ABSTRACT

TRACKING THE PATH OF A MOBILE RADIOACTIVE SOURCE USING A WIRELESS SENSOR NETWORK

by
Nipa Shah

This report describes several experiments used to characterize and test a network of radiation sensors. The purpose of these tests is to assess the feasibility of using these sensors to detect and track radioactive sources in a large field, as in a battlefield or on a military campus. Simulated radiation measurements are used to compare the result of radiation detection accuracy in tracking the moving target and to find its path as early as possible. This is done via changing the number of sensing nodes deployed (deployment density), as well as the models of the detectors. This thesis describes algorithms for both detecting the presence and tracking the position of radioactive sources. It formulates the detection problem as a nonparametric hypothesis-testing problem that is solved by comparing a statistic computed over some window of observation of the data to a threshold value. If this threshold is exceeded then it is decided that a source is present. The tracking results thus found are compared with the actual chosen path within the implemented experiment. Detection delay has been measured while trading off battery consumption and accuracy.

TRACKING THE PATH OF A MOBILE RADIOACTIVE SOURCE USING A WIRELESS SENSOR NETWORK

by

Nipa Shah

A Thesis
Submitted to the Faculty of
New Jersey Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Engineering

Department of Electrical and Computer Engineering

May 2003

APPROVAL PAGE

TRACKING THE PATH OF A MOBILE RADIOACTIVE SOURCE USING A WIRELESS SENSOR NETWORK

Nipa Shah

Dr. Constantine Manikopoulos, Thesis Advisor Date
Associate Professor, Department Electrical and Computer Engineering, NJIT

Dr. George Antoniou, Committee Member Date
Professor, Department of Computer Science, Montclair State University

Dr. Bin He, Committee Member Date
Senior scientist, XPRT Solutions Inc.

BIOGRAPHICAL SKETCH

Author:	Nipa Shah
Degree:	Master of Science
Date:	Spring 2003

Undergraduate and Graduate Education:

- Master of Science in Computer Engineering
  New Jersey Institute of Technology, Newark, NJ, 2003

- Bachelor of Science in Mechanical Engineering,
  Birla Vishwakarma Mahavidyalaya, V.V.Nagar, India, 1997

Major:	Computer Engineering

This thesis is dedicated to
my husband and my parents for giving me love, encouragement and support

ACKNOWLEDGMENT

I would like to express my deepest appreciation to Dr. Constantine Manikopoulos, my research supervisor, providing valuable and countless resources and insight. I would like to thank Ms. Ling Lee for her constant assistant and direction through the entire course of this research. I would like to thank Ms. Jacky Tadros for her valuable help accomplishing my thesis work. In addition I would like to express my deepest gratitude to my friend Vikas Gaddu who have helped me in one way or the other through this period and have always provided persistent encouragement.

TABLE OF CONTENTS

Chapter **Page**

TABLE OF CONTENTS
(Continued)

Chapter Page

TABLE OF CONTENTS
(Continued)

Chapter **Page**

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

The availability of low-power micro-sensors, actuators, embedded processors, and radios is enabling the application of distributed wireless sensing to a wide range of applications, including environmental monitoring, smart spaces, medical applications, and precision agriculture [1][2]. Most deployed sensor networks involve relatively small numbers of sensors, wired to a central processing unit where all of the signal processing is performed [3]. In contrast, this paper focuses on distributed, wireless, sensor networks in which the signal processing is distributed along with the sensing.

Why distributed sensing?

When the precise location of a signal of interest is unknown in a monitored region, distributed sensing allows one to place the sensors closer to the phenomena being monitored than if only a single sensor were used. This yields higher SNR, and improved opportunities for line of sight.

While SNR can be addressed in many cases by deploying one very large sensitive sensor, line of sight, and more generally obstructions, cannot be addressed by deploying one sensor regardless of its sensitivity. Thus, distributed sensing provides robustness to environmental obstacles.

Why distributed processing?

When wired networking of distributed sensors can be easily achieved, it is often the more advantageous approach. Moreover, when nodes can be wired to renewable (relatively infinite) energy sources, this too greatly simplifies the system design and operation. However, in many envisioned applications, the environment being monitored does not have installed infrastructure for either communications or energy, and therefore unlettered nodes must rely on local, finite, and relatively small energy sources, as well as wireless communication channels.

Finally, although sensors are distributed to be close to the phenomena, one might still consider an architecture in which sensor outputs could be communicated back to a central processing unit. However, in the context of undeterred nodes, the finite energy budget is a primary design constraint. Communications is a key energy consumer as the radio signal power in sensor networks drops off with r^4 [4] due to ground reflections from short antenna heights. Therefore, one wants to process data as much as possible inside the network to reduce the number of bits transmitted, particularly over longer distances.

CHAPTER 2

SENSOR NETWORK

In this chapter, the author will try to explore the design of a radiation sensor network.

The powers of correlated sensor systems arise from their networked nature. Part of the problem of using standalone sensors is that many sensors, particularly those that detect nuclear radiation such as gamma rays and neutrons, have a hard time differentiating between a the targeted and normal variations in the background radiation. Furthermore to compound the challenge, the farther one moves away from a nuclear source, the weaker the signals become.

As the distance between a detector and source increases, the radiation signature quickly fades into the background caused by other artificial and natural sources. One solution is to network the sensors, that is, have them share the information they gather, to allow the user to see more by creating a more complete picture of the situation. This is something, which stand-alone sensors cannot do. A sensor network could first, could provide a way to discard signals that are false alarms. Second, it could pick up on signals that might be real alarms but would have been ignored by stand-alone sensors because the signals were under a preset threshold of sensitivity.

2.1 Wireless Microsensor Networks

Wireless sensor networks represent a new paradigm for extracting data from the environment. Conventional systems use large, expensive macro sensors that are often wired directed to an end-user and need to be accurately placed to obtain the data.

These nodes are very expensive and required large amounts of energy for operation. They must be placed in exact locations, since there are a limited number of nodes extracting information from the environment.

Using mircrosensors to create networks would be fault-tolerant, as the sheer number of nodes can ensure that there is enough redundancy in data acquisition that not all nodes need to be functional. Using wireless communication between the nodes can be considered a pre-phase to eliminate the need for a fixed infrastructure.

A digital spread spectrum radio in each wireless sensing node provides a robust wireless communication link. It enables data rates of 100 kbits per second over ranges in excess of 100 meters. Two-way, peer-to-peer communication among nodes in a small neighborhood supports multi-hop data transfers, avoiding the requirement for all nodes to be in range of a base station. This feature gives users a very high degree of flexibility in the deployment of the nodes enabling strategic sensor placement in the area of interest without the constraint of line-of-sight communications to a central data collection or gateway site. The Wireless Sensing Network concept takes advantage of the fact that short-range radio hops are exponentially more power-efficient than larger hops to cover the same distance. Power control on each radio is further used to minimize the transmit power needed to communicate with its neighbors.

Wireless Sensing Network is distinguished from that in a conventional wireless data network in the following way:

1. Nodes have limited battery energy, requiring special routing schemes optimized for minimal power consumption.

2. The sensor nodes may require synchronization for time tagging of data and coherent signal processing that is implemented with power conserving, network time distribution algorithms.
3. Nodes may have multiple sensor types (e.g., seismic, acoustic,etc.), each with different coverage, accuracy, and power consumption, and allowing local sensor fusion.
4. The generated traffic patterns of the Wireless Sensing Network are generally predictable, allowing efficient tuning of protocols. While traffic is created by random events (e.g. target detections, user commands), the destinations and hence routes are constrained, as are the message volumes and allowed latencies. Detection information is forwarded to portals; however, there are many opportunities for data summarization along the network routing path.
5. Cooperative processing, such as beam-forming, requires dynamic multicast groups of nodes that are closest to the events. Since targets or other phenomena that cause events can be mobile, the set of nodes that are actively sensing them will change, moving the locus of message generators.

The requirement for simple node deployment necessitates that the network of nodes be capable of self-discovery and self-configuration. Self-organizing procedures for boot-up and automatic node incorporation into the network have been implemented. This allows nodes to be added to an operational network for improved coverage or replenishment. Mechanisms for recovering from node failures are included so that the network will be self-healing. The RSC approach is to create and evolve a power-efficient, time-division multiple access scheme supporting multi-hop communication. New, specialized protocols for RSC Wireless Sensing Network nodes are being developed to address the shortcomings of the point-to-point and multicast addressing and communication patterns supported by conventional computer networks (e.g., TCP/IP). These include large overhead, non-real-time delivery, no inherent power management and lack of spatial addressing. As one example, routing algorithms should avoid creating "power consumption hotspots" that result in sensors in a neighborhood dissipating battery energy much more rapidly than the rest of the network, causing partitions when their energy is depleted.

2.2 Design Goals for Wireless Microsensor Network Protocols

In order to design good protocols for wireless microsensor networks, it is important to understand the parameters that are important to the sensor applications. While there are many ways in which protocols are beneficial to the application, The author use the following metrics [8]:

2.2.1 Ease of Deployment

Sensor networks may contain hundreds of thousands of nodes. They may need to be deployed in remote or dangerous environments. Sensor nodes are required to be small enough and cheap enough, so that in cases of one of the above environments, they can be dropped by unmanned aerial vehicles (UAVs) which drop the sensors in predetermined locations and then act as airborne routers. These vehicles are under research to be evaluated for the use of placing, operating and maintaining sensor networks in rugged terrain. Once in place, the sensors would form a network and communicate with each other, and send information to the gateway or the sink node to be collected and transmitted by the planes about the network infrastructure created.

2.2.2 System Lifetime

These networks should function as long as possible. System lifetime can be measured using generic parameters, such as the time until the nodes die, or it can be measured using applications-specific parameters, such as the time until the sensor network is no longer providing acceptable quality results.

2.3.3 Latency

Data from sensor networks are typically time-sensitive, so it is important to receive the data in a timely manner. Long delays, due to processing or communication, may be unacceptable.

2.3.4 Quality

This parameter measures the accuracy of the result of the sensor network with what is actually occurring in the environment. Although this is an application specific and data dependent quantity, one possible application independent method of determining quality is to determine the amount of data, actual or aggregate, that is received at the base station. The more data the base station receives, the more accurate its view of the remote environment will be.

2.3 Challenges to Meet the Design Goals

In a sensor network, data sensed by each node is required at a remote base station, rather than at other nodes, and the data are being extracted from the environment, leading to large amounts of correlation among data signals. The end-user does not require all the data in the network, because the data from the neighboring nodes is highly correlated, making the data redundant, and the end-user cares about a higher-level description of events occurring in the environment the nodes are monitoring. The quality of the network is therefore based on the quality of the aggregate data set, rather than the quality of the individual data signals; protocols should be designed to optimize for the unique, application-specific quality of a sensor network.

To summarize, wireless sensor network protocols should be:

- Self-configuring, to enable ease of deployment of networks.
- Energy-efficient and robust, to extend system lifetime.
- Latency-aware, to get the information to the end-user as quickly as possible.
- Cognitive of the application-specific nature of network quality.

The research presented here focuses on ways in which least feature may be exploited to create protocol architecture that optimizes the different desired features of this network. The sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink or cluster header. Data is routed back to the sink by a multihop infrastructureless architecture through the sink [9] as shown in Figure 3.1.

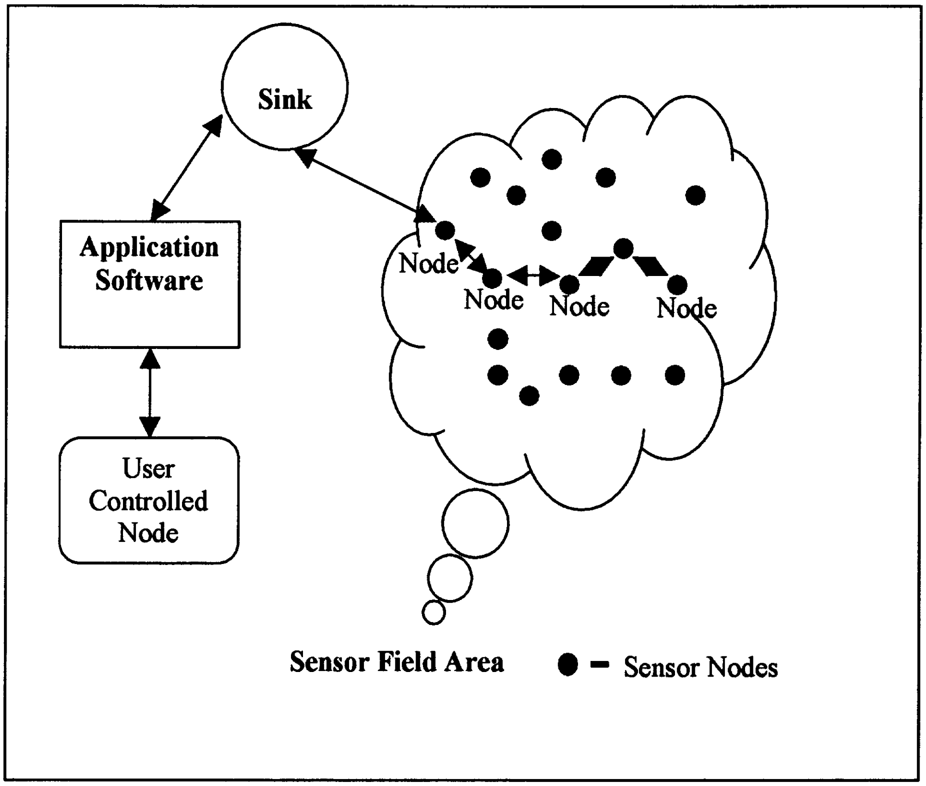

Figure 2.1 Tiered Architecture of sensor network (1st tier randomly distributed network, 2nd tier Sink or Cluster Headers and 3rd tier is the base station).

To meet the design goals the design of the sensor network is influenced by many factors such as the following.

2.3.1 Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, or have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor nodes failures. The reliability R_k (t) or fault tolerance of a sensor node is modeled in using the Poisson distribution to capture the probability of not having a failure within the time interval (0,t):

$$R_k(t) = e^{-\lambda_k t}$$

Where,

λ_k = failure rate of sensor node

k = sensor node failed

t = time period.

2.3.2 Scalability

The number of sensor nodes deployed in studying a phenomenon may be on the order of hundreds or thousands. Depending on the application, the number may be either sparse or dense in a specific area. New schemes must be able to work with this number of nodes. They must also utilize the high density of the sensor networks. The density can range from a few sensor nodes to a few hundred-sensor nodes in a region, which can be less than 20 m in diameter. The density μ can be calculated as:

$$\mu(R) \approx (N * \pi R^2)/A$$

Where,

N = number of scattered sensor nodes

A = the region in which node is scattered

R = the radio transmission range.

The density gives the number of nodes with the transmission radius of each node in a region A.

2.3.3 Production Costs

Since sensor networks consist of large number of sensor nodes, the cost of a single node is very important to be justified to the overall cost of the network. If the cost of the network is more expensive than deploying traditional sensors, the sensor network is not cost-justified. As a result, the cost of each sensor node has to be kept low.

2.3.4 Hardware Constraints

A sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit, and a power unit. They may have additional application-dependant unit as in our case where the sensor requires a location finding system, mobilizer and a power generator.

2.4 Fault Diagnosis in Wireless Sensor Network

Since the sensor network has its limitation in regards to energy supply, some protocols exploit network redundancy to achieve fault tolerance. When a sensor crashes, either because of battery depletion or due to a catastrophic event, neighboring sensors can cover, at least partially, its sensing task. However, none of these protocols provide explicit knowledge regarding the state (faulty or fault-free) of the sensors in the network. In our opinion, the extraction of explicit diagnostic information from the network could be important in those situations in which sensors repair or reconfiguration is feasible.

If there is no provisioning for sensor maintenance, eventually batteries will be depleted in the sensors and crash. As a consequence, the number of non-operating sensors in the system will increase until the system gets disconnected, and is no longer functional. In such a scenario, sensors should provide diagnostic information along with sensor data, thus enabling rangers to maintain network functionality by replacing faulty sensors or by recharging depleted batteries, whenever required. For this purpose, sensors in the network should execute a distributed diagnosis protocol, either periodically or on-demand.

However, existing distributed diagnosis protocols have been designed either for multiprocessor computers or for wired computer networks. As a consequence, all the protocols proposed so far assume that units communicate according to the one-to-one paradigm typical of wired networks. This means that, if applied to sensor networks, these models are unable to take advantage of the shared nature of communication, and are thus not feasible or at best extremely energy consuming.

For this reason, a distributed silent fault diagnosis protocol was developed, explicitly designed for wireless sensor networks. The protocol takes advantage of the shared nature of communications and aims at minimizing the total number of bits exchanged for the purpose of diagnosis, thus reducing the energy consumption entailed by the protocol execution. The protocol first constructs a spanning tree of the graph representing the network topology, and then exchanges diagnostic information only along the edges of the tree. This allows a significant reduction in the number of messages to be sent for the purpose of diagnosis. It was shown that the protocol exchanges the minimum number of bits required by any diagnosis algorithm for wireless sensor networks, thus proving its optimality.

2.5 Quality of Service (QoS) in a Wireless Sensor Network

The quality of service (QoS) of a wireless network depends on the application and the requirement of the network. A number of QoS parameters can be measured and monitored to determine whether a service level offered or received is being achieved. These parameters consist of the following.

2.5.1 Network Availability

Network availability can have a significant affect on QoS. Simply put, if the network is not available, even during brief periods of the time, the user or application may achieve unpredictable or undesirable performance.

2.5.2 Bandwidth

Bandwidth is probably the second most significant parameter that affects QoS. Bandwidth allocation can be subdivided into two types:

- Available Bandwidth
- Guaranteed Bandwidth

2.5.3 Delay

Network delay is the transition time an application experiences from the ingress point to the egress point of the network. Delay can cause significant QoS issues with time-sensitive applications. Timing out can simply cause transmission fail are under excessive delay conditions.

2.5.4 Jitter

Jitter is the measure of delay variation between consecutive packets for a given traffic flow. Jitter has a pronounced effect on real time, delay sensitive applications as they expect to receive packets at a fairly constant rate with fixed delay between consecutive packets. As the arrival rate varies, the jitter impacts the application's performance and accuracy.

2.5.5 Loss

Loss can occur due to errors introduced by the physical transmission medium. For example, most landline connections have very low loss as measured in the Bit Error Rate (BET). However, wireless connections, mobile or fixed, have a high BER that varies due to environment or geographical conditions such as fog, rain, Radio Frequency (RF) interference, and mountains. Wireless technologies often transmit redundant since packets will inherently get dropped some of the time due to the nature of the transmission medium.

2.6 Sensor Network Architecture

Conceptually, a sensor network is organized as a three-layer system infrastructure, which refers to the physical sensors, their physical characteristics and capabilities, the number of sensors and their deployment strategy. The networking protocol is responsible for dissemination of the sensed data by creating and maintaining paths between the sensors and the base station. The application is responsible for translating the observer interests into specific network-level operations.

2.6.1 Infrastructure

Although there is a large body of work in building and networking sensors, these studies focus on optimizing the application and networking protocol to improve performance. In contrast, it is obvious that there is a tradeoff in the infrastructure design and their implications on performance and the design of the networking protocol. Intuitively, it appears that a denser infrastructure leads to a more effective sensor network because higher accuracy is likely and a larger aggregate amount of energy is available in the network.

However, if not properly managed, a denser network will lead to a larger number of collisions and potentially to congestion in the network; this will increase latency and reduce energy efficiency. Moreover, the large number of samples reported by the sensors may exceed the accuracy requirements of the observer. Thus, simply increasing the reporting rate or the number of sensors may actually harm the performance of the network.

One of the lessons learned from this comparison is that a form of congestion control is necessary to make sure that the reported samples do not exceed the capacity of the network. In addition this control is necessary to optimize the lifetime of the network while meeting the minimum accuracy requirement of the application. Thus, the congestion control must not only be based on the capacity of the network, but also on the accuracy level required at the observer. The traffic in a sensor network is different from conventional networks. It is a collective communication operation with redundancy. Thus, the network protocol has the flexibility of meeting the performance demands by controlling the reporting rate of the sensors, controlling the virtual topology of the network (ex. turning off some sensors), or optimizing the collective reduction communication operation (ex. Fusing data along the way).

2.6.1.1 Infrastructure Features. In a wireless sensor network, data sensed by each node are required at the base station, rather then at other nodes, and the data is being extracted from the environment, leading to large amounts of correlation among data signals.

For a sensor the infrastructure of a sensor network refers to the characteristics of the individual sensors, the number of sensors deployed, and the deployment strategy. This will be discussing each of these in turn.

2.6.1.2 Sensors' Capabilities. A sensor typically consists of five components: sensing hardware, memory, battery, embedded processor, and transceiver. These components affect the performance of the sensor and ultimately that of the network. For example, the accuracy of the sensing hardware or transducer will affect the accuracy of the sensing at the observer. Similarly, the size of the memory affects the buffering space at the sensors and the ability of the network to handle transient bursts in traffic.

The battery size determines the amount of energy available at the sensor and affects the lifetime of the network. The capabilities of the embedded processor determine the level of optimization that is possible at the sensors without introducing excessive loss of power or intolerable levels of delay. Finally, the characteristics of the transceiver determine the transmission range of the network and the capacity of the transmission channel. Improving the characteristics of any of these subsystems increases the cost, form factor or both for the sensor.

2.6.1.3 Number of Sensors. Intuitively, for a given type of sensor, increasing the number of sensors deployed in the field should result in a better performing network with respect to the metrics identified earlier; otherwise, why pay the extra cost.

Consider:

1. The accuracy of the sensing should improve since there are more sensors in a position to report on the phenomena;
2. The available energy within the network increases; and
3. The additional sensor density offers the potential for a better-connected network with more efficient paths between the sensors and the observers. However, increasing the number of sensors in turn results in a higher number of sensors reporting their results per unit time. If this increased load exceeds the capacity of the network in terms of access to the shared wireless medium as well as congestion in intermediate nodes, increasing the number of active sensors may end up adversely affecting the performance of the network. With respect to capacity, the problem can be viewed in terms of collision and congestion. To

avoid collisions, sensors that are in the transmission range of each other should not transmit simultaneously.

The author considered in this case a phenomenon driven reporting model where a sensor reports if it is in range of the phenomenon. Assume that The author have N sensors out of which M sensors are in range of the phenomenon at a given time T. Assume that the M sensors are in interference range with each other (e.g., the transmission range is greater than or equal to the sensing range). Of the M reporting sensors, each sensor S_i will transmit data toward the observer with bit rate $b(S_i)$. The total data in transit from time T to T + δ, where δ is the average latency can be expressed as [11]:

$$\text{Data} = \sum_{i=1}^{M} b(S_i)$$

If this value reaches a certain fraction of the channel capacity, congestion will occur. Considering C_{total} is the total channel capacity then:

$$\sum_{i=1}^{M} b(S_i) <= \alpha \, C_{total}$$

Where α is a fraction of the capacity dictated by the self-interference that arises in multi-hop connections (α is typically around 0.25). Thus, the upper bound on the reporting rate is dictated by the channel capacity.

On the other hand, application specific criteria such as the required accuracy place a lower bound on the reporting rate; the reporting rate should be high enough to satisfy the desired accuracy. At any point in time, the number of active sensors should be such that the application specified accuracy requirements are met. If, in order to meet the accuracy requirements, $C_{application}$ is the required channel capacity then The author have:

$$C_{application} <= \sum_{i=1}^{M} b(S_i) <= \alpha C_{total}$$

$$C_{application} <= \alpha C_{total}$$

Not all sensors are equal in terms of accuracy. Depending on the location, a specific sensor may have a higher quality data sample, or a combination of sensors may together provide a higher accuracy than another combination. However, the author can qualitatively comment on the factors on which the number of active sensors depends. From a networking perspective, it depends on factors such as the geographic locations of the reporting sensors, buffer lengths, and packet processing times. From an application perspective, the value of information sensed by the sensor needs to be considered as well.

If a sensor is providing some unique information about some feature of the phenomenon, then the application might require that sensor to report irrespective of the location of that sensor. Thus, application level information must be used in determining what sensors to report and when to meet the application performance metrics. The authors intend to pursue such protocols in the future.

2.6.1.4 Deployment Strategies. Finally, it is important to consider the deployment strategy for the sensors (e.g., their distribution within the phenomena field). The author consider three deployment strategies:

- Random deployment – the sensors are "sprayed" with a uniform distribution within the field.
- Regular deployment – the sensors are placed with some regular geometric topology in the sensor field (for example, a grid); and
- Planned deployment – sensor deployment is planned (for example, biased to provide higher sensor density in areas where the phenomenon is concentrated).

It is unclear whether regular deployment will offer advantages over uniformly distributed random deployment; if it does not, random deployment is preferable because of its low cost.

2.6.2 Network Protocols

A power-efficient Time Division Multiple Access (TDMA) scheme has been implemented as the basic wireless sensing node link layer protocol. The TDMA scheme allows nodes to turn off their receiver and/or transmitter when they are not scheduled to communicate. A multi-hop routing scheme has also been implemented so that information from distant nodes can be forwarded to destination locations. The link layer protocols are built on top of the digital spread spectrum radio broadcast channel and provide a raw data rate of 100kb/s. Various low-overhead forward error correction schemes have also been implemented.

2.6.2.1 Communication Models. There are multiple ways for a sensor network to achieve its accuracy and delay requirements; a well designed network meets these requirements while optimizing the sensor energy usage and providing fault tolerance. By studying the communication patterns systematically, the network designer will be able to choose the infrastructure and communication protocol that provide the best combination of performance, robustness, efficiency and deployment cost. Conceptually, communication within a sensor network can be classified into two categories: application and infrastructure.

The network protocol must support both these types of communication. Application communication relates to the transfer of sensed data (or information obtained from it) with the goal of informing the observer about the phenomena. Within application communication, there are two models: co-operative and non-cooperative.

Under the cooperative sensor model, sensors communicate with other sensors to realize the observer interest. This communication is beyond the relay function needed for routing. For example, in a clustering protocol a cluster-head and the sensor nodes communicate with each other for information dissemination related to the actual phenomenon. In-network data processing is an example of co-operative sensors.

Non-cooperative sensors do not cooperate for information dissemination. Infrastructure communication refers to the communication needed to configure, maintain and optimize operation. More specifically, because of the wireless nature of sensor networks, sensors must be able to discover paths to other sensors of interest to them and to the observer regardless of sensor mobility or failure.

Thus, infrastructure communication is needed to keep the network functional, ensure robust operation in dynamic environments, as well as optimize overall performance. The author note that such infrastructure communication is highly influenced by the application interests since the network must reconfigure itself to best satisfy these interests. As infrastructure communication represents the overhead of the protocol, it is important to minimize this communication while ensuring that the network can support efficient application communication. In sensor networks, an initial phase of infrastructure communication is needed to set up the network. Furthermore, if the sensors are energy-constrained, there will be additional communication for reconfiguration.

Similarly, if the sensors are mobile or the observer interests dynamic, additional communication is needed for path discovery/reconfiguration. For example, in a clustering protocol, infrastructure communication is required for the formation of clusters and cluster-head selection; under mobility or sensor failure, this communication must be repeated (periodically or upon detecting failure). Finally, infrastructure communication is used for network optimization. Consider the Frisbee model, where the set of active sensors follows a moving phenomenon to optimize energy efficiency. In this case, the sensors wake up other sensors in the net-work using infrastructure communication.

Sensor networks require both application and infrastructure communication. The amount of required communication is highly influenced by the networking protocol used. Application communication is optimized by reporting measurements at the minimal rate that will satisfy the accuracy and delay requirements given sensor abilities and the quality of the paths between the sensors and the observer. The infrastructure communication is generated by the networking protocol in response to application requests or events in the network. Investing in infrastructure communication can reduce application traffic and optimize overall network operation.

2.6.2.2 Data Delivery Models. Ideally, the observer interest is specified in terms of the phenomenon, allowing the observer to be oblivious to the underlying sensor network infrastructure and protocol. The query is implemented as one or more specific low-level interests (e.g., requesting a specific sensor to report a specific measurement at some specific interval). Sensor networks can be classified in terms of the data delivery required by the application (observer) interest as: continuous, event-driven, observer-initiated and hybrid. These models govern the generation of the application traffic. In the continuous model, the sensors communicate their data continuously at a prespecified rate. Some researches showed that clustering is most efficient for static networks where data is continuously transmitted.

For dynamic sensor networks, depending upon the degree of mobility, clustering may be applicable as well. In the event-driven data model the sensors report information only if an event of interest occurs. In this case, the observer is interested only in the occurrence of a specific phenomenon or set of phenomena.

In the observer-initiated (or request-reply) model, the sensors only report their results in response to an explicit request from the observer (either directly, or in-directly through other sensors). Finally, the three approaches can coexist in the same network; The author refer to this model as the hybrid model.

Thus far, the author have only discussed data delivery from the application perspective, and not the actual flow of data packets between the sensors and the observer; this is a routing problem subject to the network protocol.

For any of the above-mentioned models, the author can classify the routing approach as: flooding (broadcast-based), unicast, or multicast/other. Using a flooding approach, sensors broadcast their information to their neighbors, who rebroadcast this data until it reaches the observer. This approach incurs high overhead but is immune to dynamic changes in the topology of the network. Research has been conducted on techniques such as data aggregation that can be used to reduce the overhead of the broadcast. Alternatively, the sensors can either communicate to the observer directly (possibly using a multi-hop routing protocol) or communicate with a cluster-head using one-to-one unicast. Finally, in a multicast approach, sensors form application-directed groups and use multicast to communicate among group members. The observer could communicate with any member of the group to obtain the desired data. A major advantage of flooding or broadcast is the lack of a complex network layer protocol for routing, address and location management; existing sensor network efforts have mostly relied on this approach. However, the overhead of a broadcasting approach may be prohibitive.

It is likely that the interaction between the data delivery model from the application and the routing model employed by the network protocol will significantly impact the performance of the network. Consider a scenario where a sensor network is deployed for intrusion detection. In this case, the data delivery model is event driven – the event being an intruder entering the area. If the network level routing model is flooding based, in such a case physically co-located sensors will in general sense the intruder at the same time and try to send data to the observer simultaneously. [12]

These concurrent communications in the neighborhood will contend with each other for the use of the communication medium, raising:

1. The probability of loss of critical information; and
2. The latency in event reporting

2.7 Application Specific Protocol Architectures for Sensor Networks

An important challenge in the design of wireless and mobile systems is that two key resources, communication bandwidth and energy. These are significantly more limited in a network environment. These restrictions require innovative communication techniques to increase the amount of bandwidth per user and innovative design techniques and protocols to use available energy efficiently. Furthermore, wireless channels are inherently error-prone and their time-varying characteristics make it hard to consistently obtain good performance.

Applications differ, in which features are most important. For example, an application that supports wireless data communication might prefer longer latency in exchange for longer node lifetime. On the other hand, long latency is unacceptable for a cellular phone application.

In order for us to obtain an efficient system that achieve high performance and energy efficiency in a wireless environment, The author need to consider the type of application, for which the network will be deployed. Next, the consideration of the different applications, coupled with the tight resource constraints of wireless systems, suggests the need for application-specific protocols. In conventional network architecture a network is designed based on the layering approach. In this case each layer is designed separately independent of the application of the network. Protocol architectures that exploit application-specific information in the transport, network and data link layers of this protocols stack for specific wireless applications.

Conventional network architectures are designed according to layering approach, such as the one shown in above figure. In this case, each layer of the system is designed separately. This approach is not optimal for any given application. A cross-layer architecture that exploits features of the application can achieve greater performance than general-purpose protocols. Protocol stack is explained in detail for radiation detection sensor network in next chapter.

CHAPTER 3

NETWORK ARCHITECTURE

The main function of the sensor network is data delivery. As radiation detection involves direct interaction with a physical environment; data communication in such sensor networks often has timing constraints in the forms of end-to-end deadlines. The data are distributed on the various sensor nodes; this data is collected and routed to the sink. The sink will communicate with the task manager node via Internet or satellite. In a sensor network, data sensed by each node are required at a remote base station, rather than at other nodes, and the data are being extracted from the environment, leading to large amount of correlation among data signals. The end-user does not require all the data in the network because the data from the neighboring nodes are highly correlated, making the data redundant, and the end-user cares about a higher-level description of events occurring in the environment the nodes are monitoring. The quality of the network is therefore based on the quality of the aggregate data set, rather than the quality of the individual data signals, protocols should be designed to optimize for the unique, application-specific quality of a sensor network.

To summarize, wireless sensor network protocols should be:

- Self-configuring, to enable ease of deployment of networks.
- Energy-efficient and robust, to extend system lifetime.
- Latency-aware, to get the information to the end-user as quickly as possible.
- Cognitive of the application-specific nature of network quality.

The research presented here focuses on ways in which least feature may be exploited to create protocol architecture that optimizes the different desired features of this network. This is accomplished by using application-level information in the design of all layers of the traditional protocol stack, shown in Figure 3.1.

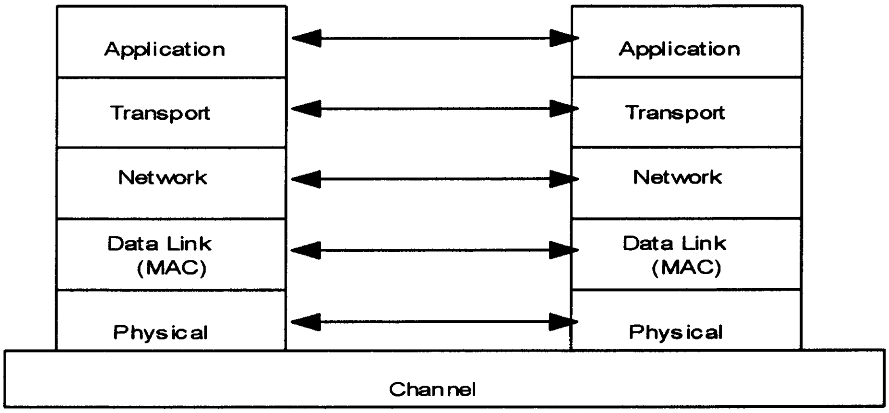

Figure 3.1 Protocol stack in a Network Model.

3.1 Protocol Stack

Four layer protocol stacks are considered for Radiation detect network. All the layers of the protocol stack are explained in detail in the following sections.

3.2 Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. Thus far, the 915 MHz industrial, scientific and medical (ISM) band has been widely suggested for sensor networks. Frequency generation and signal detection have more to do with the underlying hardware and transceiver design.

Long distance wireless communication can be expensive, in terms of both energy and implementation complexity. While designing the physical layer for sensor networks, energy minimization assumes significant importance. In general, minimum output power required to transmit a signal over a distance (d) is,

$$P \propto d^n$$

Where,

P = minimum output power required to transmit a signal

d = distance

n= exponent, $2 <= n < 4$

The exponent n is closer to four for low-lying antennae and near-ground channels, as typical in sensor network communication. This can be attributed to the partial signal cancellation by a ground reflection ray. Measurements carried out [1] indicate that the power starts to drop off with higher exponents at smaller distances for low antenna heights. Multihop communication in a sensor network can effectively overcome shadowing and path loss effects, if the node density is high enough. Similarly, while propagation losses and channel capacity limit data reliability, this very fact can be used for spatial frequency reuse.

The choice of a good modulation scheme is critical for reliable communication in a sensor network. Modulation scheme in physical layer is another important factor, which strongly impacts the power consumption. The energy consumption for Binary and M-ary modulation schemes are compared in this section.

Energy consumption for Binary modulation is given as [3],

$$E_{binary} = P_{tx-B}\,(T_{on} + T_{start}) + P_{out\text{-}B}T_{on}$$

Where,

E_{binary} = Energy consumption in binary modulation

P_{tx-B} = Power consumption of the transmitter

T_{on} = Transmit on time

T_{start} = Transmitter start time

$P_{out\text{-}B}$ = Out put transmit power

Energy consumption for M-ary modulation is given as,

$$E_{m\text{-}ary} = P_{tx-M} \left(\frac{T_{on}}{n} + T_{start} \right) + P_{out\text{-}M} \frac{T_{on}}{n}$$

Where,

$E_{m\text{-}ary}$ = Energy consumption in M-ary modulation

P_{tx-M} = Power consumption of the transmitter

T_{on} = Transmit on time

T_{start} = Transmitter start time

$P_{out\text{-}M}$ = Out put transmit power

n = Number of bits per symbol

An M-ary scheme can reduce the transmit on-time by sending multiple bits per symbol. However, it results in complex circuitry and increased radio power consumption.

The overhead energy from going to binary to m-ary modulation is defined by following equation,

$$\propto = \frac{P_{tx-M}}{P_{tx-B}}$$

The energy comparison of binary and m-ary case [3] is shown in figure 3.2, where energy ratio of m-ary and binary scheme is plotted vs. start up time for different overheads (∝ = 1.5,3). As shown in the graph, energy is reduced for smaller overhead, ∝ and higher m since the on-time (T_{on}) is shorter. Energy saving from m-ary modulation depends not only on the overhead but also on startup time. M-ary modulation reduces on-time and saves energy during active transmission, startup time is hidden cost which limits the amount of energy savings. It can be seen that for ∝ = 1.5, T_{start} must be less than 40μs in order for the m-ary scheme to achieve lower power than binary case. As ∝ is increased, it becomes more difficult for the M-ary scheme to achieve lower energy than binary case.

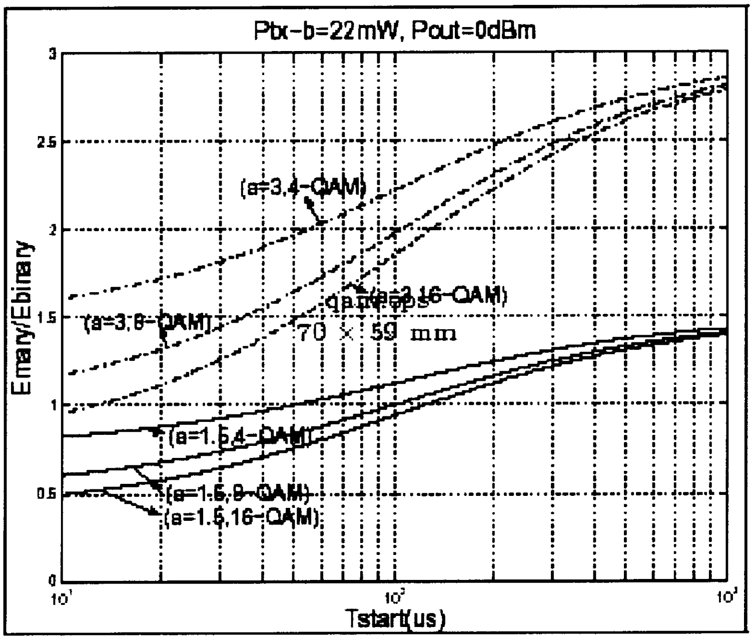

Figure 3.2 Energy Saving vs. Overhead (∝)

As the trade-off parameters are formulated above, and it concluded that under startup power dominant conditions, the binary modulations scheme is more energy-efficient.

Ultra wideband (UWB) pulses can be used to provide a high data rate, can provide fine range resolution, and precision distance and/or positioning measurement capabilities. Among the most important advantages of UWB technology is low system complexity and low cost. The main advantage of UWB is its resilience to multipath. Low transmission power and simple transceiver circuitry make UWB an attractive candidate for sensor networks.

3.2.1. Sensor Node Hardware

A sensor node is made up of four basic components, such as sensing unit, a processing unit, a transceiver unit and the power unit. Sensor node may also have location finding system depending upon application. Sensing unit is composed of two subunits sensors and analog-to-digital converters (ADCs). The analog signal produced by the sensors based on the observed phenomenon, ADC generates digital signal [10], and fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node the network. Power unit may be supported by power scavenging units such as solar cells, depending upon the application. A mobilizer may sometimes be needed to move senor nodes, when it is required to carry out the assigned tasks [1].

All these subunits may need to fit in a small unit like matchbox [11]. The required size is smaller than even a cubic centimeter. Which I light enough to remain suspended in the air.

A set of unique requirements [9] for distributed sensor network must be:

- Reconfigurable by their base station

- Autonomous to permit local control of operation and power management
- Self-monitoring for reliability
- Power efficient for long term operation
- Must incorporate diverse sensor capability with highly capable of microelectronics

3.2.2 Hardware for Radiation Detection Sensor Network

The author has considered the Low Power Wireless Integrated Microsensors (LWIM), which a Microelectromechanical System technology (MEMS). The chose is supported by the following reasons [9]. This individual node when deployed in the field is capable of transmitting continuous data to the base station, only upon alarm condition. These nodes permit base station to service a much larger network than would be possible for simple continuous communication with other sensor node. In addition low duty cycle operation, combined with proper power management, permits low power requirements. By exploiting the low power duty cycle requirements for sensor communication, large efficiencies may be obtained in sensor node and base station operation.

A LWIM node allows long operating life from compact battery systems. Typical low duty cycle, low data rate of 10 kbps and short range of 10 to 30 meters communication permits 30 μA average current and 3 Volts. A conventional Li coin cell provides this current level for greater than a three year unattended operating life.

3.3 Data Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, and medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.

The protocol Self-Organizing Medium Access Control for Sensor Networks (SAMCS) proposed in [4] is used for radiation detection sensor networks. SMACS is for network startup and link-layer organization.

SMACS is a distributed infrastructure-building protocol that forms a flat topology for sensor networks. SMACS enables a collection of nodes to discover their neighbors and establish transmission/reception schedules for communication with them without the need for any local or global master nodes. In SMACS, channel to a link is immediately assigned after the links existence is discovered. This way links begin to form concurrently throughout the network. By the time all nodes hear all their neighbors, they will form a connected network. A communication link consists of a pair of time slots operating at a randomly chosen but fixed frequency. This is a feasible option in radiation sensor networks, since the available bandwidth is much higher than the maximum data rate for sensor nodes. Such schemes avoid the necessity for network wide synchronization, although communicating neighbors in a subnet need to be time-synchronized. SMACS supports the operation of power saving modes for the sensor node. The means of power conservation is to turn the transceiver off when it is not required. Each node goes to sleep for some time, and then wakes up and listens to see if any other node wants to talk to it. During sleep, the node turns off its radio, and sets a timer to awake up later. When nodes wake up and find each other, they agree to transmit and receive during a pair of fixed time slots. This transmission/reception pattern will be repeated periodically at particular time interval. Mean time if another two nodes wake up, finds each other they will be assign another pair of slots for transmission and reception. If all the nodes operate on the same frequency band, there is possibility that some transmission will collide in the given schedule. To avoid this different frequency band are assigned to different links. When there are many frequencies from which to chose, and frequencies are chosen uniformly at random, the likelihood that the same frequency is chosen by two links with earshot of other is small.

Another important function of the data link layer is the error control of transmission data. For radiation detection sensor network the author have chose Forward Error Correction (FEC) [1].

3.4 Network Layer

Sensor nodes are scattered densely in a field either close to or inside the phenomenon in radiation detection sensor network. Multihop routing protocol between sensor node and sink is needed. The networking layer of sensor network is usually designed according to the following principles:

- Power efficiency is always an important consideration
- Radiation sensor network is data-centric
- Data aggregation is useful only when it does not hinder the collaborative effort of the sensor node.
- Attributed-based addressing and location awareness

For radiation sensor network the author is considering Greedy Perimeter Stateless Routing for Wireless Networks (GPRS). Under GPRS, packets are routed geographically and all packets are marked with the positions of their destinations. All nodes know their own positions, and the positions of the nodes are a single hop away from them. GPSR can route a packet using this local knowledge. There are two distinct algorithms that GPSR uses for routing; they are viz. greedy forwarding algorithm and a perimeter-forwarding algorithm. Greedy forwarding algorithm moves packet progressively closer to the destination at each hop, and a perimeter forwarding algorithm that forwards packets where greedy forwarding is impossible.

3.4.1 Greedy Forwarding

Under GPRS, their originator with their destinations location marks packets. As a result a forwarding node can make a locally optimal, greedy choice in choosing a packet's next hop. Specifically if a node knows its radio neighbors' positions, the optimal choice of next hop is the neighbor geographically closest to the packet's destination. Forwarding in this regime follows successively closer geographic hops, until the destination is reached. And example of greedy next hop choice appears in Figure 3.3.

Here, node 1 receives a packet destined for D. In figure dotted circle denotes the radio range of the node 1 and arc with radius equal to the distance between node 2 and D is shown as dashed arc about D. node 1 forwards the packet to node 2, as the distance between node 2 and D is less than that between D and any of node 1's other neighbors. This greedy forwarding repeats, until the packet reaches D. A simple beaconing algorithm provides all nodes with their neighbors' positions periodically; each node transmits a beacon to the broadcast MAC address, containing only its own identifier and positions. Positions are encoded by four byte floating-point quantities of x and y coordinates.

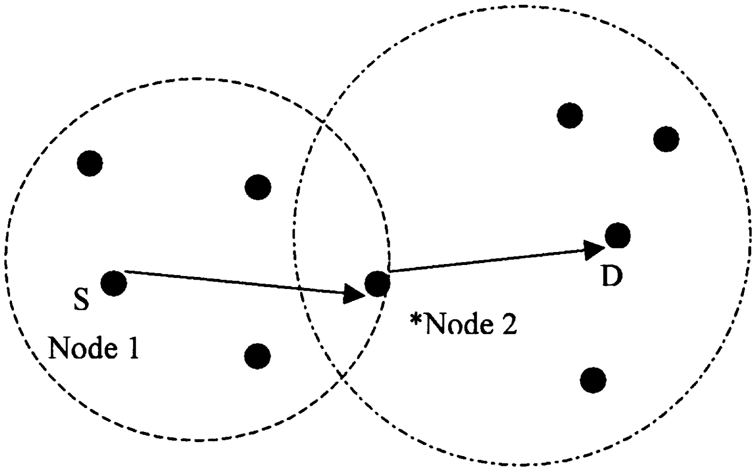

Figure 3.3 Greedy Algorithm - Node 2 is the only node, which shares range contact with source S and destination D.

3.4.2 Perimeter Forwarding

As shown in Figure 3.4, intersection of node 1's circular radio range and the circle about D of radius is empty of neighbors. Node 1 seeks to forward a packet to destination D beyond the edge of this void. Intuitively, node 1 seeks to route around the void; if a path to D exits from node 1, it doesn't include nodes located within the void (or node 1 would have forwarded to them greedily).

The right-hand rule for traversing a graph is used. The rule states that when arriving at node 1 to D, the next edge traversed is the next one sequentially counter clock-wise about node 1 from edge (node 1, node 3). Thereafter the node attempts to forward the packet to next node using greedy forwarding algorithm.

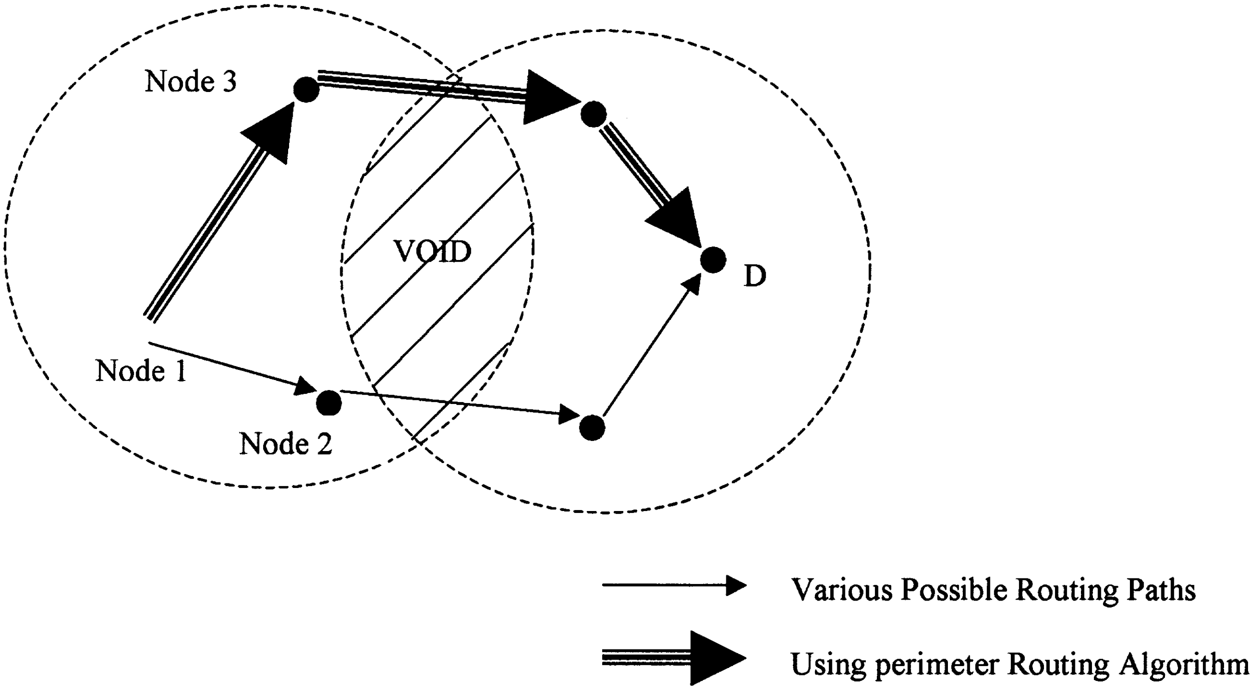
Node 3
VOID
D
Node 1
Node 2
Various Possible Routing Paths
Using perimeter Routing Algorithm

Figure 3.4 Perimeter Algorithm - For node 1 greedy algorithm doesn't work, so the node 1 uses the perimeter algorithm.

The right-hand rule for traversing a graph is used. The rule states that when arriving at node 1 to D, the next edge traversed is the next one sequentially counter clock-wise about node 1 from edge (node 1, node 3). Thereafter the node attempts to forward the packet to next node using greedy forwarding algorithm.

3.5 Transport Layer

Transport layer is specially needed when the system is planned to be accessed through the Internet or other external networks. Communication between the user and sink node is by UDP or TCP via Internet or satellite, where as communication between sensor node and sink is purely by UDP-type protocols, because each sensor node has limited memory. In radiation detection sensor networks, UDP connections are ended at sink nodes, and a special transport layer protocol can handle the communication between the sink node and sensor nodes.

3.6 Application Layer

Sensor Management Protocol [1] is used for radiation detection sensor networks. An application layer management protocol makes the hardware and software of the lower layers transparent to the sensor network management applications. System administrators interact with network using Sensor Management Protocol (SMP). Unlike many other networks, sensors networks consist of nodes that do not have global identifications are usually infrastructureless. Therefore, SMP nodes to access the nodes by using attribute-based naming and location-based addressing that provide the following administrative tasks:

- Introducing the rules related to data aggregation and attribute-based naming
- Exchanging data related to the location finding algorithms
- Time synchronization of sensor nodes
- Turning sensor on and off
- Authentication, key distribution, and security in data communication

CHAPTER 4

TRADEOFFS IN WIRELESS SENSOR NETWORK

4.1 Introduction

In a wireless sensor network some categories may affect each others during the operation of the network. In this chapter the author will shed some light about some of the tradeoffs considered in a wireless sensor network, of which the author will study one case which is the tradeoff between power (energy consumption) and the accuracy (Security [malfunction]).

In a wireless sensor network the following are the categories to consider its tradeoff with one another:

- **Security:**

  Efficiency and Accuracy (Malfunction)

  Network Security (Hacking)

- **Power:**

  Energy Consumption

  Battery life-time

- **Communication:**

  Routing protocols

- **Cost**

4.2 Infrastructure Tradeoffs with the Performance of the Sensor Networks

In a sensor network, the infrastructure plays a significant role in determining the performance of the network. As sensor network is a tool for distributed sensing of one or more phenomena, and reporting the sensed data to one or more observer, such performance of the network is best measured in terms of meeting the accuracy and delay requirements of the observer. Additional performance metrics include the life time of the network, sensors cost and their deployment, fault tolerance and scalability.

In a sensor network it appears that a denser infrastructure leads to a more effective sensor network because of higher accuracy is likely and a larger aggregate amount of energy is available in the network. However, if not properly managed a denser network will lead to a larger number of collisions and potentially to congestion in the network. This will increase the latency and reduce energy efficiency. Thus, simply increasing the reporting rate or the number of sensors may actually harm the performance of the network. One main lesson in such issue is that a form of congestion control is necessary to make sure that the reported samples do not exceed the capacity of the network. In addition, this control is necessary to optimize the lifetime of the network while meeting the minimum accuracy requirements of the application.

4.2.1 Goodput and Delay Study

In a study of the effect of increasing the sensor density on the efficiency of the network the results showed that as the data rate increases and the reporting period decreases that the goodput drops when the rate exceeds the capacity of the network and sensed packets start to be dropped.

Considering the strategy which places the sensors in a square Grid, it is interesting to note that the drop in goodput is more pronounced for the denser networks. This is due to the larger number of sensors close to the phenomenon effectively increasing the offered load to the network, resulting in more collisions and a higher number of packets dropped due to congestion. This effect is corroborated by the packet latency results. The latency increases with the data rate as well as the density of the network [14].

With the random deployment, while keeping same number of sensors, the results of the goodput and delay do not show appreciable differences in comparison to grid deployment.

4.2.2 Accuracy Study

In terms of application performance, the accuracy of the tracking of the phenomenon position was measured. The observer would generate an estimate of the Phenomenon location based on the samples that are received from the sensors. The error is measured as follows: The time is divided into small slots and averaged the samples received in each slot. A comparison of the average to the actual location of the phenomenon at that time will be done. The error is the square root of the sum of the square of the difference between the estimated location and the actual location averaged over the number of slots in the experiment. As a proof of concept approach to calculating error, any statistical measure for correlating the measured value against the actual value will suffice.

Considering again the grid deployment, the average error under different densities and for different reporting periods was observed. At high reporting rates, network capacity is exceeded, and so is the latency. Because of the latency in the receipt of the samples and the loss of many samples, the error value is high. On the other hand, if the reporting frequency is low, not enough samples are obtained and the average error rises. With sparse grid networks, the error is higher when the network is not saturated, because the number of sensors in a position to measure the phenomenon and the average distance between a sensor and the phenomenon increases. For such scenarios, the error is minimized with a higher reporting frequency. Additional samples would reduce the error and the network is slower to saturate, because there are fewer sensors competing for the shared air space [15].

With random deployment the same pattern can be observed.

4.2.3 Energy-Efficiency Study

The energy depletion is a function of the reporting rate as well as the density of the network. As mentioned before, the density of the network in the phenomenon driven scenario correlates with the number of nodes that report their data. However, as suggested by the goodput results, a large portion of this energy is wasted when the capacity of the network is exceeded. Moreover, the additional cost incurred to buy more sensors will not be rewarded by a higher lifetime for the network, because the depletion rate also increases. In fact, when we consider the normalized energy expenditure per sensor for grid deployment the average sensor gets depleted more quickly with higher density.

Thus, the lifetime of the network likely drops with increased density even though we start with a much higher total available power in the network! Accordingly, there is a need for intelligent management of the infrastructure from an energy perspective as well. To summarize, in agreement with intuition, increasing the network density can result in higher accuracy, but only if the sensing traffic is kept below the network capacity. This is an expanded form of the congestion control requirement for regular computer networks; due to the redundant collective communication nature of sensor network traffic, the network has the ability of controlling what data gets reported to meet the observer's requirements. It is likely that the observer is satisfied with less than the optimal achievable accuracy. Thus, the network protocol must control the available infrastructure and the reporting discipline to meet the accuracy requirements while minimizing the energy expenditure. The sensor network must converge on a good accuracy to reporting pattern/energy solution. This may be achieved, for example, by deciding to turn off some sensors, by adapting the reporting frequency, or by fusing sampled data within the network [14].

This happens because, in a given area, the first node which wins the medium-access contention and broadcasts the flood message first becomes the parent of all new receivers. This "winner gets all" scenario is somewhat similar to the Internet, which shows a power law network topology as well because nodes attach themselves preferentially to bandwidth-rich nodes. We intend to base our work on a combination of simulation and empirical measurements. To enhance our simulation environment, we are performing a series of experiments to create a statistical profile of connectivity among each node and run our simulations over these profiles.

CHAPTER 5

EXPERIMENT MODEL

5.1 Assumptions

The following assumptions have been made in this the experiments done:

- All sensor nodes are stationary and able to communicate with the sink node after initial deployment. The sink node knows the location of the sensors through an initial set up process.
- When a sensor node senses the radiation, sensor will send the data to the sink node without any error and loss of data.
- The sink node has more computation power than any other sensor node. Sink node is responsible for data aggregation and data calculation. The sensor nodes are only responsible for collecting the data and sending it to the sink node.
- To simplify the delay analysis, transmission delay and propagation delay is only considered. Packet loss, noise or any other issues are not considered for delay analysis.
- To simplify the energy analysis, the time for sending a certain amount of data is assumed to be the same as the time for receiving the same amount of data. Energy used in data routing is assumed for the maximum packet size that is 100 bits. No node is been assumed to be out of power. Also, all the sensors are assumed to be homogeneous, therefore the energy consumption will be same for sensing for all the nodes.

- Energy consumed is calculated based on the routing protocol used, which is Greedy Perimeter Stateless Routing (GPSR).

5.2 Sensor Detection Model

5.2.1 Basic Model

The author has considered a network consisting of N nodes deployed in the sensor network randomly. There is single radiating source, a truck carrying the nuclear bomb, is moving. One sink node which is on (0, 0) coordinates of the sensor network. Simulation time is T seconds. Sensor has communication range of R, which is circular.

Radiating source for the network is the Americium source, which has maximum of approximately 10^5 [6] counts per seconds. Each sensor is capable of detecting the minimum number of counts. If the count is below the minimum count, sensor node will not sense the radiation. When the radiation count the between the range of minimum and maximum counts, sensor node will detect the radiation.

The experiment is divided into three parts:

1) Tracking model

2) Delay model

3) Accuracy and energy trade off model

5.2.2 Tracking Model

Nine different scenarios have been considered for the tracking model. Numbers of nodes deployed in the network are 250, 500 and 750 and capable of sensing minimum of 1878.02, 1883.23 and 1936.41 counts. Scenarios are:

1) 250 nodes in a network and each node can sense 1878.02 counts of radiation

1) 250 nodes in a network and each node can sense 1878.02 counts of radiation

2) 250 nodes in a network and each node can sense 1883.23 counts of radiation

3) 250 nodes in a network and each node can sense 1936.41 counts of radiation

4) 500 nodes in a network and each node can sense 1878.02 counts of radiation

5) 500 nodes in a network and each node can sense 1883.23 counts of radiation

6) 500 nodes in a network and each node can sense 1936.41 counts of radiation

7) 750 nodes in a network and each node can sense 1878.02 counts of radiation

8) 750 nodes in a network and each node can sense 1883.23 counts of radiation

9) 750 nodes in a network and each node can sense 1936.41 counts of radiation

Sensor field is 1000*1000 units. Depending upon the scenario explained above, numbers of the nodes are randomly deployed in the 1000*1000 units of area. Radiating source is passed in the sensor field using the equation of sinusoidal wave. Following is the equation of giving the path to the radiating source.

500+100*sin (truck (j)*0.02)

As the radiating source is passing through the sensor network, sensor node coming across will check if there was any radiation detected depending upon the sensor distance from the radiation source. If the sensor detects any radiation, the sensor node will send the amount of radiation count detected to the sink node. The data is routed through the network using Greedy Perimeter Stateless Routing algorithm (GPRS). Sink node will do the computation, locating the radiating source.

When the sink node gets the data, first the sink node will calculate the distance between sensor node and radiating source, using the following equation [6]:

$$C = 1873.23 + 107962.64 / d^2$$

Where,

C = radiation counts / seconds

d = distance between the source and sensor

With data received only from one sensor node is not enough to make accurate location decision. When more than one sensor nodes detects and sends information to sink node, calculating the position will be more accurate.

When the sink node gets more than one data from the nodes, computation is done at the sink node. Sink node will sort the data according to time. For the same time if there are more than one data, sink node will sort the data with respect to radiation count. Taking the two highest radiation, computation is done with the help of circle equation.

Let,

Center of circle one = (C_{x1}, C_{y1})

Point of the circle one = (X_1, Y_1)

Distance from the point of circle one to the center (radius) = d_1

Center of circle two = (C_{x2}, C_{y2})

Point of circle two = (X_2, Y_2)

Distance from the point of circle one to the center (radius) = d_2

Equations of circles are:

$$(C_{x1} - X_1^2) + (C_{y1} - Y_1^2) = d_1^2$$

$$(C_{x2} - X_2^2) + (C_{y2} - Y_2^2) = d_2^2$$

To locate the source above two equations are used. Data sent to the sink node will contain the x and y coordinate of the sensors and distance (radius). Solving the above equation will give two or one point of intersection. If it is one point of intersection, it will be send to the base station. This will be the location predetected by sensor network. If there are two points of intersection, next data in the sink node for that time period is taken to calculate the location of the radiating node. If there is only one data from the sensor network, the coordinates of the sensor nodes are assumed to be the location of radiating source. This way the whole path of radiating source is tracked until the radiating source is in the vicinity of the sensor network.

5.2.3 Delay Model

For the delay model following scenario has been considered in this experiment:

1) 250 nodes with communication range of 20 units
2) 500 nodes with communication range of 20 units
3) 750 nodes with communication range of 20 units

Delay is the time it takes to reach the sink node from the sensor after it detects any radiation. Here the delay considered is propagation delay and transmission delay. Propagation delay is the time required for a signal to propagate from one node to another. This time is generally negligible since the signals travel very fast in the conducting media.

$$T_{\text{propagation}} = \text{distance} / \text{speed of light}$$

Where,

Speed of light = $3 * 10^8$ m/sec

In the experiment distance between the sensor nodes sending the data and the sink node is calculated. This distance calculated from the sensor to next hop and from hop to next hop until it reaches the sink node, taking into consideration the Greedy Perimeter Stateless Routing (GPRS) algorithm.

Transmission delay is the time it takes to transmit all of the bits of a packet into the medium. The transmission delay is experienced at every node. Packet size has a great effect on transmission time.

$$T_{trnasmission} = \text{number of hops} * \text{packet size} / \text{bandwidth}$$

Where,

Number of hops is counted while routing the packet from the originating node to the sink node.

Packet size = 32 bits to 100 bits

Bandwidth = 10 kbps

The author have considered for the maximum number of packet size which is 100 bits. Total delay is calculated by adding propagation delay and transmission delay.

$$\text{Total delay} = T_{propagation} + T_{trnasmission}$$

5.2.4 Accuracy and Energy Trade Off Model

Here the author has considered battery used in the sensor node and accuracy achieved by it. Network is deployed with 750 nodes.

Three scenarios has been considered here, initially the node has 8000 mW of energy and than reduced to 3375 mW, 1000 mW, and 125 mW. Energy equation [7] used is:

$$E = d^3$$

Where,

E = energy used in Watts

d = communication distance

Using the above equation, range of communication is calculated for each case.

$$8000 = d^3$$

d = 20 units,

$3375 = d^3$

d = 15 units

$1000 = d^3$

d = 10 units

$125 = d^3$

d = 5 units

Considering the above radio range of 20, 15, 10 and 5 units experiment is done. Truck carrying nuclear bomb is passed through the network. The path of the truck is trace as explained in tracking model. The tracking accuracy reflects the uncertainty in the target's location. If $(X_a(t), Y_a(t))$ is actual position and calculated value is $(X_c(t), Y_c(t))$, instantaneous tracking error is found by finding the distance between actual and calculated value using,

$\text{Error} = \surd\ (X_a(t) - X_a(t))^2 + (Y_a(t) - Y_c(t))^2$

Accuracy = 1 – Error

The graph between accuracy and battery consumption is draw to explain the trade off between both. Results are explained in the latter chapter.

CHAPTER 6

RESULTS

6.1 Tracking Model

6.1.1 Radiation Graphs

Table 6.1 shows a few of the results of the scenario where we used the 250 randomly distributed sensor nodes. The radiation sensitivity of the sensor node is 1936.41 radiation counts, to detect the mobile Radioactive Source. The results of detecting and positioning the mobile radioactive source by the sensor node ID 242 during a time interval of 18 seconds is shown in Table 6.1.

Table 6.1 Radiation Count for Node 242

AT TIME	NODE ID	DISTANCE	RADIATION COUNT
759	242	18.35756	1905.167
760	242	17	1910.471
761	242	14.76482	1922.6
762	242	12.52996	1941.782
763	242	10.29563	1974.764
764	242	8.944272	2007.763
765	242	6.708204	2112.4
766	242	4.472136	2411.362
767	242	2.236068	4025.758
769	242	2.236068	4025.758
770	242	4.472136	2411.362
771	242	6.708204	2112.4
772	242	8.944272	2007.763
773	242	10.29563	1974.764
774	242	12.52996	1941.782
775	242	14.76482	1922.6
776	242	17	1910.471
777	242	19.23538	1902.318

Figure 6.1 shows the relationship between the detected radiation count and the detecting time over the period of 18 seconds.

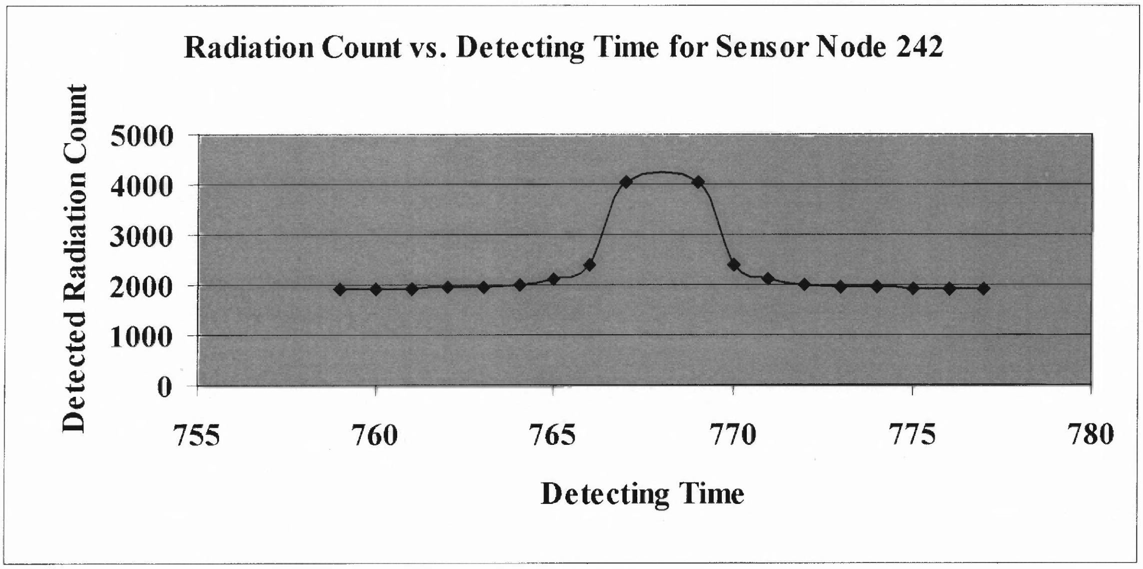

Figure 6.1 Radiation vs Time for Node 242.

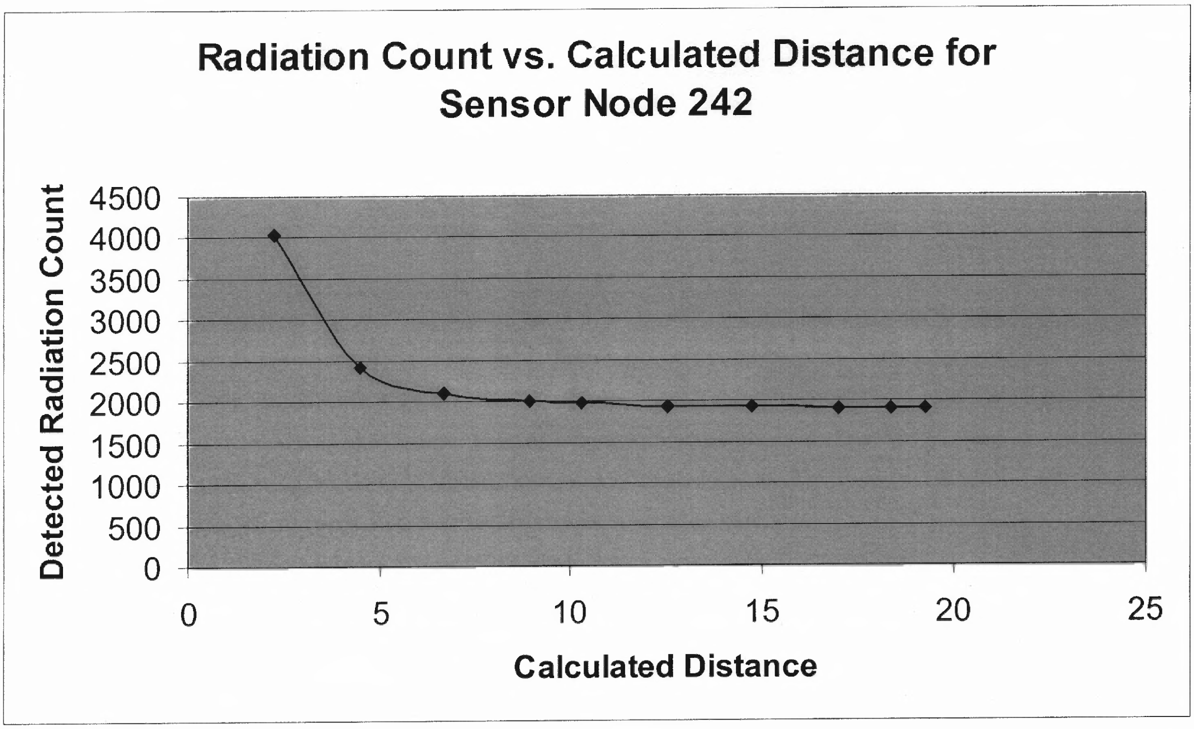

Figure 6.2 Radiation Vs Distance for Node 242. The relationship between the Calculated Distance and the Detected Radiation Count.

Table 6.2 describes the results of the scenario where we used the 500 randomly distributed sensor nodes. The same Radiation Sensitivity of 1936.41 Count of the sensor node to detect the mobile radioactive source is considered. The results shown are of detecting and positioning the mobile radioactive source by the sensor node ID 252 during a time of 12 seconds.

Table 6.2 Radiation count for Node 252

AT TIME	NODE ID	DISTANCE	RADIATION COUNT
36	252	19.31321	1902.084
37	252	18.78829	1903.719
38	252	17.49286	1908.402
39	252	17.20465	1909.59
40	252	16.27882	1913.844
41	252	16.27882	1913.844
42	252	16.40122	1913.24
43	252	16.12452	1914.625
44	252	16.55295	1912.51
45	252	17.08801	1910.088
46	252	17.46425	1908.517
47	252	18.24829	1905.55
48	252	19.1050	1902.7170

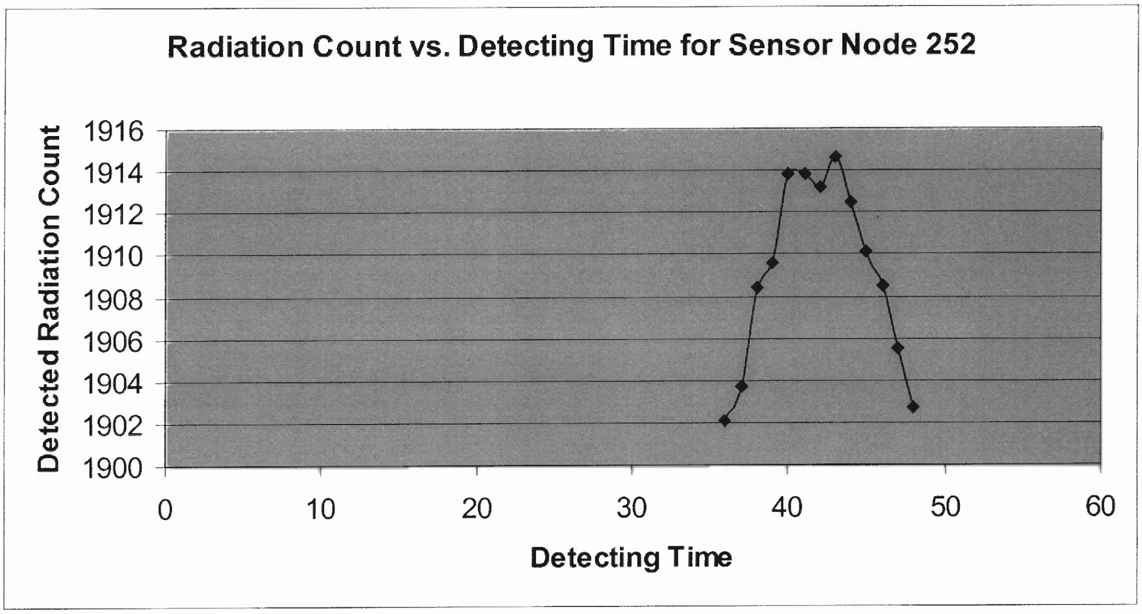

Figure 6.3 Radiation Vs Time for Node 252. Presents the relationships between the detected radiation count and the detecting time.

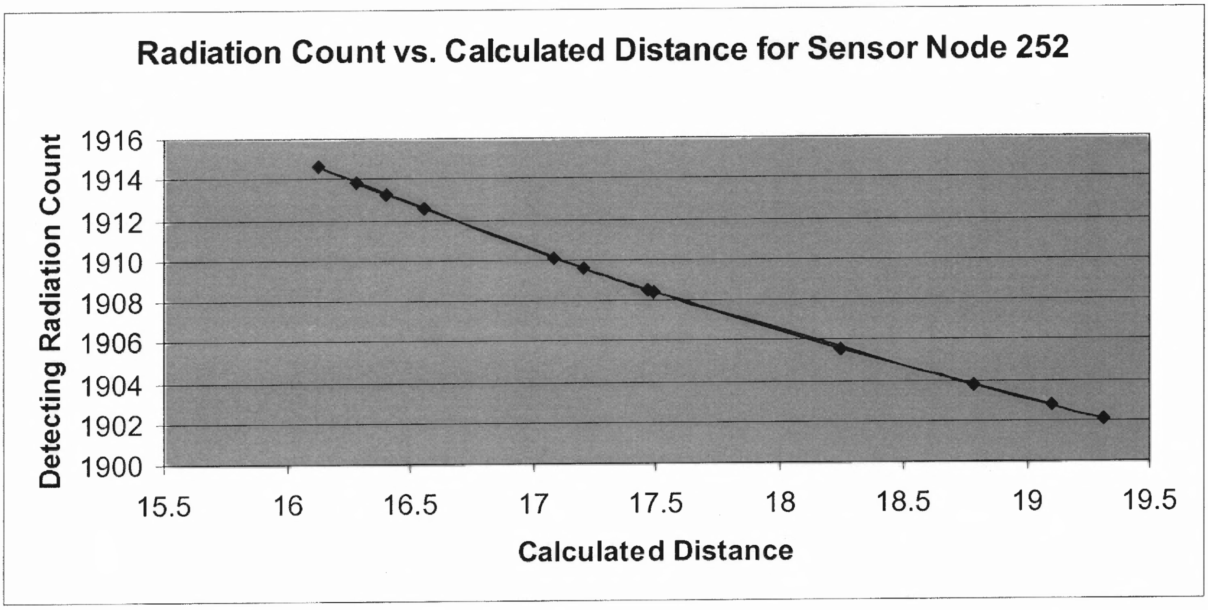

Figure 6.4 Radiation Vs distance for Node 252. Shows the relationships between the calculated distance and the detected radiation count.

Table 6.3 describes few results of the scenario where the author used the 750 randomly distributed sensor nodes. The sensor node with radiation sensitivity of 1936.41 count of radiation is used. Table 6.3 presents the results of detecting and positioning the mobile radioactive source by the sensor node ID 257 during a time of 12 seconds.

Table 6.3 Radiation table for Node 257

AT TIME	NODE ID	Distance	Radiation Count
319	257	19.7231	1900.8970
320	257	17.8885	1906.8630
321	257	16.1555	1914.4660
322	257	14.56022	1923.997
323	257	13.15295	1935.442
324	257	12	1947.971
325	257	11.18034	1959.331
326	257	10.44031	1971.97
327	257	10.29563	1974.764
328	257	10.63015	1968.475
329	257	11.4018	1956.0200
330	257	12.5300	1941.7820
331	257	13.9284	1928.7080
332	257	15.5242	1917.8880
333	257	17.2627	1909.3460
334	257	19.1050	1902.7170

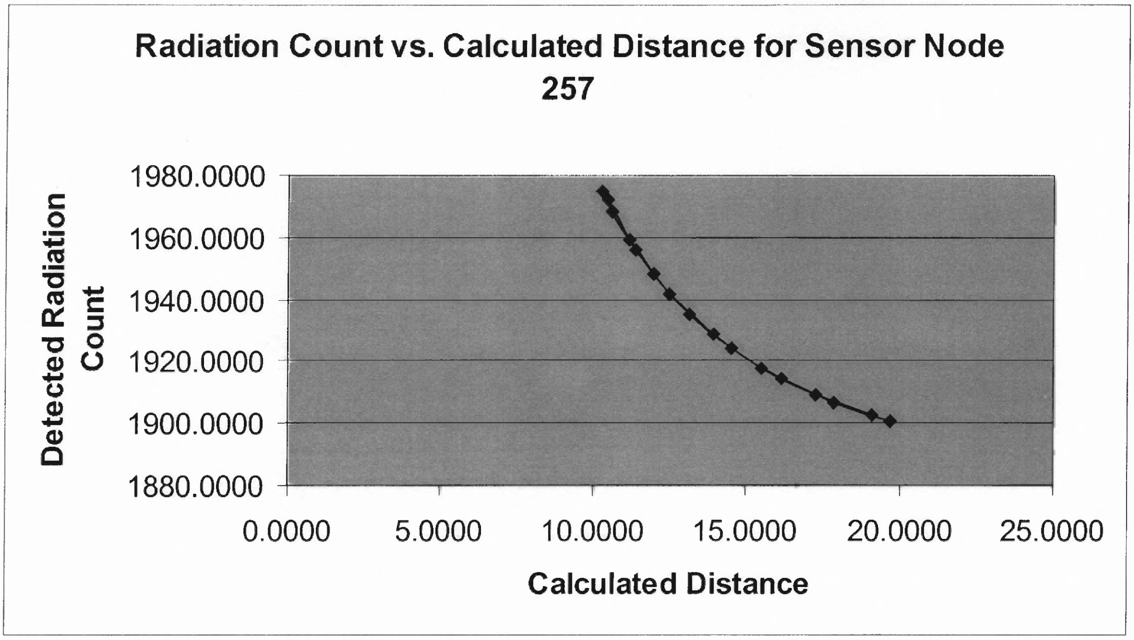

Figure 6.5 Radiation Vs Distance for Node 257. Relationships between the Detected Radiation Count and Calculating Distance.

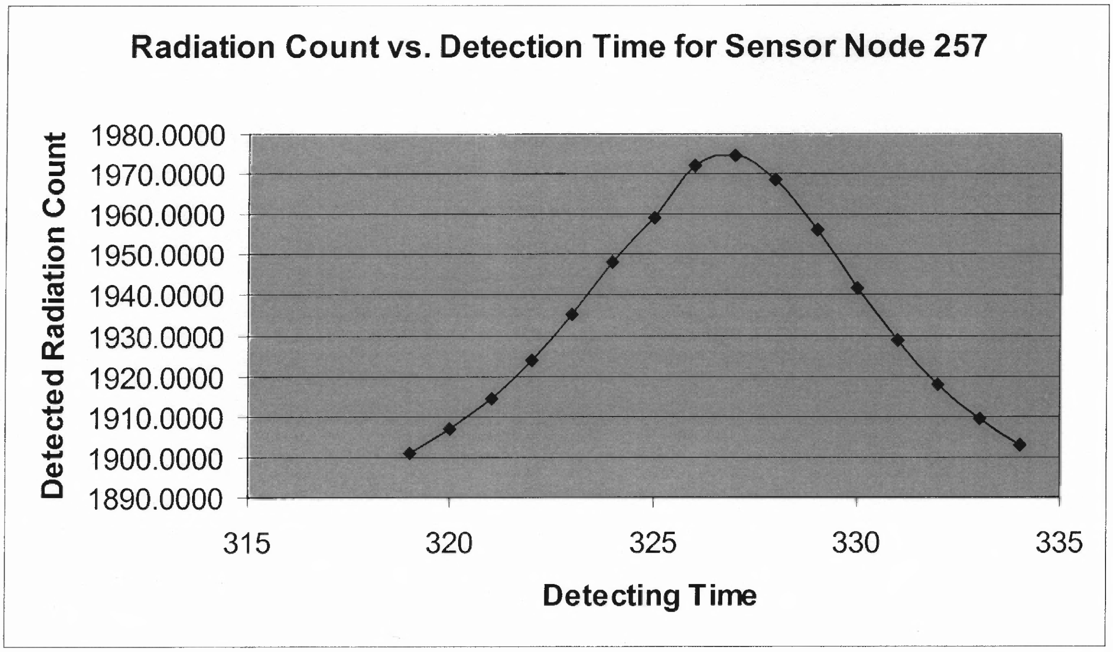

Figure 6.6 Radiation Vs Time for Node 257. Relationships between the Detected Radiation Count and the Detecting Time.

6.1.2 Tracking Graphs

In a sensor network area 250 nodes are distributed randomly in the area of 1000 * 1000 meter square. Sensor nodes with radiation sensitivity of 1936.41 are used. Radiating source is moving in the sensor area. As the radiating source is passing along the sensor network, sensor nodes are detecting the radiation.

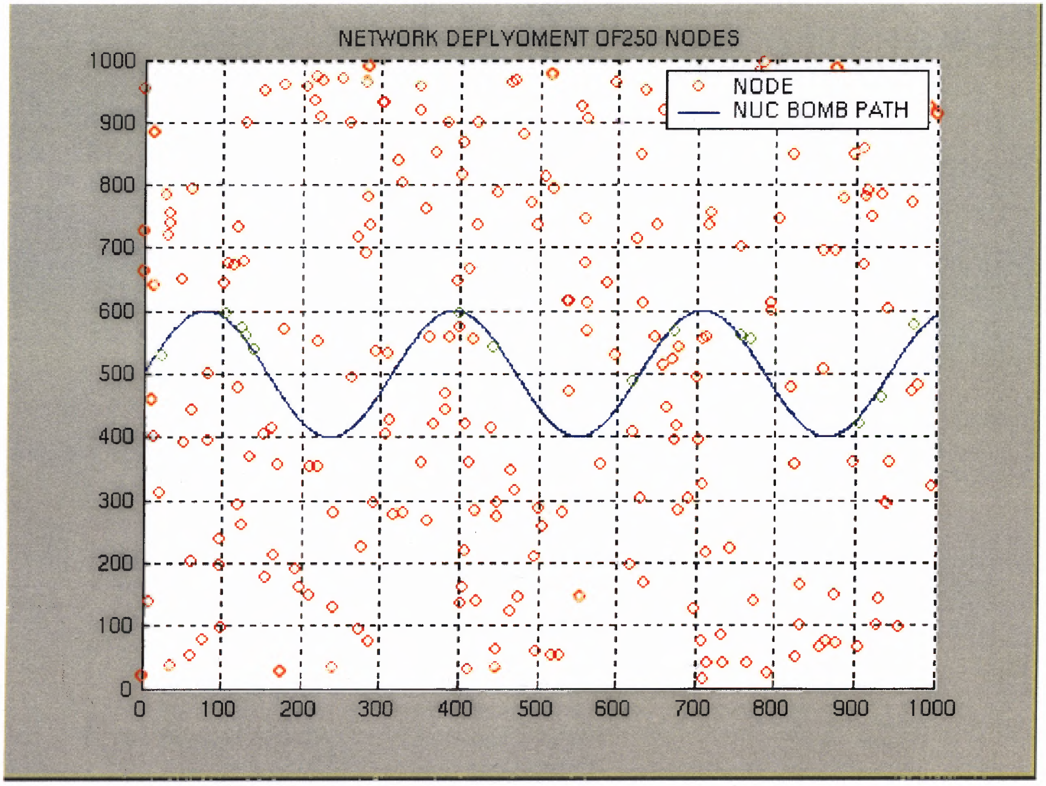

Figure 6.7 Network Deployment of 250 Nodes.

Figure 6.8 shows the actual path of radioactive source and the calculated path of the radioactive source for the network where 250 nodes are randomly distributed in the network.

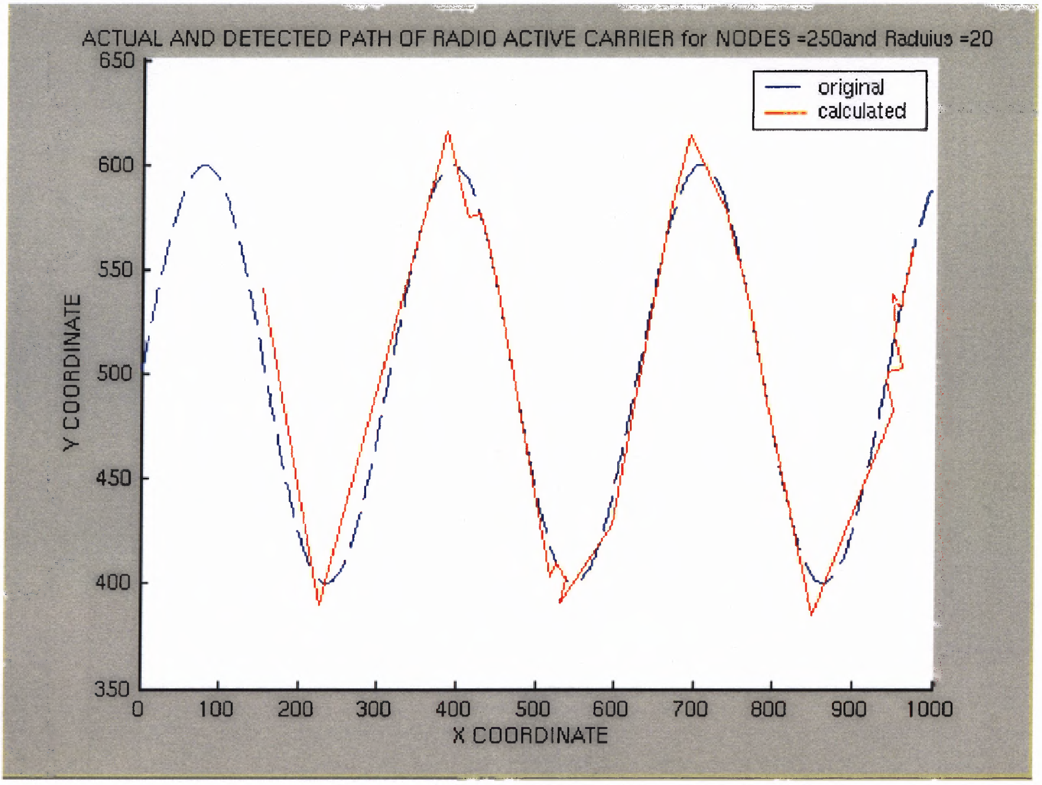

Figure 6.8 Path Trace of Radioactive Source with 250 Nodes.

In a sensor network area 500 nodes are distributed randomly in the area of 1000 * 1000 meter square. Sensor nodes with radiation sensitivity of 1936.41 are used. Radiating source is moving in the sensor area. As the radiating source is passing along the sensor network, sensor nodes are detecting the radiation.

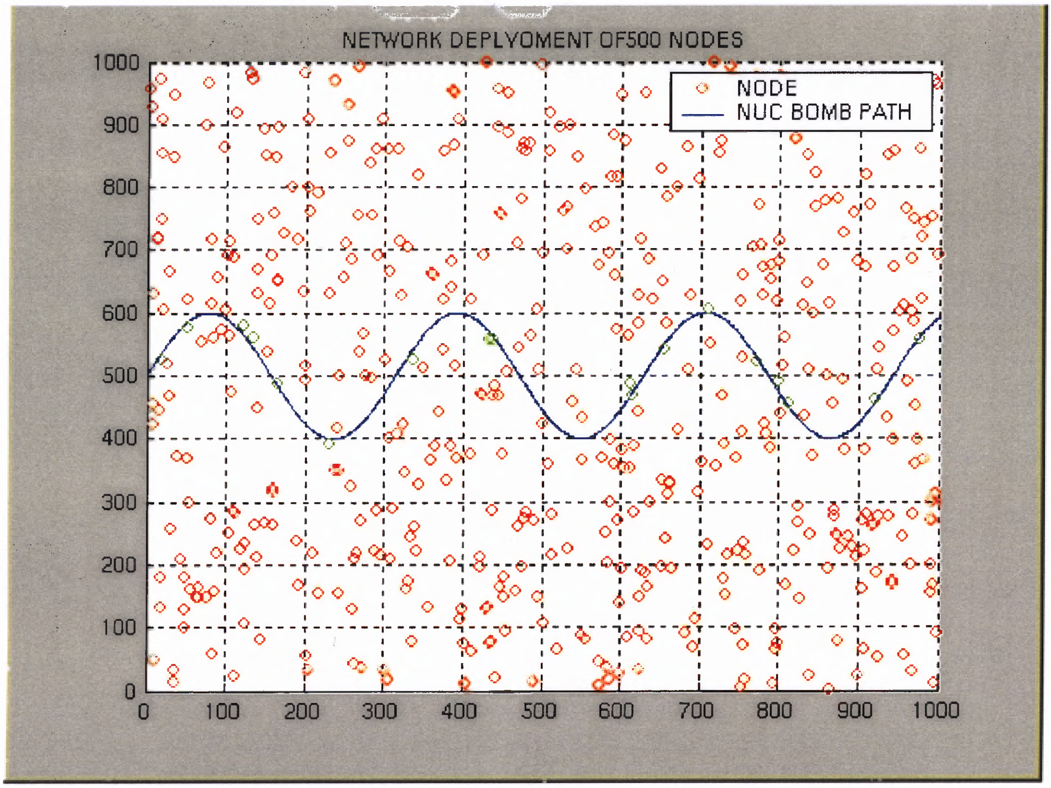

Figure 6.9 Network Deployment of 500 Nodes.

Figure 6.10 shows the actual path of radio active source and the calculated path of the radio active source for the network where 500 nodes e randomly distributed in the network. area of 1000 * 1000 meter square.

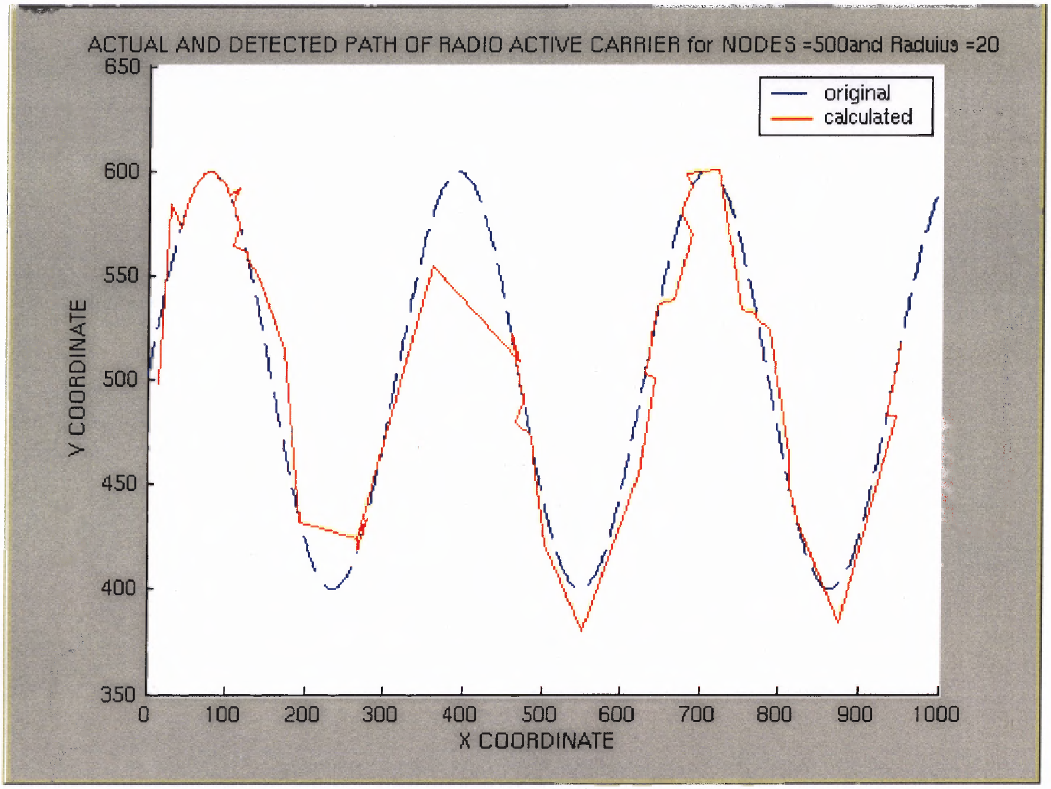

Figure 6.10 Path Trace of Radioactive Source with 500 Nodes.

Figure 6.11 shows, a sensor network area 750 nodes are distributed randomly in the area of 1000 * 1000 meter square. Sensor nodes with radiation sensitivity of 1936.41 are used. Radiating source is moving in the sensor area. As the radiating source is passing along the sensor network, sensor nodes are detecting the radiation.

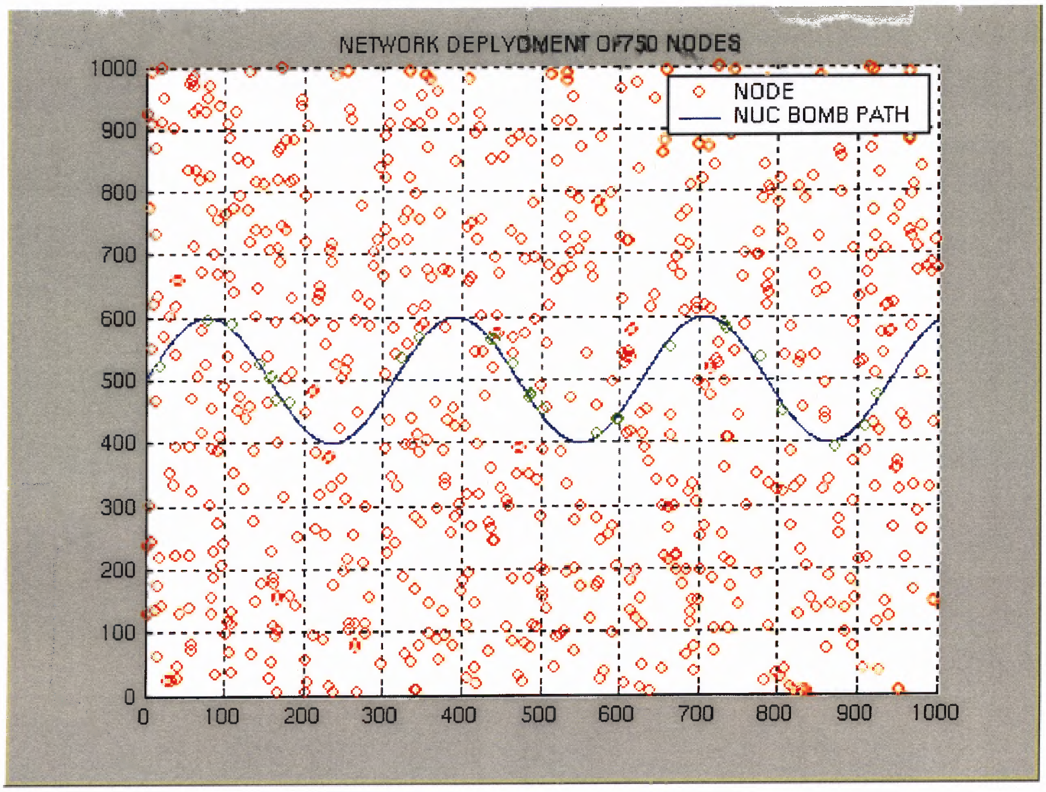

Figure 6.11 Network Deployment of 750 Nodes.

Figure 6.12 shows the actual path of radio active source and the calculated path of the radio active source for the network where 500 nodes e randomly distributed in the network. area of 1000 * 1000 meter square.

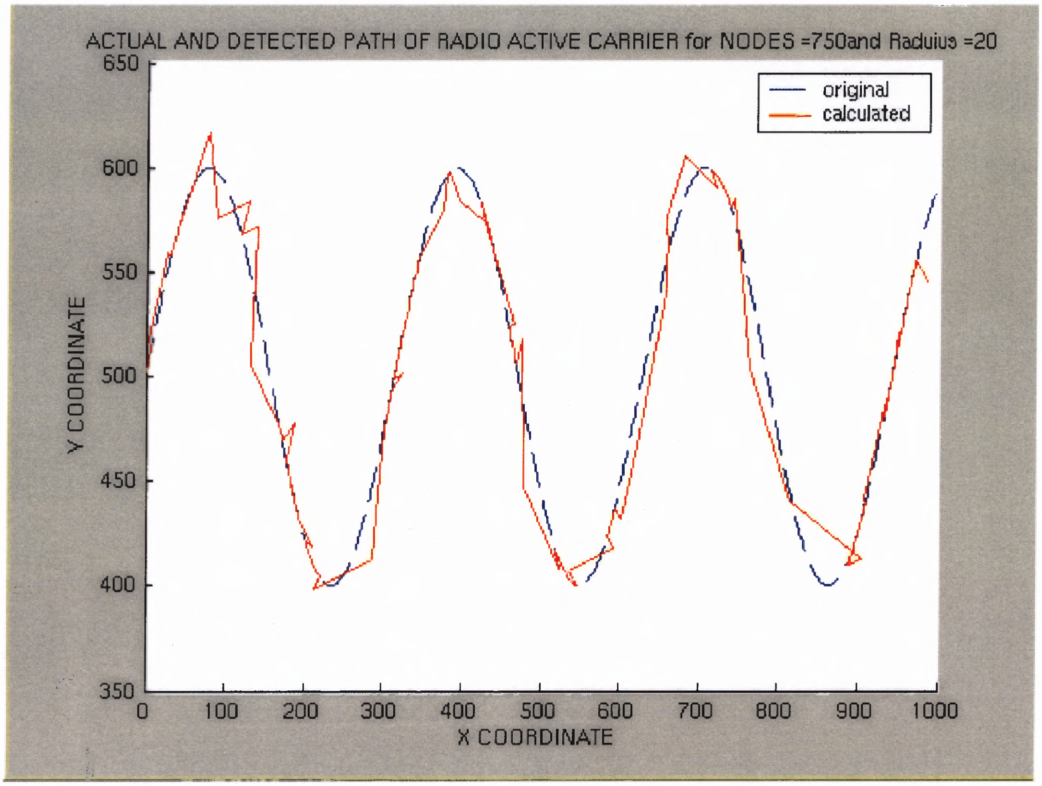

Figure 6.12 Path Trace of Radioactive Source with 750 Nodes.

6.2 Delay Model

In the following experiment the author considered the network size of 250 nodes, 500 nodes and 750 nodes in the network. Figure 6.13 shows the communication which is influence the time of the receipt of the data at the base station.

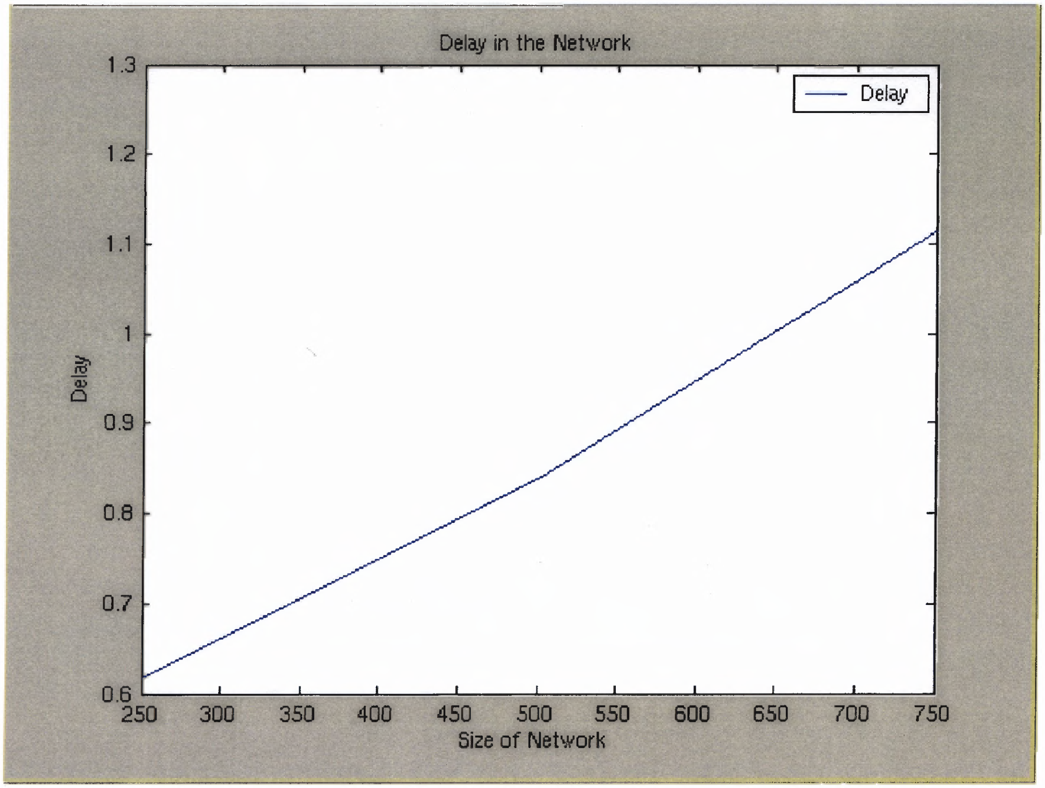

Figure 6.13 Network Delay.

6.3 Accuracy and Energy Trade-off Model

In this experiment the number of nodes was not changed but the communication range was changed and based on these changes sensor node energy consumption changed.

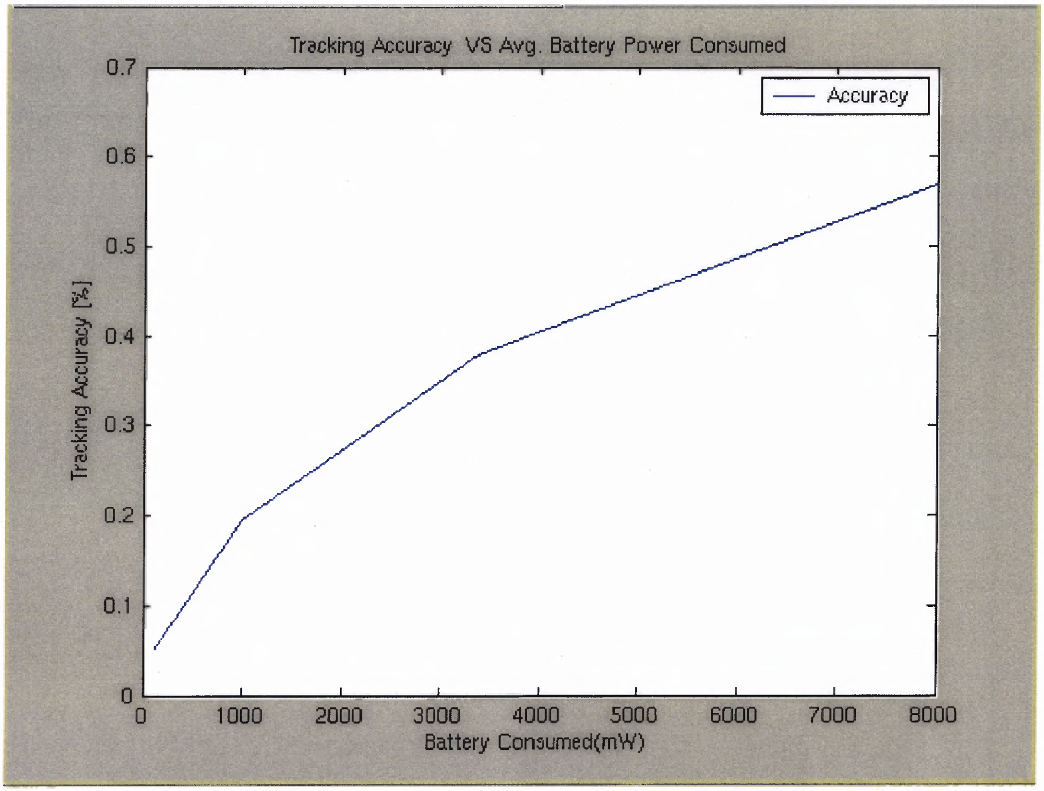

Figure 6.14 Accuracy and Energy Trade-off. Figure presents Accuracy versus energy consumption due to change in communication range.

Different percentage of accuracy achieved in different scenario with the experiment conducted. The accuracy of 56.95 % is achieved whit the 750 nodes in the network and communication range of 20 meters. The accuracy of 37.91 % is achieved in the network with the communication range of 15 meters. The accuracy of 19.46 % is achieved with communication range of 10 meters. Very low accuracy of 9.09% is achieved with the communication range of 10 meters. Very low accuracy of 9.09% is achieved with the communication range of 5 meters. The accuracy increases with the increase of communication range.

Figure 6.15 shows error versus energy consumption due to change in communication range. The network is deployed with 750 nodes. Different communication range is considered. The communication range considered is 20 units, 15 units, 10 units and 5 units. As the communication range decreases error rate increases.

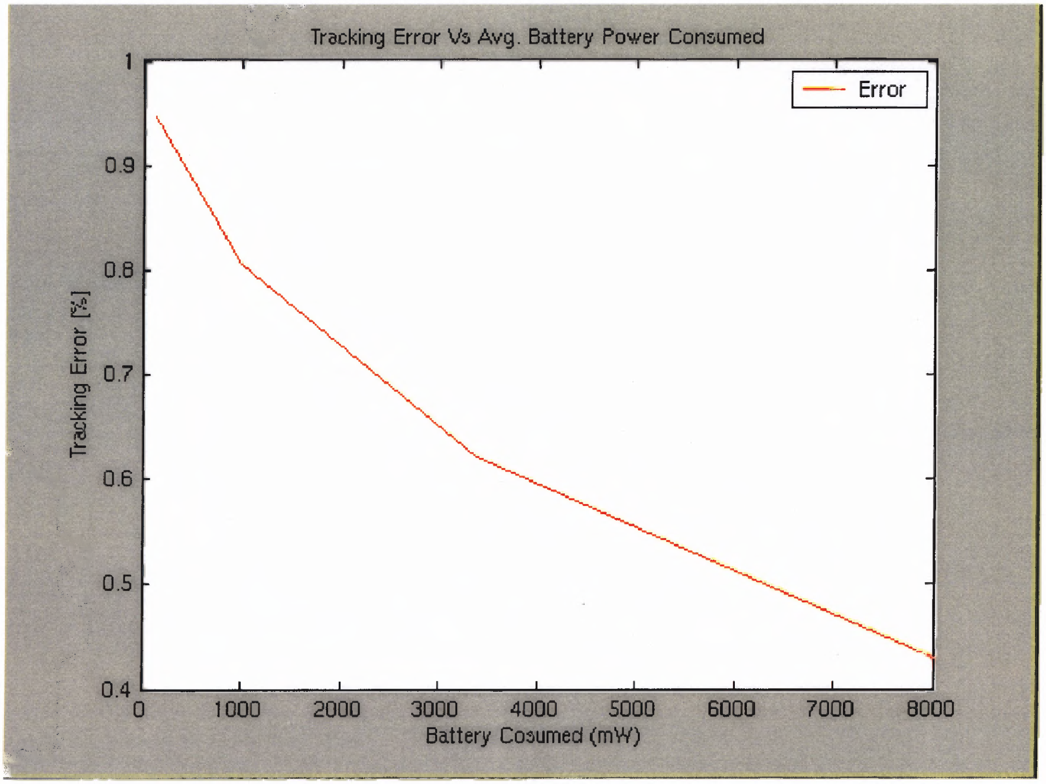

Figure 6.15 Error and Energy Trade-off.

CHAPTER 7

CONCLUSION

The following is summary of experiments done for radiation detection sensor network: The author examined the basic strategy varies with radiation detection sensitivity. This suggest that the more result from the sensor network is send to the base station more accurate result has been achieved. More the sensor network density, will give better accuracy. The radiation detection settings should be carefully chosen and kept to a minimum with these strategies.

From the second experiment to check the delay in the network was found that more the density of the network, more is the network delay. As there is more number of sensor nodes in the network, there is more data to be transferred to the sink node by the sensor nodes.

From the third experiment it is concluded that increasing the network density will give more accurate results. There is more number of nodes in the network to sense the radiation. More number of nodes will send data to the sink node, so can get the accurate results. On other hand it will use more battery. The reason is more data traffic. The number of the communication node increases. Communication energy is proportional to distance cube. More the communication range more number of nodes will transfer the data to the sink node. As a result more energy is used. Also the large part of the energy is wasted.

REFERENCES

1. Akyilidiz, I. F., Su, W., Sankarasubramaniaam Y., and Cayirci, E. (2002). A Survey on Sensor Networks. IEEE Communication Magazine.

2. Shih, E., Cho, S., I., Nathans, M., R., Sinha, A., Wang, A., & Chandrakasan, A. (2001). Physical Layer Driven Protocol and Algorithm Design for Energy Efficient Wireless Sensor Networks. Seventh Annual ACM SIGMOBILE.

3. Cho, S., and Chandrakasan, A. P. (February, 2003) Energy Efficient Protocols for Low Duty Cycle Wireless Microsensor Networks. http://www-mtl.mit.edu/research/icsystems/uamps/pubs/chosta_icassp01.pdf

4. Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J. (2000). Protocols for self-organization of a Wireless Sensor Network. IEEE Communication Magazine.

5. Zou, Y., and Chakrabarty, K. (April, 2003). Energy-Aware Target Localization in Wireless Sensor Networks. IEEE International Conference Pervasive Computing and Communication.

6. Karp, B., & Kung, H. T. (2002). GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. ACM/IEEE International Conference.

7. Howse, J. W. (March, 2003). Detection and Location of Radioactive Sources Using a Suite of Slab Detectors. http://www.c3.lanl.gov/~jhowse/Track_Tech_Rep.pdf

8. Duarte-Melo, E. J., and Liu, M. (December, 2002). http://www.eecs.umich.edu/~mingyan/pub/mwscas.pdf

9. Agrawal, P. (1998). Energy Efficient Protocol for Wireless Systems. IEEE

10. Bult, K., Burstein, A., Chang, D, Dong, M., Fielding, M, and Yao, J. Wireless Iterated Microsensors. UCLA/Rockwell – LWIM Team.

11. Charlie, L. Z., Rabaey, j., Guo, C., and Shah, R. (1999). Data Link Layer Design for Wireless Sensor Networks. IEEE GLOBECOM '98.

12. Intanagonwiwat, C., Govindan, R., and Deborah, E. (April, 2002), Sixth International Conference on Mobile Computing and Networking (MobiCom '00), Boston, Massachusetts.

13. Warneke, B. A., & Pister K. S. (2002) .MEMS for Distributed Wireless Sensor Networks. IEEE

14. Tilak, S., Abu-Ghazaleh, N. B., & Heinzelman, W. (2002). WSNA'02, Atlanta, Georgia.

15. Singh, M., & Prasanna, V. K., (2003). Optimal Energy Balance Algorithm for Selection in Single Hop Sensor Network Protocols and Applications. IEEE International Workshop on Sensor Network Protocol and Application.