively. There is significant usage at either ends of the 2.4 GHz ISM band. The average noise floor is around -80dB with peak transmissions as high as -55dB. The spectrum shows the activity in channels centered approximately at 2405, 2450, 2475MHz. Figure 6 shows the channels of the 802.15.4 and 802.11b radios. The use of 802.15.4 radios should avoid the above mentioned channels for efficient operation. These observations calls for further investigation of the BER and PER measurements of the Eaton nodes intended to be used in the project for deriving optimal co-existence conclusions.

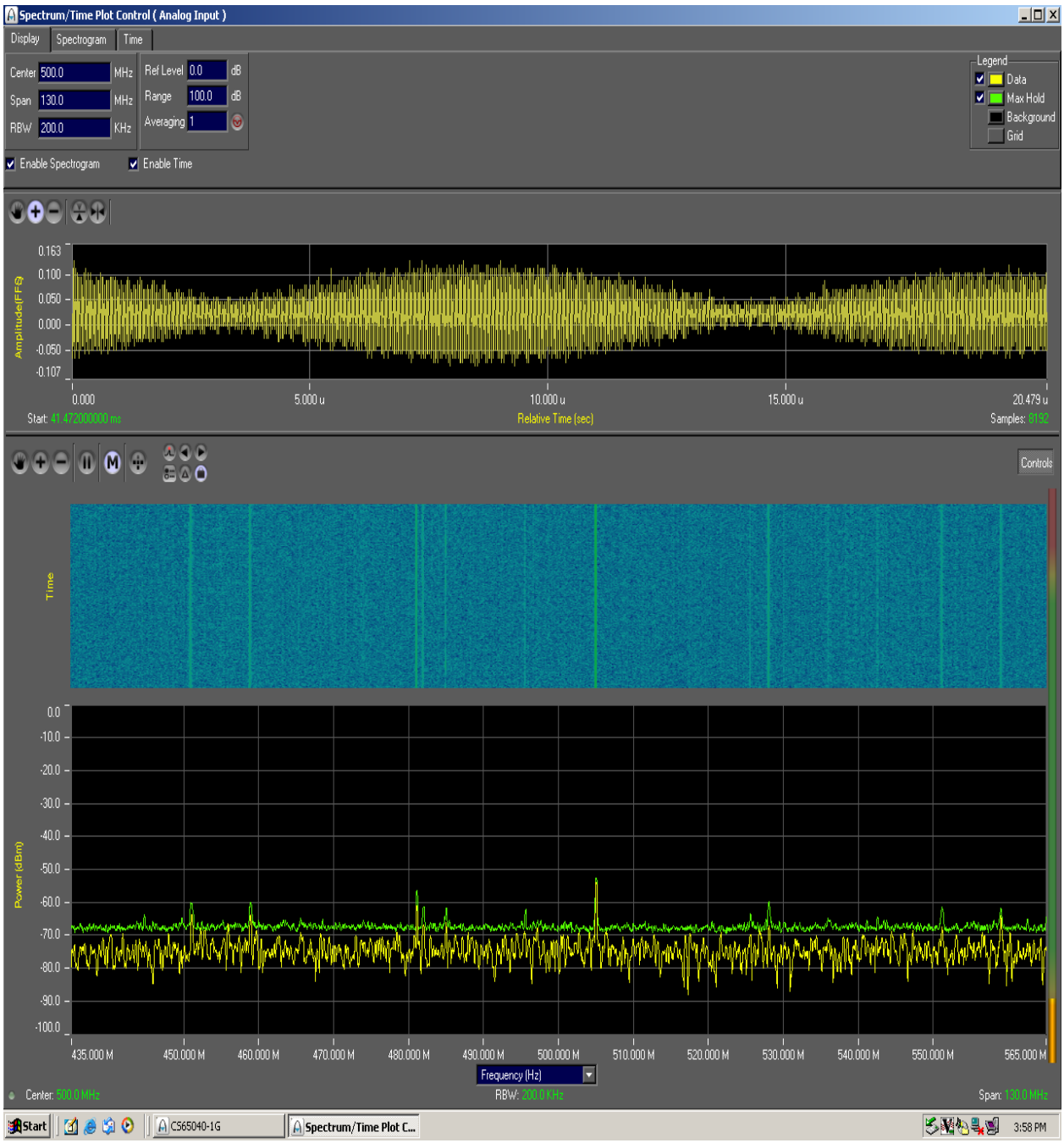


Figure 2: Plot centered at 500 MHz, 200KHz RBW

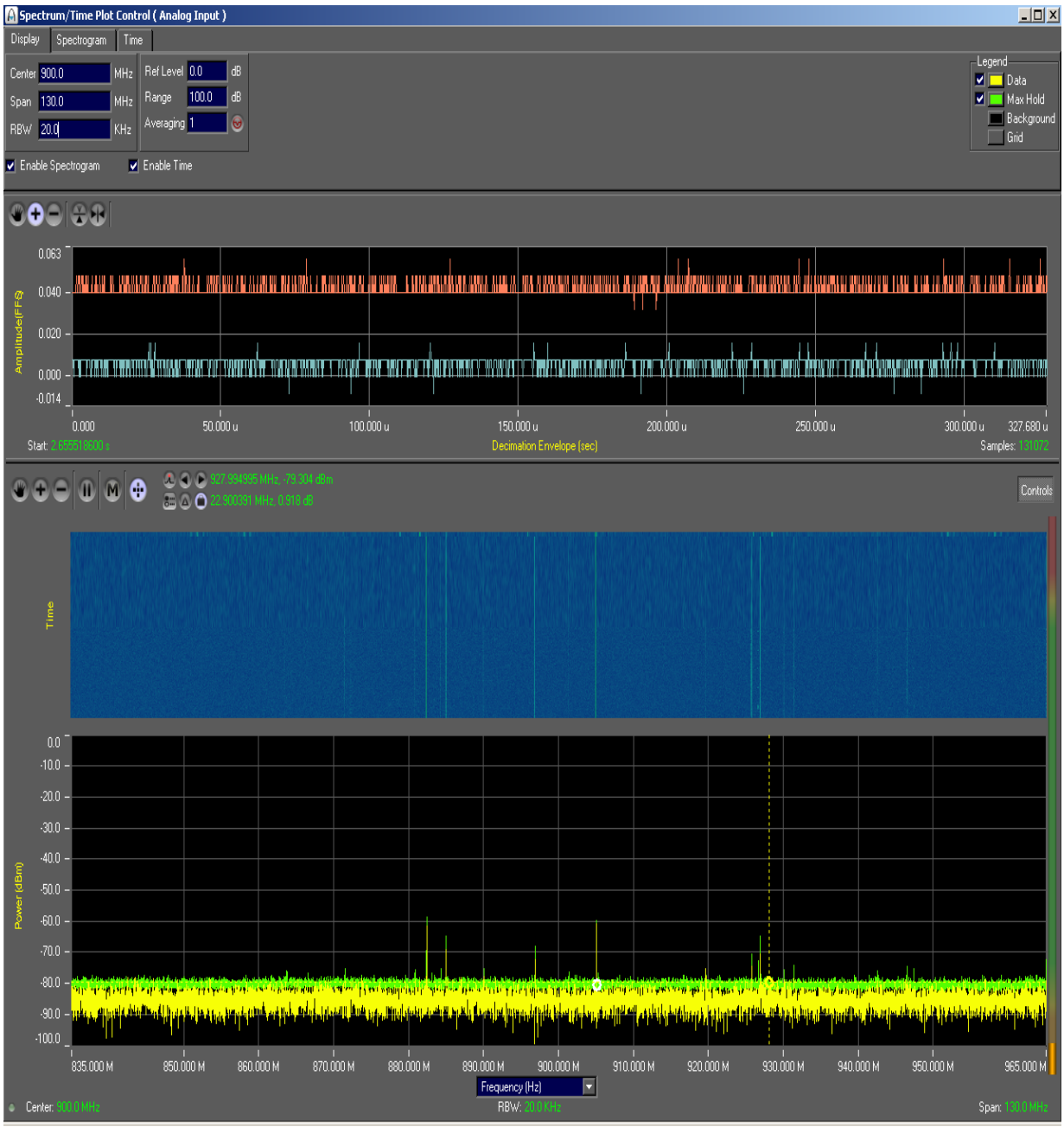


Figure 3: Plot centered at 900 MHz, 20KHz RBW

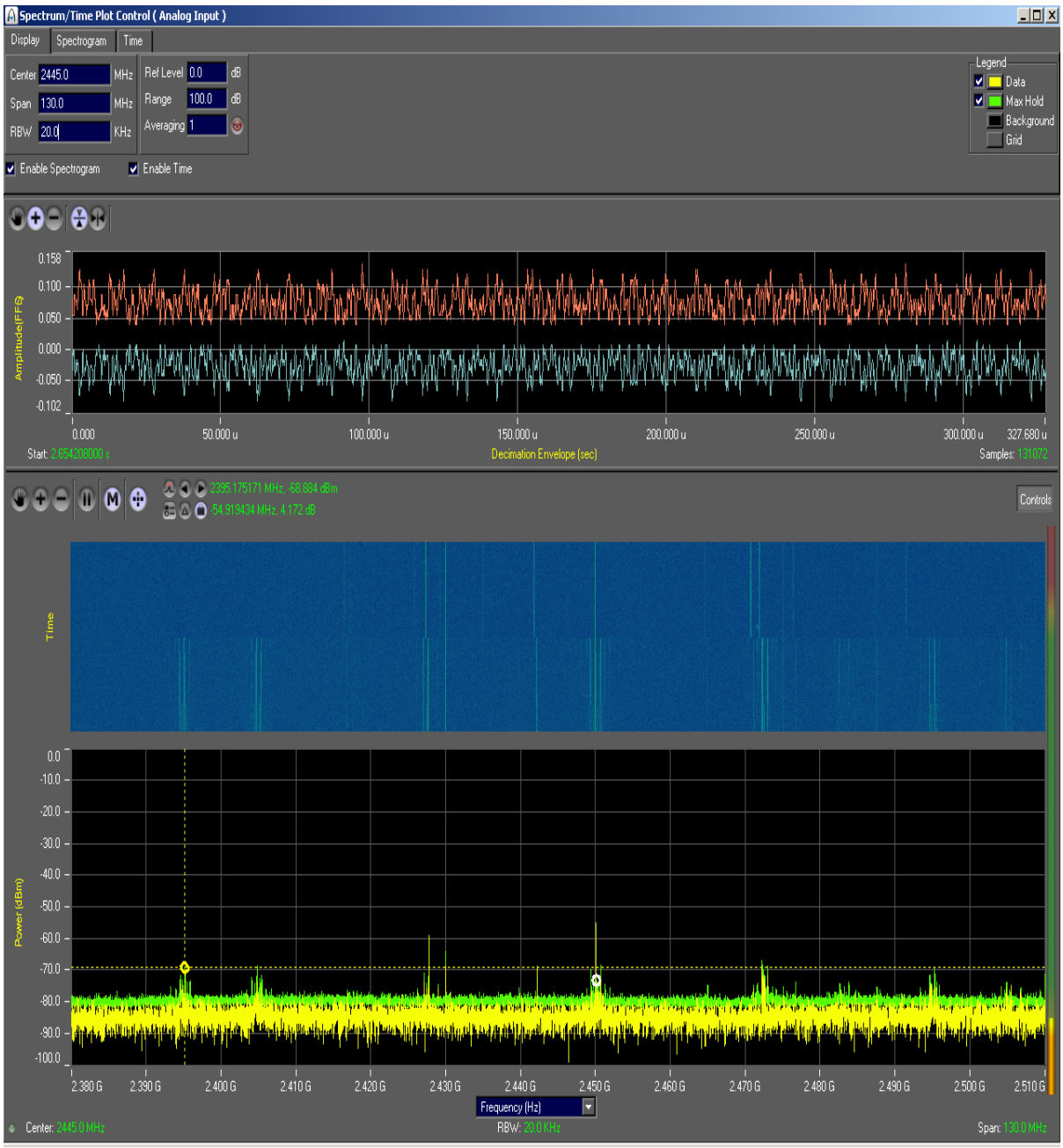


Figure 4: Plot centered at 2445 MHz, 20 KHz RBW

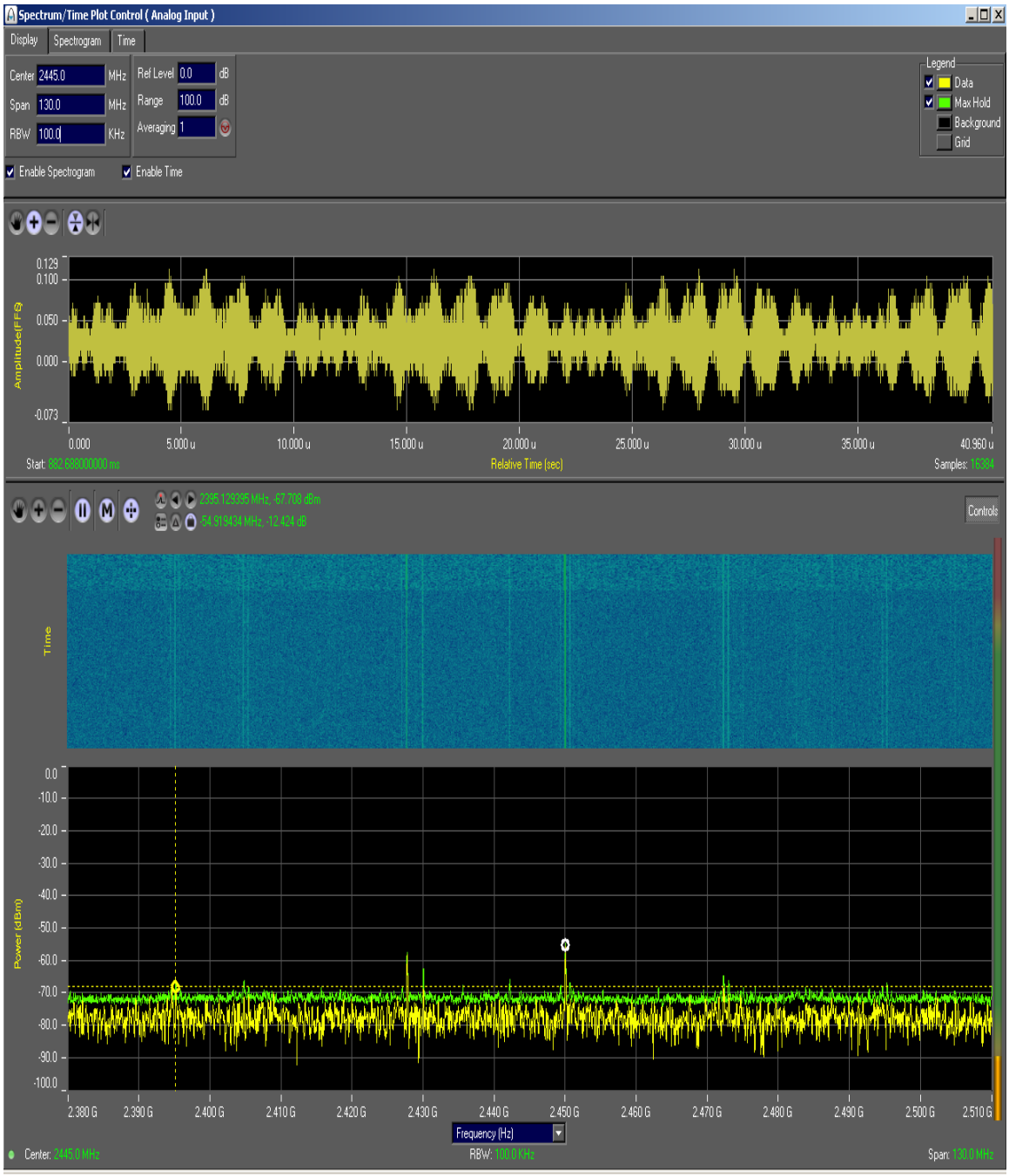


Figure 5: Plot centered at 2445 MHz, 100 KHz RBW

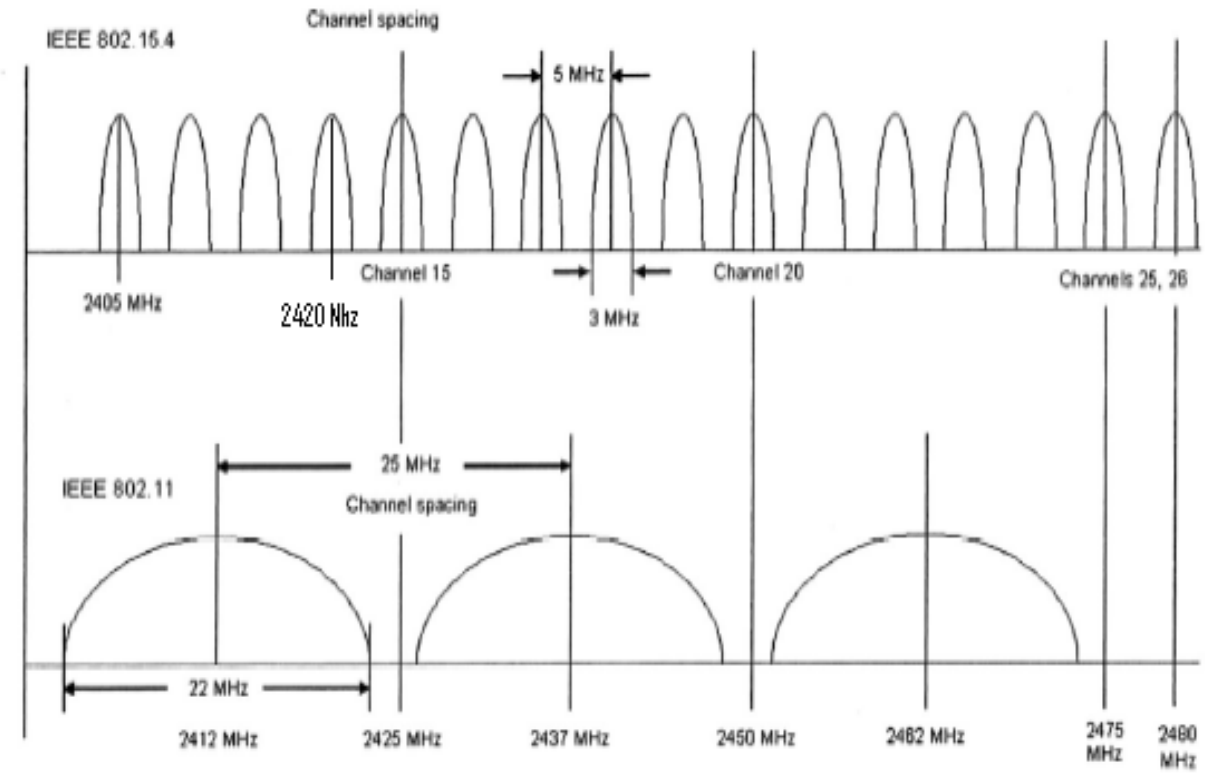


Figure 6: Channels of 802.15.4 and 802.11b radios

4.2 Location 2: Near 500V direct feeds

Elevation: 785.4 ft
N 35° 56.693'
W 84° 23.314'

Figure 7 shows a significant activity in 500MHz band and looked like the same paging system as observed in location 1. The noise floor in this band is about -70dB. Figure 8 shows the 2000MHz band. There is significant activity in ~ 1980MHz which is close to PCS cellular communications. The microwave link in the substation could be using cellular service for communications (the confirmation of which will be done with TVA). Figure 9 is a plot showing the activity in the 1500MHz band. Figure 10 shows the 2445MHz band with activity at 2445MHz and 2500MHz. The interference shown at this location is not same as location 1. Figure 11 shows the 5.8GHz band which is very clean with a noise floor of -70dB.

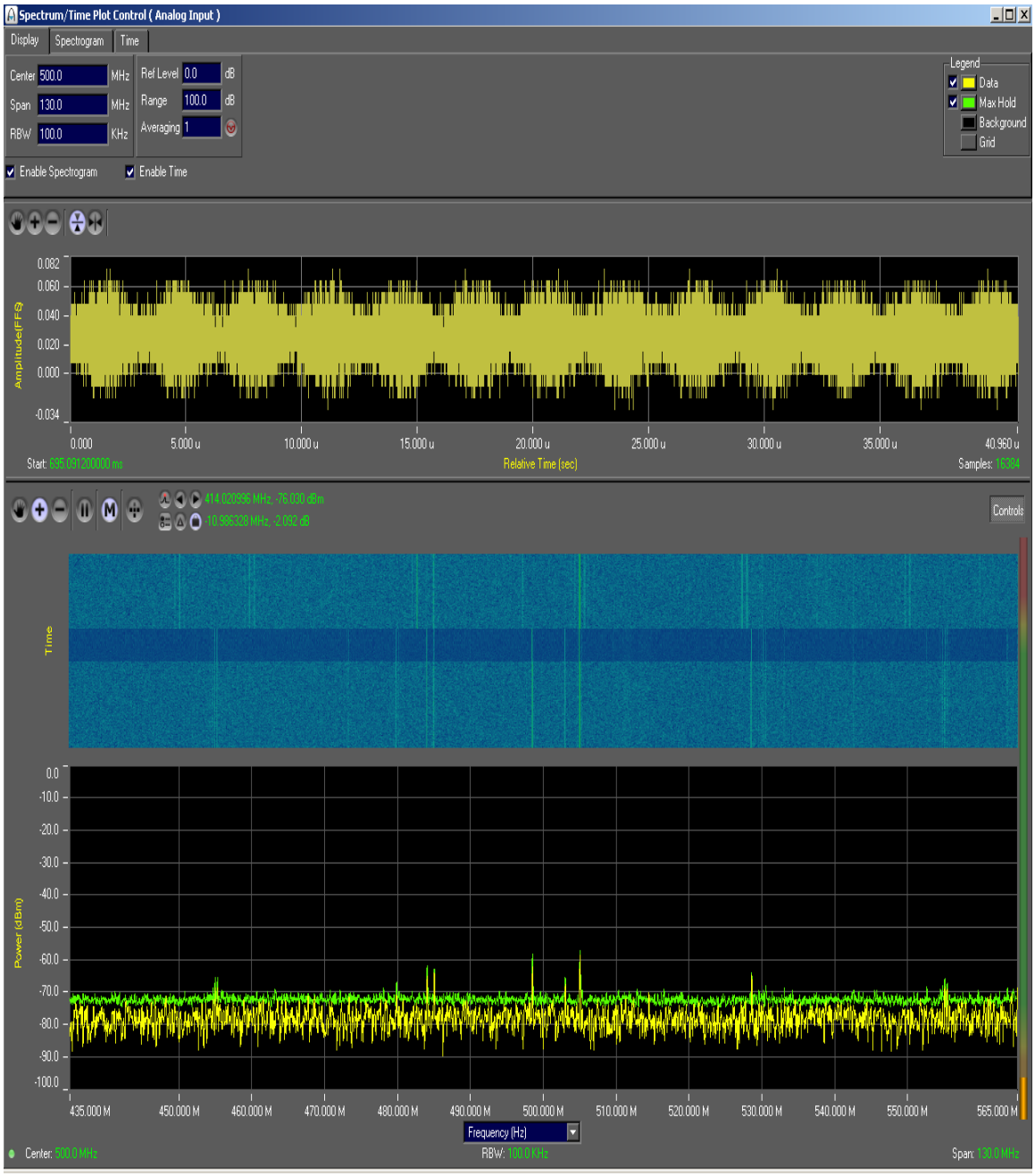


Figure 7: Plot centered at 500 MHz, 100 KHz RBW

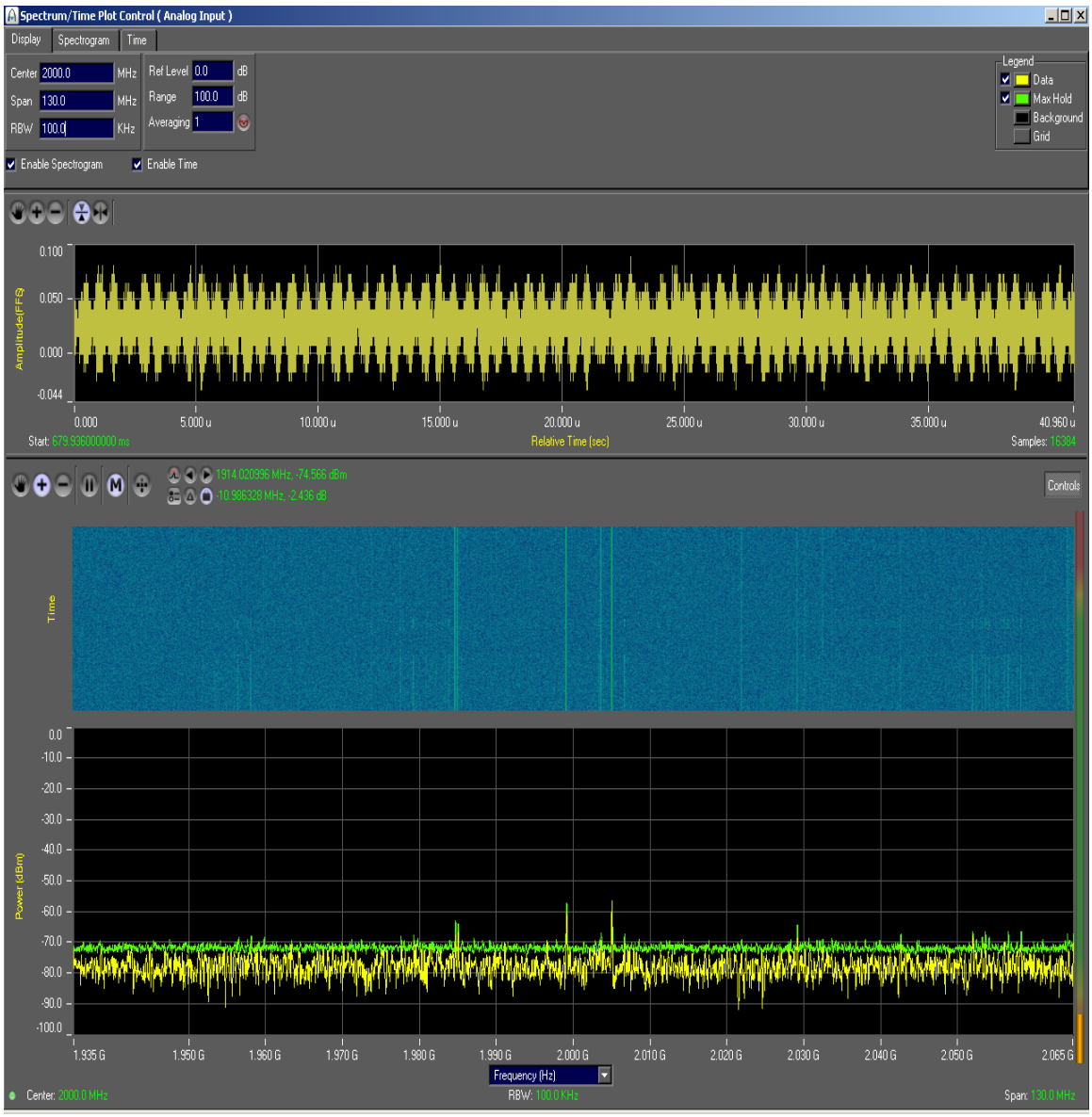


Figure 8: Plot centered at 2000 MHz, 100 KHz RBW

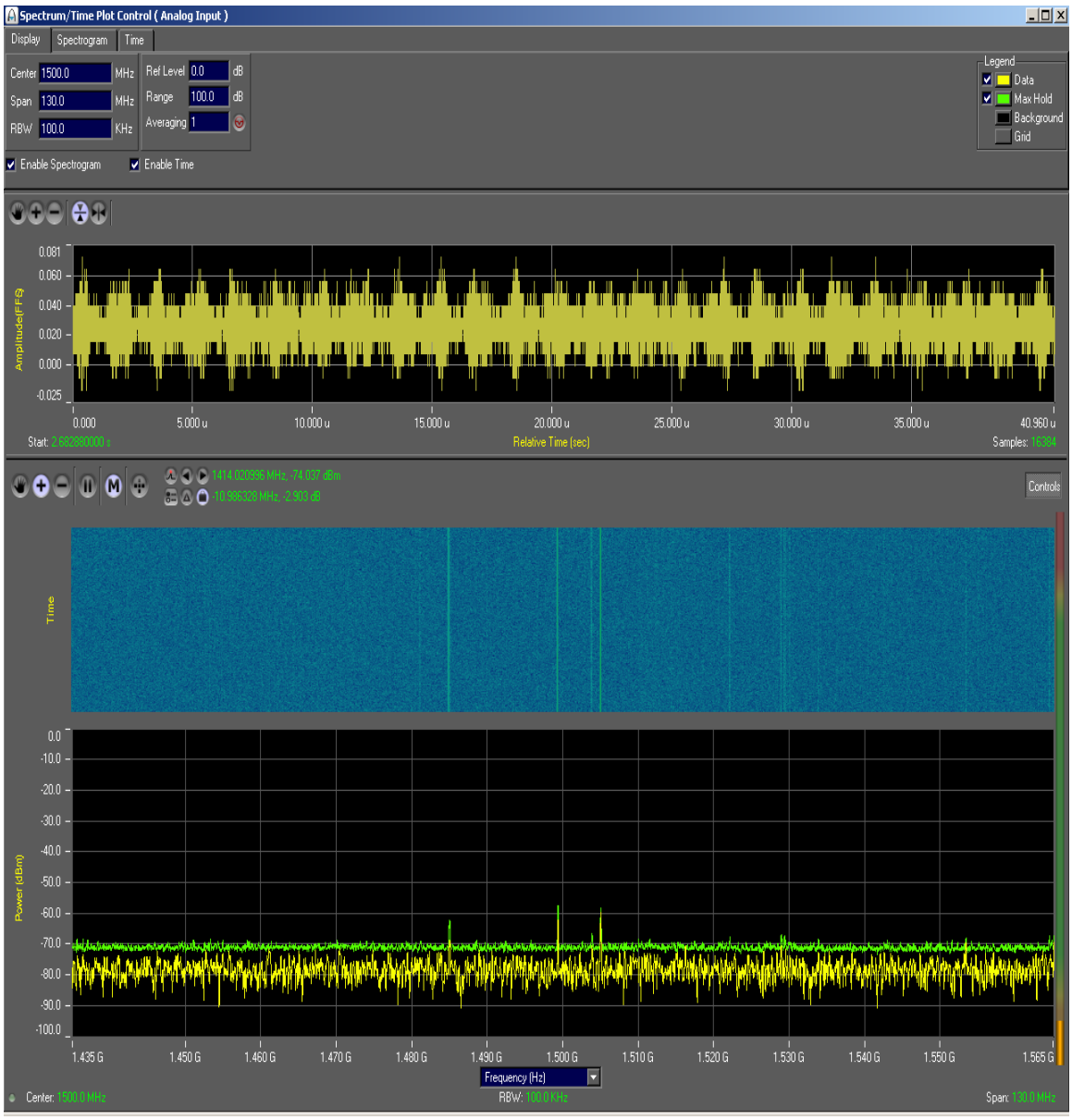


Figure 9: Plot centered at 1500 MHz, 100 KHz RBW

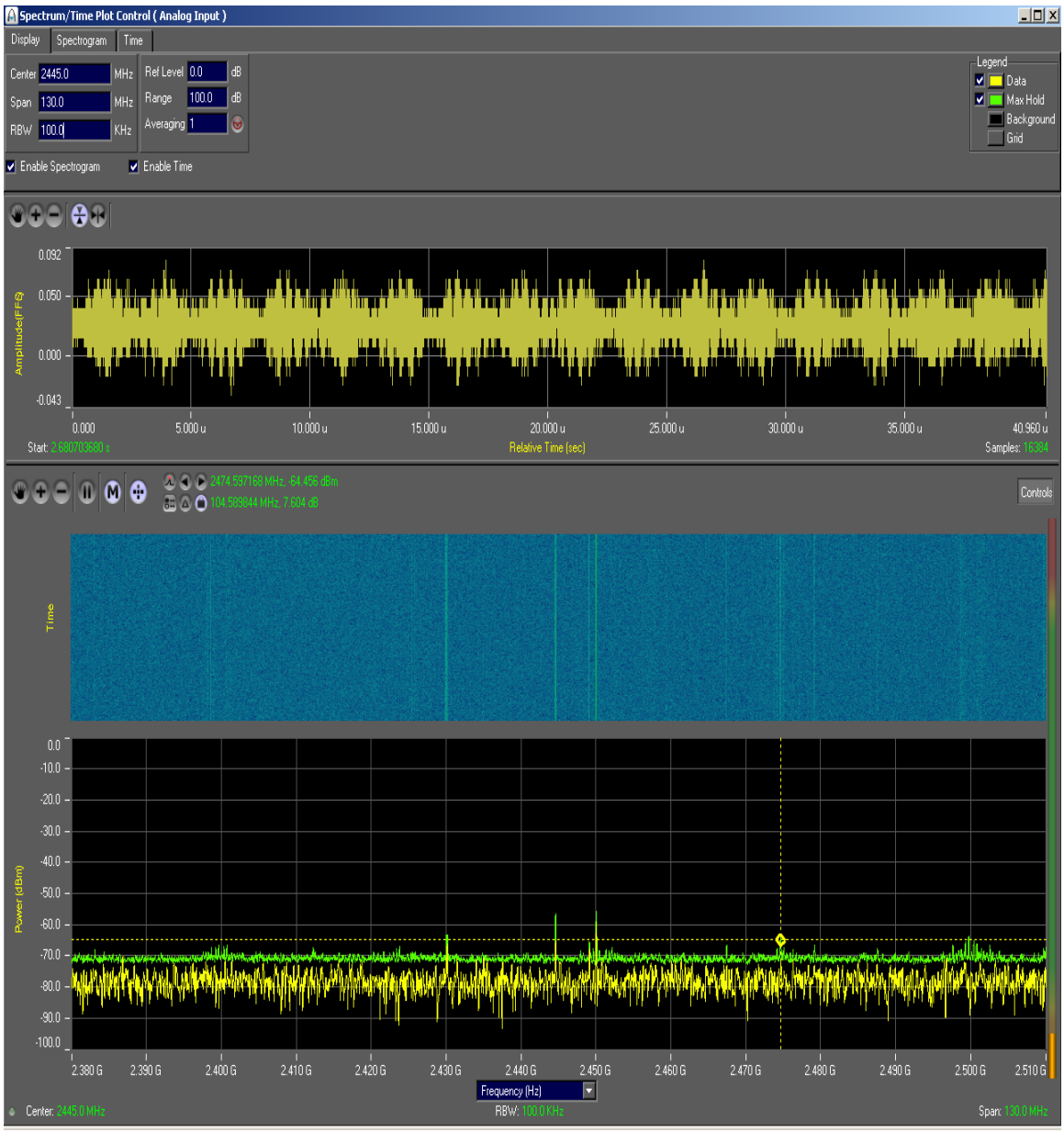


Figure 10: Plot centered at 2445 MHz, 100 KHz RBW

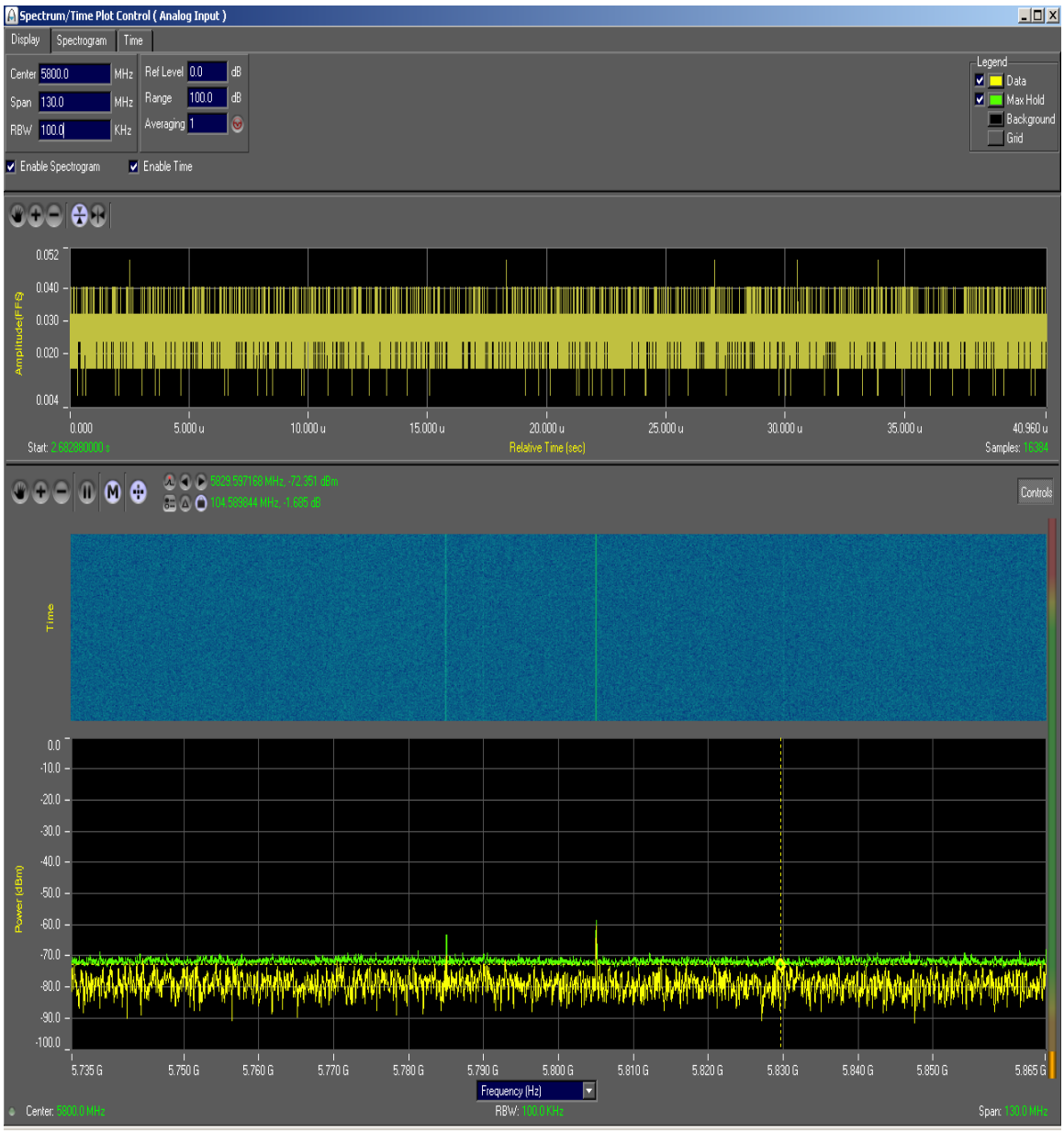


Figure 11: Plot centered at 5800 MHz, 100 KHz RBW

4.3 Location 3: Across and Behind the Control Room

Elevation: 777.3 ft
N 35° 56.710’
W 84° 23.362’

Figures 12 through 15 show similar characteristics as locations 1 and 2. The substation is open with little or no clutter EM-wise. This is both an advantage and disadvantage for the planned network. There is little multipath and the network relies purely on line of sight there by requiring a reliable and dense mesh for coverage.

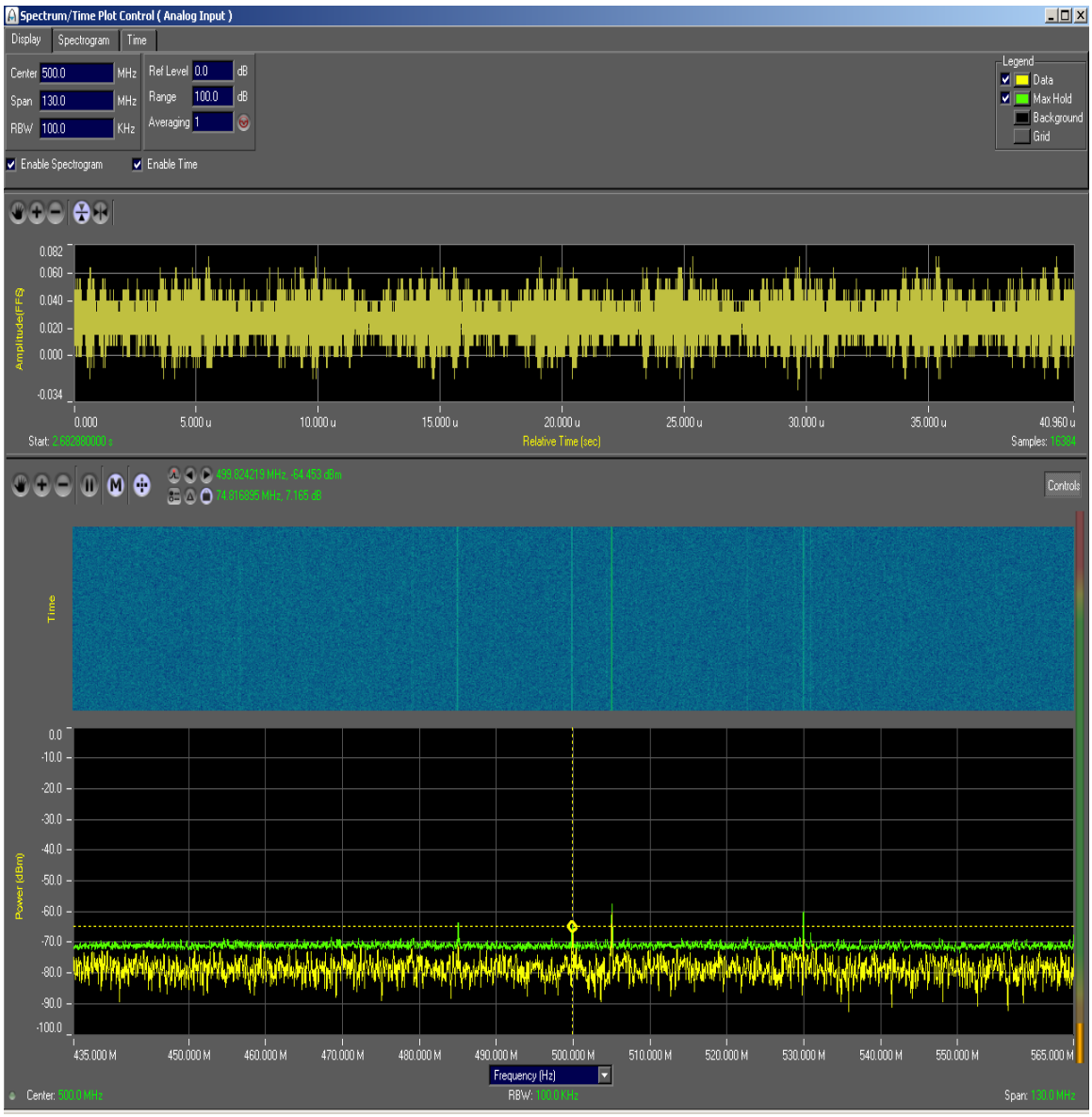


Figure 12: Plot centered at 500 MHz, 100 KHz RBW

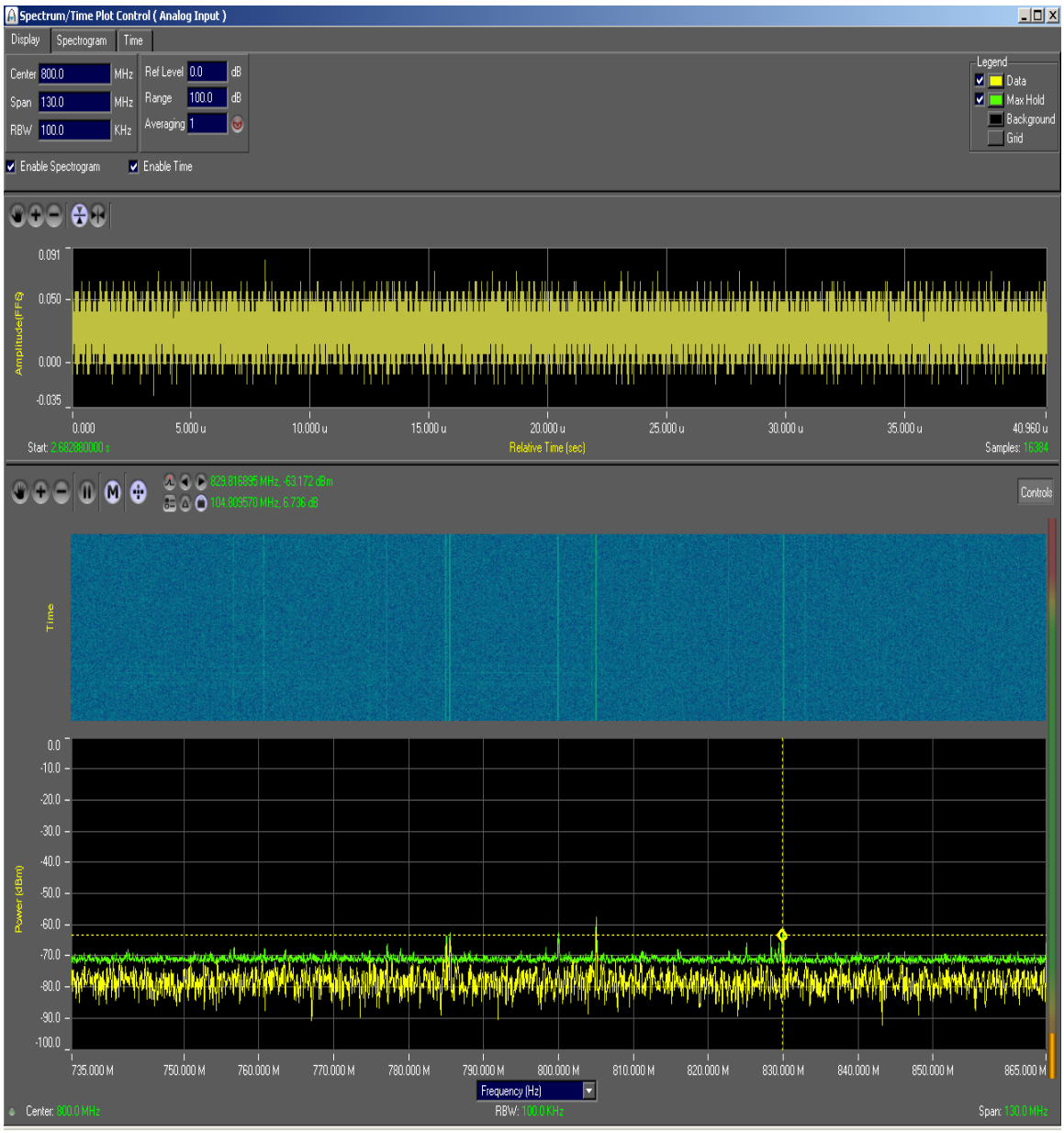


Figure 13: Plot centered at 800 MHz, 100 KHz RBW

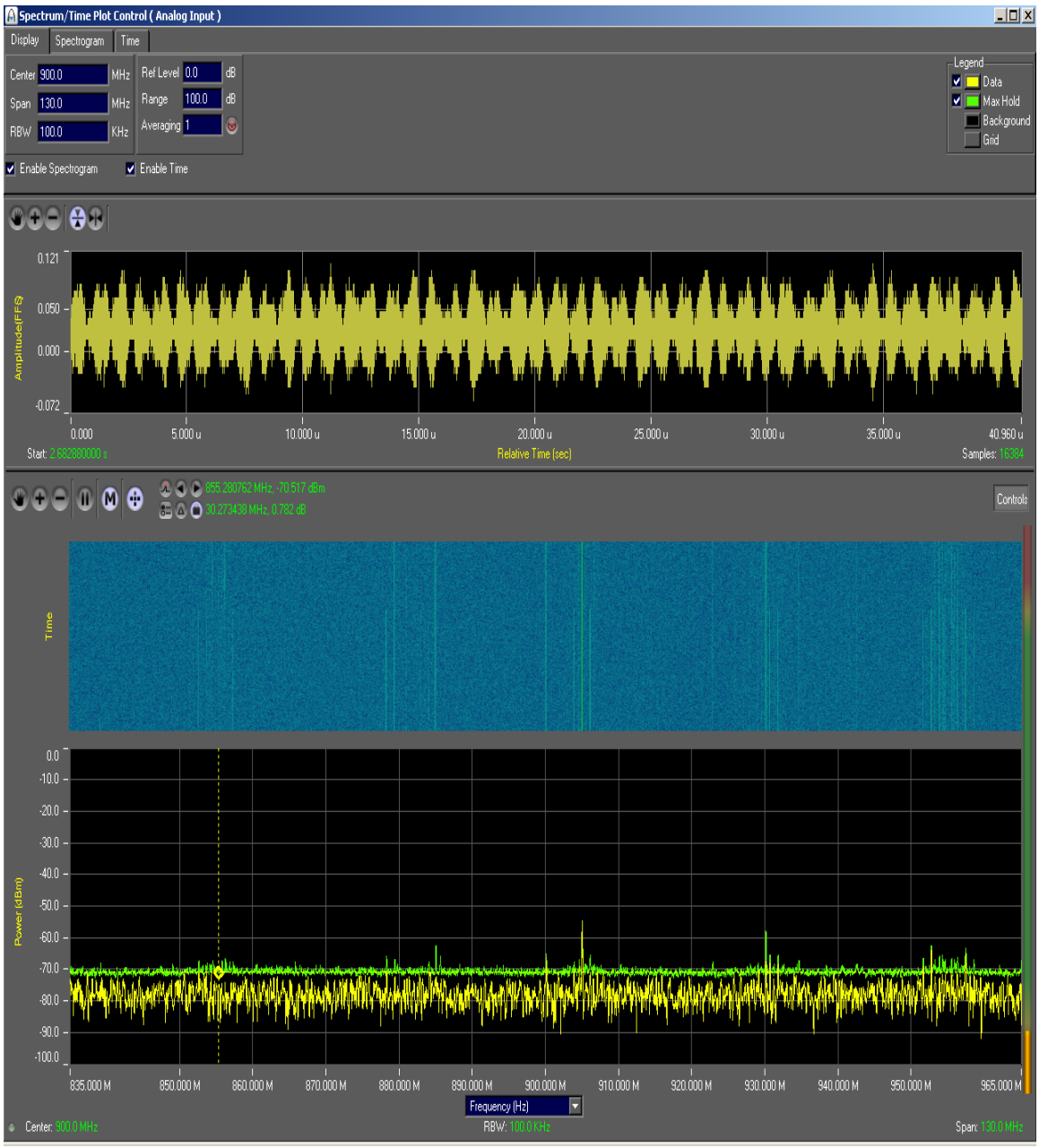


Figure 14: Plot centered at 900 MHz, 100 KHz RBW

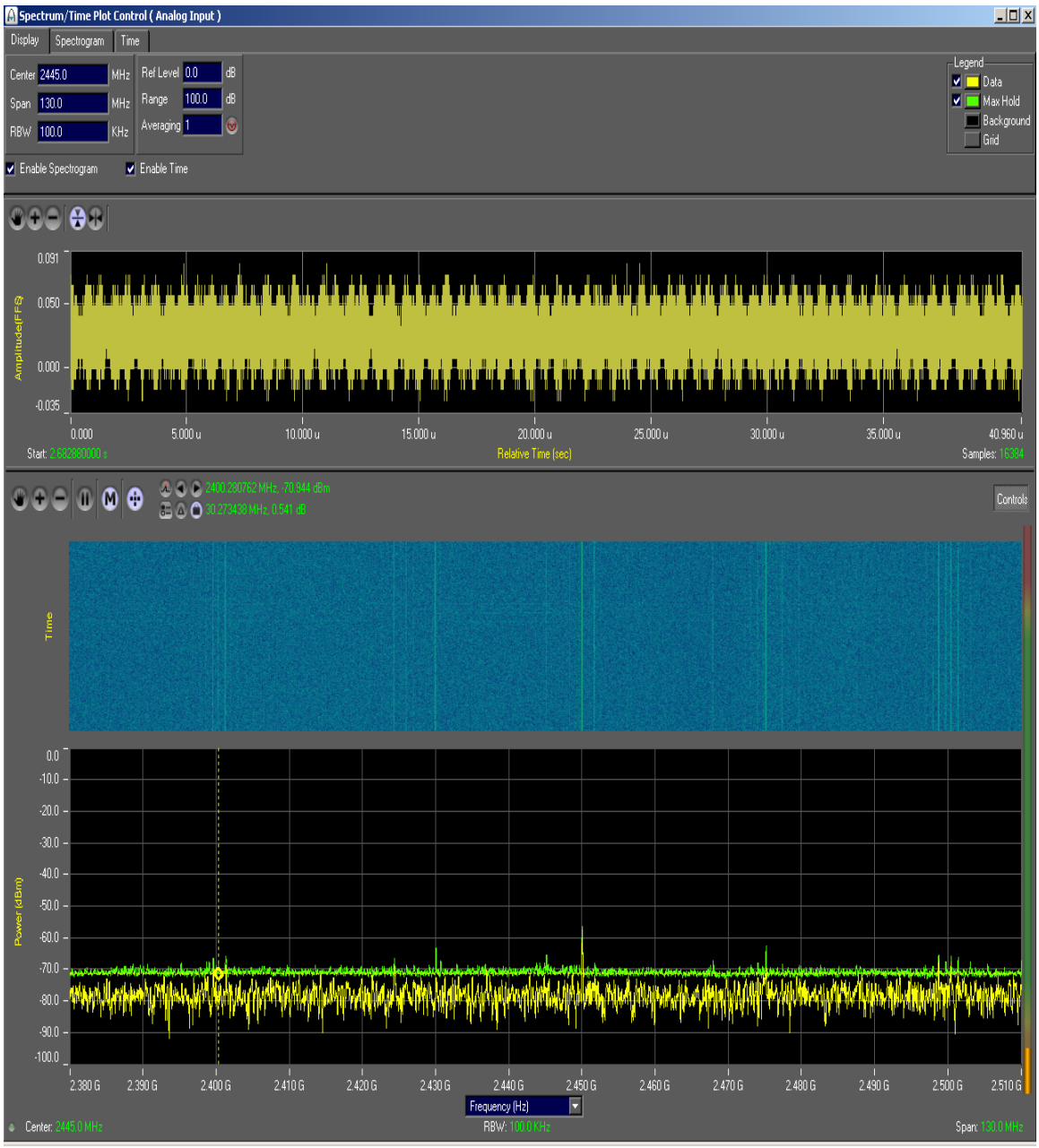


Figure 15: Plot centered at 2445 MHz, 100 KHz RBW

4.4 Frequency Domain Measurements at the Three Locations

Figures 16 through 18 shows the IEEE standard complete frequency domain sweep plots of the ambient RF at the site. The bands described here are 150KHz-30MHz, 30MHz-500MHz, 500MHz-1GHz, 1.0GHz-2.0GHz and 2.0GHz-3.0GHz. Each of the plots is a 3 min average in the respective band. Figures 19 through 21 show the zoomed plot of the band of interest, 2-3GHz band. The noise floor at all the three locations is about -65dB which is consistent with the earlier CS65040 measurements.

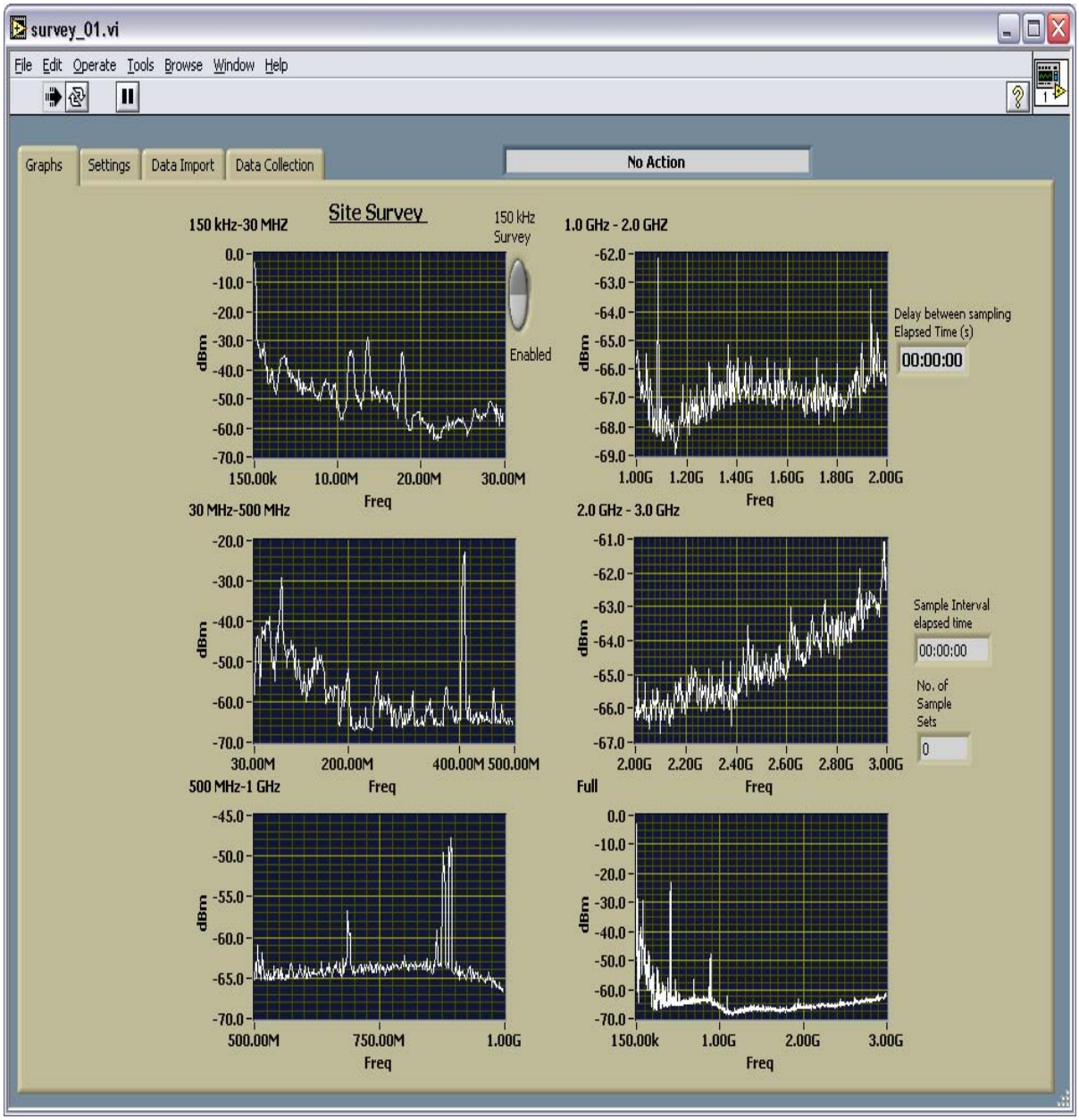


Figure 16: Frequency domain sweep of Location 1

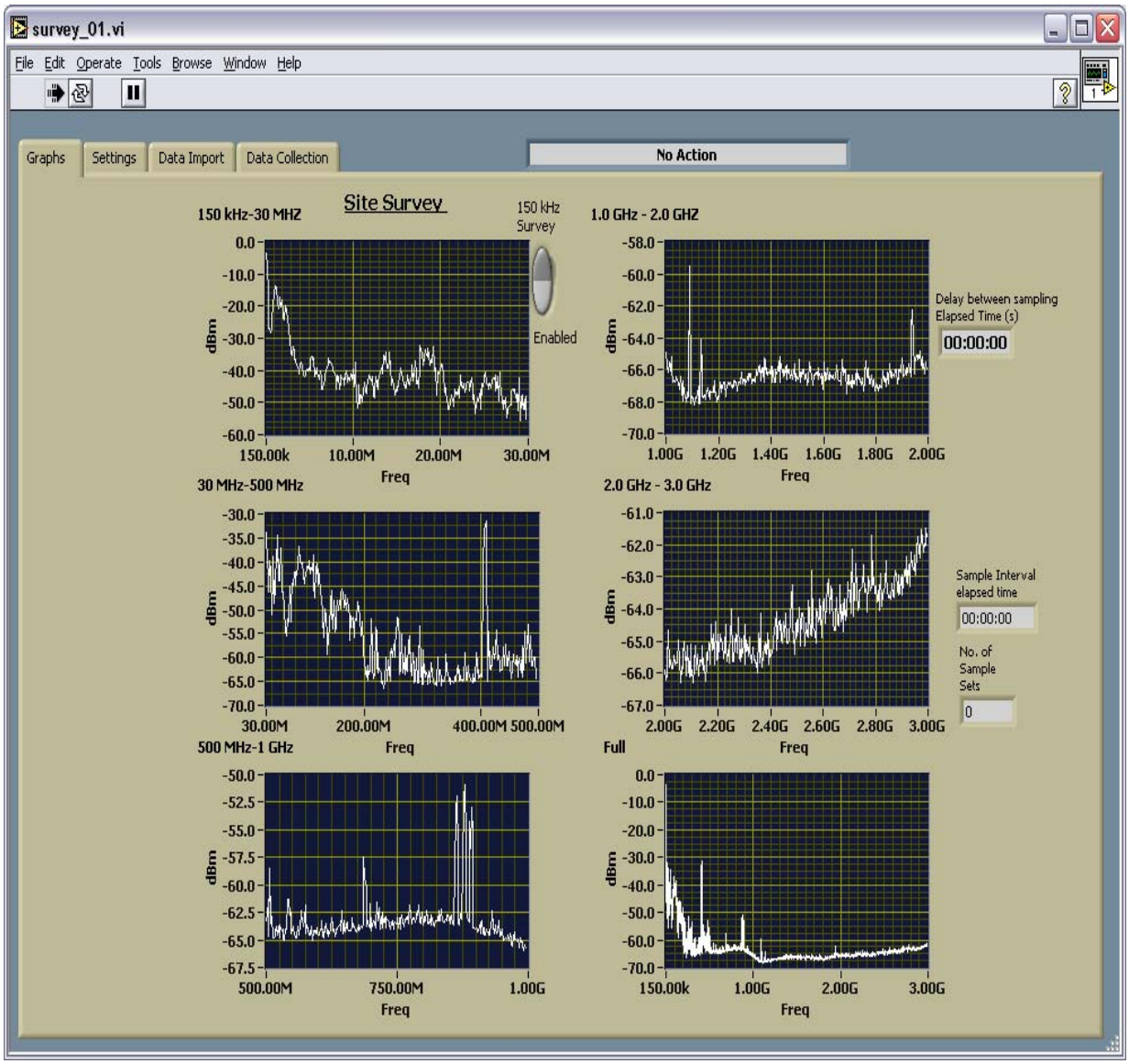


Figure 17: Frequency Domain Sweep of Location 2

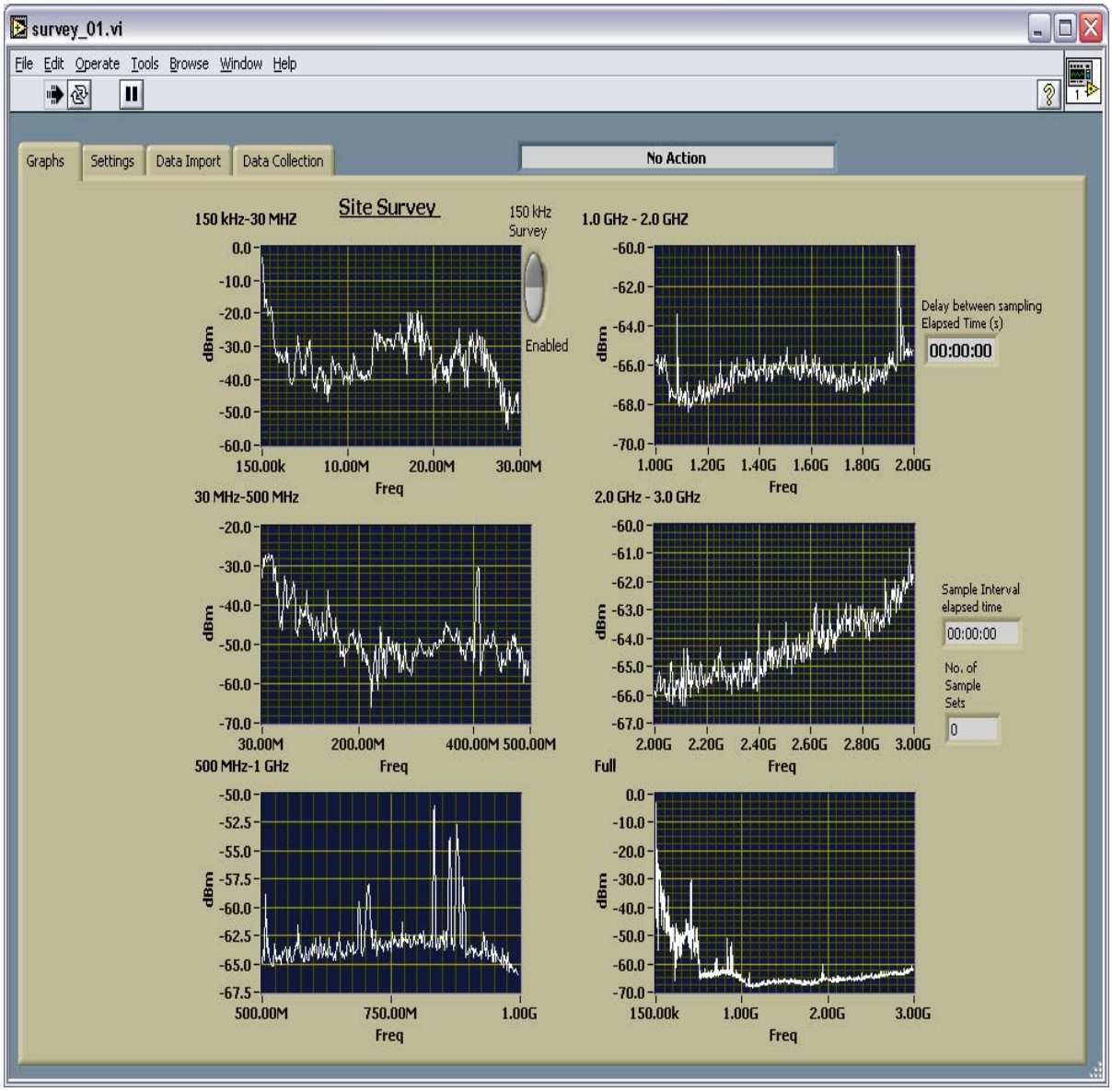


Figure 18: Frequency Domain Sweep of Location 3

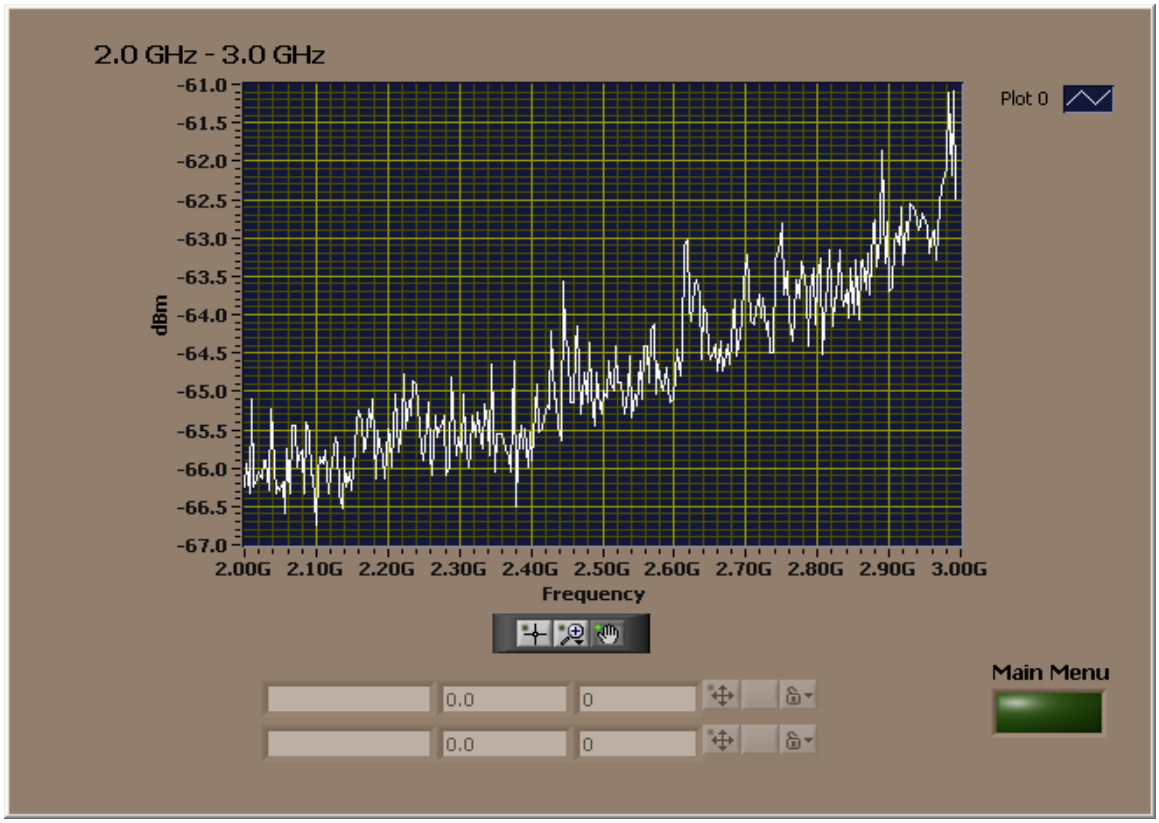


Figure 19: Zoomed Frequency Domain Sweep of 2-3GHz at Location 1

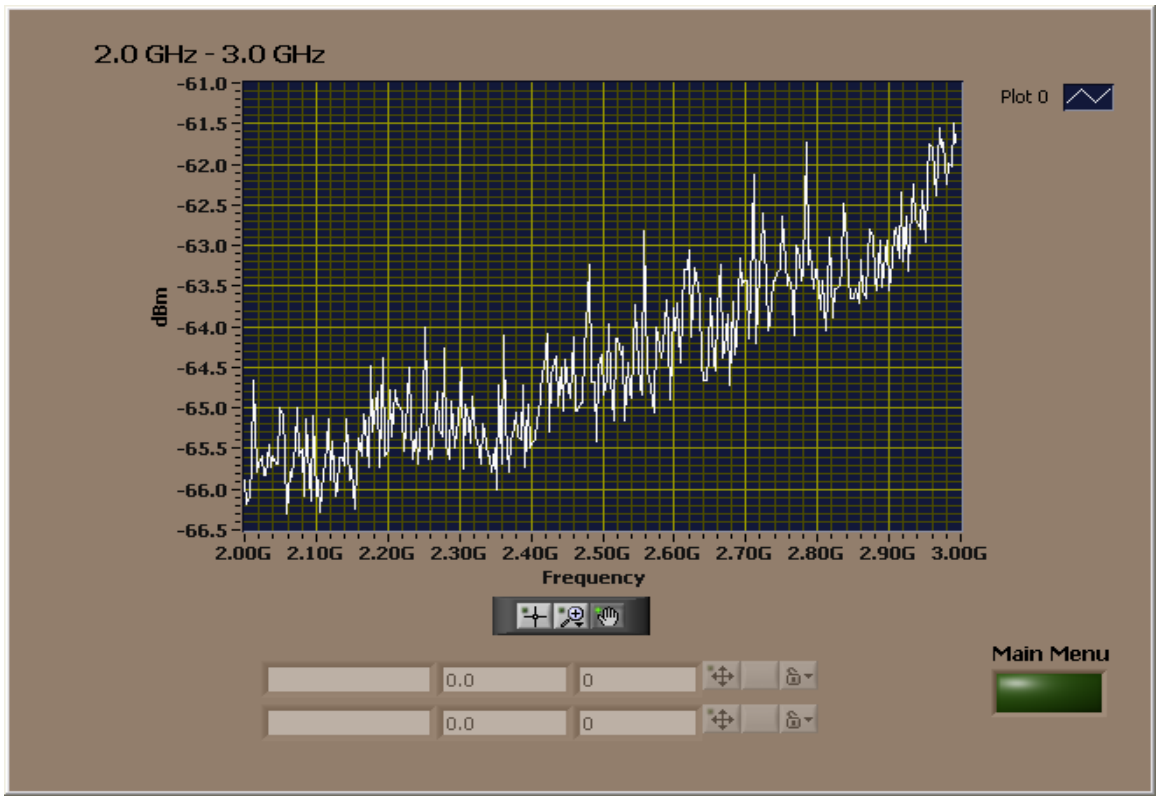


Figure 20: Zoomed Frequency Domain Sweep of 2-3GHz at Location 2

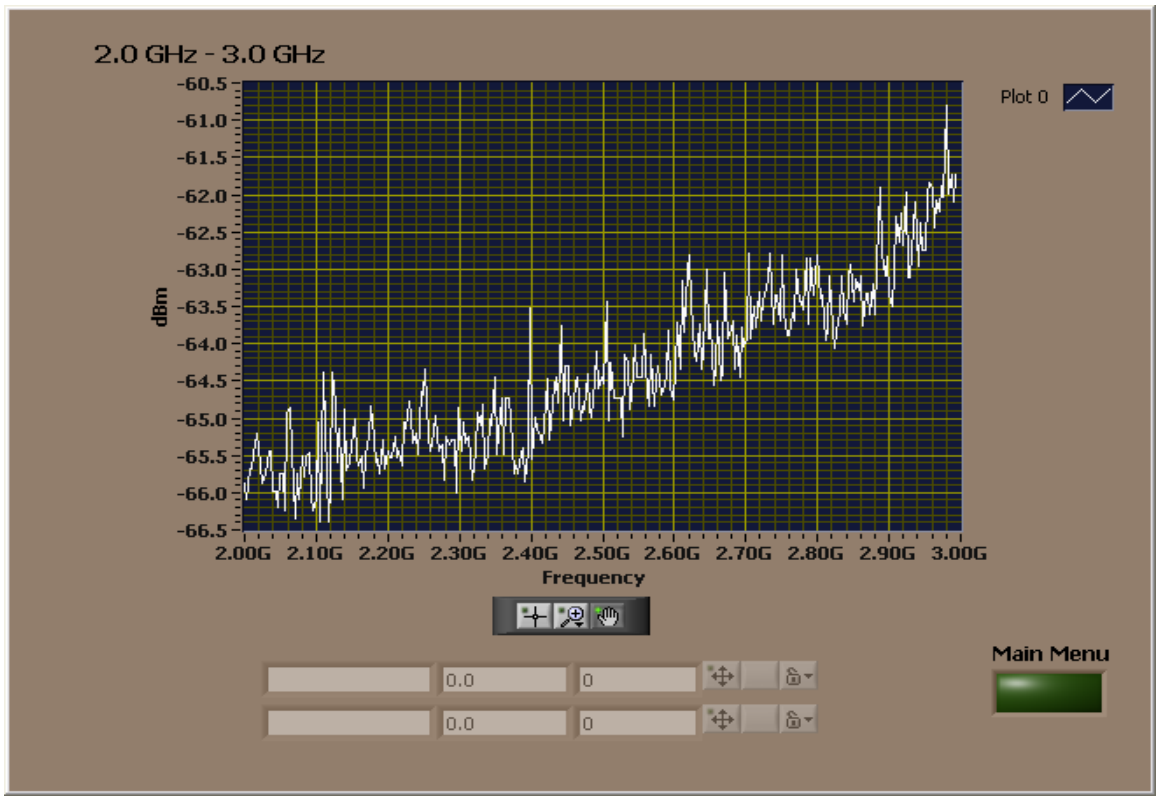


Figure 21: Zoomed Frequency Domain Sweep of 2-3GHz at Location 3

4.5 Antenna factor discone

Settings for R&S spectrum analyzers

ElectroMetrics broadband antenna. To calculate the actual power spectral density values at the antenna location, the antenna factor (in units of dB m^{-1}) is added to the voltage (units of dB re 1 V) at the input of the measuring instrument. The R&S and CS65040 analyzers display amplitude as dB re 1 mW (dBm) referenced to their 50-Ω inputs, so an additional factor of –13 dB must be included in to complete the field strength calculation.

$$E\ (dBV/m) = Reading\ (dBm) + AF\ (dB*m^{-1}) - 13\ dB(V/mW)$$

The antenna factor as a function of frequency for the ElectroMetrics broadband antenna is shown in Fig. 19.

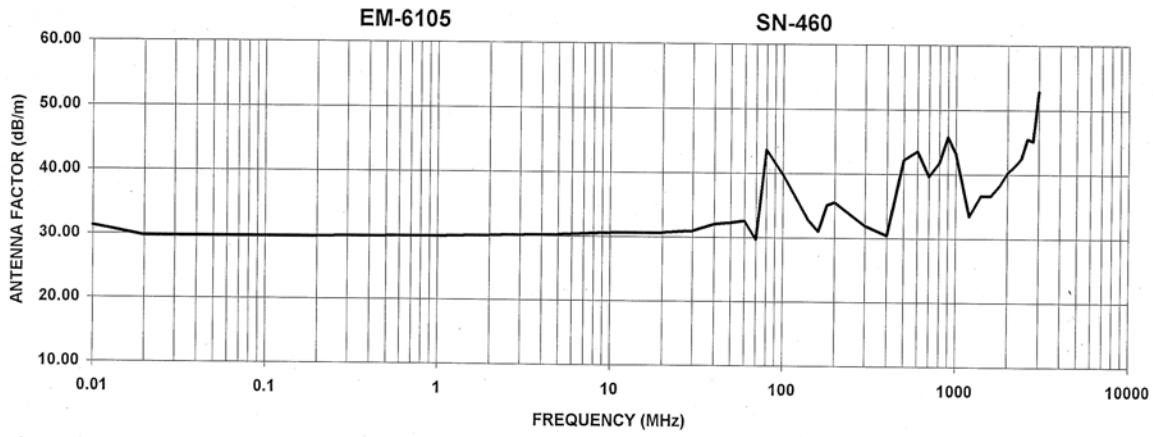


Fig. 22. Antenna factor as a function of frequency.

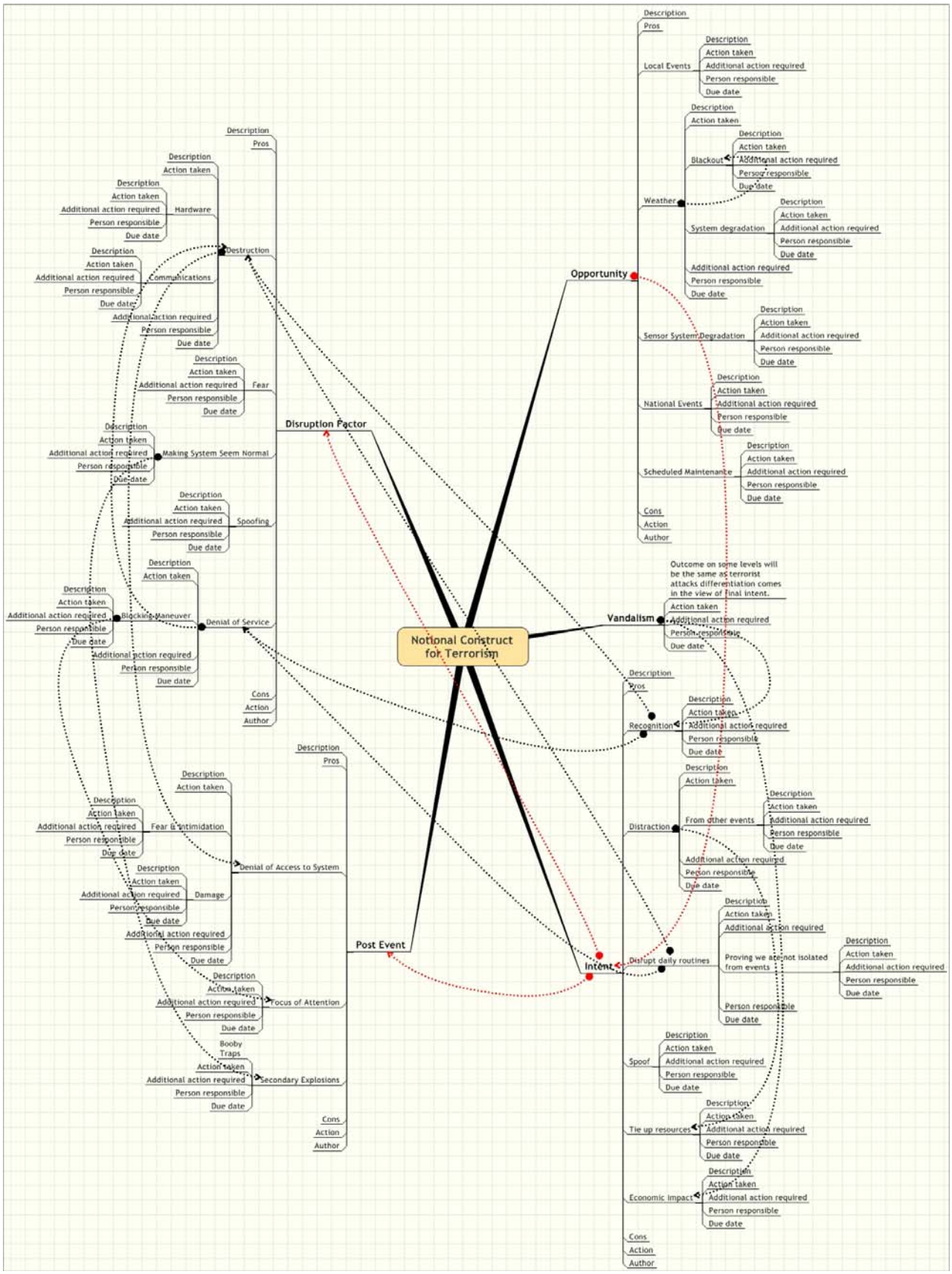
4.6 Survey Conclusions/Recommendations

As this series of plots demonstrates, sources of interference were found during the EMI tests done on November 3rd, 2005. The interferers seem to be the communications links used in the operational capability of the substation. The signals are band-limited and the particular channels can be easily avoided in our implementation of the network. There are no frequency-hopping transmissions. However it is recommended to do a complete co-existence measurement using the proposed nodes to see the affect of this ambient RF on the future network. This can be done by measuring BER and PER by varying the channels of the 802.15.4 radios over long periods of time (an automated logging and channel shifting mechanism using the proposed nodes with measurements of more than one hour in each channel is recommended for significant extrapolation of the coexistence). The location is open with minimal clutter EM-wise which could be both an advantage and disadvantage. Lack of multipath makes the reliability of transmission to be on finding proper line of sight signal. This calls for a robust and dense mesh network implementation for efficient coverage of the substation. Alternate tradeoff is by using an enhanced power amplifier to boost the 15.4 radios to maximum power limited by ISM band. The delay-spread and signal fading characteristic measurements will provide more insight on how to tackle this problem.

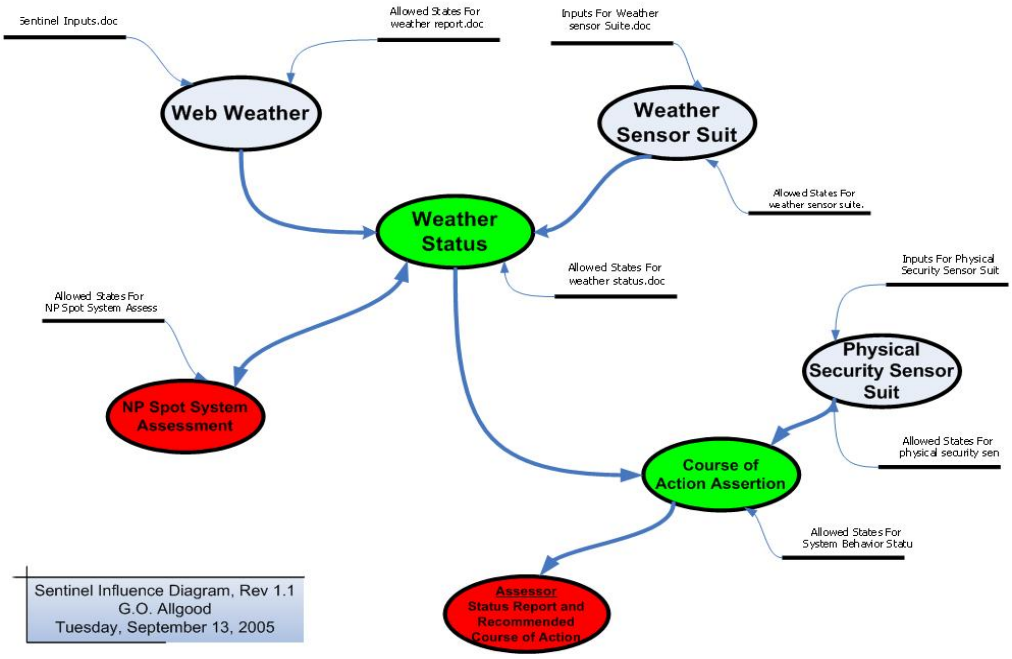
The 900-MHz ISM band was free from interfering signals in all the locations

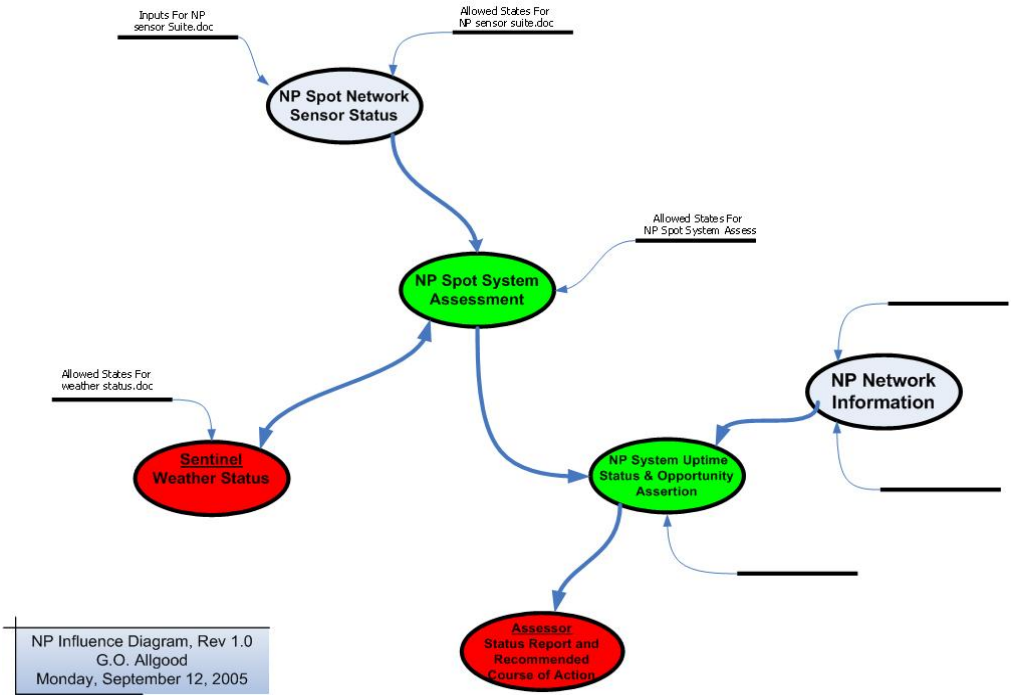
The 5-GHz ISM band was free from interfering signals in all the locations.

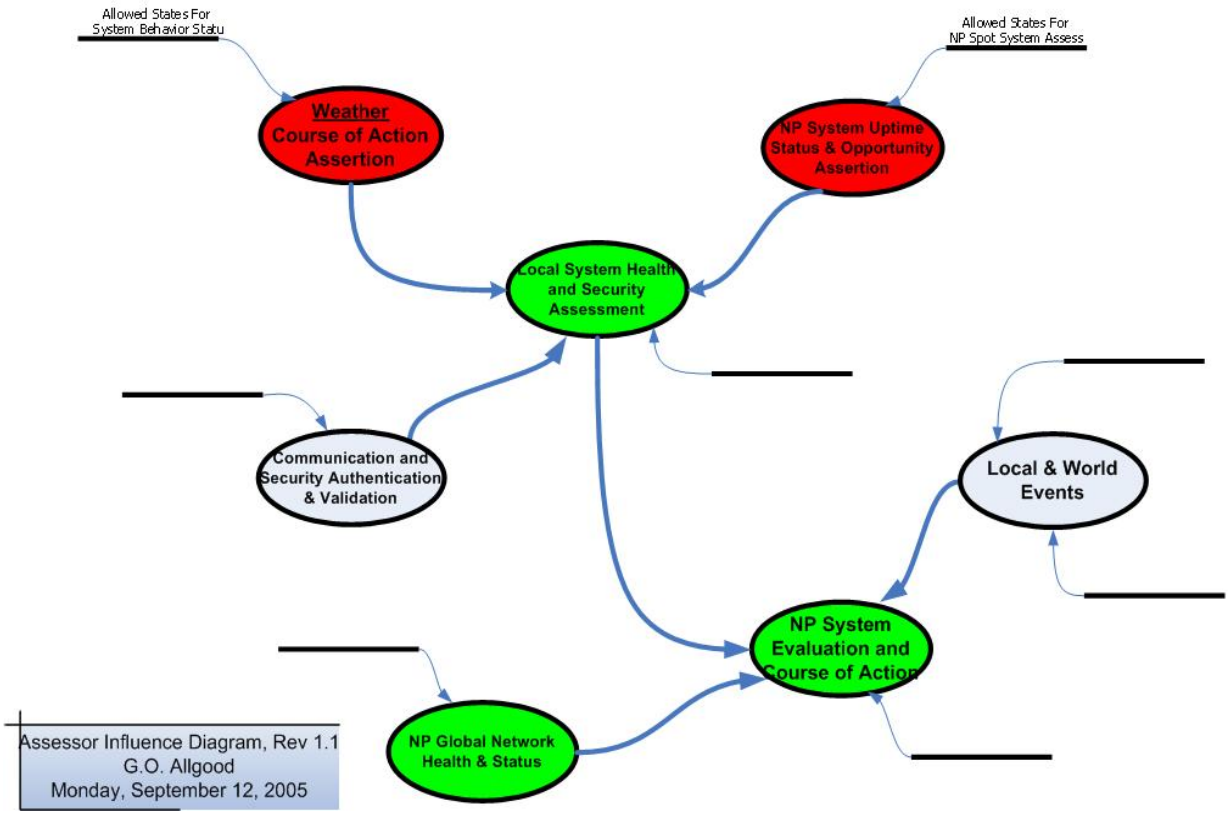
5. NOTIONAL CONSTRUCTS


Notional Construct for Terrorism
Disruption Factor
Opportunity
Vandalism
Intent
Post Event
Description
Pros
Cons
Action
Author
Action taken
Additional action required
Person responsible
Due date
Hardware
Communications
Destruction
Fear
Making System Seem Normal
Spoofing
Blocking Maneuver
Denial of Service
Fear & Intimidation
Damage
Denial of Access to System
Focus of Attention
Booby Traps
Secondary Explosions
Local Events
Weather
Blackout
System degradation
Sensor System Degradation
National Events
Scheduled Maintenance
Outcome on some levels will be the same as terrorist attacks differentiation comes in the view of final intent.
Recognition
Distraction
From other events
Disrupt daily routines
Proving we are not isolated from events
Spoof
Tie up resources
Economic Impact

6. INFLUENCE DIAGRAMS (EVENT TOPOLOGY)







7. CLASSIFICATION TECHNIQUES:

This project is based on using Bayes' decision theory to derive various formulae for the classification and the parameter estimation of the given data. The Bayes' rule is given as follows:

$$\mathbf{P(w_j/x) = p(x/\ w_j\ )P(w_j\ )/p(x)}$$

The parameters are estimated using the following formulae:

$$\mu = \frac{1}{n}\sum_{i=0}^{n} Xi$$

$$\sum = \frac{1}{n}\sum_{i=1}^{n}(Xi-\mu)(Xi-\mu)^{t}$$

From the parameters obtained the decision rule is designed to classify the given data. The designed decision rule is run on the testing data said using the pre-calculated parameters. After running the classification each data is classified as category 1 or category 2. The obtained results are compared with the available data and the error rate and the accuracy are calculated.

Bayesian Estimation of parameters and classification.

In this the parameters μ and Σ are estimated again by treating this parameters as random variables themselves. The new formulae for the μ and Σ are as follows:

$$\mu_n = \left[\frac{n\sigma_0^{\,2}}{n\sigma_0^{\,2} + \sigma^2} \right] \left(\frac{1}{n} \sum x_k \right) + \left(\frac{\sigma^2}{n\sigma_0^{\,2} + \sigma^2} \right) \mu_0$$

$$\sigma_n = \frac{\sigma_0^{\,2}\sigma^2}{n\sigma_0^{\,2} + \sigma^2}$$

The values of μ_0 and σ_0 are randomly chosen values by observing the given data. However I chose μ_0 by looking at the mean-matrix of the whole given data in the testing set , similarly the σ_0.

The classification is done based on the probabilities obtained by plugging in the Gaussian equation with the new parameters.

$$p(x) = \frac{1}{\sqrt{\sum_n (2\pi)^{d/2}}} \exp\left(-\frac{1}{2}(x-\mu_n)^t \sum^{-1} (x-\mu_n)\right)$$

K-Nearest Neighborhood Estimation:

In KNN estimation, the volume is allowed to vary depending on the training data set. To estimate the *p(x)* from *n* samples, we can center a cell at *x* and let it grow until it contains *Kn* samples, and *Kn* can be some function of *n.* Ususally *Kn* is taken as square root of *n*. If we wish to determine the statistics, a hypersphere of volume V which just encloses *k* points from the combined set. If within that volume, *Km* of these points belong to class *m*, then we estimate the density for class m by :

$$p(x/w_m) = k_m / n_m \quad p(w_{m)} = n_m/n \quad p(x) = k/nV$$

The decision rule tells us to look in a neighborhood of the unknown feature vector for *k* samples. If within that neighborhood, more samples lie in class *i* than any other class, we assign the unknown as belonging to class *i*.

8. BAYESIAN BELIEF NETWORK

Bayesian belief networks are directed acyclic graphs where each node represents a random variable as described in Figure 1. The nodes in a Bayesian network represent propositional variables of interest and the links represent informational or causal dependencies among the variables. The intuitive meaning of an arrow from a parent to a child is that the parent directly influences the child. The direction of this influence is often taken to represent casual influence. These influences are quantified by conditional probabilities which give the strength of causal influence. Perhaps the most important aspect of Bayesian networks is that they are direct representations of the world, not of reasoning processes. The arrows in the diagram represent real causal connections and not the flow of information during reasoning (as in rule-based systems and neural networks).

The Bayesian network supports the computation of the probabilities of any subset of variables given evidence about any other subset. It allows one to calculate the conditional probabilities of the nodes in the network given that the values of some of the nodes have been observed. As new evidence comes in, it is tempting to think of the probabilities of the nodes changing, but, of course, what is changing is the conditional probability of the nodes given the changing evidence.

Bayesian belief networks are effective and practical representations of knowledge for reasoning under uncertainty. They have many successful applications in many fields such as diagnosis, planning, learning, vision, natural language processing, and decision support systems. The latter involves interaction with human users, and therefore it is crucial that users be able to understand the underlying probabilistic model, its assumptions, and its recommendations. Since Bayesian networks are graphical models, they are cognitive and similar to human reasoning constructs, distributed algorithms for inference and learning, modular representation of knowledge, and intuitive (possibly causal) interpretation. In many of these applications, systems are fairly autonomous and their most important characteristic is the ultimate reasoning performance.

A Bayesian network represents the assumption that each node is conditionally independent of all its ancestors given its parents. To specify the probability distribution of a Bayesian network, one must give the prior probabilities of all root nodes (nodes with no predecessors) and the conditional probabilities of all non-root nodes given all possible combinations of their direct predecessors. The conditional independence assumptions expressed by a Bayesian network allow a compact representation (fewer parameters) of the joint distribution and therefore lower sample and time complexity. As a consequence, it requires less data for learning and less time for inference.

An example for detecting an attack on power substation using Bayesian network is shown in Figure 23. In this example, three seismic and three acoustic sensors are used to detect such an attack. The data collected from these sensors are fed into a pattern recognition program which allows each sensor to recognize a car (C), a man (M) or an animal (A) with certain probability. The classified objects for each sensor are fed into a regional central unit (one for acoustic and another for seismic) which makes a final decision on whether the detected object is C, M, or A. Note that seismic sensors are more accurate than acoustic sensors. This is reflected on the parameters of conditional probabilities for each sensor. Finally, based on the outputs of all regional central units, an attack is detected according to certain predefined criteria (cars means higher occurrence probability of attack, men less probable, and animals are the least probable).

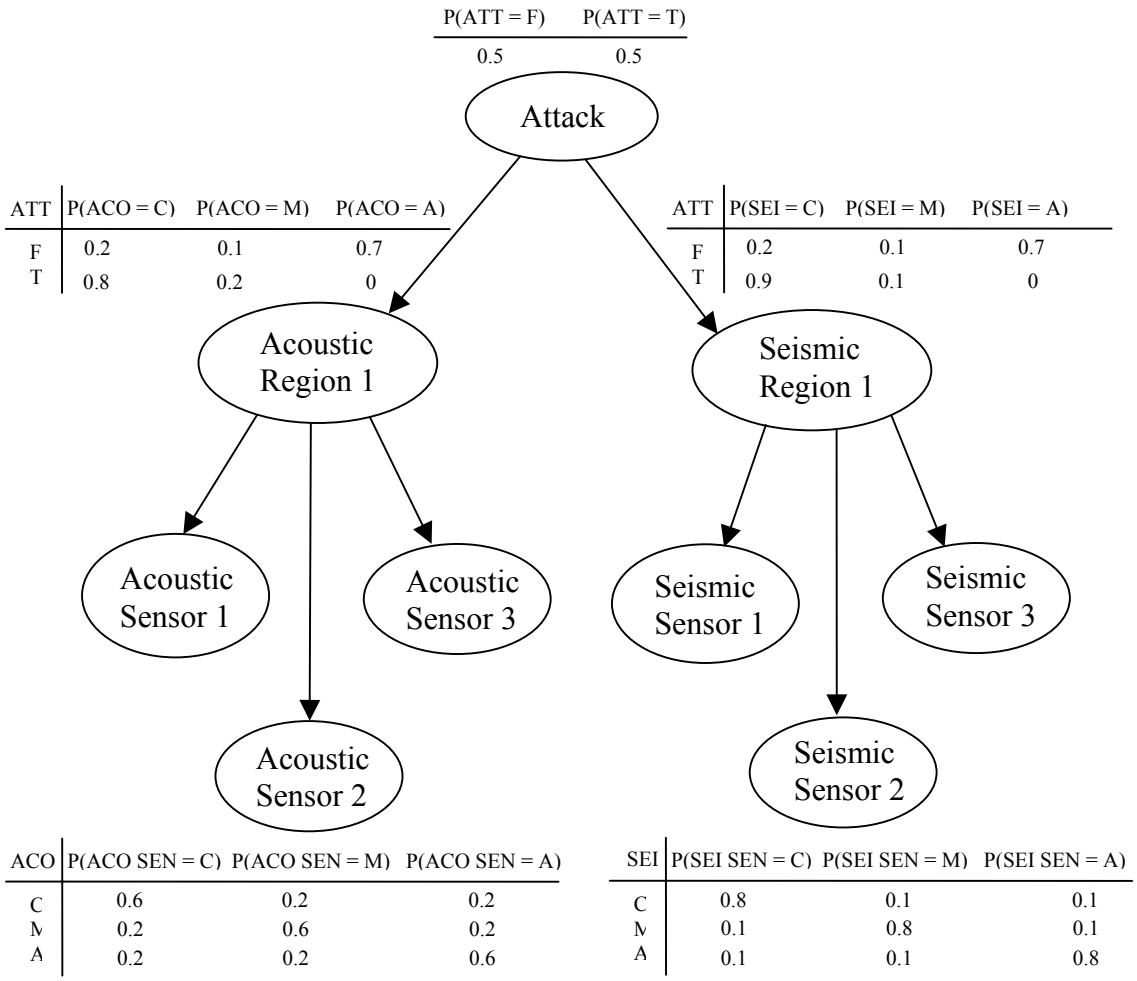


Figure 23: A Bayesian network for the attack detection problem.

The above example is simulated using Bayesian network toolbox in Matlab. The sensor nodes are chosen as observed discrete nodes. The probabilities of attack based on the readings of the sensors are computed and shown in Table 1. The probability distribution of attack for the third case (ACO S1 = C, ACO S2 = M, ACO S3 = M, SEI S1 = C, SEI S2 = M, SEI S3 = M) is plotted in Figure 24.

Table 1: Probability of attack for various sensor readings.

Acoustic Sensor Readings			**Seismic Sensor Readings**			**P(ATT = T)**
S1	**S2**	**S3**	**S1**	**S2**	**S3**	
C	C	C	C	C	C	0.94
C	C	M	C	C	M	0.92
C	M	M	C	M	M	0.75
M	M	M	M	M	M	0.63
C	M	A	C	M	A	0.5
M	M	A	M	M	A	0.33

M	A	A	M	A	A	0.008
A	A	A	A	A	A	0.001

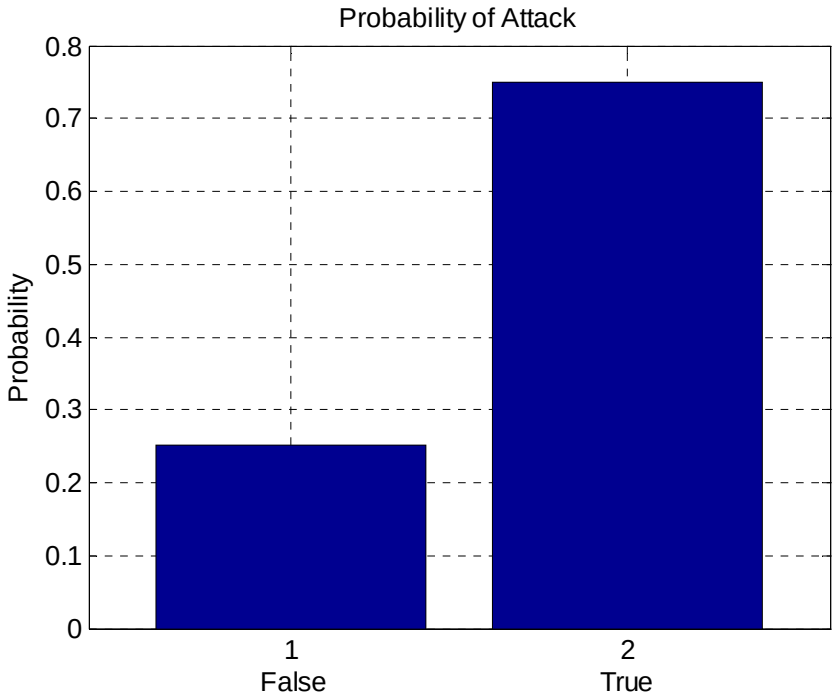


Figure 24: Probability distribution of attack for case (ACO S1 = C, ACO S2 = M, ACO S3 = M, SEI S1 = C, SEI S2 = M, SEI S3 = M).

9. A WIRELESS SENSOR NETWORK FOR AN ANTICIPATORY THREAT AWARE APPLICATION

Scope:
This section describes the design of the Wireless Sensor Network for the Anticipatory Threat Aware Application (ATA), hereafter referred to as A-WSN. The A-WSN goal is to gather the information needed by ATA to assert the presence of a threat.

9.1 A-WSN Overview

The A-WSN is comprised of:

- Passive Infrared sensors
- Acoustic Sensors
- Seismic sensors
- Coordinator
- Relay nodes
- Computer

The physical components of the WSN are depicted in Figure 25.

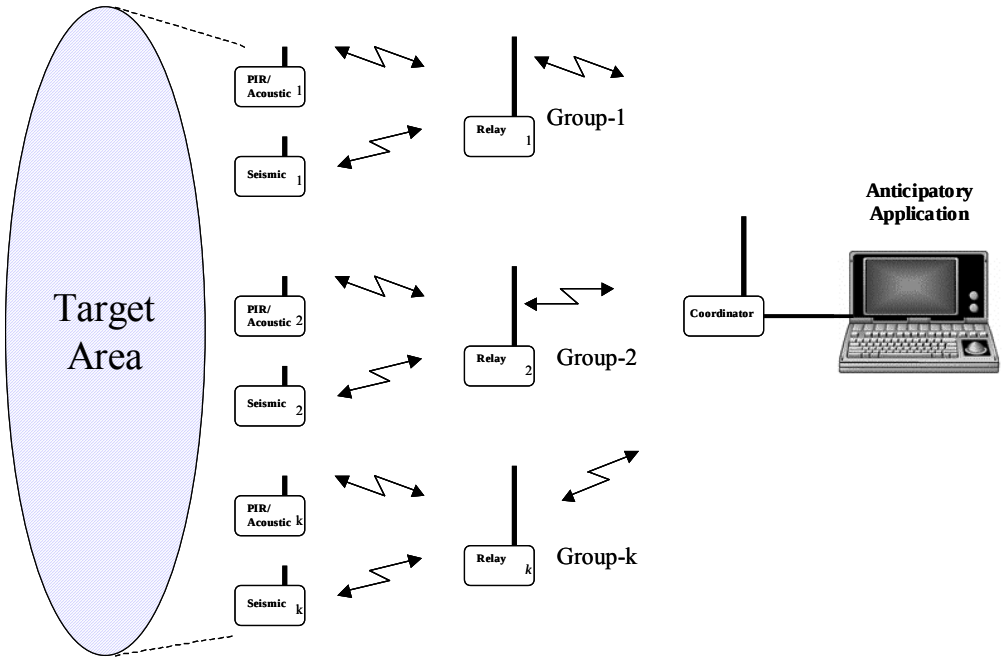


Figure 25 WSN for Anticipatory Threat Aware Application

The logical structure of the WSN is depicted in Figure 26. It is a hierarchical structure with three tiers. The third tier is comprised of sensor nodes, second tier is comprised of relay nodes that group sensor nodes logically associated with them, and the third tier is a group of relay nodes associated with the coordinator of the WSN. The main purpose of the hierarchical structure, from the WSN perspective, is to reduce the amount of

unnecessary data forwarded from the sensors to the computer where ATA is running, and to extend the coverage of the WSN. The former helps make the WSN scalable. The sensor nodes perform sensor-node processing to send relevant detection information. The relay nodes correlate the messages from the sensor-nodes in their corresponding groups and further reduce the unnecessary data transmission through group processing. Finally the coordinator forwards the group messages to the computer for the final assessment/classification via the ATA.

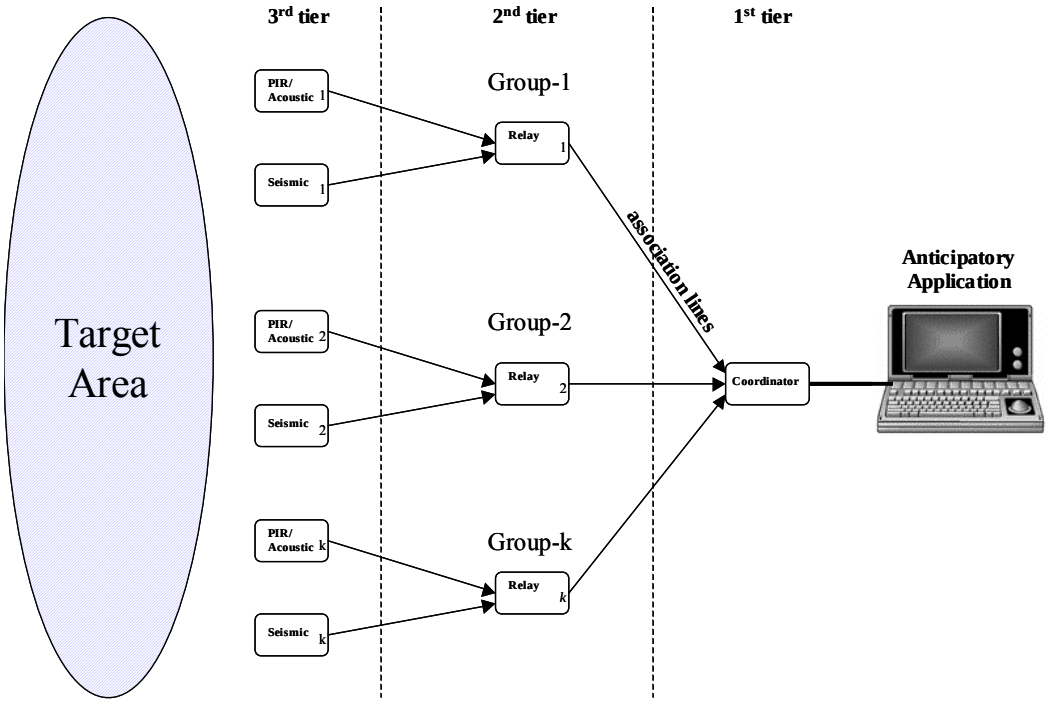


Figure 16 Logical architecture of the WSN

- The network takes care of routing and other higher layer communication protocols using the Figure 8 stack (http://www.chipcon.com/).
- The association between the sensor nodes and the relay nodes is done manually by assigning an application-layer address off-line that tells the node the group it belongs to and the type of node it is (i.e., sensor: PIR, acoustic, seismic; relay, or coordinator).
- The operation of the A-WSN is given in Section 8.2.
- The target area is approximately 10m long by 3m wide. The coverage of the WSN is based on the PIR sensors' specifications (see Section 8.2.1) and it is depicted in Figure 27. Figure 27 shows the minimum number of PIR sensors needed. The actual number of sensors depends on the level of redundancy and confidence level sought.

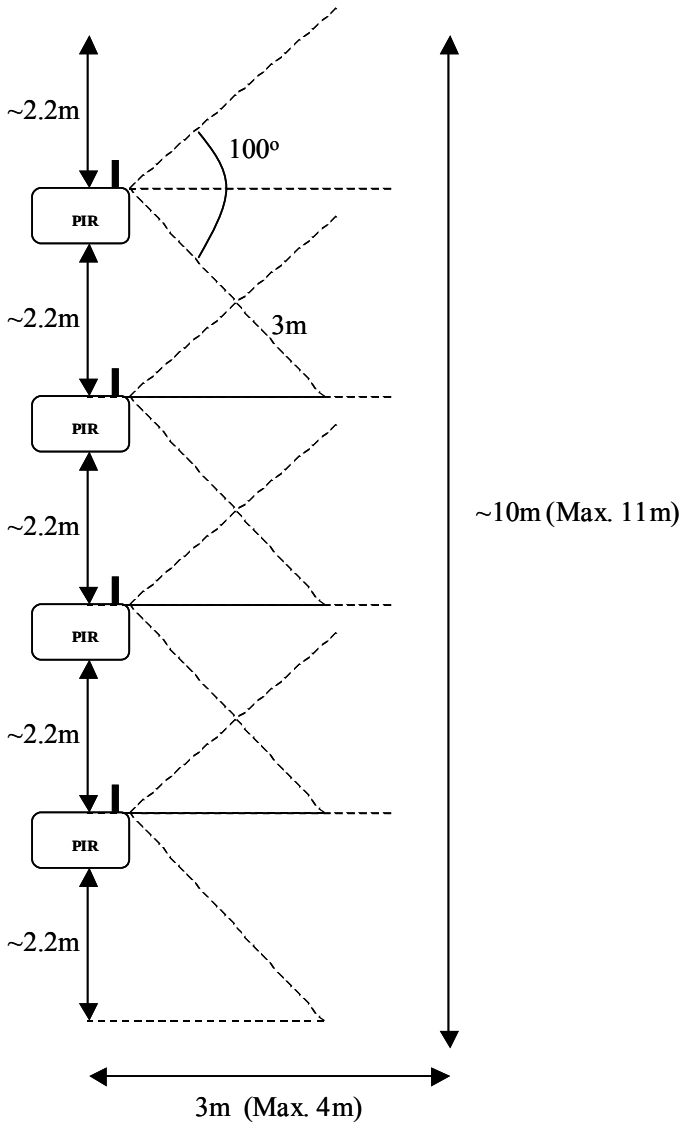


Figure 27 WSN coverage area based on PIR sensors' specifications

9.2 WSN Nodes

All sensor-nodes have an ATMEL 128L/Chipcom CC2420 module. The antenna to use in the Relays and Coordinator are 9dBi gain antennas: (http://www.hyperlinktech.com/web/24ghz_802.11_rubber_duck_antenna_9dbi_nm.php) , and the antennas for the sensor nodes are 2.5dBi antennas.

It has been shown in several studies that near-ground communications tends to have higher path loss [1], [2]. The difference between path loss with antenna highs at a standing position with respect to lying position could be as much as 20dB. This can be resolved with more transmission power and higher antenna gains.

9.2.1 Passive Infrared (PIR) Sensor Node

The PIR sensor node is provided by Crossbow Technologies (http://www.xbow.com/). A picture of this device is shown in Figure 28. The PIR has the following specifications:

- Sensor: LHI878
- Min. range: 0.2m
- Max. range: 4m
- Horizontal angle: 100◦
- Vertical angle: +/- 45◦
- Interface: 1-channel ADC

Figure 28 PIR/Acoustic sensor

Sensing algorithm of PIR sensor

The sensing algorithm of the PIR sensor is based on [3] since the authors used the same micro-controller ATMEL128L.

The PIR response is highly sensitive to weather conditions and surrounding vegetations. For example, moving foliage and thermal variations in the wind can affect the noise floor of the PIR sensor. It has been recommended in [3] to perform a frequency domain

processing of the signals out of the PIR sensor circuitry rather than a time domain processing.

The signal values out of the PIR are passed through a digital high-pass filter given by the following recursion,

$$\begin{aligned} m_0 &= 0 \\ m_n &= s_n - s_{n-1} + k_{PIR} m_{n-1} \end{aligned} \qquad (1)$$

The k_{PIR} parameter is found by experimentation, the authors in [3] use 0.9. This parameter depends on the desired cut-off frequency of the filter for the particular PIR. The noise level e_n is computed as follows,

$$e_n = \begin{cases} p_0 & n = 0 \\ k_1 e_{n-1} + k_2 p_n & e_{n-1} < p_n \\ k_3 e_{n-1} + k_4 p_n & e_{n-1} \geq p_n \end{cases} \qquad (2)$$

Where p_n is the maximum power of the filtered signal within a time window of W_{PIR_noise} samples, and $k_1 + k_2 = k_3 + k_4 = 1$. The parameters used in [3] are: $k_1 = 0.98$, $k_2 = 0.02$, $k_3 = 0.75$, $k_4 = 0.25$. The rationale behind (2) is to choose k_2 small when p_n is larger than the noise ($e_{n-1} < p_n$) to avoid increasing the noise too fast when a target is detected, and choose k_4 large when a target is not around in order to decrease the noise quickly. The threshold of detection is proportional to e_n.

$$Th_{PIR} = he_n \qquad (3)$$

A crossing event for the PIR sensor is counted if,

$$s_t > Th_{PIR} \qquad (4)$$

If (4) is true the algorithm considers that the PIR threshold has been crossed. The PIR confidence level is computed based on the ratio of total crossing events to total samples in a window of size equal to W_{PIR_CDL} samples (actual value may vary depending on experimentation). *The PIR confidence detection level is the only value transmitted to the associated relay node.*
The nominal sampling rate for the PIR sensor is 50Hz in [3] based on email exchanged with Lin Gu (author in [3]).

9.2.2 Acoustic Sensor Node

The acoustic sensor node is provided by Crossbow Technologies (http://www.xbow.com/). The acoustic sensor is physically located in the same box of the PIR sensor (see Figure 4). This is a microphone with following specs:

- Frequency range of 20-16KHz,
- Sensitivity –46dB +/-4Db,
- Omnidirectional
- 1-cahnnel ADC interface.

Sensing algorithm of Acoustic sensor

The signal values out of the acoustic sensor are passed through the following moving average operation [3],

$$\begin{aligned} m_{1,0} &= s_0 \\ m_{1,t} &= \alpha_1 s_t + (1-\alpha_1) m_{1,t-1} \end{aligned} \qquad (5)$$

where $m_{1,t}$ is the current value of m_1, $m_{1,t-1}$ is the previous value of m_1, s_t is the current microphone reading and α_1 is a constant. The authors in [3] use $\alpha_1 = 0.001$.

In order to determine whether the acoustic threshold has been crossed we find out if

$$E_t > m_{2,t} + d_{2,t} \qquad (6)$$

Where

$E_t = |s_t - m_{1,t}|$, and

$$\begin{aligned} m_{2,t} &= \alpha_2 E_t + (1-\alpha_2) m_{2,t-1} \\ v_{2,t} &= \alpha_2 (E_t - m_{2,t})^2 + (1-\alpha_2) v_{2,t-1} \\ d_{2,t} &= \sqrt{v_{2,t}} \end{aligned} \qquad (7)$$

$\alpha_2 = 0.02$, $m_{2,t} = 0$, and $v_{2,t} = 0$ in [3].

If (6) is true the algorithm considers that the acoustic threshold has been crossed. The Acoustic confidence level is computed based on the ratio of total crossing events to total samples in a window of nominal size equal to W_{Acou_CDL} samples (actual value may vary depending on experimentation). *The Acoustic confidence detection level is the only value transmitted to the associated relay node.* The nominal sampling rate for the Acoustic sensor is 1000Hz in [3] based on email exchanged with Lin Gu (author in [3]).

9.2.3 Seismic Sensor Node

The seismic sensor node is provided by Geospace Technologies (http://www.geospacelp.com/). A picture of the seismic sensor form factors is shown in Figure 29. The one in this project is the PC801 LPC. The response of the seismic sensor is shown in Figure 30.

Figure 29 Seismic sensor

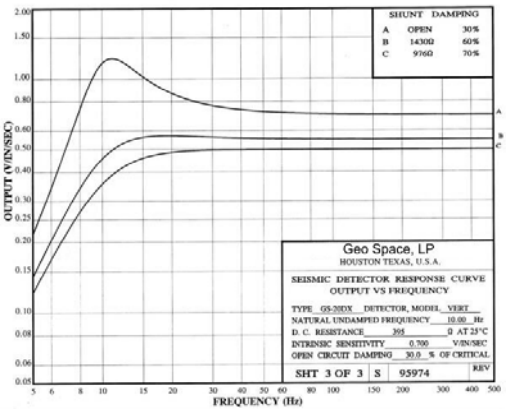


Figure 30 Seismic sensor frequency response

Sensing algorithm of Seismic sensor

The manufacturer does not specify any signal conditioning. However, due to the low frequency response of the sensor we will implement a moving average with tunable parameters as follows.

The signal values out of the seismic sensor are passed through the following moving average operation,

$$\begin{aligned} m_{3,0} &= s_0 \\ m_{3,t} &= \alpha_3 s_t + (1-\alpha_3) m_{3,t-1} \end{aligned} \qquad (8)$$

where $m_{3,t}$ is the current value of m_3, $m_{3,t-1}$ is the previous value of m_3, s_t is the current seismic reading and α_3 is a constant that needs to be found based on experimentation. Note that if $\alpha_3 = 1$ the entire samples are untouched by any signal conditioning.

In order to determine whether the seismic threshold has been crossed we find out if,

$$m_{3,t} > Threhold\_seis \qquad (9)$$

If (9) is true the algorithm considers that the seismic threshold has been crossed. The Seismic confidence level is computed based on the ratio of total crossing events to total samples in a window of nominal size equal to W_{Seis_CDL} samples (actual value may vary depending on experimentation). The Seismic confidence detection level is the only value transmitted to the associated relay node. The nominal sampling rate for the Seismic sensor is 20Hz.

9.2.4 Relay Node

The relay node serves as a message-forwarding node between the sensor nodes and the coordinator. These nodes are used to extend the coverage range of the WSN and correlate the information coming from their associated sensors in order to reduce the probability of false positives and avoid forwarding data that is deemed unnecessary. The antennae of these nodes ideally have a higher gain than the ones used for the sensor nodes in order to ensure better communication between the sensor nodes and the coordinator.

The relay node data processing Algorithm

- The relay node gathers the confidence detection levels (CDL) of its associated PIR, acoustic, and seismic sensors and constructs a vector of CDLs. Note that all the sensors of the same type have the same parameter values.

- The relay node stores the values of the CDLs sent by all sensors associated with it. This data is used to construct the vector of confidence detection levels (V-CDL), based on the V-CDL's content the relay node decides whether to transmit or discard the V-CDL as follows,

    a) The relay node will transmit the V-CDL towards the coordinator if it has more than one CDL from different sensors of the same kind with a value higher than or equal to Th_{V-CDL_X}. Where X in the sub-index identifies the sensor type (i.e., PIR, acoustic, or seismic). Different sensors imply same type of sensor, but different units (e.g., two PIR sensors).
    b) The relay node will transmit the V-CDL if within the last N_{V-CDL_X} consecutive V-CDLs there is at least one satisfying a) above.
    c) The relay node will discard the V-CDL if conditions a) and b) above are not satisfied.

- The different type of sensors have different reporting rate, therefore the relay node will receive more CDLs from the sensors that are sampled faster (e.g., Acoustic sensor). This has no impact on the application. The V-CDL is formed with a fix number of CDLs (e.g., Ten (10) CDLs) collected from all sensors in its associated group.

An example of a V-CDL construction is shown in Figure 31. Figure 31 assumes that the relay node has six sensors associated with it, two PIR, two acoustic, and two seismic and that $Th_{V-CDL\_X} = 0.5$ (i.e., 0.5 for all sensors). Figure 31 shows that we have one CDL from PIR1, one from PIR2, one from SEIS1, one from SEIS2, four from ACU1, and two

from ACU2 (Total of ten CDLs). This V-CDL is sent to the coordinator because it satisfies condition a) above since at least two different sensors of the same type show $CDL_X > Th_{V-CDL\_X}$.

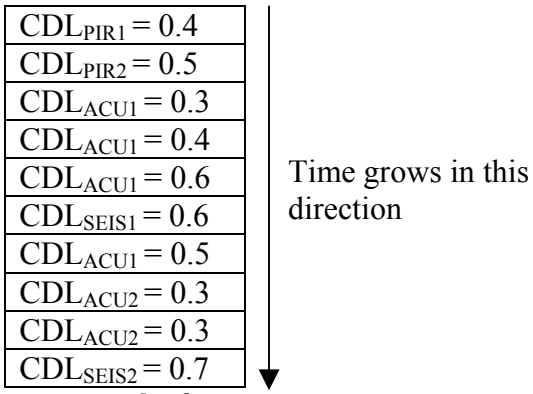


Figure 31 Example of a V-CDL.

9.2.5 Coordinator node

- There is only one coordinator node per WSN. It collects the V-CDLs from the associated relay nodes and transfers that data via serial interface to the computer.

- The antenna of the coordinator is the same as the ones used for relay nodes.

- The coordinator does not processes the data received from the relay nodes. The coordinator forwards the information from the relay nodes to the ATA in a format specified in this document, and to the application that manages the WSN.

9.2.6 WSN parameter configuration

Adjustable Parameters

It is necessary to be able to adjust relevant parameters of the WSN automatically in order to tune the sensitivity of the WSN to different targets and make experimentation and efficient data gathering a possibility. The way the user adjust this parameters is detailed in this document.

The adjustable parameters are divided in two sets:

1) The in-node sensing algorithm parameters
2) The relay node data processing algorithm parameters

In-node sensing algorithm parameters

- All the sensors of the same type have the same parameters
- In the following the values in parentheses are the ones used in [3] when available. Also the range for the parameter is specified after the semicolon.

1) PIR adjustable parameters are:

k_{PIR}: High-pass filter gain (.9): [0,1]

k_1, k_2, k_3, k_4 : Error threshold adjustment gains (.98, .02, .75, and .25): [0,1]
(Constrained to $k_1 + k_2 = k_3 + k_4 = 1$).
h: Proportionality factor of PIR crossing threshold: (0,100]
f_{PIR} : Sampling frequency of PIR sensor (50Hz): [10, 100]
W_{PIR_noise} : Window size for noise estimation (250 samples): [1, 500]
W_{PIR_CDL} : Window size for confidence detection level: [1, 500]

2) Acoustic adjustable parameters are:

α_1 : Constant for moving average (0.001): [0,1]
α_2 : Constant for moving variance (0.02): [0,1]
f_{Acou} : Sampling frequency of Acoustic sensor (1000 Hz): [500, 2000]
W_{Acou_CDL} : Window size for confidence detection level: [1, 100]

3) Seismic adjustable parameters are:

$Threshold\_seis$: Seismic crossing event threshold: [0, 5]
α_3 : Constant of moving average: [0,1]
f_{Seis} : Sampling frequency of Seismic sensor: [5, 30]
W_{Seis_CDL} : Window size for confidence detection level: [1, 50]

Relay node data processing algorithm parameters

- All relay nodes have the same parameters

Relay node adjustable parameters and ranges:

Th_{V-CDL_PIR} : V-CDL Threshold for PIR: [0,0.99]
Th_{V-CDL_Acous} : V-CDL Threshold for Acoustic: [0,0.99]
Th_{V-CDL_Seis} : V-CDL Threshold for Seismic: [0,0.99]
N_{V-CDL_PIR} : Number of V-CDLs in a window for PIR: [1, 10]
N_{V-CDL_Acous} : Number of V-CDLs in a window for Acoustic: [1,10]
N_{V-CDL_Seis} : Number of V-CDLs in a window for Seismic: [1,10]

9.3 WSN Operation Modes

9.3.1 WSN Normal Operation

During normal operation the PIR, acoustic and seismic sensors will report their corresponding CDLs to its associated relay node, and the relay nodes will report their V-CDLs to the coordinator if necessary. All parameters can be determined based on the targets that want to be detected via experimentation and during the SETUP operation mode of the WSN.

Normal Operation Messaging

In what follows, *node* refers both to the relay and sensor-nodes unless explicitly specified. In Normal operation the user of the WSN can START or STOP monitoring data from the WSN. During START the nodes report data to the PC application, and during STOP the nodes are idle and do not send any data, waiting for a command.

The high level messages in NORMAL operation are:

- NORMAL_START_REQUEST (unicast msg.: coordinator to nodes, and application to coordinator)
- START_RESPONSE (unicast msg.: coordinator to application)
- NORMAL_STOP_REQUEST (unicast msg.: coordinator to relay; relay to sensors)
- STOP_RESPONSE (unicast msg: sensors to relay; relay to coordinator)
- CONFIDENCE_DET_LEVEL (unicast msg: sensor to relay)
- VECTOR_DET_LEVEL (unicast msg: relay to coordinator)
- SANITY_CKECK (unicast msg: relay to coordinator)

Figure 32 shows the **START monitoring** procedure.

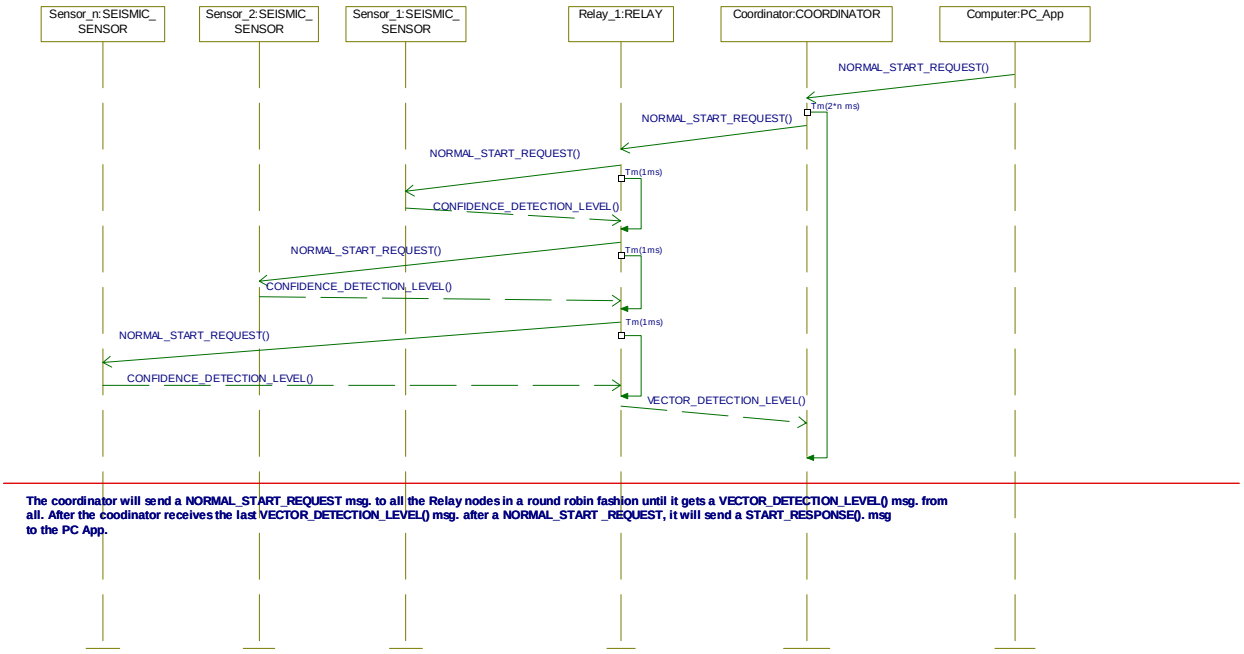


Figure 32 Message exchange diagram for WSN START monitoring procedure

The procedure is explained next.
From the coordinator and computer perspective:

1) The application in the computer sends a NORMAL_START_REQUEST message to the coordinator.
2) The coordinator starts by sending a NORMAL_START_REQUEST message addressed to the first Relay node. After the coordinator receives the VECTOR_DETECTION_LEVEL message from the first Relay node it continues and sends a NORMAL_START_REQUEST message addressed to the second

relay node if any. This procedure continues until the coordinator receives the VECTOR_DET_LEVEL of the last Relay node, after which the coordinator sends a START_RESPONSE message to the application

3) All the VECTOR_DET_LEVEL messages sent by the relay nodes are received by the coordinator and forwarded to the application. After the last VECTOR_DET_LEVEL the coordinator sends a START_RESPONSE message to the PC application.

From the relay node perspective:

1) When receiving a NORMAL_START_REQUEST message the relay node will start by sending a NORMAL_START_REQUEST message addressed to the first sensor node in its group. After the relay receives the CONFIDENCE_DET_LEVEL message from the first sensor node it continues and sends a NORMAL_START_REQUEST message addressed to the second sensor node. This procedure continues until the relay receives the CONFIDENCE_DET_LEVEL of the last sensor node in the group.
2) After receiving the last CONFIDENCE_DET_LEVEL, the Relay node constructs the V-CDL and forwards it to the coordinator regardless of the values in the V-CDL and the size of it. The latter is to let the coordinator know if all nodes started. In normal state the V-CDL values are checked as detailed in to decide whether the V-CDL will be forwarded to the coordinator or not.

Figure 33 shows the **STOP monitoring** procedure.

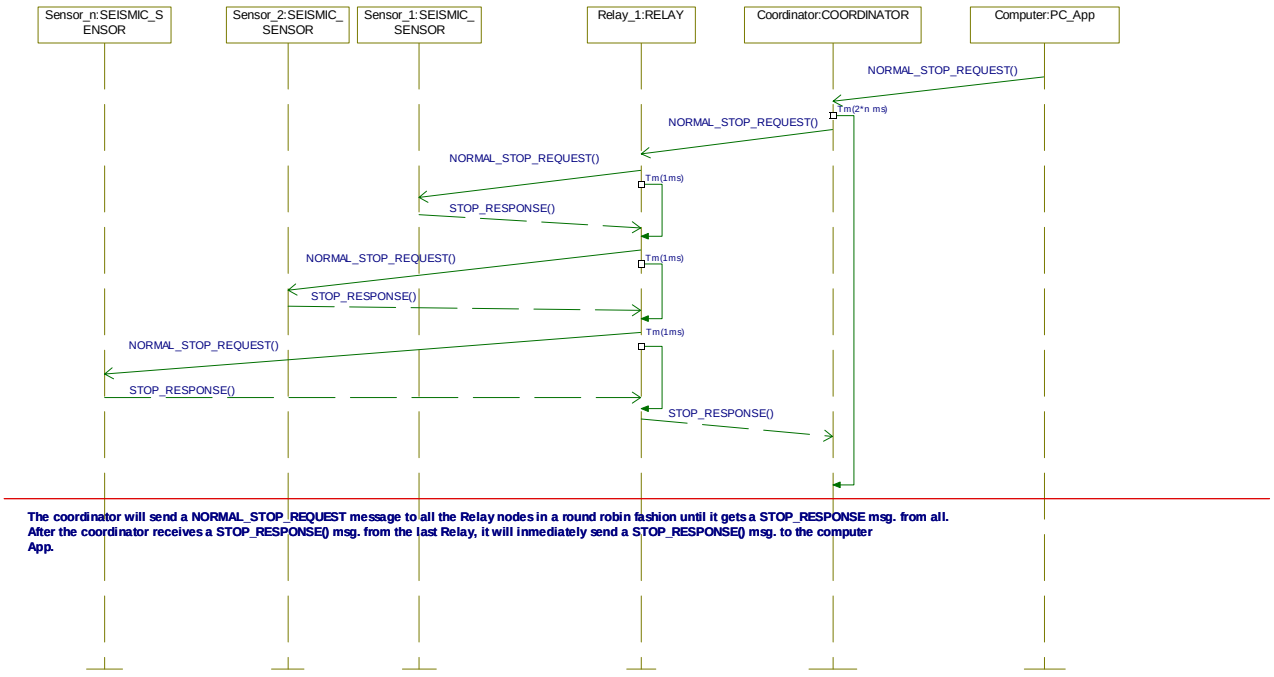


Figure 33 Message exchange diagram for WSN STOP monitoring procedure

The SANITY_CHECK message is sent periodically from every relay to the coordinator in order to inform whether the group of sensor nodes, and the relay node itself of that group, is alive. Every relay node needs to keep track of its associated sensor nodes. If a node is not responding it is assigned a status = 0, otherwise it is status = 1 in the SANITY_CHECK message.

If a sensor node does not reply with a STOP_RESPONSE (or a CONFIDENCE_DET_LEVEL) message (after the Fig8 protocol stack tries all its corresponding trials) the corresponding Relay node sends the STOP_RESPONSE (VECTOR_DET_LEVEL) message anyways and mark this node with status = 0 in the next SANITY_CHECK message it sends to the coordinator.

Normal Operation Message Formats

NORMAL_START_REQUEST (6 Bytes)

Type: (0 = normal mode, 1 = setup mode)	8 bits (0)
Message:	8 bits (0)
Destination address	16 bits
Source address	16 bits

START_RESPONSE (6 Bytes)

Type: (0 normal mode, 1 setup mode)	8 bits (0)
Message:	8 bits (1)
Destination address	16 bits
Source address	16 bits

NORMAL_STOP_REQUEST (6 Bytes)

Type:	8 bits (0)
Message:	8 bits (2)
Destination address	16 bits
Source address	16 bits

STOP_RESPONSE (6 Bytes)

Type:	8 bits (0)
Message:	8 bits (3)
Destination address	16 bits
Source address	16 bits

CONFIDENCE_DET_LEVEL (8 Bytes)

Type:	8 bits (0)
Message:	8 bits (4)
CDL	16 bits
Destination address:	16 bits
Source address	16 bits

SANITY_CHECK (18 Bytes) (There are two (2) sensor types per group)

Type:	8 bits (0)
Message:	8 bits (5)
PIR: node ID/status (status = 0 or 1)	8 bits+8bits
PIR: node ID/status (status = 0 or 1)	8 bits+8bits
Acu: node ID/status (status = 0 or 1)	8 bits+8bits
Acu: node ID/status (status = 0 or 1)	8 bits+8bits
Seis: node ID/status (status = 0 or 1)	8 bits+8bits
Seis: node ID/status (status = 0 or 1)	8 bits+8bits
Destination address:	16 bits
Source address:	16 bits

VECTOR_DET_LEVEL (38 Bytes + 2 bits)

Type:	8 bits (0)
Message:	8 bits (6)
CDL	16 bits
Sensor_Type (PIR:01, Acu: 10, Seis: 11)	2 bits
Node ID	8 bits
CDL	16 bits
Sensor_Type (PIR:01, Acu: 10, Seis: 11)	2 bits
Node ID	8 bits
CDL	16 bits
Sensor_Type (PIR:01, Acu: 10, Seis: 11)	2 bits
Node ID	8 bits

.
.
. (seven (7) more CDLs for a total of 10 CDLs

Destination address:	16 bits
Source address:	16 bits

The application's addressing scheme identifies whether the node is a relay, sensor or coordinator node, the type of sensor node (PIR, Acu, or Seis), and the group it belongs to. The address is divided as follows:

- Node type (2 bits): 00-coordinator, 01-relay, 11-sensor
- Group (4 bits): 0000 is reserved for the coordinator; Max. of 15 groups
- Sensor type (2 bits): 00 is reserved for the coordinator and the relay nodes, 01-PIR, 10-Acu, 11-Seis.
- Node ID (8 bits): Unique ID.

Normal Operation Application and User Interface

The front of the user interface is shown in Figure 34.

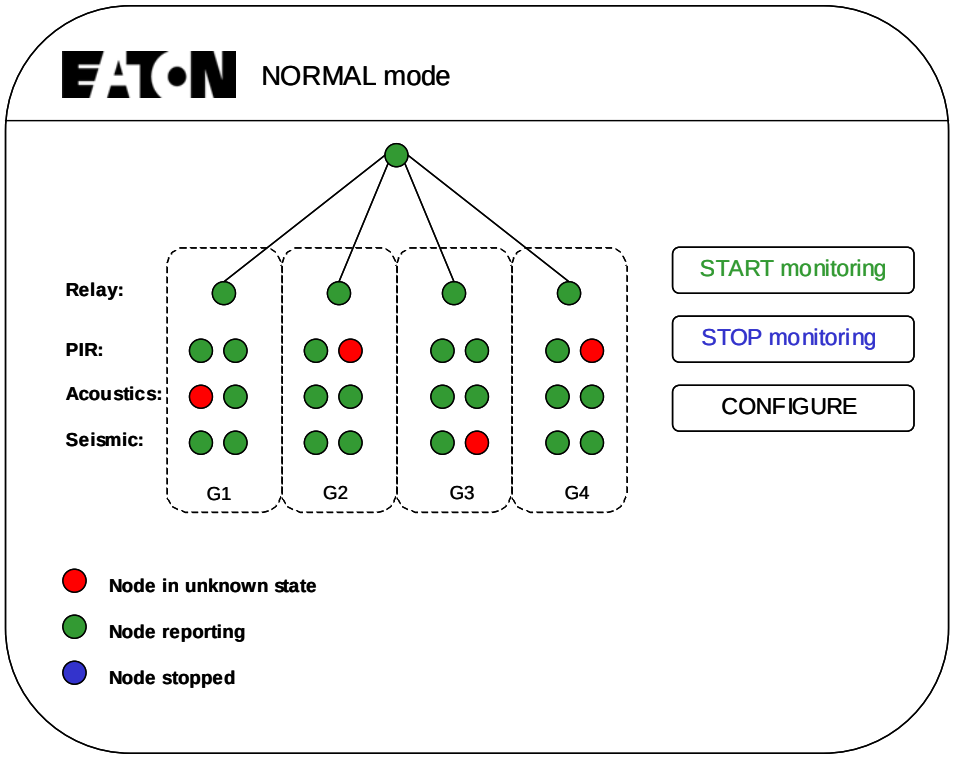


Figure 34 User interface in NORMAL mode

- The user can START, STOP or CONFIGURE the WSN. The application in the laptop will gather the data from the coordinator and make it available to the ATA. The messages from the relay nodes will also be used to update the tree shown in Figure 8, and indicate if a node is in unknown state (no data received from this node), operating normally or it has stopped after a STOP command has been sent.
- At initialization (beginning of the network life) the user can START or CONFIGURE the network.
- After the user presses the CONFIGURE button the application will take the user to the SETUP page.
- While monitoring, the application will not respond to the CONFIGURE and START buttons. The user must press the STOP button and wait until the network stops monitoring (indicated by blue nodes) to either START or CONFIGURE the network.

Note: It is assumed that if a node does not respond it will be manually fixed (a person will go and reset or fix the node).

Figure 35 shows the state diagram of the PC application. For the look of the SETUP mode interface.

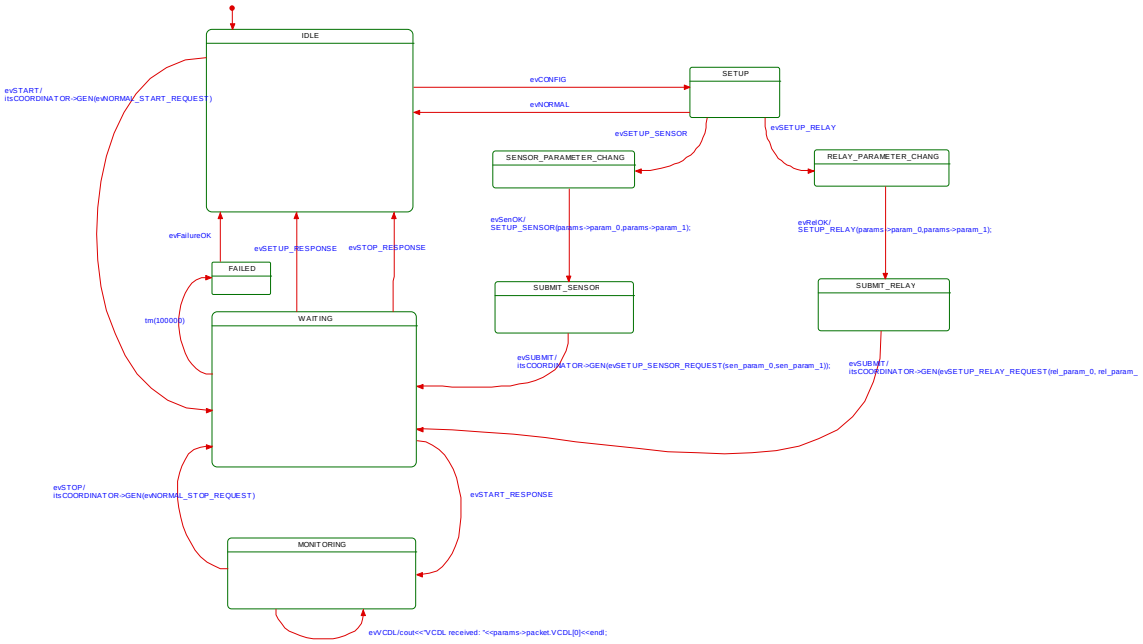


Figure 35 PC Application State Diagram

9.3.2 WSN Setup Operation

During SETUP operation the user of the WSN will adjust the parameters for the entire network via the user interface in the computer (see Figure 25). The coordinator will send a message to each sensor node individually in the WSN and wait for confirmation.

Setup Operation Messaging

The high level messages in SETUP operation are:

SETUP_REQUEST_SENSOR
SETUP_REQUEST_RELAY
SETUP_RESPONSE

Figure 36 shows a **SENSOR setup** operation and Diagram 37 shows a **RELAY setup** operation.

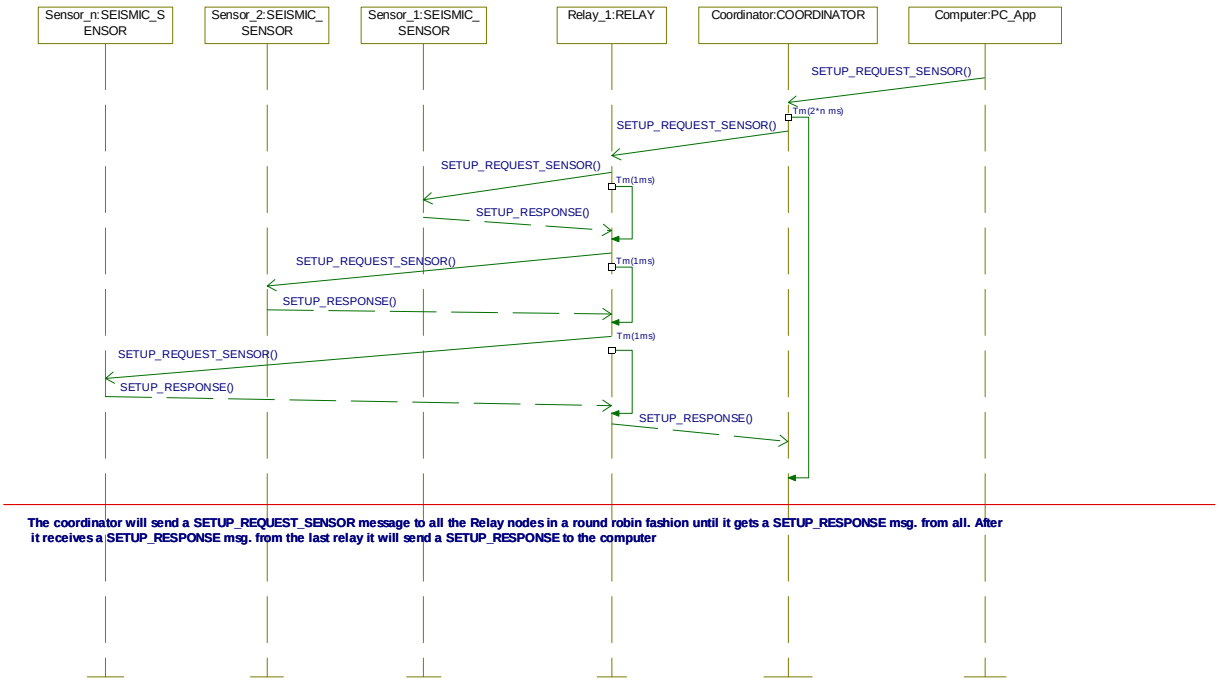


Figure 36 Message exchange diagram for sensor setup procedure

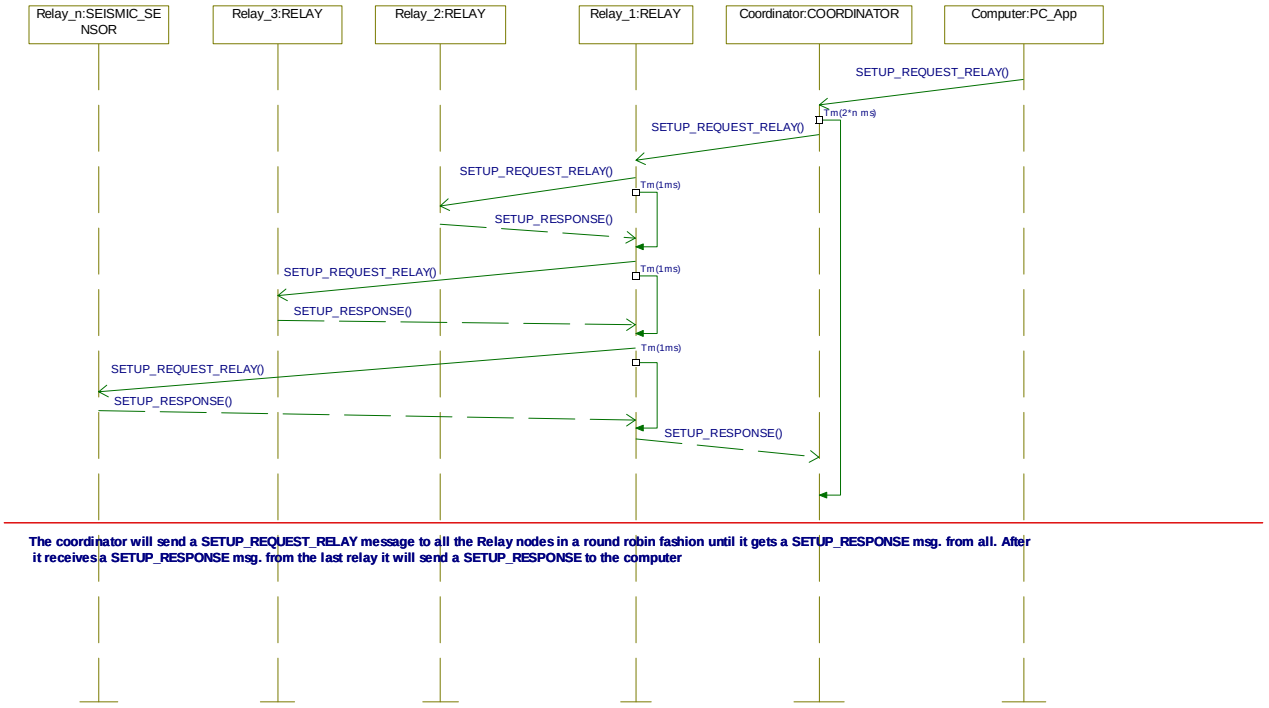


Figure 37 Message exchange diagram for relay setup procedure

SETUP_REQUEST_SENSOR (39 bytes)

Type: (0 normal mode, 1 setup mode)	8 bits (1)
Message:	8 bits (0)
PIR	
Filter gain:	16 bits
Error threshold 1:	16 bits
Error threshold 2:	16 bits
Error threshold 3:	16 bits
Error threshold 4:	16 bits
Threshold Proportional factor:	16 bits
Sampling rate:	8 bits
Noise Window:	16 bits
CDL window size:	16 bits
Acoustic	
Alpha 1:	16 bits
Alpha 2:	16 bits
Sampling rate:	16 bits
CDL window size:	16 bits
Seismic	
Threshold_seis	16 bits
Alpha 3	16 bits
Sampling rate:	16 bits
CDL window size:	16 bits
Destination address:	16 bits
Source address:	16 bits

SETUP_REQUEST_RELAY (18 Bytes)

Type:	8 bits (1)
Message:	8 bits (1)
V-CDL PIR Threshold:	16 bits
V-CDL ACU Threshold:	16 bits
V-CDL SEI Threshold:	16 bits
N-V-CDL PIR	16 bits
N-V-CDL ACU	16 bits
N-V-CDL SEI	16 bits
Destination address:	16 bits
Source address:	16 bits

SETUP_RESPONSE (6 Bytes)

Type:	8 bits (1)
Message:	8 bits (2)
Destination address:	16 bits
Source address:	16 bits

Setup Operation Application and User Interface

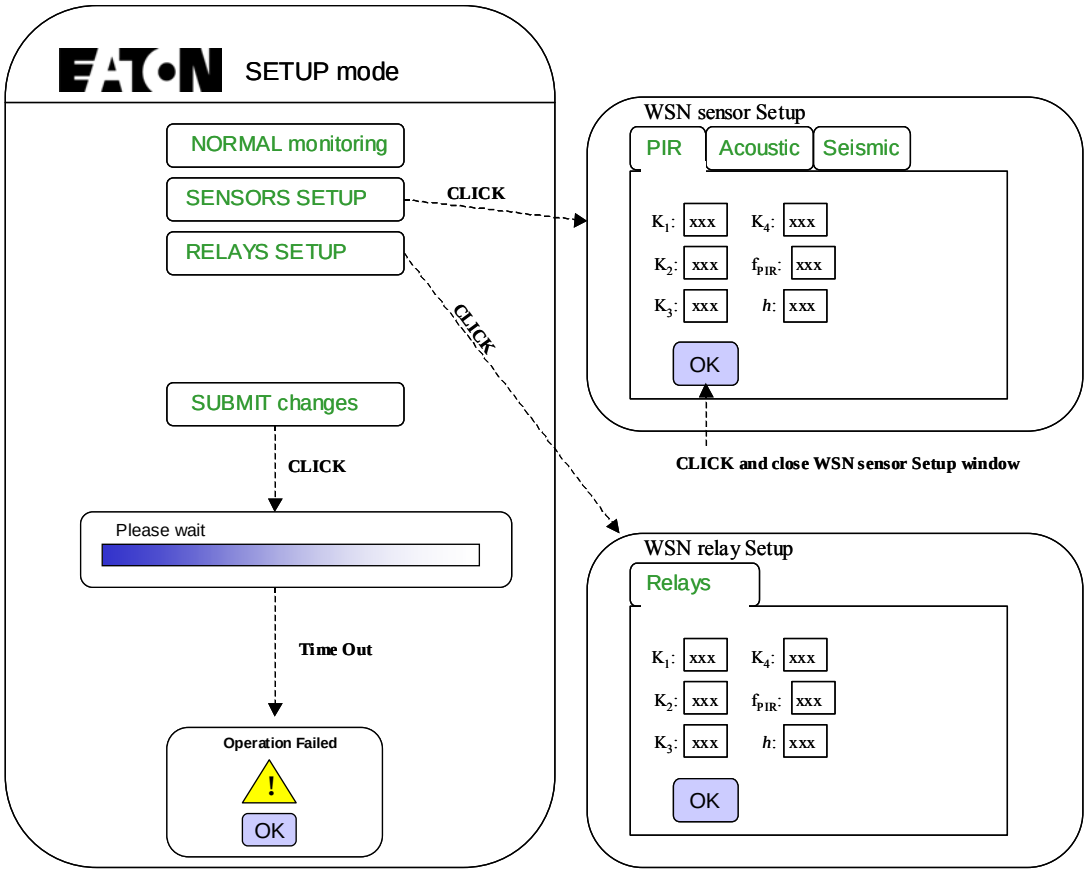


Figure 38 User interface in SETUP mode

- Once in the SETUP mode page the user can select to go back to NORMAL mode. It can also change the sensor parameters using the SENSORS SETUP button, and finally submit the new parameters using the SUBMIT button shown in Figure 38.
- After pressing the SENSORS SETUP button a WSN sensor Setup window will pop-up as shown in Figure 38. The user can change the parameters of the sensors in this window. After the user is done changing the parameters in all the desired sensors He/She must press the OK button, which will close the window.
- In order for the changes to take effect the user must press the SUBMIT button. After pressing SUBMIT, the SETUP window closes and a waiting window opens. If operation success the user is taken back to the NORMAL window, which remains open all the time (until the user closes the application). If the operation fails, an *Operation failed* Window pops-up. The user clicks OK in this latter window and the user is taken back to the NORMAL window.
- Some nodes may not respond to the SETUP. These nodes will turn red. Otherwise they will go back to blue.

9.3.3 State Diagrams for Coordinator/Relay/Sensor nodes

The state diagrams that follow are a slightly simplified version of the actual state machines that will be implemented. These state machines have been tested/validated by executing them in the Rhapsody Model Driven Development (MDD) environment.

Coordinator

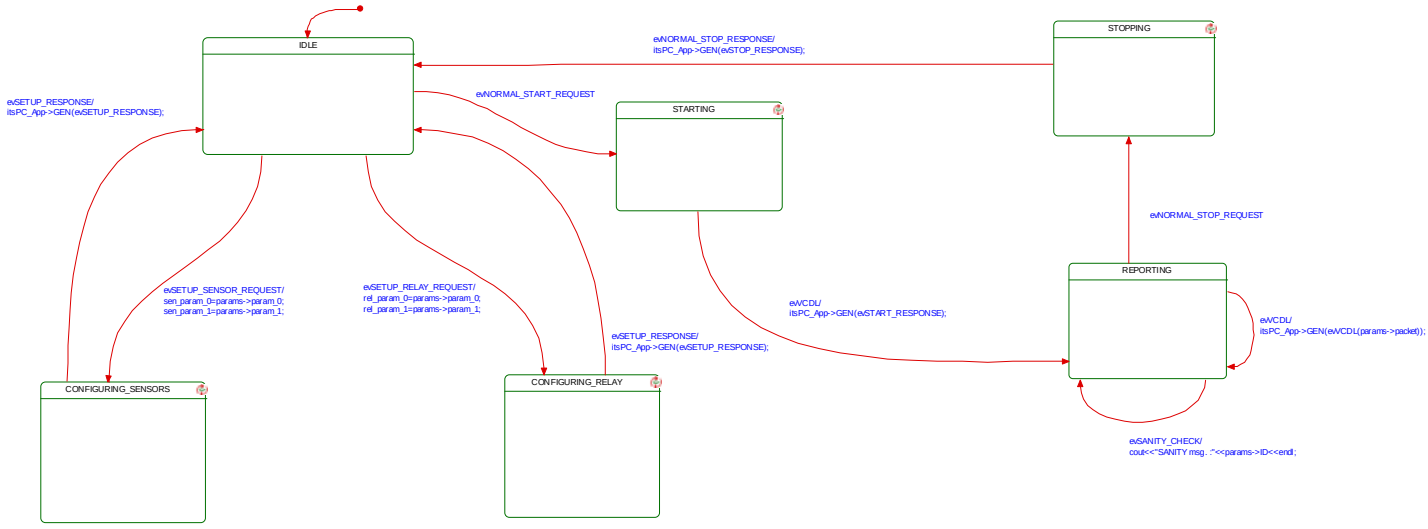


Figure 39 Coordinator state diagram

Relay

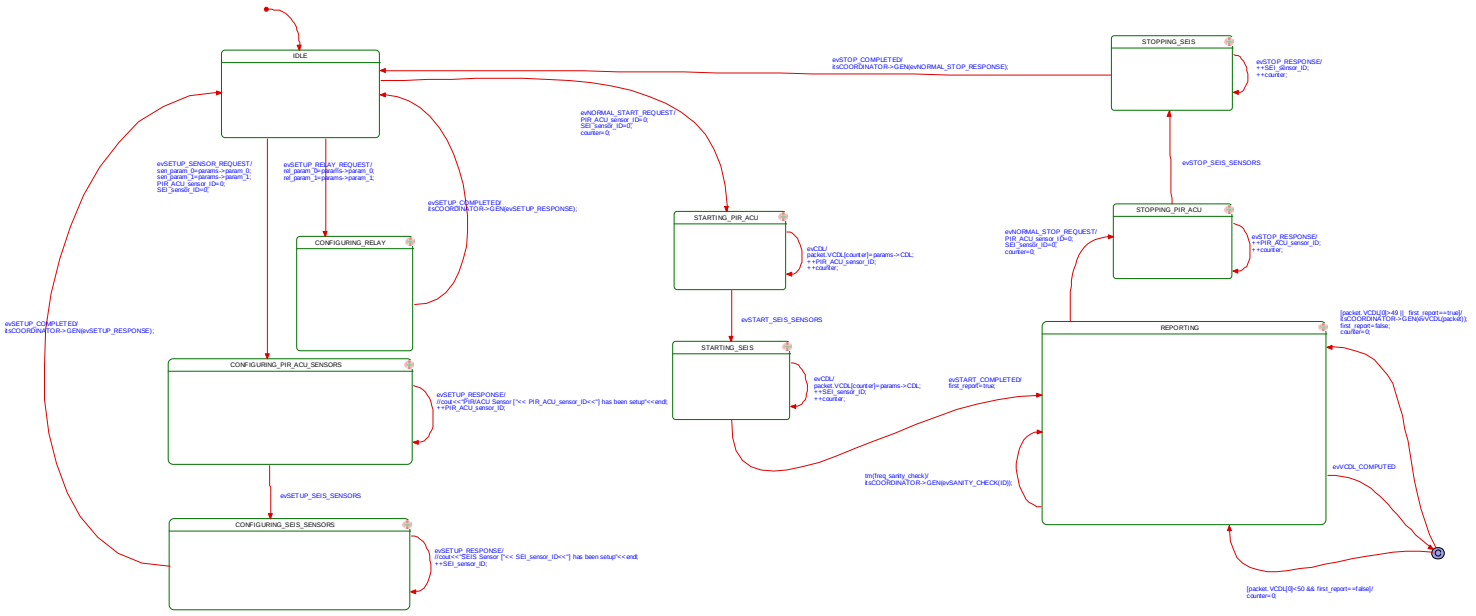


Figure 40 Relay state diagram

PIR/Acoustic sensor

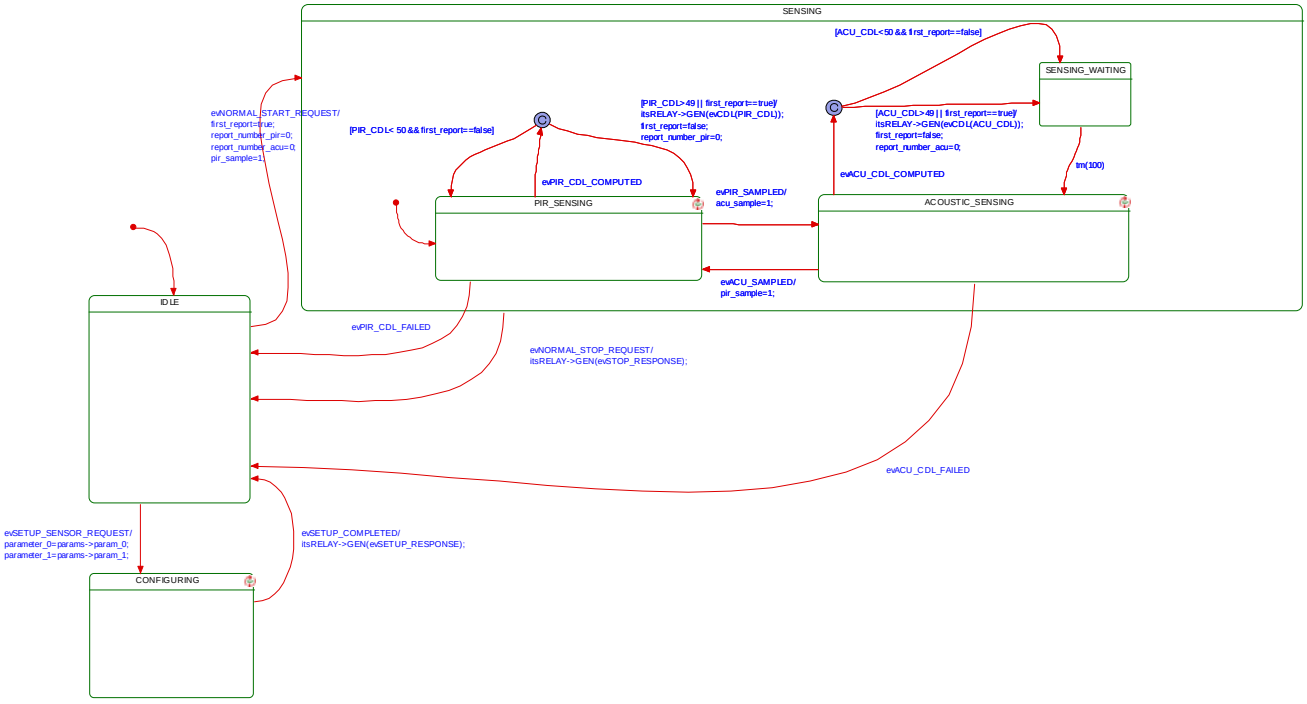


Figure 41 PIR/Acoustic state diagram

Seismic sensor

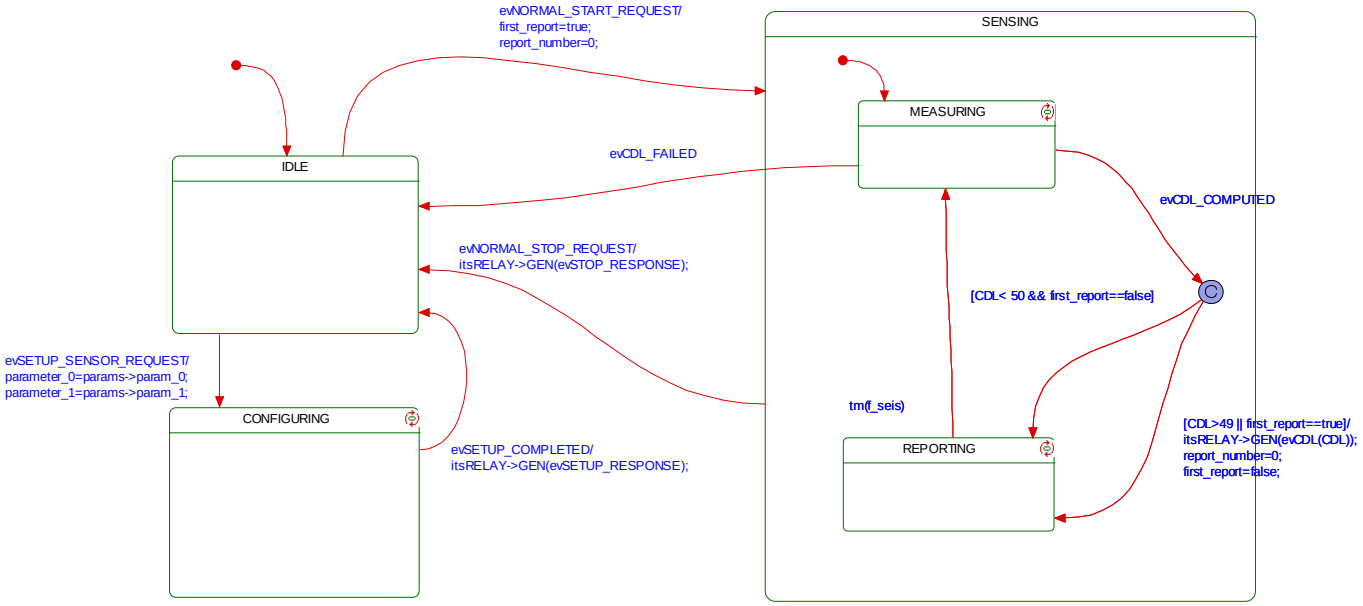


Figure 42 Seismic state diagram

Table interface between PC Application and Anticipatory Theory Application

The PC application receives VCDL messages from the coordinator and writes to a file with the format shown in Table 1 in a comma separated value (CSV) file format.

	Group 1							Group 2							...	Group k						
timestamp	PIR1	PIR2	ACU1	ACU2	SEIS1	SEIS2	status code	PIR1	PIR2	ACU1	ACU2	SEIS1	SEIS2	status code		PIR1	PIR2	ACU1	ACU2	SEIS1	SEIS2	status code
	CDL	...					sc	CDL	...					sc		CDL	...					sc
	...	...						...	...							...	...					
			...							...								...				
				...							...								...			
					...							...								...		
						...							...								...	

Table 2 Table that stores the data from the sensors in the WSN

The data in Table 1 grows up to a certain point and then the oldest values are discarded as soon as new values arrive due to memory limitations. Physical location of the groups and sensors is known *a-priori*.

The status code (sc) identifies the sensors that are not reporting normally. Sensors that are not reporting normally are not reliable and need to be fixed manually, which involves removing the sensor node from the network. The sc is constructed based on the SANITY_CHECK message received from the coordinator. The sc is encoded following the order in Table 1, and indicating with a Zero (0) that the node is not reporting, and with a One (1) that the node that is reporting normally. For instance, if sc = 100101 => PIR2, ACU1, and SEIS1 are not reporting normally in this group at the time indicated by the timestamp. In order to decode sc a possible way is to perform six "AND" operations between the sc and all the unitary basis vectors of dimension 6 (i.e., 000001, 000010, 000100, 001000 etc).

The data in Table 1 is also used by the PC app GUI of the WSN to show the status of the nodes in the network.

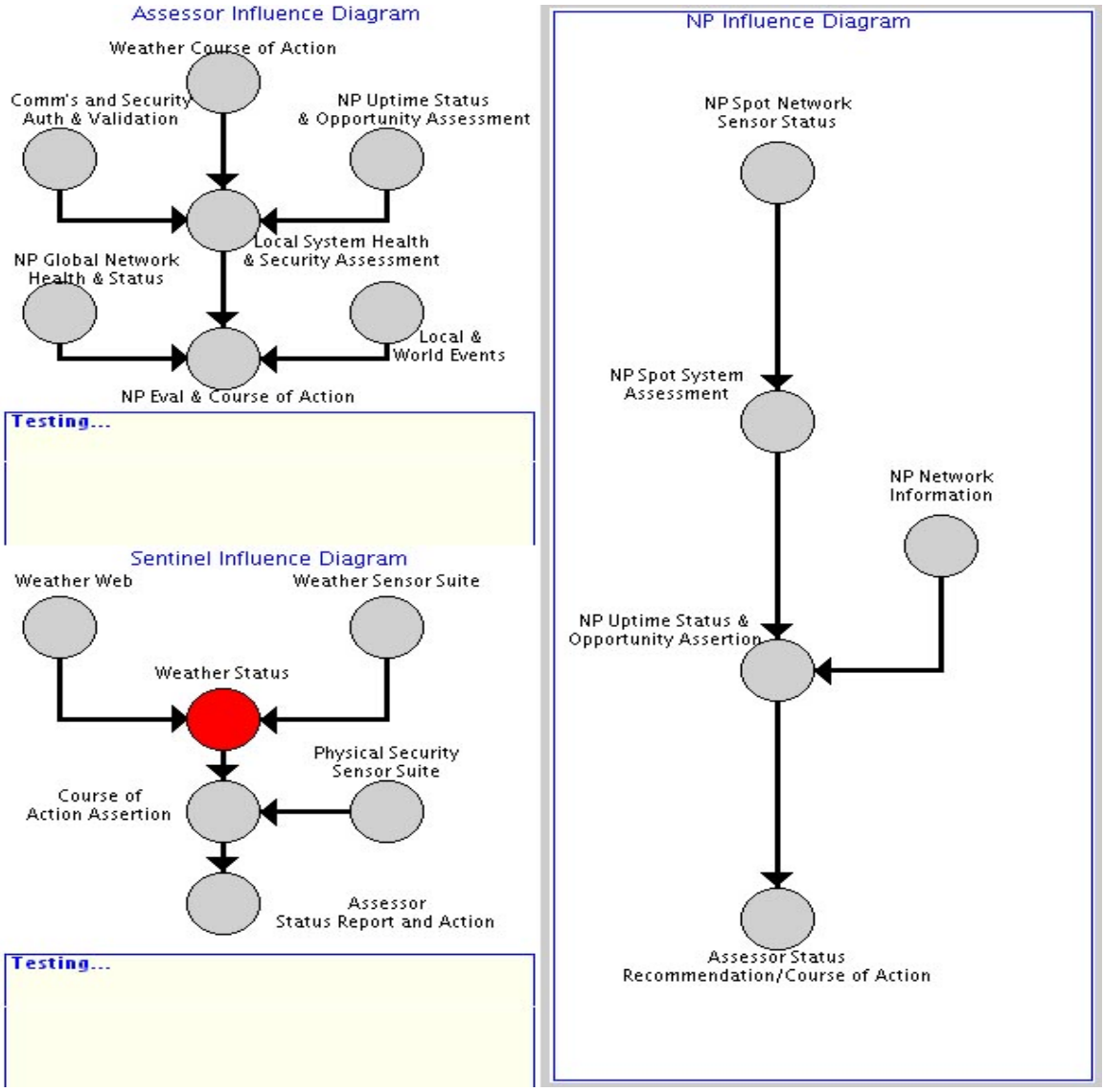
References:

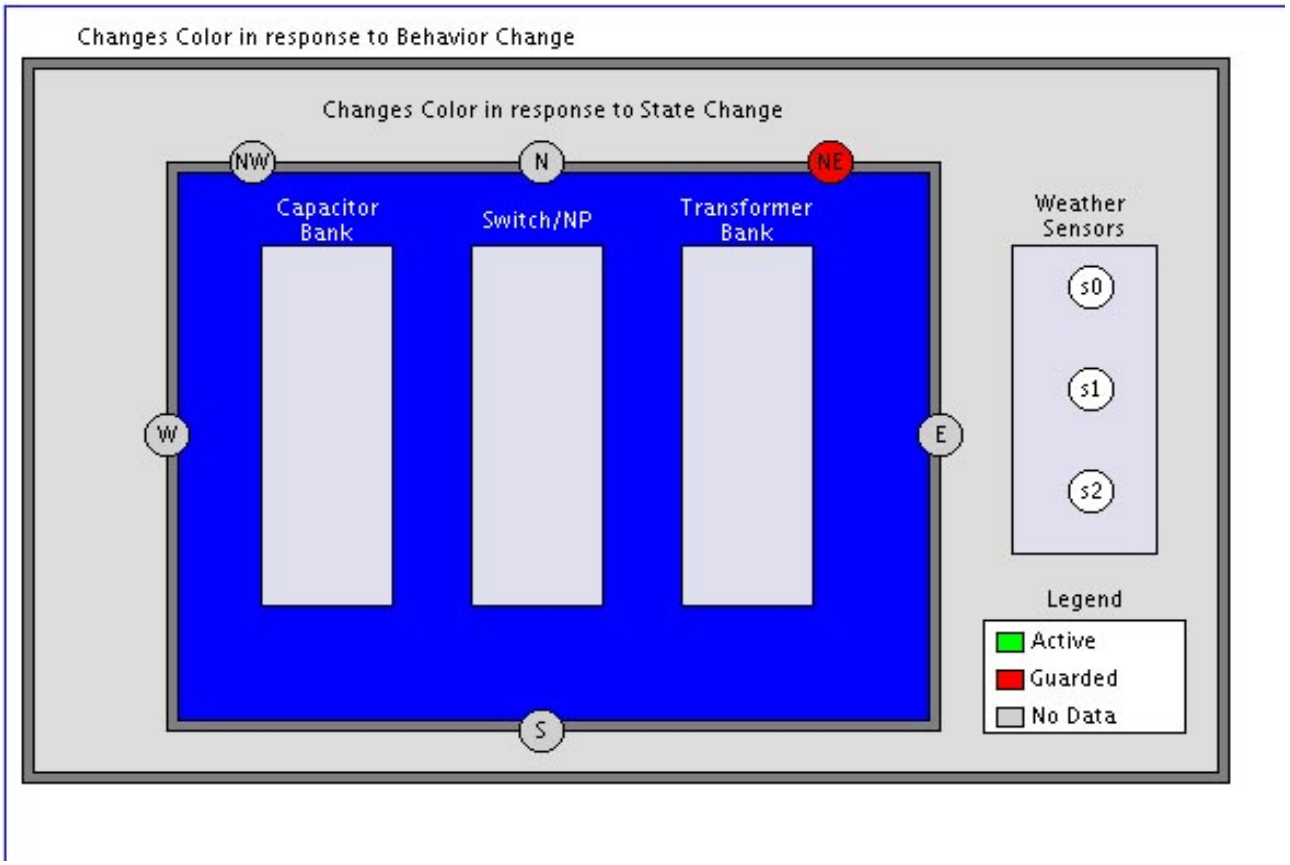
[1] Foran, R.A, et. al., "Very near ground radio frequency propagation measurements and analysis for military applications," IEEE Conf. On Military Communications MILCOM, 1999, Vol.1, pp. 336-340.

[2] Welch, TB, et. al., "Very near-ground RF propagation measurements for wireless systems," IEEE Conf. On Vehicular Technology VTC 2000, Vol. 3, pp. 2556-2558.

[3] Lin Gu et. al., "Lightweight detection and classification for wireless sensor networks in realistic environments," SenSys'05 November 2005, USA.

APPENDIX I - DEMO




Changes Color in response to Behavior Change
Changes Color in response to State Change
NW
N
NE
Capacitor Bank
Switch/NP
Transformer Bank
Weather Sensors
s0
s1
s2
W
E
S
Legend
Active
Guarded
No Data