ON DESIGN FACTORS, COMMUNICATION PROTOCOLS, AND APPLICATIONS OF WIRELESS SENSOR NETWORKS

By

Sumanth Dommaraju

Problem Report submitted to the College of Engineering and Mineral Resources
At West Virginia University
In partial fulfillment of the requirements
For the degree of

Master of Science
In
Electrical Engineering

Natalia A. Schmid, Ph.D., Chair
Brian D. Woerner, Ph.D.
Matthew C. Valenti, Ph.D.

Lane Department of Computer Science and Electrical Engineering
Morgantown, West Virginia

2007

ABSTRACT

On Design Factors, Communication Protocols, and Applications of Wireless Sensor Networks

Sumanth Dommaraju

Wireless Sensor Networks offer a whole new generation of real-time embedded systems with communication constraints that are considerably different from traditional wired networked systems. This problem report briefly discusses the history and evolution and the various design factors affecting the wireless sensor networks. It also reviews the various communication protocols implemented by the contemporary sensor networks and the operating systems running on them. In addition, this work also discusses the different types of sensors and the various wireless standards governing the wireless communication in these networks. Wireless Sensor Networks have applications in many different fields such as military surveillance, environmental monitoring, health monitoring, process monitoring, etc. and this work provides an overview of their applications.

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation and gratitude to my advisor, Dr. Natalia Schmid, for giving me this opportunity to work on this topic. Her knowledge and encouragement have been of great value throughout the course of my research.

I wish to express my sincere thanks to the members of my committee, Dr. Brian Woerner, and Dr. Matthew Valenti. Their understanding and constructive comments have been important throughout this work.

Lastly, I owe my sincere thanks to my friends and family, for their constant support and valuable encouragement throughout this endeavor.

Table of Contents

CHAPTER 1: Introduction

A wireless sensor network is a network that consists of autonomous devices equipped with sensors that are distributed spatially to cooperatively monitor environmental and physical conditions, such as temperature, pressure, vibration, motion, sound or pollutants, at different locations [1]. The motivation for the development of wireless sensor networks originally came from the military applications such as battlefield surveillance. Wireless sensor networks are presently being used in many civilian applications, such as healthcare, traffic control, environment and habitat monitoring and home automation.

Each node in a wireless sensor network is equipped with a wireless communications device such as a radio transceiver, a small microcontroller, an energy source, usually a battery in addition to one or more sensors. The size of a single sensor node can vary largely from that of a shoebox to the size of a grain of dust. Similarly the cost of a sensor node can vary largely, from hundreds of dollars to a few cents, depending on the complexity required of individual sensor nodes and the size of the sensor network. Constraints such as the size and cost of sensor nodes result in corresponding constraints on resources such as computational speed, energy, bandwidth, and memory.

Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. The base stations are one or more distinguished components of the wireless sensor network with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user.

1.1 History and Evolution:

The early research and development in sensor networks was motivated by the requirements of military and defense applications, as is the case with many other technologies [2]. This could be traced back to the times of the Cold War. During the Cold War, a system of acoustic sensors (hydrophones) deep inside the ocean, called SOSUS (the Sound Surveillance System), was deployed to detect and track quiet moving Soviet submarines at strategic locations. This was one of the first sensor networks ever to be deployed. Over the years, more newer and well-developed acoustic networks have been designed for use in submarine surveillance. The SOSUS is now being used by the National Oceanographic and Atmospheric Administration (NOAA) for observing events related to marine life and seismic activity inside the oceans. Similarly, radar networks for air defense applications were developed and deployed by the United States and Canada during the Cold War. These defense systems have been developed over the years to include more sophisticated sensors such as aerostats.

The modern research on sensor networks was started around the year 1980, when the Defense Advanced Research Projects Agency (DARPA) initiated the program of Distributed Sensor Networks (DSN). The various technology components for the Distributed Sensor Networks were identified in a DSN workshop in 1978 [2], which included acoustic sensors, self-location algorithms for sensors and processing techniques, communication (which included high-level protocols for linking processes in a resource-sharing network), and distributed software. Researchers at Carnegie Mellon University (CMU) focused their efforts on developing a network operating system which enables flexible and transparent access to distributed resources required by a fault-tolerant DSN. They also developed sufficient protocols for network inter-process communication, a system supporting dynamic load balancing and fault reconfiguration of DSN software, and an interface specification language for distributed system software.

Also, researchers at the Massachusetts Institute of Technology (MIT) developed knowledge-based signal processing techniques for the purpose of tracking helicopters, by means of signal abstractions and matching techniques using a distributed array of acoustic microphones. They also developed the Signal Processing Language and Interactive Computing Environment (SPLICE) for analysis of data and development of algorithms for Distributed Sensor Networks. In the 1980s, Advanced Decision Systems (ADS), located at Mountain View, CA, introduced a new Multiple-hypothesis tracking algorithm to cope with difficult scenarios involving false alarms, high target density, and missed detections. They then decomposed the algorithm for implementation on distributed networks. The Multiple-hypothesis tracking algorithm is presently used as a standard approach for difficult tracking problems.

The sensor network research in the present millennium has undergone major changes with the recent advancements in computing and communication. They are being brought closer to reaching the original vision because of these rapid developments.

Tiny and low-cost sensors developed using micro electro-mechanical system (MEMS) technology, inexpensive low-power processors, and advancements in wireless networking technologies enable the deployment of wireless sensor networks for a wide variety of applications. DARPA also introduced the Sensor Information Technology (SensIT) [2] program that came up with two important research and development techniques for wireless sensor networks. They developed new networking techniques and networked information processing techniques.

Current wireless sensor networks are able to exploit technologies that were not available 20 years ago and perform tasks that were not even thought of during that time. All the components of sensor networks such as sensors, communication devices, and processors are all becoming much smaller in size and cheaper, thus enabling sensor networks to be deployed in newer applications. Wireless networks using the IEEE 802.11 standards are now able to provide bandwidths comparable to that of wired networks.

1.2 Applications:

There is a wide variety of applications of wireless sensor networks. They can be deployed to monitor some environmental conditions in remote and uninhabitable areas, where they would remain for many years. They can also be deployed to monitor data in commercial applications such as industrial monitoring that would be expensive or difficult to monitor using wired sensors [1]. There are different technical issues for different application areas that are currently being studied by researchers in the field. Some of the applications of wireless sensor networks are:

- Environmental Monitoring
- Military Surveillance
- Area Monitoring
- Habitat monitoring
- Medical monitoring
- Seismic Detection

- Acoustic Detection
- Process Monitoring
- Inventory Management

CHAPTER 2: Design Factors Influencing Sensor Networks

A typical wireless sensor network consists of sensor nodes that are scattered in a field as shown in figure 1. Each sensor node can collect data and route the data packets back to the sink by means of multi-hop network architecture [3]. The sink can communicate with the task manager node through Internet or satellite. There are various design factors affecting the design of wireless sensor networks such as hardware constraints, reliability, production costs, scalability, operating environment, transmission media, sensor network topology, and power consumption.

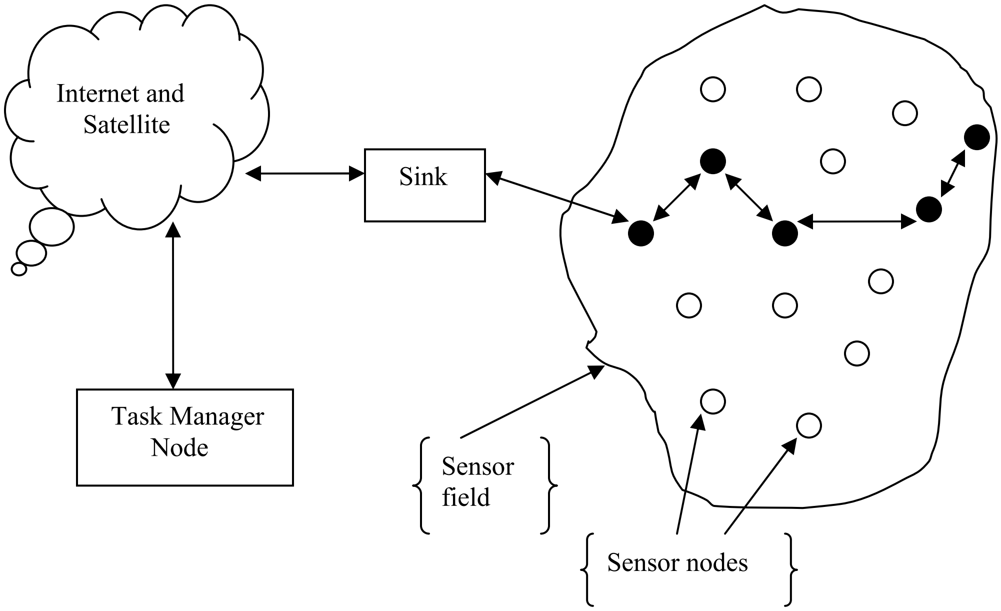

Figure 1: Sensor nodes scattered in a sensor field.

.2.1 **Hardware Constraints:**

As shown in figure 2 given below, a sensor node is made up of four basic components such as a sensing unit, a processing unit, a transceiver unit, and a power unit. They may also include additional components such as a location finding system, a mobilizer, and a power generator if needed, based on the particular application they are used. The sensing unit is made of two subunits, namely, sensors and analog-to-digital converters (ADCs). Sensors produce analog signals based on some observed phenomenon which are converted by the ADC to digital signals and fed to the processing unit [3]. The processing unit carries out the required procedures that are needed for each sensor node to collaborate with the other nodes in the network to perform the required sensing tasks. The power unit is one of the most essential components of a sensor node which may be supported by solar cells. Each node is connected to the network by a transceiver unit. The network also has other application-dependent subunits. The sensor node usually has a location finding system since most of the network routing techniques and sensing tasks demand highly accurate knowledge of location. A mobilizer is needed sometimes to move the sensor nodes in the network to perform the assigned tasks.

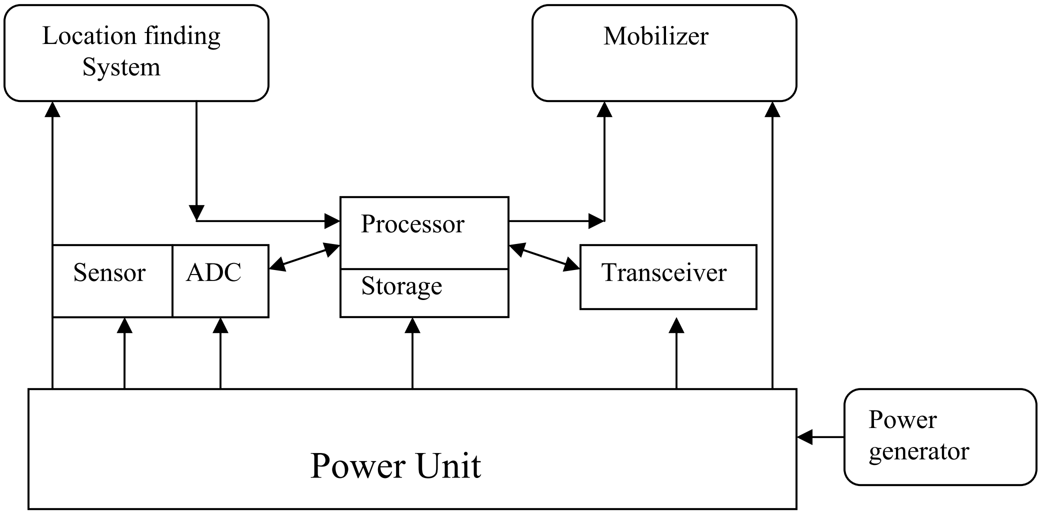

Figure 2: The components of a sensor node.

2.2 Environment:

Sensor nodes are usually densely installed in remote geographic areas either directly inside the environment where the phenomenon is observed or very close to it and hence they are generally unattended. They may also be deployed in a battlefield beyond the enemy borders, inside a large building, in a biologically contaminated field and also deep inside an ocean.

2.3 Sensor Network Topology:

The sensor field consists of hundreds to several thousands of nodes deployed in a distance of several feet from each other. Careful handling of topology maintenance is required in deploying a large number of nodes whose densities could be as high as 20 nodes/cubic meter [3]. The issues concerned with topology maintenance and change may be examined in three phases:

- *Pre-deployment and deployment phase:* The sensor nodes are usually deployed by either placing one after another in the sensor field or can be thrown in as a mass in random by dropping from an airplane, a rocket, or a missile, or also can be delivered in an artillery shell.
- *Post-deployment phase:* After the deployment phase, the changes in network topology are due to change in nodes' position, malfunctioning of certain nodes, availability of energy and their accessibility.
- *Redeployment phase:* Owing to the changes in task dynamics and to replace certain malfunctioning nodes, additional sensor nodes can be redeployed at any time.

2.4 Scalability:

Based on the application, the number of sensor nodes that is deployed may be in the order of hundreds or thousands and in some cases, it can be millions. They should be installed in such a way that new schemes must be able to be employed without any difficulty and such that they also use the high density of sensor networks. The density in an area which can be less than 5 m in radius can vary from few tens to few hundreds of sensor nodes. The density μ can be calculated according to [3] as,

$$\mu(R) = \left(N \cdot \pi \cdot R^2\right) / A,$$

where, $\mu(R)$ is the number of nodes within the transmission radius of each node in a region A, N is the number of scattered sensor nodes and R is the radio transmission range in region A.

2.5 Reliability:

Sensor nodes may fail to operate due to physical damage, lack of sufficient power or environmental conditions which should not alter the ultimate task of the network. Reliability of a sensor network is an important issue that needs to be addressed. The reliability or fault tolerance of a sensor network is its ability to sustain its functionalities without any delay caused due to failure of its sensor nodes. According to [28], the reliability $R_k(t)$ of a sensor node is modeled using Poisson distribution to calculate the probability of not facing a failure over an interval (0, t):

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

where, t is the time period, and λ_k is the rate of failure of node k.

2.6 Production Costs:

The cost of a single sensor node plays a major role in determining the overall cost of the sensor network as they consist of a large number of nodes. The cost of each sensor node has to be kept low to see that the cost of the network is less expensive than installing traditional sensors and the network is cost-justified.

2.7 Transmission Media:

The sensor nodes are connected by a wireless medium such as a radio, infrared, or optical media for communication in a multi-hop sensor network. The selected transmission medium must be available elsewhere to enhance the global operation of these networks.

At present, the hardware used for sensor nodes is based mostly on RF circuit design. The Wireless Integrated Network Sensors (WINS) architecture [4] uses radio links, the low-power sensor device described in [5] uses a single-channel RF transceiver operating at 916 MHz, and the μAMPS wireless sensor node uses a Bluetooth-compatible 2.4 GHz transceiver with an integrated frequency synthesizer[6].

Infrared communication is another means of communication between the sensor nodes which is robust to interference caused by electrical devices. Transceivers built on infrared technology are cheaper and easier to build. Transmission can also be done using optical medium. Smart Dust mote [7] system is one of the recent developments, which uses the optical medium for autonomous sensing, computing and communication. A line of sight is needed for systems operating based on the optical and infrared medium.

2.8 Power Consumption:

The wireless sensor node is a micro-electronic device which can be supplied only with a minimal power source (< 0.5 Ah, 1.2 V) [3]. Moreover, replacement of power supplies is impossible in certain application areas. Hence, the battery lifetime strongly determines the lifetime of the sensor node. Each node acts as both data originator and data router in a multi-hop sensor network. Therefore, failure of some nodes affects the network topology and might require data rerouting. Thus, power management and conservation account for extra importance and for these reasons, researchers are focusing primarily on the development of power-aware algorithms and protocols for sensor networks. Power consumption can be divided into three domains based on the tasks of a sensor node: sensing, data processing, and communication.

CHAPTER 3: Communication protocols for Sensor Networks

The protocol stack used by the sink and sensor nodes in the sensor networks is as shown in figure 3. The protocol stack consists of the physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane, and task management plane [3]. It integrates data with networking protocols, combines power and routing awareness, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes.

The needs of simple but robust modulation, transmission, and receiving techniques are addressed by the physical layer. The medium access control (MAC) protocol must be power-aware and able to minimize collision with neighbors' broadcasts, since the environment is noisy and sensor nodes can be mobile. Routing the data supplied by the transport layer is controlled by the network layer. The flow of data is maintained by the transport layer if the sensor networks application requires it. Different types of application software can be built and used on the application layer, depending upon the sensing tasks. The power, movement, and task distribution among the sensor nodes are monitored by the power, mobility, and task management planes. These planes help the sensor nodes in coordinating the sensing tasks and lowering overall power consumption.

The usage of power by a sensor node is managed by the power management plane. The movement of sensor nodes is detected and registered by the mobility management plane, so that the sensor nodes can keep track of who their neighbor sensor nodes are, and a route back to the user is always maintained. The sensing tasks given to a specific region are balanced and scheduled by the task management plane. These management planes are important for the sensor nodes to work together in a power-efficient way, share resources between sensor nodes, and route data in a mobile sensor network.

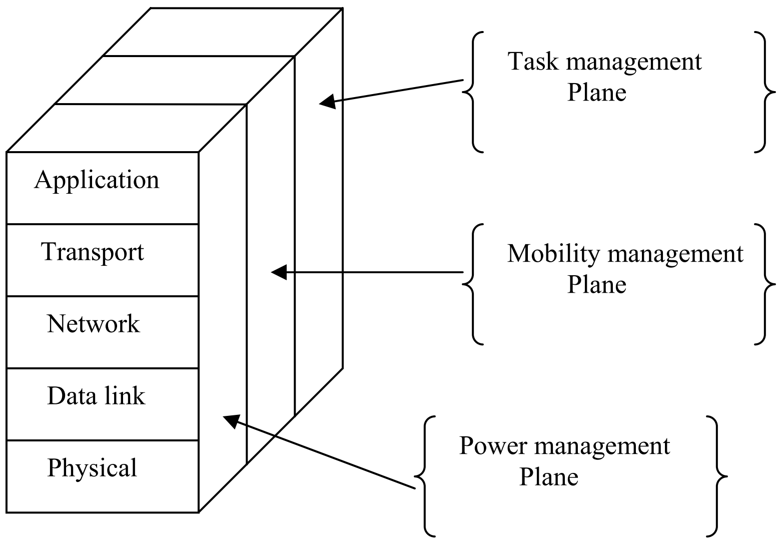

Figure 3: Protocol Stack of the sensor networks.

3.1 SPIN Protocol:

SPIN (Sensor Protocols for Information via Negotiation) is a family of adaptive communication protocols that is used for efficient dissemination of information between sensors in an energy-constrained wireless sensor network [8]. Sensor nodes using the SPIN protocol can use both application-specific knowledge of data and knowledge of available resources to make their communication decisions. This enables efficient distribution of data by the sensors in a limited power supply scenario.

Conventional protocols are based on sending data by each node to every neighboring node, each of which saves a copy of that data and sends that data to all other neighboring nodes. This simple way of communication has its disadvantages namely: a) *Implosion*, caused by the sending of data by a node to all of its neighbors without any knowledge of receipt of the same data from other nodes. b) *Overlap*, caused by the nodes gathering similar packets of data by covering overlapping geographic areas. c) *Resource blindness*, caused due to the lack of knowledge of a sensor node of its available resources and the resulting inability to regulate its tasks based on it.

The SPIN family of protocols overcomes these deficiencies by adapting two important strategies: *negotiation* and *resource-adaptation*. Negotiation ensures that only valuable information is communicated between nodes, which negotiate with each other prior to transferring data and thus overcomes the implosion and overlap problems. Also, each node is equipped with a resource manager which maintains a record of resource consumption and is accessed before sending or processing data. This makes sure that the sensor nodes stop some activities when there is a shortage of energy resources. This overcomes the resource blindness problem.

Thus, this family of protocols is built on two basic ideas. The first one is the sensor node applications must operate efficiently and conserve energy by sharing their knowledge with other nodes about the data they already possess and the data needed to obtain. The second one is all the nodes in the network must keep a track of its energy resources and adapt according to resource availability to ensure longevity of the system.

Sensor nodes adapting the SPIN protocols use three types of messages to communicate:

- ADV- When a node is ready to share its data, it advertises by sending an ADV message containing meta-data to its neighboring nodes. Meta-data are the high-level data descriptors used by the nodes running the SPIN communication protocol to name their data.
- REQ- This is a request for data message sent by the SPIN node when it needs to receive data.
- DATA- This is a data message sent by the SPIN node that consists of actual data with a meta-data header.

Both ADV and REQ messages are smaller and cheaper to transmit and receive compared to their corresponding DATA messages as they consist of only meta-data.

The SPIN family of protocols is comprised of two protocols, SPIN-1 and SPIN-2 [8].

SPIN-1: The SPIN-1 protocol is a simple handshake protocol that works in three stages, i.e. ADV-REQ-DATA, for disseminating information through a lossless network. Though it is designed for lossless networks, this protocol can be easily adapted and used in mobile networks. The main advantage of this protocol is it is very simple. The energy wastage in computation is less since each node performs little decision making upon receipt of new data. Also, SPIN-1 protocol can be run in a totally unconfigured network with a minimal initial cost of determining closest neighboring nodes.

SPIN-2: This protocol is obtained by adding a simple energy-conservation dimension to the SPIN-1 protocol. The sensor node using this SPIN-2 protocol adapts accordingly when it observes that its energy resource is approaching a minimum threshold by minimizing its participation in the protocol. Otherwise, when it has the required energy resource, the node communicates with others by using the same SPIN-1 protocol. This implies that a sensor node initiates the three-stage protocol to participate in the full protocol with its neighboring nodes only when it determines it has enough energy resources.

Thus SPIN protocols achieve high performance at a very low cost in terms of energy, communication, computation, and complexity.

3.2 SPEED: A Spatiotemporal Communication Protocol

SPEED is a spatiotemporal communication protocol designed specifically for wireless sensor networks [9]. Most of the sensor networks are designed to track rapidly changing events in a real-time scenario and hence communication delays in sensing might directly impact the actual task of the network. Since communication is physically bounded in multi-hop wireless sensor networks, the end-to-end time delay is affected not only by a single hop delay, which is a time-constraint, but is also affected by the total distance that a data packet travels (a spatial-constraint). Hence the SPEED protocol is developed with an aim to provide a spatiotemporal communication service with a specific delivery speed across the network that maintains the end-to-end delay proportional to the source-destination separation. The delivery speed here denotes the rate of approach of a data packet along a straight path from the source towards destination.

The SPEED protocol combines a feedback control mechanism (which is time-aware) and a nondeterministic geographic forwarding scheme (which is spatial-aware) to achieve the desired spatiotemporal requirements. This protocol has been implemented on the Berkeley motes, which is one of the most versatile wireless sensor network prototypes available in market.

The results showed that SPEED protocol improves the system lifetime by balancing the traffic load on the network.

The following are some of the design objectives achieved by the SPEED protocol:

- *Minimal State Architecture:* Sensor networks suffer from physical limitations such as limited memory capacity, large scale deployment and high failure rate. These limitations necessitate a minimal state approach in the design architecture of the sensor networks. SPEED protocol requires minimal memory requirements, since it maintains information of only immediate neighbors.
- *Soft Real-Time:* SPEED protocol provides a delay guarantee per unit delivery distance (speed guarantee) called the soft real-time guarantee, by which we can calculate a predictable end-to-end communication delay under given distance (spatial) constraints before hand.
- *Localized Behavior:* In SPEED protocol, all the distributed operations are localized to achieve high scalability. This ensures that there are no broadcast storms which may result in significant power consumption and cause a sensor network meltdown, where some thousands of nodes are communicating with each other.
- *Minimum MAC Layer Support:* SPEED ensures a minimal MAC layer support since it uses a feedback control scheme allowing all existing best effort MAC layers and hence does not require a real-time MAC layer support.
- *Traffic Load Balancing:* Bandwidth and energy are limited resources available in sensor networks compared to a wired network. Hence, SPEED implements a nondeterministic forwarding scheme to balance each flow of data packets among multiple concurrent routes, which uses several simultaneous routes to carry packets from the source to destination.
- *QoS Routing and Congestion Management:* SPEED uses a novel backpressure rerouting scheme to reroute packets around large-delay links with minimum control overhead. Thus it overcomes the problems of rerouting when a route becomes congested in a scenario where congestion patterns keep changing rapidly in the network.

3.2.1 **Components of SPEED protocol:**

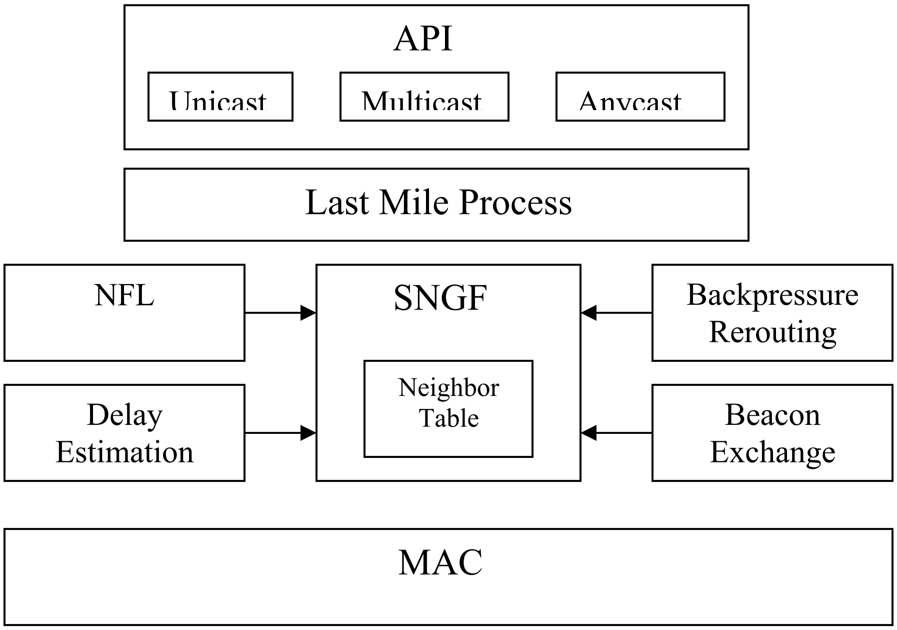

Figure 4: SPEED Protocol.

The SPEED protocol consists of the following components:

- An API.
- A delay estimation scheme.
- A Neighborhood Feedback Loop (NFL).
- Backpressure Rerouting.
- A Nondeterministic Geographic Forwarding algorithm (NGF).
- A neighbor beacon exchange scheme.
- Last mile processing.

SPEED achieves a desired delivery speed across the network by adapting a two-tier method for diverting traffic at the network layer and locally regulating packets sent to the MAC layer.

As shown in figure 4, the SPEED protocol consists of a component called last mile process that supports three types of real-time communication services for sensor networks called real-time unicast, real-time area multicast and real-time area anycast [9]. The desired delivery speed in the network is achieved by a routing module called NGF. The congestion problem is taken care of by the modules, NFL and Backpressure Rerouting, which reduce or divert traffic in such a situation. The geographic location of the neighboring nodes is provided by beacon exchange, which helps NGF perform routing based on geographic location. Delay estimation is a process by which a node can estimate congestion problem.

To conclude, SPEED is the protocol specifically designed for wireless sensor networks to meet its real-time requirements under spatial constraints and provide desired performance during congestion and voids in the network.

3.3 DEEPS Protocol:

DEEPS (Deterministic Energy-Efficient Protocol for Sensor Networks) is a new communication protocol which is designed to increase the lifetime of the sensor network [10]. In most of the sensor network applications, replenishment of power sources is impossible and hence efficient use of energy is a necessity.

DEEPS is aimed at maximizing the sensor network lifetime by using efficient distributed algorithms for continuous and event-driven sensor network models. This protocol proved to be reliable and shows a two fold increase in the network lifetime when compared with several known target-monitoring protocols.

The main idea behind the development of DEEPS protocol is as follows: In an object tracking application, it can be said that the best schedule for any individual target *T* is to activate all the covering sensors in sequential time periods. In fact, the total battery supply for *T* decreases two times faster, when any of the two covering nodes are active simultaneously. Hence, minimizing the energy-consumption rate for energy-poor targets while allowing higher energy consumption for sensors with higher total supply proves to be a good strategy. Thus the off-rule for DEEPS turns off the poorer sensors covering a sink until a single left sensor is turned on according to the on-rule.

A simple application of this rule may result in the loss of reliability requirement. Thus, it is necessary to place at least one sensor in charge of each target *T* in order to restore reliability. The sensor in charge of *T* should not turn off unless it knows that another switched-on sensor node covers it. It is necessary for any sensor to know the battery supply of all the targets of the neighbors in order to learn for which targets it is in charge of. This can be obtained either by simply increasing the communication range to four times the sensing range, or by making two broadcasts to the neighboring sensor nodes.

- *On-rule.* Whenever a sensor node has a target covered only by itself, it turns itself on, i.e. switches into 'on' state.
- *Off-rule.* Whenever a sensor node is not covering any target except those already covered by 'on' sensors, it turns itself off, i.e. switches into 'off' state.

The reliability of DEEPS is assured by the fact that each target has a sensor node that is in charge of it. DEEPS also guarantees that the sensor cover is minimal, since each sensor *S* has a target covered only by *S*. Sensor networks adopting DEEPS have less sensors active at a time, spend less total energy increasing their life-time, have sensors alive for a longer time, and cover larger portion of monitored area for a longer time.

CHAPTER 4: Operating Systems

Wireless sensor networks are made of several thousands of tiny sensor nodes, each of which executes concurrent and reactive programs [12]. The nodes operate with severe energy and memory constraints. The challenges posed by limited resources, low-power operation and event-driven concurrent applications drive the design of specific operating systems for sensor networks. 'TinyOS' is one such open-source operating system designed specifically for wireless sensor networks [11].

There are other operating systems designed for sensor networks apart from TinyOS such as, SOS [13] and Contiki [14]. These operating systems are implemented in C programming language, and like TinyOS, both SOS and Contiki are event-driven operating systems.

TinyOS is perhaps the first operating system designed specifically for sensor networks. It is a tiny (lesser than 400 bytes) and flexible operating system developed from a set of reusable components that are integrated into an application-specific system. TinyOS supports an event-driven concurrency model based on asynchronous events, split-phase interfaces, and deferred computation called 'tasks'. It has a component-based programming model, implemented in the NesC language which is an extension to the popular C programming language. TinyOS enabled sensor networks to be used innovatively in a wide variety of applications.

TinyOS has been under development for several years and is currently in its third generation. Its current version provides application developers with a large number of components which include abstractions for sensors, power management, routing, single-hop networking, and non-volatile storage.

The design of TinyOS has been motivated by four requirements [12]:

- *Limited Resources.* The sensor nodes are equipped with limited physical resources such as power and memory, in order to meet its objectives of low cost, low power usage, and small size. TinyOS has been designed to overcome these limitations.
- *Flexibility.* Sensor networks are subject to change in their hardware composition and applications, which requires an operating system that is flexible in nature. TinyOS is designed to be flexible, that is both application-specific and independent of the boundary between hardware and software.
- *Reactive Concurrency.* A typical application of a sensor network is to observe different aspects of its operating environment through its sensors, perform some data processing locally, transmitting and routing those data to other nodes, and participating in various distributed processing tasks. Most of these actions call for real-time responses. TinyOS deals with concurrency management that is required to take care of these aspects, meeting the timing and resource constraints at the same time.
- *Low Power.* An important goal of the sensor network design is low-power operation to meet their low-size and low-cost conditions. TinyOS addresses extremely low-power operation, power-management and duty-cycle strategies providing a great deal of flexibility.

4.1 TinyOS-Programming Overview:

TinyOS is not exactly an operating system that is understood in the traditional sense, instead it can be viewed as a programming framework and a set of components designed for embedded systems, which enable building of an application-specific operating system into each application. A typical application has a size of about 15K bytes, of which the base OS is about 400 bytes. The largest application, a database-like query system, is around 64K bytes in size.

A TinyOS program is a graph of components, each of which is an independent computational entity that has one or more interfaces. Each component has a set of three computational abstractions, namely, *events, commands* and *tasks* [12]. ‘Tasks’ are mechanisms used to express intra-component concurrency, while ‘events’ and ‘commands’ are the mechanisms used for inter-component communication. Typically, a *command* is a request sent to a component to perform some service, such as for example, initiating a sensor reading. An *event* is used to signal the end of that service. Events are analogous to up calls and commands are analogous to down calls, from the perspective of a traditional operating system. Instead of performing a computation immediately, commands and event handlers may post a *task*. Task is a function that is executed at a later time by the TinyOS scheduler. Task represents the internal concurrency within a component and can only access state within that component.

4.2 Some Applications of TinyOS:

4.2.1 Object Tracking:

The object tracking application utilizes a sensor network to detect, localize and track an object that is moving in a sensor field; the object is a remote-controlled car in the prototype. Every action and communication of the motes is determined by the movement of the object through the sensor field. Each mote samples its magnetometer periodically, and transmits the reading with a significant change to its neighboring nodes. The node with the largest reading change estimates the target position based on the calculation of the centroid of the readings of its neighbors. Then the node routes this estimated target position to the base station using geographic routing. The base station then performs the necessary actions on the target. TinyOS execution model helps run these various distributed services, such as routing, localization, power management, time synchronization, and data sharing, concurrently with limited resources.

4.2.2 Habitat Monitoring:

Another application is a habitat monitoring system that has been deployed to monitor the activities of Leach’s Storm Petrels in their underground burrows on Great Duck Island, which is several miles off the coast of Maine. The network was designed to operate unattended for a minimum of 7-9 months. The motes that were deployed in burrows monitored light, pressure, humidity, and temperature broadcasted their readings back to a base station equipped with an internet connection via satellite. These readings were then uploaded to a database. These nodes used a simple TinyOS program, which sampled the sensors periodically, i.e. every 68 s, and relayed data back to the base station. Nodes used the efficient power management strategies provided by TinyOS, thus consuming only 35µA in low power state, compared to 18-20mA when active.

TinyOS thus provides a flexible and efficient platform for developing various wireless sensor network algorithms, applications and systems. It even facilitates sensor networks to be deployed on a wider scale and enables innovation in sensor network design. The following table presents some of the criteria met by the TinyOS and SOS operating systems [27]:

	TinyOS	SOS
1) Concurrency	Event-driven architecture	Event-driven architecture
2) Modularity	OS + application compiles into single executable	Micro-kernel + application modules
3) Code communication	Uses event/command model translated to function calls; FIFO and non pre-emptive scheduling	Function calls within a module; scheduling at module level, 2-level priority
4) Application boundary	No kernel/application boundary	Clear application boundary

CHAPTER 5: Sensors

A sensor is one of the key components of a wireless sensor network. It is a device which produces a measurable response to a change in a physical condition, such as humidity, temperature, pressure and thermal conductivity, or to a change in chemical composition of a material [15]. The sensor is primarily responsible for converting some type of physical phenomenon into a measurable quantity by a data acquisition system.

There are various key factors to be considered when selecting a sensor for a particular application of the wireless sensor network. They are:

- *Accuracy.* Accuracy is measured in terms of the statistical variance about the exact reading. The sensor has to be pretty accurate in order to obtain reliable data.
- *Cost.* The cost of a single sensor plays a major role in determining the overall cost of the sensor network. Hence sensors those are relatively cheaper are preferred.
- *Repeatability.* The sensor has to be very consistent in its readings when a particular physical condition is measured repeatedly.
- *Calibration.* The sensors have to be well calibrated for most of the measuring systems since their readings will drift over time.
- *Measurement Range.* The upper and lower limits of measurement of a sensor play a key role in its selection for an application.
- *Resolution.* Resolution is nothing but the smallest variation that the sensor can detect and good sensors are required to have a high resolution.
- *Environmental Conditions.* Sensors are typically deployed in areas with hostile environmental conditions. Hence sensors having good temperature and/or humidity limits are preferred.

5.1 <u>Types of Sensors:</u>

There are many different types of sensors that are being developed and used depending upon the type of sensor network application that they are put to use [15]. Sensors are classified according to the following basic physical phenomena measured by them:

i) *Temperature.* There are many different types of sensors to measure temperature such as thermocouples, thermistors, fiber optic temperature sensors, and radiation pyrometers.

'Thermocouple' is a pair of dissimilar metal alloy wires joined at least at one end, which depending upon the size of the temperature difference between the two ends, the uniformity of the wire's relative Seebeck coefficient and the relative Seebeck coefficient of the wire pair, generates a net thermo-electric voltage.

'Thermistor', also called as Resistance Thermometer, is a device that measures temperature by relating the variation in resistance of a material as a function of temperature.

'Fiber Optic temperature sensor' measures temperatures ranging from -200C to +600C accurately and safely, and are ideal for use in extremely hazardous and high electromagnetic field environments, because of their glass-based technology that is inherently immune to corrosion and electrical interference.

'Radiation pyrometer' is a type of sensor that measures temperature of an object by sensing the thermal radiation emitted from the object.

ii) *Pressure.* There are different types of sensors for measuring changes in pressure such as the barometric pressure, height of a column of liquid, vacuum, altitude, and volumetric displacement. These sensors are more commonly called as 'Pressure transducers'. A transducer is a device which converts observed physical phenomenon such as pressure and temperature, into an electric signal.

'Capacitance transducers' are used in automobile applications to produce capacitance changes proportional to changes in applied pressure.

'Piezo-resistive transducers' are used to output a voltage that is proportional to changes in pressure.

iii) *Humidity.* The humidity sensors are primarily used to measure the amount of humidity in the air, as a fraction of the maximum amount of water that the air can absorb at a particular temperature. The value can vary between 0 (i.e. absolute dry point) and 100 (i.e. condensation starting point), at a given temperature under normal atmospheric conditions.

The sensors used to measure humidity must be consistent in its readings and should not change by pressure and temperature changes. Hence, resistive type sensors and mechanical devices cannot be used to measure humidity, and Capacitance sensors are the type of sensors used to measure humidity which also provide excellent stability and good resistance to pollutants.

iv) *Chemical/ Gas Concentrations.* There are quite a number of different types of sensors to measure chemical and gas concentration levels in industrial applications. These are infrared and thermal conductivity-based sensors that detect Carbon-dioxide and flammable gases, and electrochemical sensors that detect oxygen and some toxic gases [15].

v) *Acoustic.* The sensors used to detect and measure sound are called microphones. They can be differentiated into different types based on their conversion system, such as dynamic, piezoelectric, and electrostatic microphones.

The electrostatic-type microphones are the most popular among these as they can measure responses over a wide range of frequencies and are highly stable. The piezoelectric-type microphones are mainly used to record sound levels at relatively lower frequencies.

vi) *Magnetic fields.* The sensors used in the magnetic fields are termed as Magneto-resistive sensors, which calculate the change in earth's magnetic field because of a ferromagnetic object and can also determine its position within the magnetic field.

They can be used to detect vehicles and other ferrous objects moving at high speeds because of the high bandwidths. The primary applications of these types of sensors include vehicle detection, medical instruments, and compassing and navigation.

CHAPTER 6: Wireless Standards

There are various standards for wireless communications that have been developed specifically for wireless sensor networks, such as IEEE 802.15.4 standard [16], Zigbee, and Wireless HART.

6.1 IEEE 802.15.4:

The IEEE 802.15.4 standard was developed by the IEEE organization for wireless sensor network applications, home automation, and remote controls [16]. This standard specifies the medium access control (MAC) layer and physical layer for low data-rate wireless personal area networks (WPAN) [17]. It is being maintained by the IEEE 802.15 working group. This standard defines only the lower levels of the 7-layer OSI communication model that is shown in figure 5.

Some of the primary features of the IEEE 802.15.4 standard are it provides an effective power management scheme to ensure low power consumption and a long battery life ranging from months to years, offers a fully hand-shaked protocol for reliable transfer of data, and offers low data rates.

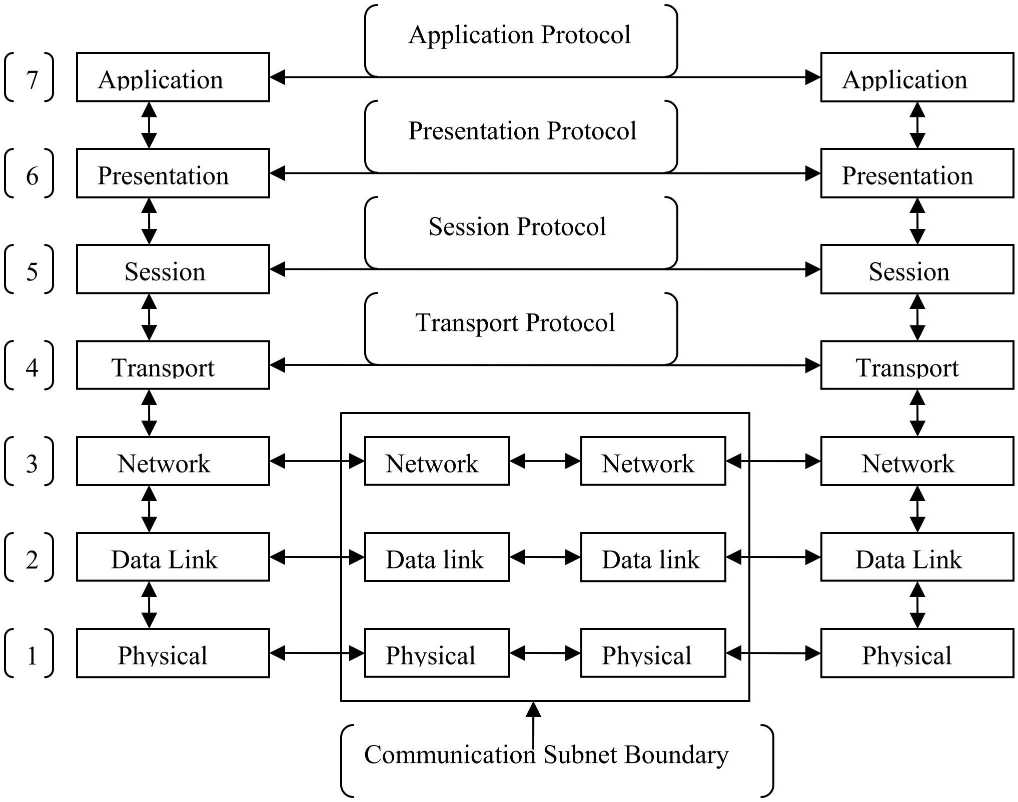

Figure 5: The 7-layer OSI Communication Model.

6.2 Zigbee:

Zigbee is one of the more recent standards developed for low-cost and high-reliability wireless sensor networks [18]. The Zigbee wireless technology focuses on RF applications providing low data rates, long battery life, and secure networking. It also supports large-scale sensor networks.

Zigbee is developed on top of the IEEE 802.15.4 standard and intends to provide a complete networking solution by developing the upper layers of the OSI communication model, shown in figure 5, that are not defined by the IEEE 802.15.4 standard. The Zigbee standard is being further developed to be implemented in sensor network applications such as industrial process control, monitoring cargo to avoid tampering of products and detect improper handling, precision agriculture, and in health equipment used in medical care.

6.3 Wireless HART:

Wireless HART is an open and interoperable wireless communication standard that is designed to provide secure, robust, and reliable wireless communication in industrial plant applications [19].

The specifications of the Wireless HART wireless standard are largely based on the OSI communication model. This technology has been largely built based on the established standards such as IEEE 802.15.4 radio and frequency hopping, spread spectrum, and mesh networking technologies. The primary sensor network applications of Wireless HART are in inventory management, unmanned offshore gas production, and health monitoring.

CHAPTER 7: Applications of Wireless Sensor Networks

7.1 Military Surveillance:

Military Surveillance is one of the most important application areas of wireless sensor networks. Surveillance focuses on acquisition and verification of information about the capabilities and hostile target positions of enemies in the battlefield [20]. It often requires stealth ness of a high degree as it involves the element of high risk for human personnel involved in it. Hence, wireless sensor networks are of great importance for military applications, as they provide with an ability to deploy unmanned surveillance systems.

The sensor devices are now being manufactured in large quantities at a very low cost and in very low sizes. They can be installed and be stealthy in a hostile environment as they can be miniaturized into a cubic millimeter package (for example, Smart Dust [21]). The main objective of this application is to alert the military command and control unit of the occurrence of events observed in hostile regions, in advance. The system should be able to track the current position of an enemy vehicle (target) with required precision and accuracy for the successful detection and tracking. Also, the obtained information has to be sent to a remote base station within an acceptable latency.

7.1.1 Application requirements:

This system should be able to meet several application requirements discussed below, for successful implementation in practice:

- *Stealthiness.* It is very important for surveillance systems to have a minimum probability of being detected and intercepted. Sensors can be produced in miniature sizes and thus made hard to be detected physically, where as, RF signals can be intercepted easily. Therefore, in the absence of significant surveillance events, a zero communication exposure is desired.
- *Longevity.* A typical surveillance application lasts from a few days to several months. During the course of the mission, it may be impossible to replenish the power resources of the sensor devices because of the confidential nature of the mission and the inaccessibility of the hostile territories. Hence, it is inevitable to implement energy-aware

schemes which extend the lifetime of the sensor devices and make them available for the complete duration of the mission.

- *Effectiveness.* Effectiveness of a surveillance system is determined by the degree of precision in the location estimate, and the latency in reporting an observed event of interest to the base station. In general, it may be acceptable to receive a detection report within a couple of seconds and to obtain location estimation within a couple of feet.
- *Adjustable Sensitivity.* To accommodate different kinds of environments and security requirements, it is desired that the system has an adjustable sensitivity. A high degree of sensitivity is required to detect all potential targets even at expense of possible false alarms in critical missions. Otherwise, depending upon the requirements of the system and to avoid inappropriate actions and unnecessary power dissipation, the sensitivity of the system can be lowered resulting in a low probability of false alarms.

7.1.2 Description of a typical surveillance system:

A typical ground surveillance system is deployed with 70 tiny sensor devices, called MICA2 motes, in a grassy field along a 280 ft. long perimeter. Each mote is equipped with a 433 MHz Chipcon radio having 255 selectable transmission power settings. This radio is sufficient enough that allows all the motes deployed in the field to communicate with each other. In this prototypical deployment, a mote that is connected with a portable device, such as a laptop, is used as the base station, and serves as the destination of the surveillance information. This information can be visualized at the base station through the portable device. Each mote is equipped with a sensor board that includes acoustic, photo, and magnetic sensors on it. The different types of sensors used on a mote, make it possible for them to detect different types of targets.

This system is implemented on top of TinyOS, which is an event-driven computation model written in NesC language specifically for the motes platform, as discussed earlier. TinyOS provides the system with a set of important components such as basic communication protocols, scheduler, and hardware drivers, which provide low-level support for various application modules of the system.

The lower-level components of the surveillance system described here are time synchronization, localization, and routing, which form the basis for implementing the higher-level services, such as power management and aggregation. The key components of the surveillance application are time synchronization and localization, which provide the spatio-temporal correlation between the tracking reports sent by multiple motes. The time synchronization module synchronizes the local clocks of the motes with that of the base station, where as the localization module makes sure that each mote is aware of its location. In actual battlefield deployment of the wireless sensor networks, dynamic localization schemes are required to track the absolute geographic locations of the hostile enemy tanks. The routing component is responsible for establishing routes through which the motes exchange information with each other and with the base station.

In the surveillance system that is presented here, all the deployed motes are programmed to run the distributed application. This system also provides the motes with the ability to reprogram themselves dynamically with new configuration parameters such as sensitivity, which eliminates the need to download the application code into every mote present in the system each time its configuration is altered. Many experimental studies have been run on this system to study the various individual components of the system and how they contribute to energy-efficient tracking application of the system.

7.2 **Health Monitoring:**

Present health care systems which are structured to respond to crisis and managing illness face new challenges, notably, rapid rise in elderly population and increasing health care spending [22]. The recent technological advances in wireless communications, low-power integrated circuits, and sensors have enhanced the design and development of low-cost, intelligent, miniature, and light-weight physiological sensor nodes. These sensor nodes are capable of sensing, processing, and communicating one or more important signs, and can be used for health monitoring by easily integrating into wireless personal/body area networks (i.e. WPANs or WBANs).

Wearable health monitoring systems allow an individual to closely observe variations in his/her health signs and helps maintain an optimal health condition by providing an effective feedback. These systems can even track life threatening changes in health conditions and alert medical personnel, when integrated into a telemedical system. In addition, these systems can be used for continuous long-term monitoring, thus benefiting patients in their diagnostic procedure, their recovery from a surgical procedure or an acute event can be supervised, and can also be used to achieve optimal maintenance of a chronic condition. They can also help patients to monitor their health condition during stroke rehabilitation, brain trauma rehabilitation, or physical rehabilitation after knee or hip surgeries [22].

Traditionally, personal health monitoring systems, such as Holter monitors, were used to collect data only, and data processing and analysis were performed offline, thus making these systems impractical for monitoring continuously and early detection of medical disorders. They featured unwieldy wires between sensors and monitoring system, thus affecting the comfort level and patient’s activity yielding not so useful results, and were also not very affordable. But, recent developments in wireless networking, integration and miniaturization of physical sensors, radio interfaces, and microcontrollers on a single chip enabled a whole new generation of wireless sensor networks, leading to the development of wearable health monitoring devices, ranging from simple activity monitors, portable Holter monitors, and pulse monitors, to much sophisticated and expensive implantable sensors.

A Wearable Wireless Body/Personal Area Network (WWBAN) is one such implementation of a wireless sensor network, which is an integration of a number of physiological sensors that monitor vital signs, environmental sensors (temperature, light, and humidity), and a location sensor. The WWBAN can allow unobtrusive, long-term, ambulatory health monitoring that provides the current health status of its user and real-time updates of the patient's medical records using instantaneous feedback. For example, users can be warned about impeding medical conditions and catastrophic events by using intelligent heart monitors. The WWBAN promises to be a revolution in medical research through data mining of all collected information, when it is integrated into a broader telemedical system.

7.2.1 Requirements for Wireless Medical Sensors:

Wireless medical sensors must meet various requirements such as *reliability, security, wearability,* and *interoperability.*

- *Reliability.* Reliable communication is the most important requirement for medical applications relying on WWBANs. The communication requirements of different medical sensors vary according to the required sampling rates, from less than 1 Hz to 1000 Hz. A careful trade-off between computation and communication requirements is very important for optimal system design.
- *Security.* Overall system security is another major issue in these systems. Wireless medical sensors should meet necessary privacy requirements required by law and must also guarantee data integrity. These requirements can be met by using a relatively small number of nodes and short communication ranges in a typical WWBAN.
- *Wearability.* Wireless medical sensors must be small and lightweight to ensure user wearability and their level of comfort, and to obtain unobtrusive continuous health monitoring. The size and weight of batteries predominantly determine the size and weight of sensors, and thus their wearability.
- *Interoperability.* These sensors must allow the users to easily assemble a robust WWBAN depending on their state of health thus providing interoperability.

7.2.2 WWBAN Architecture:

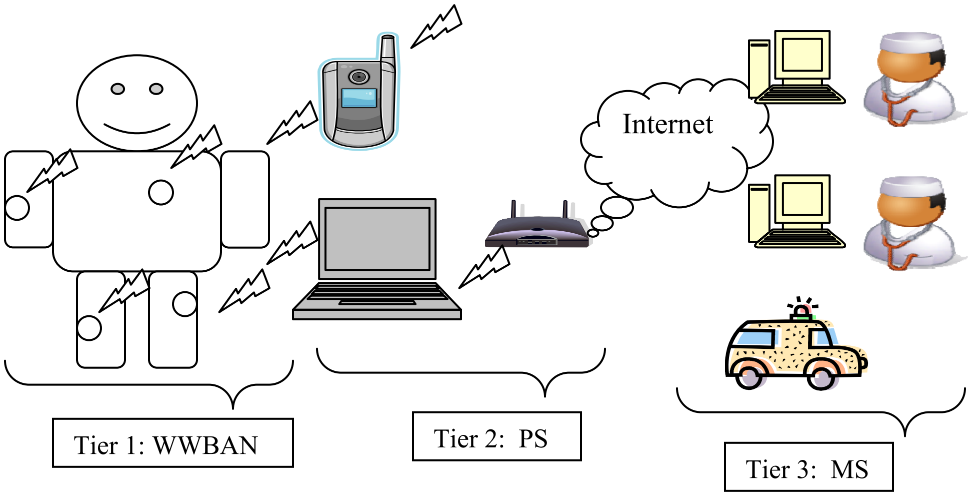

Figure 6: WWBAN integrated into a telemedical system for health monitoring.

As illustrated in figure 6, WWBANs form a pivotal component of a multi-tier telemedical system used for health monitoring [22]. Tier 1 includes a number of wireless medical sensor nodes integrated into a WWBAN. Each sensor can be an electrocardiogram (ECG) sensor used for monitoring heart activity, an electroencephalogram (EEG) sensor used for monitoring brain electrical activity, or a blood pressure sensor that monitors blood pressure. These sensor nodes can sense, sample, and process different physiological signals as discussed above. Tier 2 consists of a personal server (PS) application that runs on a personal computer, a cell phone, or a Personal Digital Assistant (PDA). The PS provides a transparent interface to the wireless medical sensors, to the user, and to the medical server. Tier 3 encompasses a medical server accessed via the Internet. It may also include other servers such as commercial health care providers, informal caregivers, and also emergency servers. Medical server is responsible for setting up the communication channel to the users' personal server, and gathering user reports and integrating the data into their medical record.

This system can be deployed at home, in workplace, or in hospitals. Wireless medical sensors that are attached to the user send the observed data to a PDA or a laptop, which forms a short-range wireless network using either IEEE 802.15.3/4 or 802.15.1 standards. The laptop or the PDA is equipped with a WLAN interface using IEEE 802.11a/b/g standards and sends the information to the personal or home server. The personal server establishes a secure communication channel to the medical server using the Internet, which sends regular updates to the medical record of the user.

7.3 Industrial Process Monitoring:

Industrial automation or process monitoring applications is a class of wireless sensor network applications aimed at eliminating the need for cabling and manual control in an industrial environment [23]. Sensors play a pivotal role in Industrial automation, by providing the essential link between the physical world and the control systems. The recent developments both in the hardware and software platforms for control systems are establishing new paradigms for automation in refineries, processing plants, and in factories.

The following are some of the driving factors for exploring wireless alternatives over wired connections in the industrial applications:

a) High failure rate of connectors and difficulty involved in their troubleshooting, accompanied with their high cost of installation.

b) The cost of wiring and maintaining wired sensor networks is very expensive.

c) In constricted and dangerous areas of industrial automation, running and maintaining cables come with various safety and regulatory issues.

d) There is a considerable amount of protocol incompatibility between control system hardware/software and different sensor types.

7.3.1 Network Architecture:

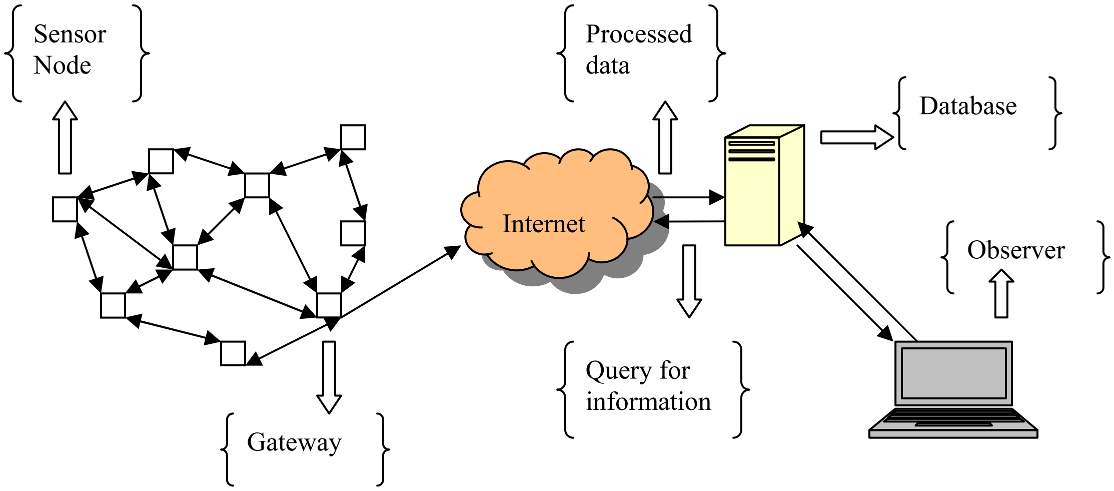

Figure 7: Network architecture for a typical industrial monitoring application.

As shown in the figure 7, the sensor nodes are installed in appropriate locations of the process control or machine, which use multi-hop routing and in-network aggregation to transmit data through the gateway to the Internet. This system allows remote industrial monitoring to be possible as the observer can query for information from the sensor network.

The wireless sensor networks used in industrial applications ensure that they function with maximum reliability and efficiency, by implementing flexible multi-hop networking that follows several network topologies. Mesh topology (as shown in figure a.) is the best choice for ensuring maximum reliability and flexibility, as every node in mesh topology is in direct communication with its immediate neighbors. Even if a single node fails to function for any reason (for example, due to the introduction of a strong RF interference), messages can be rerouted automatically using alternate paths.

On the other hand, sensor networks based on star topology (as shown in figure b.) cannot provide desired reliability when a physical or RF interference occurs. Networks based on this topology use a central access point that controls the communication between nodes, which provide an efficient single-hop (localized) communication [23]. When RF interference occurs, the network cannot recover until the source causing interference and blocking communication between the nodes and the access point is removed.

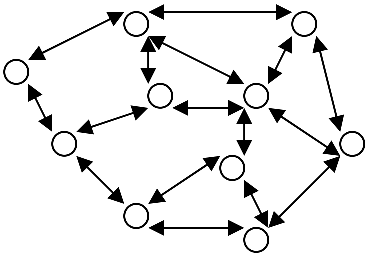

Figure a. Mesh topology.

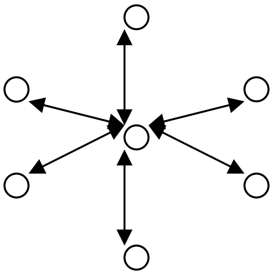

Figure b. Star topology.

7.3.2 Typical Scenarios:

a) Oil Refineries.

Oil refineries adopt a heat tracing mechanism to monitor continuously in extreme locations. Heat tracing method keeps pipes within a particular temperature range and safeguards them from freezing. Traditionally, these systems used wired connectivity for heat control and temperature sensing. Wired system provides local control but cannot provide global monitoring, and also the wiring costs can become tremendously expensive as the number of temperature sensing points increase and run into thousands. Hence wireless sensor networking systems are effective in such a scenario, as they can be easily deployed with low installation costs. They can avoid a system failure by identifying malfunctioning sensors using sophisticated peer-to-peer communication.

b) Inventory management in Chemical plants.

Inventory management plays a major role in the supply chain of a chemical plant. Traditional approaches for inventory management were based on dedicated hard-wired computing systems or on manual methods. Both these methods have their limitations in producing timely and accurate data in large chemical plants having a large number of distributed sensor points. Manual monitoring was limited from specific safety regulations. Sensor networks provide reliable and effective inventory data in real-time conditions, thus helping producers and their suppliers to schedule, replenish, and efficiently manage their inventory stocks, and also ensuring successful business operations without interruptions, by providing a constant supply of raw materials.

7.4 Environmental/ Habitat Monitoring:

Wireless sensor networks provide significant advantages in the field of habitat and environmental monitoring. The sensor devices can operate for prolonged periods in challenging, ecologically too sensitive, or inhospitable habitats for human presence [24]. One of the keys for studying natural phenomena is unobtrusive observation, and wireless sensor networks can be embedded unobtrusively in the natural environment without causing conspicuous landmarks that affect the behaviors of its inhabitants.

The duration of these experimental observations can be increased sufficiently by the advent of contemporary low-power microelectronics. Measurements can be obtained at spatial and temporal scales that are unattainable with sparsely deployed devices or human observers, by long-term unattended operation. Moreover, automation enhances the uniformity of measurements and information quality, reducing the costs of data collection at the same time, as compared with traditional human-centric methods.

7.4.1 Architecture:

The tiered network architecture of a typical habitat monitoring application is shown in figure 8. The lowest end consists of the sensor nodes which perform sensing, computation, and communication. They are deployed typically in sensor patches. Each sensor patch is equipped with a gateway, which transmits observed information from the sensor patch to a remotely located base station via the base station gateway through a transit network. The deployment, management, and debugging of the installation can be carried out with proper interaction between the on-site users and the base station and sensor nodes with the aid of mobile field tools.

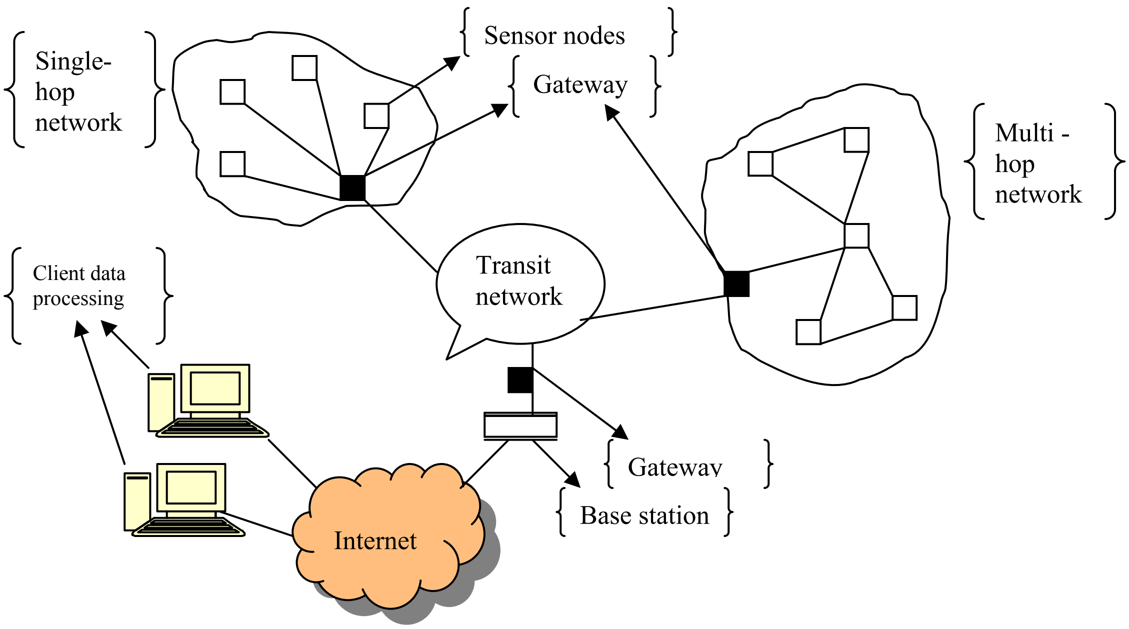

Figure 8: Tiered architecture of a typical habitat monitoring system.

The sensors nodes used are tiny devices running on batteries that are capable of application-specific sensing, bi-directional wireless communication, and general-purpose computation. Their life-times vary from months to years depending on their power consumption and duty cycles. This system uses analog and digital sensors to sample the surrounding environment, and to carry out basic signal processing such as filtering and thresholding. These sensor nodes communicate with other nodes in the system either directly or indirectly by routing the data through other nodes.

The base station provides the database services and the Internet connectivity, and also handles the network operation during disconnection from the Internet. Another important feature of a base station is it provides remote management facilities. The sensor network can consist of more than one sensor patches those are spanned by a common base station and transit network. The base station is connected via Internet to remotely based users allowing client data browsing and processing.

This particular sensor network system has been deployed on an off-shore breeding colony on Great Duck Island, Maine, during a study on the abundance and distribution of sea birds on the island. The monitoring system that was deployed on the island measured the occupancy of small nesting burrows located in the underground, and studied the role of micro-climatic factors in the birds' habitat selection.

7.5 Seismic Monitoring:

Wireless sensor networks can be used effectively in the pursuit of geophysical studies of volcanic activity. The study of active volcanoes typically involves a large number of arrays of sensors built to detect and measure infrasonic or low-frequency acoustic, and seismic signals [25]. A key feature of volcanic signals is that much of its data analysis focuses on the study of discrete events, such as tremor activity, eruptions, or earthquakes. The volcanic data-collection application poses a number of challenging computer science problems, since this application requires high data rates, high data fidelity, and less number of arrays with large separation between sensor nodes. This field requires further research and innovative engineering, since they present computer science problems when the current wireless sensor network nodes' capabilities meet with the above mentioned scientific requirements.

The typical volcanic data-collection station comprises of a set of heavy, bulky, high power components that are difficult to move and require car batteries for power. Equipment installation and maintenance often need vehicle or helicopter assistance in remote deployments. In spite of these limitations involved in the large-scale deployment of the networks with existing equipment, these experiments can help in achieving vital insights into inner activities of volcanoes.

7.5.1 Network Hardware:

A typical volcanic sensor network monitoring system that has been deployed on Reventador volcano in northern Ecuador is presented below in figure 9. The sensor array deployed on the volcano consisted of 16 nodes provided with seismo-acoustic sensors spread over 3 km.

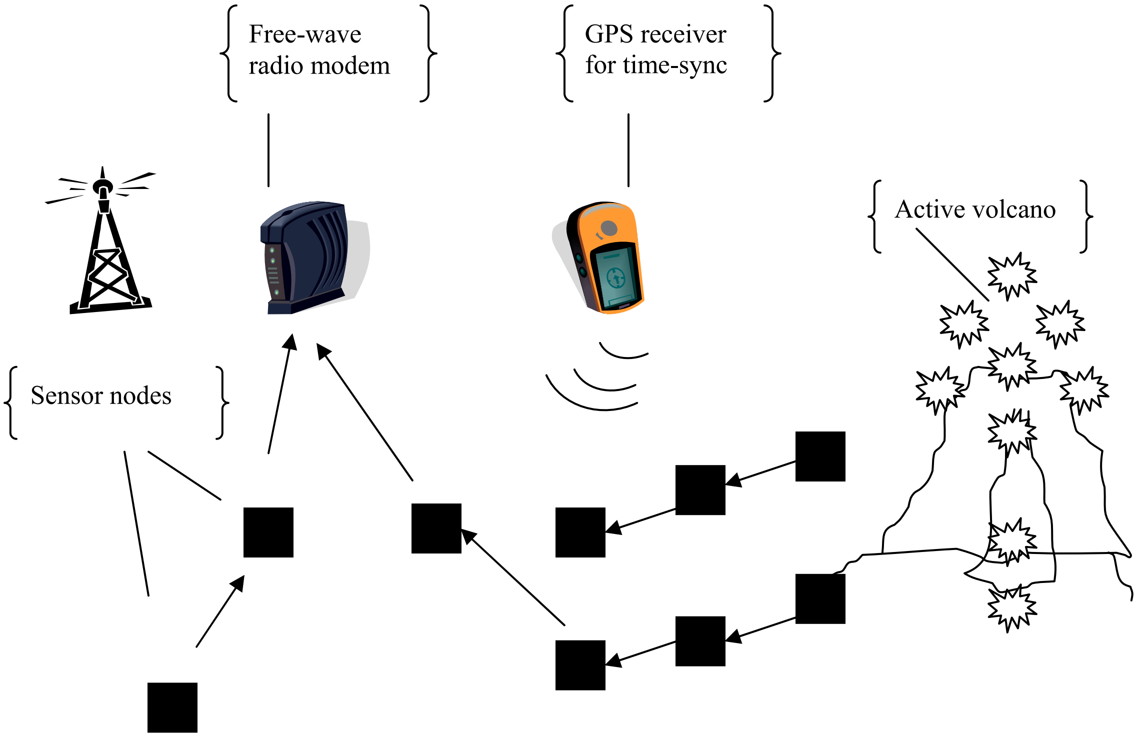

Figure 9: The volcano monitoring sensor network architecture.

The 16 stations deployed in the network are equipped with seismic and acoustic sensors. Each station comprised of a Moteiv TMote Sky wireless sensor network node [26], a microphone, a seismometer, an 8-dBi 2.4 GHz external omni-directional antenna, and a custom hardware interface board. The TMote Sky mode is very similar to the Berkeley Mote sensor node that is designed to run on the TinyOS operating system.

7.5.2 Network Operation:

Each sensor node samples two or four channels of acoustic and seismic data at a frequency of 100 Hz, storing the collected data in local flash memory. The sensor nodes also perform time synchronization and transmit status messages periodically. When a node records an event of interest, it sends a message to the laptop computer at the base station. The laptop at the base station initiates data collection that proceeds in a round-robin fashion, if an event is reported within a short time interval by enough number of nodes. The laptop uses a reliable data collection protocol and downloads around 30 to 60 seconds of data from each sensor node, thus ensuring that the system receives all the buffered data from the observed event. The sensor nodes then return to sampling and storing sensor data after the completion of data collection.

Study of volcanic activities requires large inter-node separations to obtain widely separated views of infrasonic and seismic signals as they propagate. The array configurations often consist of more than one possibly intersecting lines of sensors, which result in topologies that offer new challenges to sensor network design.

CONCLUSIONS

Wireless Sensor Networks hold a lot of promise in applications where sensing and gathering useful information in remote locations is required. It is an evolving field and offers scope for a lot of research and development. Their energy-constrained nature necessitates us to look at more possibilities of energy-efficient design and operation. We have reviewed various design factors and communication protocols implemented in sensor networks. In addition, we also discussed various wireless standards and applications of wireless sensor networks. Further work is necessary in the areas of media access control, security and privacy of sensor networks.

REFERENCES

[1] "Wireless Sensor Network", In *Wikipedia, the Free Encyclopedia,* June 2007, accessed from: http://en.wikipedia.org/wiki/Sensor_networks

[2] Chee-Yee Chong, and S.P. Kumar, "Sensor networks: evolution, opportunities, and challenges", *Proceedings of the IEEE,* vol. 91, no. 8, Aug. 2003, pp. 1247-1256.

[3] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine,* vol. 40, no. 8, Aug. 2002, pp. 102-114.

[4] G. J. Pottie and W. J. Kaiser, "Wireless Integrated Network Sensors," *Communications of the ACM,* vol. 43, no. 5, May 2000, pp. 551-558.

[5] A. Woo, and D. Culler, "A Transmission Control Scheme for Media Access in Sensor Networks," *Proceedings of the ACM MobiCom '01*, Rome, Italy, July 2001, pp.221–235.

[6] E. Shih et al., "Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks," *Proceedings of the ACM MobiCom '01*, Rome, Italy, July 2001, pp. 272–286.

[7] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," *Proceedings of the ACM MobiCom '99*, Washington, DC, 1999, pp. 271–278.

[8] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", *Proceedings of the ACM MobiCom '99,* Seattle, Washington, Aug. 1999, pp. 174-185.

[9] T. He, J.A. Stankovic, T.F. Abdelzaher, and C. Lu, "A Spatiotemporal Communication Protocol for Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems,* vol. 16, no. 10, Oct. 2005, pp. 995-1006.

[10] D. Brinza, and A. Zelikovsky, "DEEPS: Deterministic Energy-Efficient Protocol for Sensor networks", *Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2006*, Jun. 2006, pp. 261-266.

[11] http://www.tinyos.net/.

[12] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, Eric Brewer, and David Culler, "TinyOS: An Operating System for Sensor Networks", accessed from: http://www.dbis.ethz.ch/education/ss2007/tatbul/hotdms/papers/tinyos_chapter.pdf

[13] Chih-Chieh Han, Ram Kumar, Roy Shea, Eddie Kohler, and Mani Srivastava, “A Dynamic Operating System for Sensor nodes”, accessed from: http://www.cs.ucla.edu/~kohler/pubs/han05dynamic.pdf

[14] http://www.sics.se/contiki/about-contiki.html.

[15] “Introduction to Sensors –Engineers’ handbook”, accessed from: http://www.engineershandbook.com/Components/sensors.htm

[16] http://www.ieee802.org/15/pub/TG4.html.

[17] http://en.wikipedia.org/wiki/IEEE_802.15.4.

[18] http://wireless.industrial-networking.com/articles/articledisplay.asp?id=1661.

[19] http://www.hartcomm2.org/hcf/press/pr2007/hart7released.html.

[20] Tian He, Sudha Krishnamurthy, John A. Stankovic, Tarek Abdelzaher, Liqian Luo, Radu Stoleru, Ting Yan, and Lin Gu, “Energy-Efficient Surveillance System Using Wireless Sensor Networks”, accessed from : http://www.cs.virginia.edu/papers/tracking-mobisys04.pdf

[21] “Smart Dust”, accessed from: http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/SmartDust/index.html

[22] Aleksandar Milenkovic, Chris Otto, and Emil Jovanov, “Wireless Sensor Networks for Personal Health Monitoring: Issues and an Implementation”, accessed from: http://www.ece.uah.edu/~jovanov/papers/milenkovic_compcomm06.pdf

[23] Xingfa Shen, Zhi Wang, and Youxian Sun, “Wireless Sensor Networks for Industrial Applications”, *Proceedings of the 5th World Congress on Intelligent Control and Automation,* vol. 4, Jun. 2004, pp. 3636-3640.

[24] Robert Szewczyk, Alan Mainwaring, Joseph Polastre, John Anderson, and David Culler, "An Analysis of a Large Scale Habitat Monitoring Application", accessed from: http://www.polastre.com/papers/sensys04-gdi.pdf

[25] Geoffrey Werner-Allen, Konrad Lorincz, Matt Welsh, Omar Marcillo, Jeff Johnson, Mario Ruiz, and Jonathan Lees, "Deploying a Wireless Sensor Network on an Active Volcano", published by the *IEEE Internet Computing,* vol. 10, no. 2, March-April 2006, pp. 18-25.

[26] http://www.moteiv.com.

[27] http://www.cs.umass.edu/~gmathur/misc/tinyos-sos.pdf.

[28] G. Hoblos, M. Staroswiecki, and A. Aitouche, "Optimal Design of Fault Tolerant Sensor Networks", *IEEE International Conference on Control Applications*, Anchorage, AK, Sept. 2000, pp. 467–72.