PATTERNS FOR WIRELESS SENSOR NETWORKS

by

Anupama Sahu

A Thesis Submitted to the Faculty of

The College of Engineering and Computer Science

in Partial Fulfillment of the Requirements for the Degree of

Master of Science

Florida Atlantic University

Boca Raton, Florida

December, 2010

PATTERNS FOR WIRELESS SENSOR NETWORKS

by

Anupama Sahu

This thesis was prepared under the direction of the candidate's thesis advisor, Dr. Mihaela Cardei, and co-advisor Dr. Eduardo B. Fernandez, Department of Computer & Electrical Engineering and Computer Science, and has been approved by the members of her supervisory committee. It was submitted to the faculty of the College of Engineering and Computer Science and was accepted in partial fulfillment of the requirement for the degree of Master of Science.

SUPERVISORY COMMITTEE:

Mihaela Cardei, Ph.D.
Thesis Advisor

Eduardo B. Fernandez, Ph.D.
Thesis Co-Advisor

Ionut Cardei, Ph.D.

Borko Furht, Ph.D.
Chair, Department of Computer and
Electrical Engineering and Computer Science

Karl K. Stevens, Ph.D., P.E.
Dean, College of Engineering and Computer Science

Barry T. Rosson, Ph.D.
Dean, Graduate College

November 16, 2010
Date

ACKNOWLEDGEMENTS

It is a pleasure to thank all those who have been instrumental in the successful completion of my thesis work. I am indebted to my advisor Dr. Mihaela Cardei for her continued support, guidance and mentoring. She is also my role model and I will always strive to be as hardworking and as successful as her. I am grateful to my thesis co-advisor Dr. Eduardo B. Fernandez whose encouragement and guidance from the initial to the final level enabled me to develop an understanding of the subject. It was from him that I derived the confidence to complete my work in time. I express my thanks to Dr. Ionut Cardei for being highly involved with my research and for his advice. I also wish to thank Mrs. Jean Mangiaracina for her guidance through administrative needs. I am thankful to Motorola and NSF for supporting my studies.

I wish to express my heartfelt thanks to my patient and understanding husband Dr. Ravi Kadambala, for his help and support throughout the masters program. Last, but not the least I want to thank my parents, for their blessings, continued encouragement and moral support without which this task would not have been a success.

ABSTRACT

Author: Anupama Sahu

Title: Patterns for Wireless Sensor Networks

Institution: Florida Atlantic University

Thesis Advisor: Dr. Mihaela Cardei

Thesis Co-Advisor: Dr. Eduardo B. Fernandez

Degree: Master of Science

Year: 2010

Sensors are shaping many activities in our society with an endless array of potential applications in military, civilian, and medical application. They support different real world applications ranging from common household appliances to complex systems. Technological advancement has enabled sensors to be used in medical applications, wherein they are deployed to monitor patients and assist disabled patients. Sensors have been invaluable in saving lives, be it a soldier's life in a remote battlefield or a civilian's life in a disaster area or natural calamities. In every application the sensors are deployed in a pre-defined manner to perform a specific function. Understanding the basic structure of a sensor node is essential as this would be helpful in using the sensors in devices and environments that have not been explored.

In this research, patterns are used to present a more abstract view of the structure and architecture of sensor nodes and wireless sensor networks. This would help an application designer to choose from different types of sensor nodes and sensor network architectures for applications such as robotic landmine detection or remote patient monitoring systems. Moreover, it would also help the network designer to reuse, combine or modify the architectures to suit more complex needs. More importantly, they can be integrated with complete IT applications.

One of the important applications of wireless sensor networks in the medical field is a remote patient monitoring system. In this work, patterns were developed to describe the architecture of patient monitoring system. This pattern describes how to connect sensor nodes and other wireless devices with each other to form a network that aims to monitor the vital signs of a person and report it to a central system. This central system could be accessed by the patient's healthcare provider for treatment purposes.

This system shows one of the most important applications of sensors and it is an application which needs to be integrated with medical records and the use of patterns makes this integration much simpler.

PATTERNS FOR WIRELESS SENSOR NETWORKS

LIST OF FIGURES

1 INTRODUCTION

1.1 Motivation

Sensors are shaping many activities in our society with an endless array of potential applications in military, civilian, and healthcare. They are found as standalone units in household appliances like microwave ovens, air conditioning units, motion detecting systems, and smart phones. In applications such as fire alarm systems, robotic landmine detection, battlefield surveillance, target tracking, environmental monitoring, wildfire detection, air-traffic control, industrial automation, and traffic regulation [Cho03] [Gov99], sensor nodes are not used individually, but are part of a larger and more complex system. In order to monitor these kinds of systems, a group of sensors are deployed. Networked sensors technology is a key technology for the future. Hence it is important to know the structure of the nodes used in these environments or in similar situations, either as standalone units or as parts of networks. A sensor network is composed of a large number of sensor nodes that are massively deployed either inside the phenomenon or very close to it. In every application different types of sensor nodes are used having different sensing capabilities like pressure, humidity, light, acoustic, temperature, and various others. They could have different transmission capabilities-short range or long range, different battery life and other specific features. With so many different types of sensor nodes available in the market, it becomes difficult to choose the right type of sensor nodes for an application.

For some application scenarios, the network could be wired but for other applications, however the need to wire together all the sensor nodes could give rise to considerable obstacle to success, so wireless sensor network is an inevitable requirement [Kar05]. A Wireless Sensor Network could be described as a deployment of large number of small, inexpensive, self-powered devices that can sense, compute, and communicate wirelessly with other devices for the purpose of gathering local information to make decisions about a physical environment. It encompasses three main objectives namely information sensing, computation, and communication wherein the collected information has to reach the right place where it is needed in a timely manner and also provide a precise picture of the real world. Although the flexibility of wireless sensor networks is commendable, it also poses a challenging research and engineering problem because there is no single set of requirements that clearly classifies all kinds of wireless sensor networks. In such a scenario, it might be better to come up with an abstract view of a wireless sensor network that will only focus on the broader aspects of the network. The abstract view can then be modified to suit more complex networks involving millions of nodes or downgraded to suit a simple application. This research uses patterns to describe the abstract view of the sensor network. A pattern is an encapsulated solution to a recurrent problem and it is described using a template. Patterns capture the knowledge and experience of designers so they can be used by less experienced designers in solving some problem [Bus96].

Wireless sensor networks have a wide variety of applications. Technological advances have led to the development of wearable sensor nodes that are widely used in health monitoring applications for example pulse oximeter for monitoring the pulse rate, electrocardiograph (EKG) for measuring the activity of the heart, motion analysis sensor nodes for monitoring the movement of a person and various others[Ott06], [Jaf05]. Wireless healthcare applications are highly beneficial because they can be used in remote patient monitoring systems and can also be used for patients who have to be closely monitored and have a lot of wired sensor nodes surrounding their body. In a healthcare application the patient can wear sensor nodes on his body and these nodes would measure the patient's vital signs and transmit it to a central system creating a body area network. Now this network would coordinate with other network elements to transmit the data over long distance. Several architectures for health monitoring have been proposed so far [Shn05], and this research uses patterns to describe the abstract view of these architectures.

1.2 General Problem

There are physical environments that need to be monitored for the presence of living beings or for recording some physical attributes or for detecting any abnormal conditions. These environments could be inside buildings or could be external environments. For example, a battlefield may be monitored for detecting the presence of enemy soldiers and tanks, a wildlife sanctuary may be monitored for recording the population of migratory birds, and industrial plants could be monitored for detecting fire accidents [Cho03]. There are certain situations where a person's vital signs need to be monitored in order to help him recover from a medical condition or to detect any abnormal health condition. The monitoring could take place in a hospital environment or outside. For example, patients can be monitored in a hospital ward in order to detect any abnormal health condition. Without a way to sense some attributes of the physical environment these situations can go undetected with probably bad consequences. Human monitoring is not convenient or efficient either. In other words life- critical situations may go unnoticed if nobody is watching for them.

As discussed earlier, an application can use same or different type of sensors. For example, a sensor node used in battlefield surveillance would be different than a sensor node used in medical applications. The basic structure of both the nodes would be the same but there would be subtle difference between the two depending upon the application they are used for. Again every network has some objectives that the architecture should satisfy. For example, the sensor network in a battlefield has to have wide reach, fast, and reliable communication and can withstand node failure. A sensor network used for patient monitoring does not require a wide reach but should still have fast and reliable communication. Moreover the patient monitoring system cannot afford node failure because it is a life critical situation. Similarly sensor network used for environmental monitoring should have an extended battery life. Sensor networks deployed for detecting fires should have fast and reliable communication.

Thus we see that in every application, the sensor nodes are deployed in a pre-defined manner to perform a specific function appropriate for that application. Since no two applications have the same objective, the architecture of their wireless sensor networks would be different although both the networks would still follow the basic wireless sensor network structure. The number of sensor nodes used in the application would also have a direct affect on the structure of the network, it could either be a simple network or a layered network. Two different problems have to be considered here – how to select the right kind of sensor node and the right kind of network architecture for any application. It is also essential to know if certain aspects of existing network architecture can be modified to suit another one. For example the communication method of sensor nodes would be different in a battle field as compared to a patient monitoring system. So whether to use just one communication method in both of the networks by modifying them accordingly is another question to be considered.

1.3 Research Objectives

It is essential to understand the structure of a sensor node and a wireless sensor network as this is helpful in using them in different types of devices and different kinds of application environments. For a specific application, the sensor nodes have to be equipped with the right type of sensors. The first objective is to describe the structure of the nodes used in these environments or in similar situations, either as standalone units or as parts of networks. Every application has some specific objectives that the sensor network architecture should satisfy such as wider coverage, fast, and reliable communication, extended battery life and various others. The second objective is to design the architecture or manner in which the sensor nodes are deployed in order to accomplish a specific function appropriate for that application. Sensor network architectures should be extensible so that they can be modified to suit different applications. The third objective is to find out how the basic network architecture can be modified to support an application in the healthcare domain.

1.4 Contributions

This research develops patterns to provide a better understanding of the structure of a sensor node and of the architecture of a wireless sensor network. We define our patterns using the POSA template [Bus96].

Objective 1: Describe the structure of a sensor node

Approach: The architecture and components of a sensor node were studied and a pattern was developed that describes their structure and operations. This pattern also mentions about additional components that could be used to design a specific type of sensor node having a specific capability.

Objective 2: Describe the architecture of a wireless sensor network.

Approach: Different components of a wireless sensor network were studied and a second pattern was developed to present an abstract view of the structure and general architecture of wireless sensor networks. This pattern describes the organization of sensor nodes and other wireless devices and the way they are connected with each other to achieve some objective, e.g. signal reach, performance, security, reliability, or other quality factors.

Objective 3: Describe a network architecture that supports a healthcare application.

Approach: A remote patient monitoring system was studied and a third pattern was developed to present an abstract view of the structure and general architecture of the patient monitoring system. This pattern describes how to connect sensor nodes, medical devices and other wireless devices with each other to form a network for monitoring of vital signs.

Figure 1.1 shows how the three patterns relate to each other. The developed patterns would provide an overall idea and implementation details sufficient to design any new application involving sensor nodes. With the help of this approach, new sensor applications could be designed more conveniently as the patterns would serve as a reference guide for selecting different sensor nodes, network architectures and implementation platforms for any application. Moreover it would also widen the scope of reusing, combining or modifying the architectures to suit more complex needs.

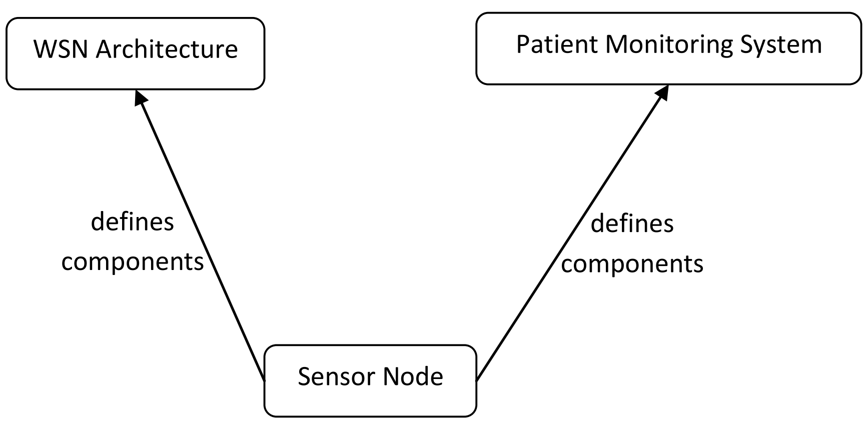

Figure 1.1 Pattern Diagram for Wireless Sensor Network

1.5 Organization of the Thesis

This thesis is presented in 7 chapters. Chapter 1 presents motivation, general problem, research objectives, and contribution. Chapter 2 presents the background information that will be useful for the reader to understand this work in a better way. Chapter 3 describes the pattern for a sensor node. Chapter 4 describes the pattern for sensor network architecture. Chapter 5 describes the pattern for a remote patient monitoring system. Chapter 6 presents some related work and discussion in this area. Chapter 7 presents some conclusions and possible future work.

2 BACKGROUND

In order to have a better understanding of this work, this chapter describes some basic concepts of Wireless Sensor Networks (WSNs) such as their characteristics, architecture, operations and applications. This work makes use of patterns which are also defined and described in this chapter.

2.1 Wireless Sensor Networks

Wireless sensor networks are one of the most important technologies for the 21st century. Technological developments in wireless communications and electronics have enabled the development of low cost, multifunctional sensor nodes that are not only small in size but also communicate efficiently over short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, constitute wireless sensor networks. Wireless sensor networks represent a significant improvement over traditional wired sensor network in terms of cost, quality, mobility and maintainability. Research in wireless sensor network spans a period of three decades and includes two important programs of the Defense Advanced Research Projects Agency (DARPA) --- the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SensIT) programs. In other words it can be said that military applications have cradled the growth and progress of wireless sensor networks. Wireless sensor network consists of individual sensor nodes that are capable of interacting with the environment by sensing physical parameters and collaborating with other nodes by using wireless communication to route information to the proper destination. Sensor nodes have a processor, so instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

2.1.1 Characteristics of WSNs

Some of the characteristics of a wireless sensor network are [Aky02]:

- WSNs are application specific, thus sensors nodes are equipped with sensors accordingly. Some applications (e.g. building monitoring) require a smaller number of sensors that can be placed individually. Others (e.g. surveillance of a battlefield) require a large number of sensors (e.g. thousands or even millions) that will be deployed ad-hoc. The IrisNet (Internet-scale Resource-Intensive Sensor Network Services) project [Gib03] at Intel Research is envisioning a worldwide sensor web of millions of widely distributed, heterogeneous sensors.
- These networks have random deployment as compared to deterministic deployment
- These networks may have a dynamic topology due to node mobility, node failure and node's active and idle state.
- Due to the involvement of large number of nodes, the network mainly uses a broadcast communication paradigm.
- Sensor nodes have limited resources: sensor nodes have finite battery resources, low CPU speed , little memory, and small transmission range. For example, the Crossbow MICAz mote [Cro10] operates on the 2.4GHz ISM band, uses two AA batteries, and

has an ATmega 128L processor at 8 MHz, 4 K bytes RAM, and a transmission range up to 30 m (indoor) /100 m (outdoor).

- These networks may be autonomous in nature which means they may possess self-configuring, self-calibrating, self-identifying, and self-reorganizing capability.
- These networks are highly scalable.
- An important issue in WSNs is network lifetime. Sometimes is impossible or infeasible to recharge the sensors. Therefore the algorithms and protocols designed must be energy-efficient to prolong network lifetime.
- WSN security is another critical and challenging issue due to the resource constrained nature of sensor nodes. A secure communication protocol in WSNs must ensure data secrecy, authentication, and replay protection [Luk07]. Various security aspects have been studied, focusing on threats and possible countermeasures [Per04].
- For applications requiring a large number of sensor nodes, the protocols designed must be scalable and localized.
- In general WSNs have a dynamic topology. This is due to the fact that some of the sensors will die in time due to physical damage or energy depletion, and also because some of the sensors may go in the sleep mode to save energy.
- Quality of service requirements are different than those of the traditional networks. They may include concepts like reliable detection of events and amount and quality of information that can be extracted at given sinks about monitored objects or area [Kar05].

2.1.2 Architecture of WSNs

As described earlier, a WSN consists of a number of sensor nodes which are known to have two roles: to sense the physical environment and to participate in data forwarding to a sink, from where data is retrieved by users. A user can collect the data from the sink by connecting a laptop or personal digital assistant or by downloading the data over another network. There are various types of sensor network architectures [Car08].

- **Basic Architecture:** This includes one sink, many sensors and data is collected at the sink as shown in Figure 2.1.

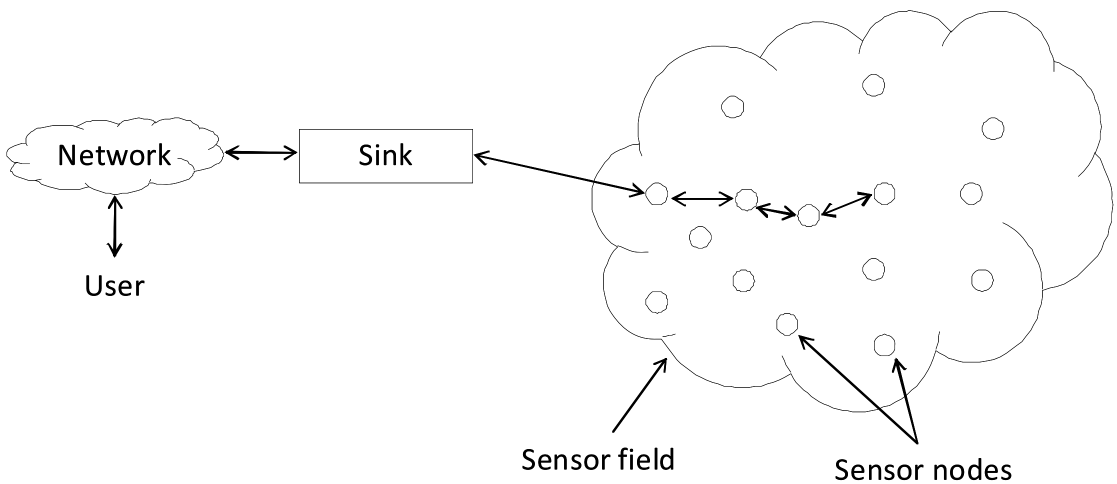

Figure 2.1 Basic Architecture

- **Clustered Architecture:** This includes one or more sinks and sensor nodes are organized into clusters, and each cluster has a cluster head that controls the data collection within the cluster. Data is transmitted from sensor nodes to cluster heads and from cluster heads to the sink as shown in Figure 2.2. The cluster heads alternate in time.

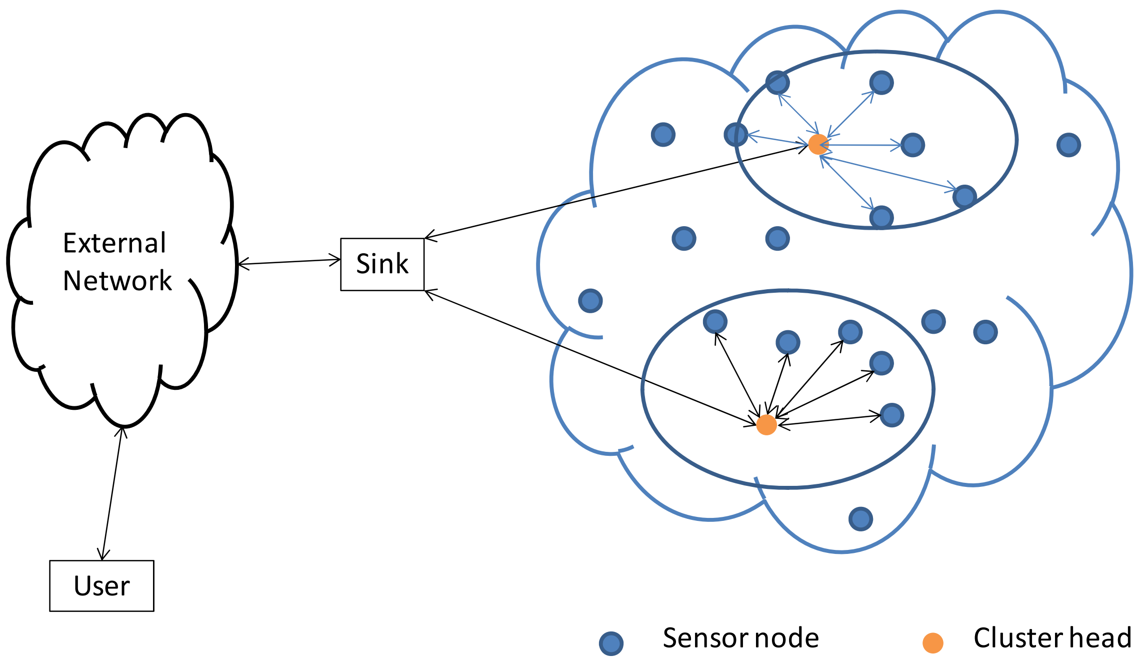

Figure 2.2 Clustered Architecture

- **Heterogeneous Architecture:** This includes one or more sinks, many heterogeneous sensor nodes capable of measuring different types of attributes, super nodes which are more resource-rich than the sensor nodes (they can have for example more energy resources), larger transmission range, higher data rate, etc. Nodes may be connected to other nodes and all are connected to the sinks as shown in Figure 2.3.

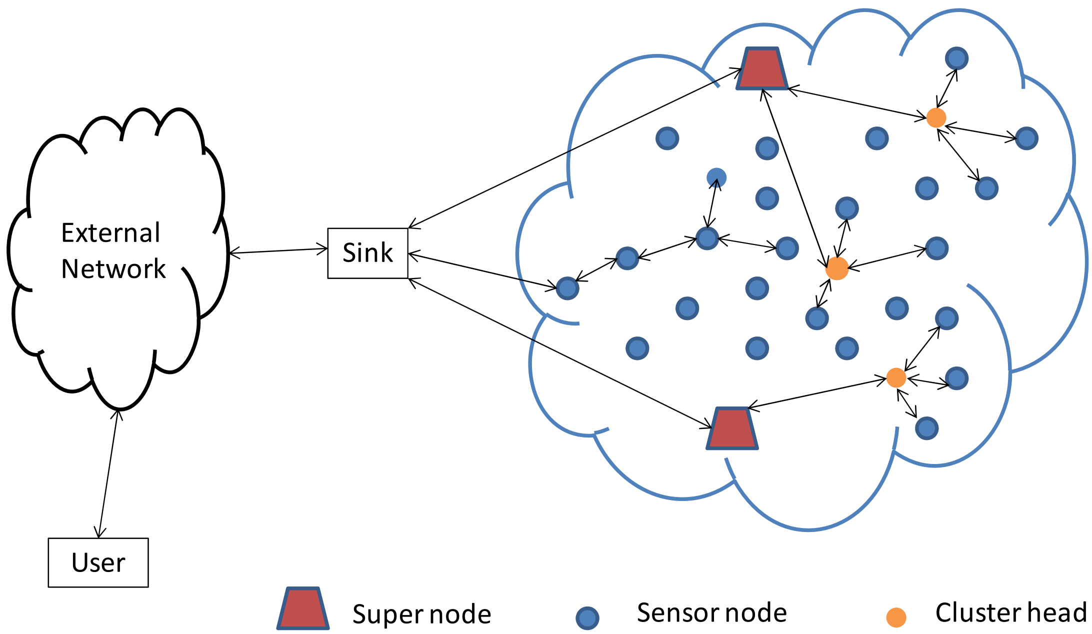

Figure 2.3 Heterogeneous Architecture

- **Wireless sensor and actor (actuator) networks (WSAN):** This includes one or more sinks, sensor nodes that gather information about the physical world, and actuators that take decisions and then perform appropriate actions on the environment. Examples are water sprinklers in buildings and agricultural lands. A diagrammatic representation of this architecture is shown in Figure 2.4

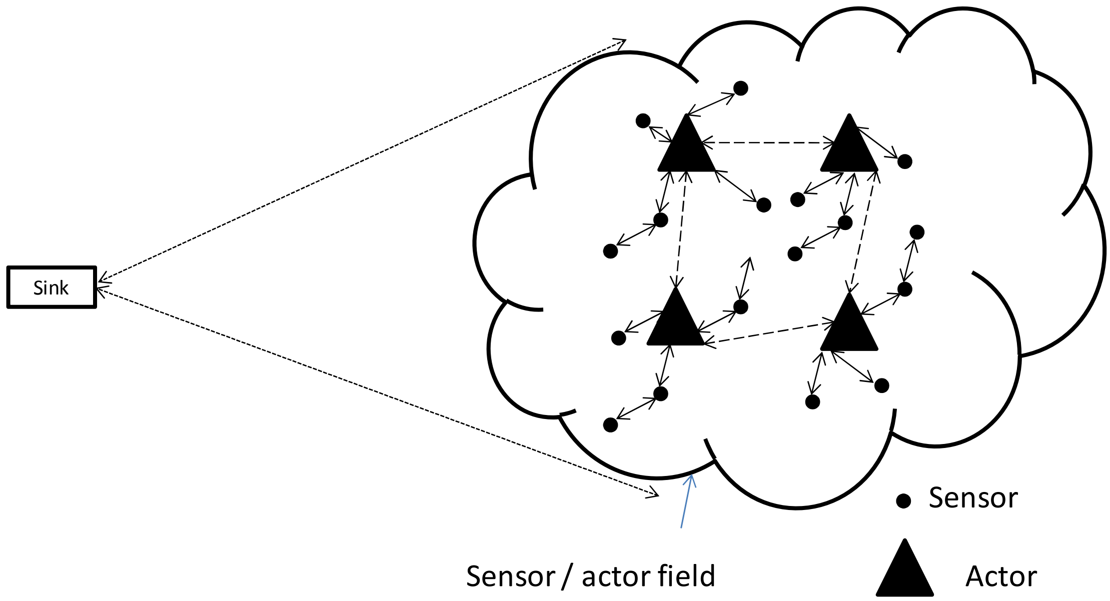

Figure 2.4 Wireless Sensor and Actor (actuator) Networks (WSAN)

2.1.3 Activities performed by a WSN:

Various activities can be performed by sensor networks such as [Kar05]:

- **Event Detection:** Sensor nodes would report to the sink(s) once they have detected an occurrence of a specific event. Simple events can be detected locally by a single sensor node such as exceeding a temperature threshold. Other events could be more complex and would require the collaboration of nearby or even remote sensors to decide if a composite event has occurred. For example, fire detection in a building. In order to detect fire the sensor node must be able to detect high temperature and smoke.
- **Periodic Measurements:** Sensor nodes can be made to report periodically measured values at certain time intervals to the sink.

- **Function Approximation and edge detection:** Sensor nodes can be made to report average and mean values by processing the samples collected at each individual node. Sensor nodes can be tasked to find out areas or points of the same given value. An example is to find the isothermal points in a forest fire application to detect the border of actual fire. This can be generalized to finding "edges" in such functions or to sending messages along the boundaries of patterns in both and time [Kar05].
- **Tracking:** The source of an event can be mobile (e.g. approach of enemy tanks in a battlefield). The sensor nodes can be made to report updates on the event source's position, with estimates about speed, distance and direction. But in order to do that, the sensor nodes have to co-operate before updates can be reported to the sink.

2.1.4 Operations in WSNs

WSNs have various operations to perform, some of which are basic while others are application specific. Some of the basic operations are:

- **Data/interest dissemination:** In this operation, the sinks broadcast the interest to or query the sensors, or sensor nodes broadcast an advertisement for the available data and wait for request from interested nodes. Flooding, gossiping [Hed88], rumor routing [Bra02], directed diffusion [Int00] are some of the available methods.
- **Data gathering:** In this operation, the sink is fixed and located far from the sensor nodes. So data is gathered from each sensor node and forwarded to the sink. Data reporting could be periodic or event based and it could be organized in rounds. Low-Energy Adaptive Clustering Hierarchy (LEACH) [Hei00] is a clustering based data gathering protocol. Power-Efficient Gathering in Sensor Information Systems

(PEGASIS) [Lin02] is a proactive data gathering protocol and directed diffusion is a reactive routing technique which means that routes are established on-demand [Int00]

- **Data aggregation / data fusion:** In this operation data coming from multiple sensor nodes is aggregated or combined into a set of meaningful information, if they are related to the same attribute of the phenomenon. This is good approach to solve implosion (duplicate message sent to the same node) and overlap (close nodes sense and report the same parameters) problems.
- **Data storage:** This operation deals with various data storage options such as external storage in which a centralized server, outside the sensor network is used for collecting and storing sensed data. The second type of storage is the data-centric storage in which the data is stored at nodes in the network, depending on the event type. The third type of storage is local storage (e.g. directed diffusion) in which a source sends data to the sink only when the sink has queried the data. The last type of storage is the index-based data storage in which, information about storing nodes is maintained at index nodes, based on the event type.

2.1.5 Applications of WSNs

WSNs support a wide variety of real world applications due to their flexible nature. Depending upon the sensing, computational and communication capabilities, many different types of applications can be developed with very different type of nodes or even use different type of nodes within a single application. Some of the applications are as follows.

- **Disaster Relief:** A striking example of this is wildfire detection. Sensor nodes used in this application are equipped with thermometers and are deployed from airplanes on the area to be monitored. They can detect their own location relative to each other in absolute co-ordinates. The nodes collectively produce a “temperature map” of the area or determine the perimeter of high temperature areas that can be accessed externally by a fire fighter using a personal digital assistant. In case of natural calamity, WSNs help locate survivors, find safe evacuation paths as well as alert the nearest emergency response team. In avalanche rescue operations, avalanche rescue beacons continuously transmit signals that rescuers can use to locate the wearer in time of emergency. These are used by skiers and other mountaineers in avalanche prone areas [Kar05].
- **Military Applications:** Sensor networks are used in battlefield surveillance and can be used to replace guards and sentries around defensive borders, keeping soldiers away from harm. In addition to such defensive applications, deployed wireless sensor networks can be used to detect and recognize targets for potential attack. They may be equipped with acoustic microphones, seismic vibration sensors, magnetic sensors, radar, and other sensor nodes.
- **Environment control and monitoring:** Wireless sensor networks may also be used for low-power sensing of environmental contaminants such as mercury or other chemical pollutants in a garbage dump site [Bri88]. It could be used to monitor ground moisture because irrigation is expensive, so it is important to know which fields have received rain, so that irrigation may be omitted, and which fields have not and must be irrigated. Ranchers may use wireless sensor networks to determine the

location of animals within the ranch and, with sensors placed on each animal, they can also determine the need for treatments to prevent parasites. It can be used in ocean bottom surveillance for understanding erosion process for construction of off shore wind farms and to monitor seismic and animal activity on the ocean bed. The small size, wire free operation and autonomous nature of WSNs allow for close observation of plants and animals.

- **Intelligent buildings:** There is a lot of expense involved in the installation of lights in a large building and the control of these lights — where the wired switches will be, which lights will be turned on and off together, dimming of the lights, etc. A flexible wireless system can employ a handheld controller that can be programmed to control a large number of lights. Buildings waste large amounts of energy by inefficient heating, ventilating, and air conditioning (HVAC) and WSNs can help prevent this [Kar05].
- **Facility management:** In keyless entry applications, people wear badges and WSN checks which person is allowed to enter which areas of a facility. Sensor networks could also have video, acoustic, and other sensors deployed around critical buildings and facilities like museums and bank. They are also used in fire alarm systems in buildings. They can support multiple sensors relevant to industrial security, including passive infrared, magnetic door opening, smoke, and broken glass sensors, and sensors for direct human intervention such as the "panic button" sensor requesting immediate assistance [Kar05].
- **Machine surveillance and preventive maintenance:** In this application, sensor nodes are fixed at difficult to reach areas in machines such as robotics and axle of

trains so that they can detect vibration patterns and indicate whenever there is a need for maintenance. The main advantage of using WSN in this application is that --- it has a cable free operation and no additional maintenance problem in itself.

- **Industrial sensing and monitoring:** The control room of an industrial facility has indicators and displays that describe the state of the plant such as the state of valves, the condition of equipment, the temperature and pressure of stored materials, as well as input devices that control actuators in the physical plant such as valves and heaters. The sensors describing the state of the physical plant, their displays in the control room, the control input devices, and the actuators in the plant are often all relatively inexpensive when compared with the cost of the cable that must be used to communicate between the devices in a wired installation. Wireless sensor networks deploy sensor nodes to detect the presence of noxious, poisonous, or otherwise dangerous materials, providing early detection and identification of leaks or spills of chemicals or biological agents before serious damage can result and before the material can reach the public. Wireless networks may be autonomous and make use of distributed routing algorithms and have multiple routing paths, so they are resilient in case of accidents and provide critical plant status information under very difficult conditions.
- **Precision agriculture:** The network can be fitted with chemical and biological sensors and the data thus provided by such a network gives the farmer a graphical view of soil moisture, temperature, and received sunshine. The system also lets the farmer know when there is a need for pesticides, herbicides, and fertilizers. This type of application is especially important in vineyards, where subtle environmental

changes may have large effects on the value of the crop and how it is processed [Kar05].

- **Logistics:** In this application, goods are equipped with sensor nodes that enable tracking of these objects during transportation or even facilitate inventory tracking in stores or warehouses. Items have attached tags, stick-on sensors attached to walls or embedded in floors and ceilings to track the location history and use of items.
- **Traffic Control:** Intersections use sensors to detect vehicles and control traffic lights. Sensor nodes can be embedded in streets and roadsides to gather information about traffic conditions. Senor nodes are attached to vehicles and during movement, vehicles can exchange information on traffic jams, speed and density of traffic (VANET).
- **Healthcare:** Applications in this field include post operative and intensive care, in-home monitoring, doctor and patient tracking in the hospital, monitoring elderly people in assisted living centers and various others [Fer10]. Wireless sensor networks can monitor vital signs for example, tracking the pulse and respiration rate via wearable sensors and sending the information to a personal computer for later analysis [Ber05]. WSNs are also used in in-home health monitoring, for taking care of elderly people or for personal weight management [Pär00]. The patient’s weight may be wirelessly sent to a personal computer for storage. Some other applications are daily blood sugar monitoring and recording by a diabetic, and remote monitoring of patients with chronic disorders [Lub02]. The use of wireless sensor networks in health monitoring is expected to accelerate due to the development of biological sensors compatible with conventional CMOS integrated circuit processes [Yan02].

These sensors, which can detect enzymes, nucleic acids, and other biologically important materials, can be very small and inexpensive, leading to many applications in pharmaceuticals and medical care.

2.2 Patterns

A pattern can be defined as a packaged solution to a recurrent problem in a particular context. Patterns capture the knowledge and experience of designers so they can be used by less experienced designers in solving related problem [Fer08]. Patterns can be used to build software architectures with specific properties. [Bus96] lists several properties of patterns when applied to architectures:

- A pattern addresses a recurring design problem that appears in some design step and provides a solution for it.
- Patterns can be used to document design experience and specific architectures.
- Patterns are concerned with sets of classes, above the abstractions presented by classes or objects.
- Patterns provide a communication vocabulary for designers.

All patterns are described using a template, which has predefined sections. This type of structured description ensures a systematic use of the pattern and provides a guideline for the pattern writer. There are different types of patterns such as design patterns, architectural patterns, analysis pattern, organizational patterns and various others. However, the most important aspect to consider before developing a pattern is the selection of template because it defines the type and characteristics of the information about the pattern. The solution is generally expressed with enough detail and precision so that it is convenient for a designer to understand and implement it. There is usually an informal diagram to describe the idea, which is then followed by a UML class diagram to describe the structure of the static information. A pattern can have several sequence diagrams describing the dynamics of the main use cases. Other UML diagrams such as state charts and activity diagrams could be used as well because it is convenient in describing complex cases. Generally UML solutions can be readily implemented in appropriate languages such as Java, Smalltalk, C++, or C# [Fer08]. Our work uses the POSA template for patterns which is briefly described in the next paragraph. A more detailed understanding about patterns can be found in [Bus96].

The POSA template has the following sections:

Intent: Every pattern starts with an intent section which is the thumbnail of the problem the pattern is solving and maybe a brief description of how it solves the problem.

Example: This section describes a problematic situation where this pattern is not yet used.

Context: This section describes context where the pattern solution is applicable. It can also explain the relevant characteristics of the context.

Problem: This section gives a generic description of what happens when there isn't a good solution available. It also indicates the forces that affect the possible solution.

Solution: This section describes the idea of the pattern. A descriptive figure may be present to help to visualize the solution.

Structure: This section describes the structure (static view) of the solution.

Dynamics: This section describes the dynamic aspects in the form of sequence diagrams for a use case.

Implementation: This section describes how the pattern can be implemented. This can be a set of general recommendations or a sequence of what to do to use the pattern. It may include some sample code if appropriate.

Example Resolved: This section describes what happens in the example after the pattern solution has been applied.

- Consequences: This section mentions about the advantages and disadvantages of the solution embodied in the pattern. The advantages should match the forces in the problem section. However, emergent advantages that do not correspond to any force may also be stated here.
- Known Uses: This section describes three examples of the solution's use in real systems in order for the solution to be accepted as a pattern.
- Related Patterns: This section relates the current pattern to other known patterns which could be complementary patterns, variations of the current pattern, or extensions of it. A Variants section is also possible.

3 A PATTERN FOR A SENSOR NODE

3.1 The Sensor Node Pattern

Aka: Mote, Sensing Node.

3.1.1 Intent

This pattern describes the architecture of a Sensor Node, a unit intended to sense, store, and communicate local information about a physical environment.

3.1.2 Example

Consider a chemical plant where crude oil is processed and refined into more useful petroleum products. In this system the pipes can burst due to excessive pressure. The pipes also may have high temperatures that may lead to fires. The plant has already had some accidents. If this situation continues, the chemical plant could incur huge losses. It would also endanger the lives of its employees.

3.1.3 Context

There are physical environments that need to be monitored for the presence of living beings, recording physical attributes, or detecting abnormal conditions. These environments could be inside buildings or could be external environments. For example, a battlefield may be monitored for detecting the presence of enemy soldiers and tanks, a wildlife sanctuary may be monitored for recording the population of migratory birds, and industrial plants can be monitored for detecting fire accidents [Cho03]. This pattern can be used to describe the nodes used in those environments or in similar situations, either as standalone units or as parts of a network.

3.1.4 Problem

Important events may get missed if nobody is watching for them. For example, in the battlefield, an attack by the enemy can take an army by surprise; in a wildlife sanctuary the population of migratory birds may be reduced due to a change in an environmental factor to which we did not respond; fires in homes, industrial plants and offices can lead to loss of lives and property. Without a way to sense some attributes of the physical environment these situations can go undetected for so long that effective countermeasures can no longer be taken. Human monitoring is not a convenient or efficient alternative.

A possible solution to this problem is constrained by the forces defined below, which have been grouped into related aspects.

Forces about the functions of the device:

Functionality: The device should be able to sense and collect local information about its surrounding environment such as temperature, pressure, light, smoke, humidity, or sound.

Controllability: If required, the device should have the ability to support actuators such as switches, servos, and motors that would allow it to control various actions [Bos09].

Extensibility: The architecture of the device should be extensible so that new functions can be added if required. For example, some nodes may need human-readable displays.

Forces about the use of the information collected:

Storage: The device should have sufficient memory in order to store the collected data. It should also be able to perform simple computations and transmit only the required data and routing information if the device is part of a network.

Conversion: The information detected by the sensors should be converted to appropriate formats for storage and processing.

Communication: The device should be able to communicate (send and receive) with other devices in order to gather or forward information about the physical environment.

Forces about the use of the devices:

Power autonomy: The device should have its own source of power.

3.1.5 Solution

Place a collection of one or more sensing devices together with other components in a common container to collect, store, process, and transmit sensor information. The sensor node may also contain some optional components that provide more specialized functions. A sensor node can act both as a data collector and as a data router. A sensor node can have different types of sensors that can detect pressure, humidity, light, acoustic, temperature, and various other physical properties. A sensor node includes some basic components that are organized as shown in the block diagram of Figure 3-1 [wik]:

- The processor is responsible for managing and coordinating various activities of the sensor node and for processing data. The sensors measure some properties of the physical environment. The Analog-to-Digital Converter (ADC) converts the analog data measured by the sensors to digital format so that it can be stored and processed.

- The transceiver is a radio device that can receive and transmit information. If the node is part of a network, data can be transmitted from the source to the destination using single hop or multiple hops communication.
- The power source supplies power to the sensors and to the other components of the sensor node. The power source may be supported by power scavenging units such as solar cells [Aky02].
- The processor also stores the collected data in the memory until it is forwarded to the next node.
- The processor generates control messages that direct the sensor to start or stop collecting information about the environment and direct the transceiver to be either in the receiving mode or transmitting mode depending upon the scenario.
- When the node is part of a network, the processor also keeps information about its neighboring nodes, decides the routing path and communicates the routing information to the other nodes.

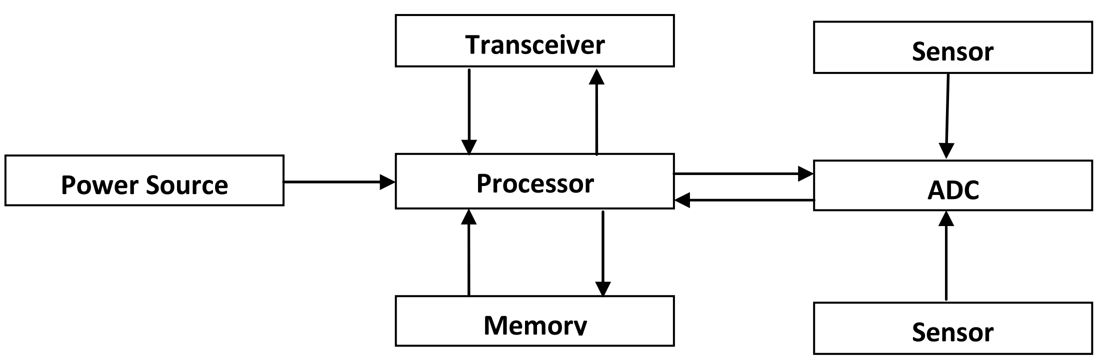

Figure 3.1 Block Diagram of a Sensor Node

3.1.6 Structure

Figure 3.2 shows the PowerSource supplying power to the Sensor, ADC, Processor, Memory, and Transceiver according to the block diagram of Figure 3.1. This class diagram is a precise description of the physical and information aspects of the device.

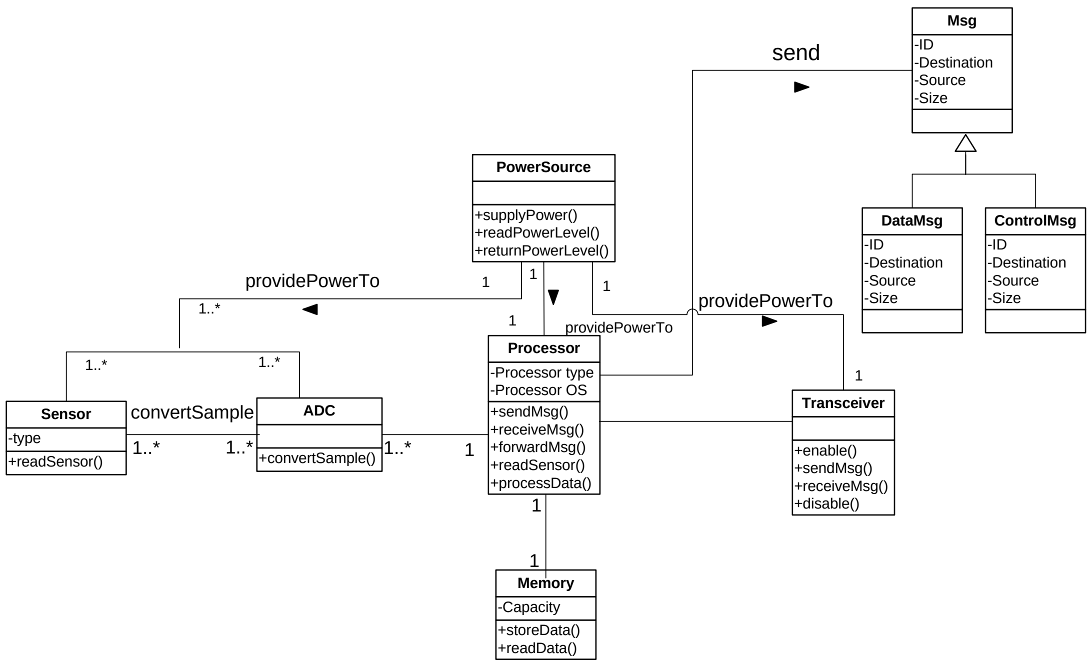

Figure 3.2 Class Diagram of a Sensor Node

3.1.7 Dynamics

Figure 3.3 describes the dynamic aspects of the sensor node using a sequence diagram for its use cases Sense, Collect, and Transmit data.

Description:

1 The processor sends a control message to enable the sensor.

2 The sensor reads the information in analog form and sends to the ADC.

3 The ADC converts the analog information into digital format and sends it to the processor.

4 The processor processes the data locally.

5 The processor stores the collected information.

6 The processor sends the collected information to the transceiver and/or memory.

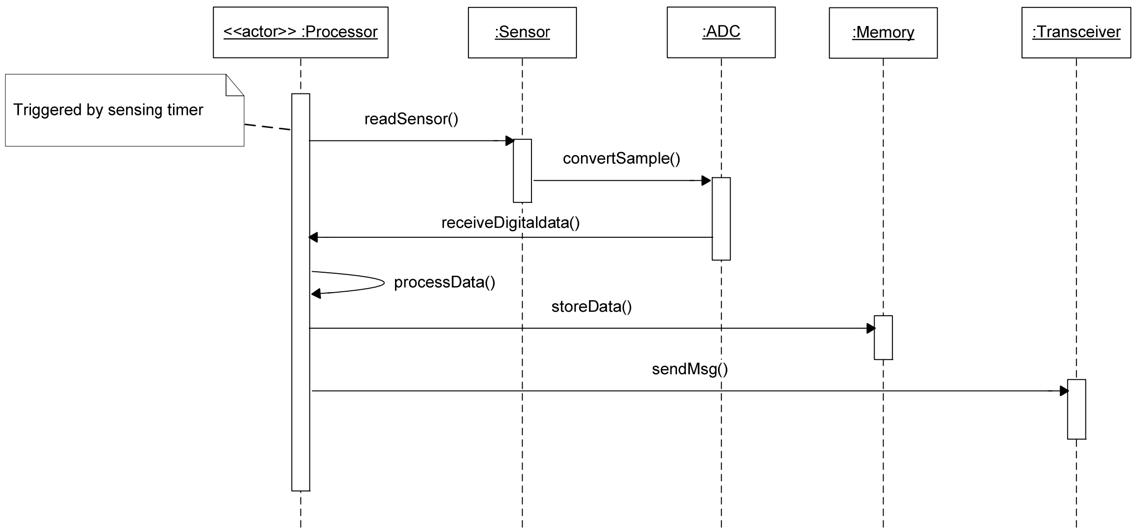

Figure 3.3 Sequence Diagram for Use Cases Sense, Collect and Transmit Data

3.1.8 Known Uses

This model corresponds to the architecture that is seen in commercially manufactured sensor nodes such as:

1. Berkeley Motes like MPR400 manufactured by Crossbow Technologies [Ber10]. Some of its specifications are:

- Frequency range of 902-928 MHz and T1 CC1000 transceiver
- ATmega 128L processor
- 4K bytes of RAM, 10 bit ADC
- Light, humidity, and temperature sensors

2. IPsensor Node manufactured by Arch Rock [IPS10]. Some of its specifications are:

- TelosB-compatible, 2.4 GHz IEEE 802.15.4 low-power radio
- T1 MSP 430 processor
- 10K bytes of RAM and 12 bit ADC
- Temperature, humidity, and total solar radiation sensors

3. Squidbee Mote manufactured by Libelium [Squ10]. Some of its specifications are:

- Frequency range of 2.4 GHz, data rate of 250 Kbps
- ATmega8 processor
- 8K bytes of flash memory 1K byte RAM
- Light, humidity ,and temperature sensors

3.1.9 Implementation

Users can buy commercially manufactured sensor nodes from the market based upon what kind of sensors they want for their application. These nodes are either pre-programmed and start collecting information once they are installed or they can be programmed depending on the application characteristics. Sensor nodes are configured to transmit their data using a transceiver. Data can be transmitted to the user directly or using a network [Int00] [Hei00].

Implementation of a sensor node involves two main steps: hardware implementation and software implementation. Hardware implementation depends on the characteristics of the application, expected performance, etc. The designer has to selected the hardware components (see Figure 3-1) and the interconnections (e.g. buses), to meet the application requirements. These components are laid out on a circuit board in order to promote extensibility. Depending on the application requirements and circuit parameters, the power budget must be determined, and an appropriate power source selected. Several sensor platforms are available on the market and they can be customized to different applications, for example Crossbow sensor nodes [Ber10].

The software implementation involves operating system and application code (firmware). The operating system manages the system resources and access to them, and is designed to be application independent to promote reusability. The operating system usually contains services for data message transmission and reception using the radio transceiver. The application code implements behaviors specific to the sensing application. Off-the-shelf sensing platforms come with the operating system and a software development kit for applications. The kit also provides a mechanism for uploading the application firmware on the sensor node program memory. For example, Crossbow motes come with TinyOS operating system and the NesC programming language and tools.

Aspects that are important in the use of sensor nodes are:

Ruggedness: The device should be able to operate in harsh environmental conditions.

Autonomy: The device should be able to operate autonomously and unattended.

Dimensions: The device should be small in size so that it can be easily deployed in large numbers [Bos09].

Cost: The device should have a relatively low cost if it needs to be used in large quantities.

3.1.10 Example resolved

Sensor nodes were installed in the pipes of the chemical plant. The sensor nodes constantly monitor and report if there is an abnormal increase of pressure and temperature in the pipes or in the chemical processing units. The sensor nodes can also activate water sprinklers in case of a fire. It is now possible to minimize the bursting of oil pipes and fire accidents in the refinery. This implies that the personnel are also safer.

3.1.11 Consequences

The Sensor Node pattern has the following advantages:

Functionality: This solution performs the required functions of sensing and collecting local information.

Controllability: This device can control actuators.

Extensibility: It is possible to easily add new functions

Autonomy: This device has its own processor, memory and power supply and can operate on its own.

Communication: This device can communicate with other devices for the purpose of gathering and forwarding information in the network.

Storage: This device can store the collected data.

The Sensor Node pattern has the following disadvantages:

1. Because of their size and cost, they have limited resources in terms of processor performance, radio reach, memory capacity, and battery life.
2. Sensor nodes are usually unattended so they can be physically tampered or destroyed.

3 Their use can potentially affect the privacy of individuals and their deployment must take this possibility into consideration.

3.1.12 Variants

Apart from the basic components, the sensor node might also have some additional application- specific components. For example, a sensor node can have a location-finding system or GPS to keep a track of its location and of its neighbors. The sensor node can have a mobilizer which can help the sensor node to move short distances if required, or it can have a power generator which supplies continuous power to a node having some additional functionality [Aky02]. Some of the sensors may have human-readable displays to facilitate data reading. Another important variant is a secure node, able to withstand some intentional attacks.

3.1.13 Related Patterns

A pattern for sensor network architectures that can be built using the Sensor Node pattern as a unit is presented in [Car10]. The Sensor Node pattern is also used as a component in the SCADA pattern [Fer10].

4 A PATTERN FOR SENSOR NETWORK ARCHITECTURE

4.1 The Sensor Network Architecture Pattern

4.1.1 Intent

This pattern describes the organization of sensor nodes and other wireless devices and the way they are connected with each other to achieve some objective, e.g. signal reach, performance, security, reliability, or other quality factors.

4.1.2 Examples

A vast battlefield should be monitored for detecting the presence of enemies and their vehicles. Having the troops patrol the field periodically may be dangerous and sometimes infeasible for large areas. Using a remote mechanism to sense and track the presence of enemies would benefit the army without endangering solders' life.

Another example is monitoring forests in critical areas for early detection of fires, in order to minimize the damage and casualties. In August 2003, a forest fire in Okanagan Mountain Park in British Columbia, Canada burned an area of 25,912 hectares and the total cost was $33.8 million [Hef09]. Using a remote mechanism to monitor various parameters such as temperature, humidity, and smoke can be used to detect forest fire.

4.1.3 Context

Wide-area physical environments need to be often monitored for the presence of living beings, for recording some physical attributes, or for detecting specific conditions. These environments could be inside a building or could be external areas.

4.1.4 Problem

Every network has some objectives that the architecture should satisfy. For example, the sensor network in a battlefield has to have high reach, fast, and reliable communication. A sensor network used for environmental monitoring should have an extended battery life. Sensor networks deployed for detecting fires should have fast and reliable communication.

In physical environments such as battlefields or agricultural lands, a large number of sensor nodes may need to be deployed. In this case, in order to prolong network lifetime, the design of the architecture must consider the energy-efficiency aspects. If data is forwarded hop-by-hop to the sink over a large number of sensor nodes, these nodes deplete their energy faster. Also the nodes around the sink deplete their energy at a faster rate, resulting in network partitioning.

The possible solution is constrained by the following forces:

- The data collected by sensors must be sent to a sink or to a set of sinks to be processed or integrated with a larger system. Without reaching the sink, this data collection is wasted.

- Some nodes may not be able to reach the sinks directly. Other nodes need to help those nodes reach the sink.
- For management or security purposes we may need to divide the network into sections which are independent in some sense.
- To reach our optimization goals we might need to have some specialized nodes.
- We might need to be able to integrate our network with other networks. These might be peer to peer interconnections or our network might be a component of a larger system.

4.1.5 Solution

A wireless sensor network (WSN) can be used to monitor a wide area. Figure 4.1 shows the general architecture of a WSN. Sensor nodes might be homogeneous (measure same attributes) or heterogeneous (measure different types of attributes). Some of the nodes, named supernodes in this chapter, are more resource-rich than the sensor nodes. They can have for example more energy resources, larger transmission range, higher data rate, etc. In addition, a sensor network can be organized in clusters. Each cluster has a cluster head which has certain role within the cluster (e.g. aggregates data received from the nodes in the cluster).

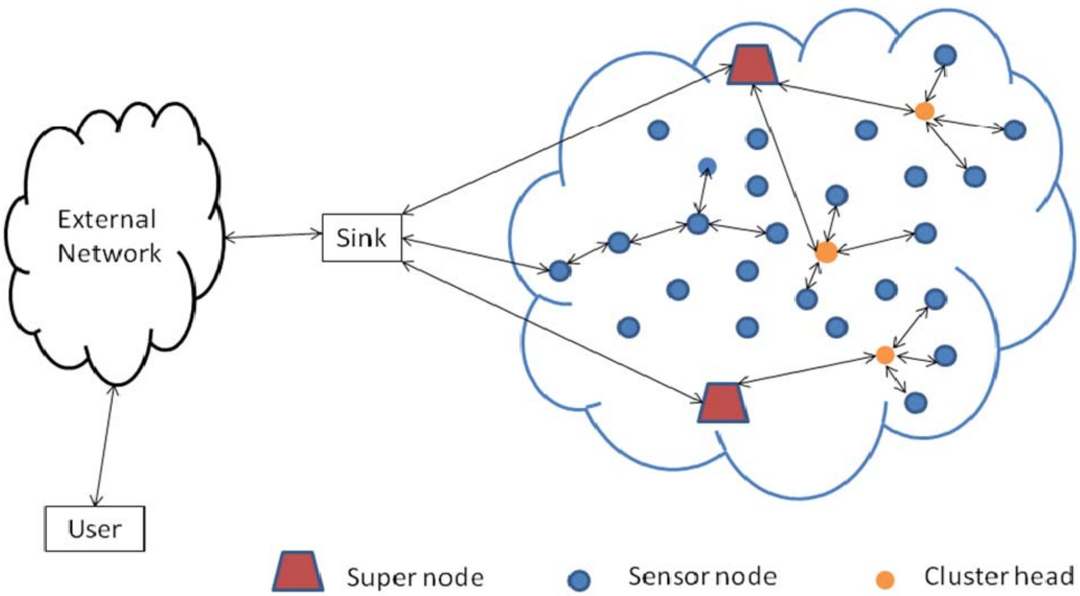

Figure 4.1 Wireless Sensor Networks

4.1.6 Structure

Figure 4.2 shows a Network composed of several Nodes and zero or more Sinks. Networks can be connected to other networks. Nodes may be connected to other nodes and all are connected to the sinks. Nodes can be Sensor nodes (regular data-collection nodes) or Supernodes (that collect data from other nodes). Nodes can be organized into clusters, and each cluster has a Cluster Head that controls the data collection within the cluster.

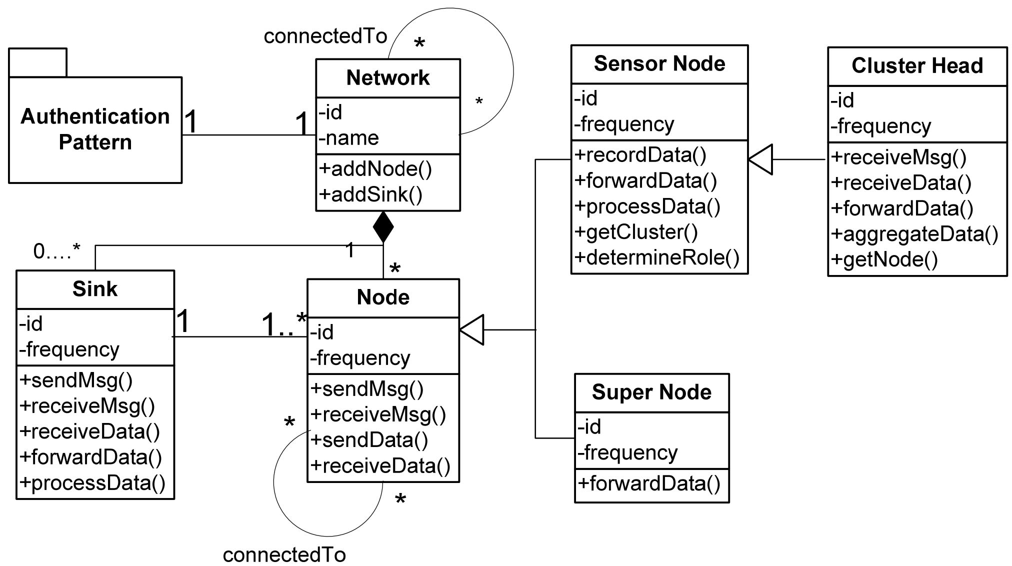

Figure 4.2 Class Diagram of a Wireless Sensor Network

4.1.7 Dynamics

Several use cases are possible with this information, which include Initialize Network, Reconfigure Network, Query Request, Data Gathering, Create Cluster, and Forward Data. Figure 4.3 shows a sequence diagram for the use case Forward Data.

Description:

- **Precondition:** The processor stores routing Tables and can execute routing protocols in order to route the data from one node to the other.
- The processorP1 sends a message to the transceiverTx1 which then routes the data to transceiverTx2 of the neighboring sensor node.
- The transceiverTx2 of the neighboring node forwards the data to its processorP2.
- The processorP2 processes together the received data from transceiverTx2 and its own data and sends them to transceiverTx2.

- TransceiverTx2 might send this data to the transceiver of another sensor node so it can be further forwarded.
- Sometimes, the processor might store the data locally in its memory until it is ready to be routed to the next sensor node.

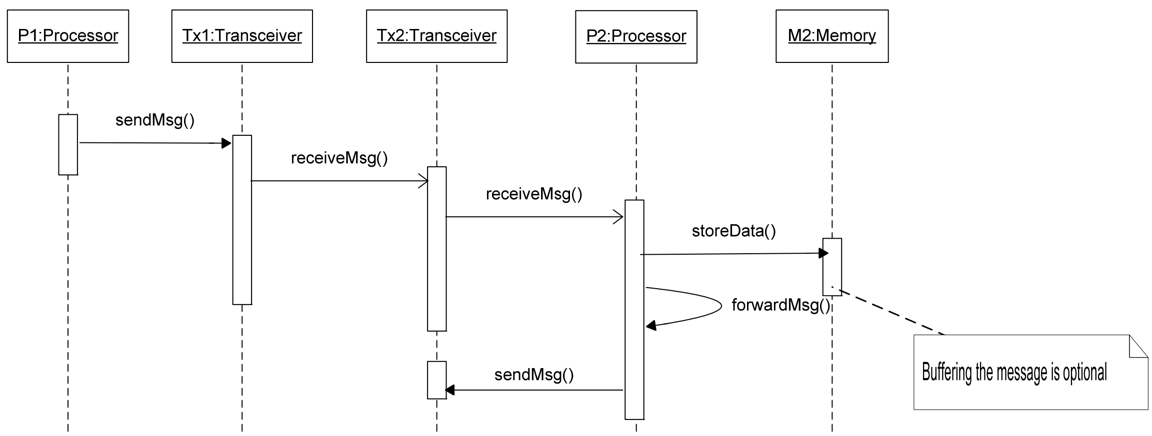

Figure 4.3 Sequence Diagram for Use Case Forward Data

4.1.8 Implementation

A group of sensor nodes can be used to build a WSN that can be implemented inside buildings or in external environments.

- Sensor nodes can be programmed using a general purpose programming language such as C or a specialized language such as NesC or LabVIEW. Crossbow MICA motes [Cro10] uses TinyOS and are programmed using NesC.
- After the sensors are programmed, they are deployed inside buildings or external environments. Once they are deployed, they initialize, discover their neighbors, and start sensing and transmitting data. Sensed data can be transmitted periodically or event based.

- A wireless communication protocol is used to specify message relaying between nodes. For example, IEEE 802.15.4/Zigbee standard [IEE03] specifies the Physical and MAC layer of the wireless communication.
- A WSN implementation must also specify a routing protocol. Operations such as query request (from a sink) and data gathering (to one or more sinks) have to be supported. One such mechanism is Directed Diffusion [Int00].
- In addition, other mechanism for security, data aggregation, quality of service, etc. can be implemented.

4.1.9 Examples Resolved

The isolated sensor nodes deployed in a battlefield or in a large forest to measure various attributes have been organized into a network. Now the information of all active sensors can reach long distances with the help of other sensors that can relay them. If a sensor is destroyed or runs out of power its function can be replaced by a nearby sensor. Supernodes can provide extra processing power to filter or reformat the data before being forwarded to the sink.

4.1.10 Consequences

- If some nodes cannot reach the sinks, other nodes can help them by relaying their data.
- Clusters allow the management or securing of sections of the network by defining a cluster head that can control different functions or distribute encryption keys.

- Specialized nodes can be inserted in the network to add more processing power to do filtering, to keep logs, or to store authentication information.
- UML provides a standard and unified description of network topology and functions, which makes their integration with other systems quite simple. Associations such as aggregation or relationship allow any type of network combinations.

4.1.11 Known Uses

- During the summers of 2002 and 2003, scientist deployed three WSNs for habitat monitoring on Great Duck Island, to monitor the Leach's Storm Peterel [Mai02]. Temperature, humidity, occupancy, and pressure sensing attributes were used to correlate nesting patterns with microclimates.
- A WSN for structural health monitoring has been deployed and tested on the 4200ft long main span and the south tower of the Golden Gate Bridge [Kim07]. The network had 64 nodes and measured ambient structural vibrations at 1kHz rate.
- In August 2005, scientists deployed a WSN on Volcan Reventador in northern Ecuador [Wer06]. The array consisted of 16 nodes, each equipped with a microphone and seismometer, deployed over 3 km. Over three weeks, the network captured 230 volcanic events.

4.1.12 Variants: Secure Sensor Network Architecture

We can analyze threats and superimpose security patterns to control these threats. We indicated one possible mechanism in Figure 4.2. We are not describing all possible threats but only showing the approach. We indicate where the patterns for the relevant mechanisms can be found.

Some specific threats and their defenses include:

- A network or node impersonating another node. Can be prevented by mutual authentication. The Authenticator pattern [Bro99] in the Network class of Figure 4.2 indicates that communications between networks would require authentication to prevent impostors.
- Illegal access to the data in a sensor node. This threat requires the use of some type of access control, e.g. Access Matrix or Role-Based Access Control [Sch06].
- Message interception. The objective can be illegal reading or writing of a message in transit. This attack can be controlled through cryptography.
- Repudiation. Can be controlled using digital signatures.
- A captured node can stop the relaying of information. There is no way to avoid this threat, except by having many nodes.
- Some other attacks such as node capture, physical tampering, denial of service attacks, and traffic analysis are discussed in [Per04].

4.2 Related Patterns

A pattern for a sensor node is presented in [Sah10]. Patterns addressing various security aspects are described in [Bro99], [Sch06].

5 A PATTERN FOR A REMOTE PATIENT MONITORING SYSTEM

5.1 Introduction

A patient monitoring system can be described as observing or watching a patient's vital signs such as heart beat rate, pulse rate, blood glucose level, brain activity, muscle activity and various others. Monitoring is necessary to warn against an impending medical condition or recovery from a serious illness or surgery. Health monitoring helps in detecting medical conditions before they get worse. Health monitoring has been carried out in different ways over the years. In early days health monitoring was manual wherein the physicians would check the vital signs of the patients at regular time intervals. With technological advancement, health monitoring was done using wired electronic devices. Though it was better than manual monitoring and gave accurate results, but it turned out to be clumsy and inconvenient as the patient was surrounded by wires all over his body. The advent of wireless sensor technology gave a new direction to health monitoring as unobtrusive, wearable sensors were developed to measure the vital signs of a person. With this technology in place it became possible to measure the vital signs of a patient remotely. It is no longer necessary for the patient to be in the hospital amidst huge medical devices for monitoring to take place. The patient could be monitored even if he is in a remote hospital ward in a huge hospital or if he is receiving treatment at his home.

Wearable senor nodes could be placed on the patient body which would transmit data to a computer representing the sink all of which combine to form a body area network. This body area network would interface with other network elements such as servers, routers, gateways, internet and wireless network to form a remote patient monitoring system. Several health monitoring systems have been proposed in [Shn05], [Vir06] and [Wal00]. With the help of remote patient monitoring system, medical data would be collected and reported automatically thereby reducing the cost and inconvenience of regular visits to the hospital.

5.2 Remote Patient Monitoring System Pattern

5.2.1 Intent

This pattern describes an architecture to monitor patients by measuring their vital signs and transmitting that information to medical personnel. This can be done by placing sensor nodes on their body which will transmit their vital sign values to a central station using a wireless network.

5.2.2 Example

Consider a patient who recently had a severe heart attack. When the patient was in the hospital, his physicians closely monitored his vital signs and his medication. After his condition was stabilized, he was discharged from the hospital, but his physicians want to supervise his recovery so that he gets back to a normal lifestyle and the probability of another heart attack is minimized. His physicians want to put him on drug therapy and monitor the effects, but each time the physicians change the medication or the dosage, the patient has to come to the hospital for a check up to make sure his vital signs are within the normal range. The physicians also want the patient to do some cardiovascular exercise and monitor his vital signs during the exercise to make sure that the duration and intensity of the workout is appropriate for his recovery. For every workout session the patient has to make an appointment with his physical therapist and has to visit the hospital. During his recovery phase, the patient has to visit the hospital whenever there is a change in medication or he has to do some exercise. It is very inconvenient for the patient to make appointments and visit the hospital multiple times.

5.2.3 Context

There are certain situations where a person's vital signs need to be monitored in order to help him recover from a medical condition or to detect any abnormal health condition. The monitoring could take place in a hospital environment or outside. For example, the blood sugar level of a diabetic person could be monitored and recorded regularly in order to come up with an efficient treatment plan. The vital signs and overall health of patients with chronic disorders such as Alzheimer's and Parkinson's could be continuously monitored for patient well-being and research purposes. The tissue and bone health of patients with knee and hip surgeries could be monitored during physical rehabilitation.

5.2.4 Problem

Life- critical situations may go unnoticed if nobody is watching for them. For example, the blood glucose level of a diabetic person may reduce suddenly and she may become unconscious; a person recovering from knee surgery may fall down and injure himself severely, a person recovering from a heart condition may be following an exercise routine and his heart rate may increase abnormally resulting in a cardiac arrest. Lack of a system to constantly measure and observe the vital signs of a person may give rise to life-threatening conditions and even death. Constant medical supervision is not possible all the time because it is costly and it is hard to find appropriate personnel. A possible solution to this problem is constrained by the forces defined below:

- **Functionality**: The system should be able to measure and collect the vital signs of a person at regular time intervals and forward the data to a medical server. It should also be able to generate alerts in case of an emergency situation.
- **Flexibility**: If required, the system should have the ability to support devices such as cell phones, personal digital assistants, laptops, and pagers. For example, the person using the system should be able to get reminders and alerts on his PDA or cell phone to perform certain tasks.
- **Extensibility**: The architecture of the system should be able to accommodate new medical applications and new network devices for data communication.
- **Storage**: The system should be able to store some data locally.

- **Communication**: The components of the system should be able to communicate (send and receive) efficiently with each other in order to gather or forward medical information.
- **Security**: The confidentiality of the stored and in-transit information should be preserved.
- **Availability**: The system should be available most of the time.

5.2.5 Solution

Create a network consisting of wearable sensor nodes, a personal server that is implemented either on a personal digital assistant or cell phone or home personal computer, a medical server and a wireless network. The network can also consist of additional devices like routers and intermediate servers to provide medical data storage on remote servers. Figure 5.1 shows the components of a remote patient monitoring system.

- The patient wears *sensor nodes* on his body that measure his vital signs and forward them to the *personal server* consisting of either a cell phone or PDA or computer.

- The *personal server* processes the data and forwards the information to the *medical server* through the wireless *network* using appropriate communication protocols.

- The *healthcare provider* retrieves the patient's information from the *medical server.*

- The *emergency team* can receive alarms from the *personal server* in case of an emergency through the *network* and can access the patient's medical data from the *medical server*.

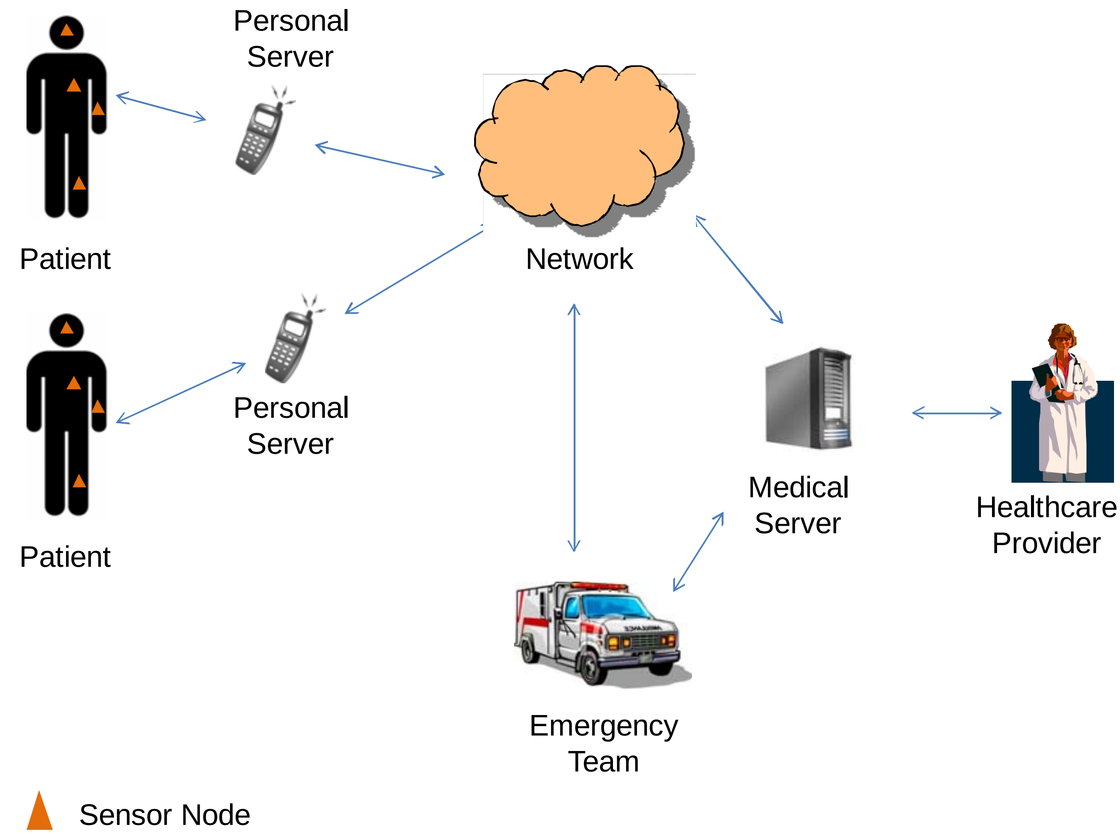

Figure 5.1 Components of a Remote Patient Monitoring System

5.2.6 Structure

Figure 5.2 shows the Patient wearing SensorNodes on his body capable of measuring his vital signs. The SensorNode forwards the collected information to the PersonalServer. The PersonalServer establishes communication with the MedicalServer through the Network and uploads the patient's medical data on the MedicalServer. The HealthcareProvider sends commands to the MedicalServer in order to retrieve patient information. In case of emergency, the Network sends an alert to the EmergencyTeam. The EmergencyTeam can get the patient data from the MedicalServer. Note that the SensorNode class is a façade for a Sensor Node [Sah10].

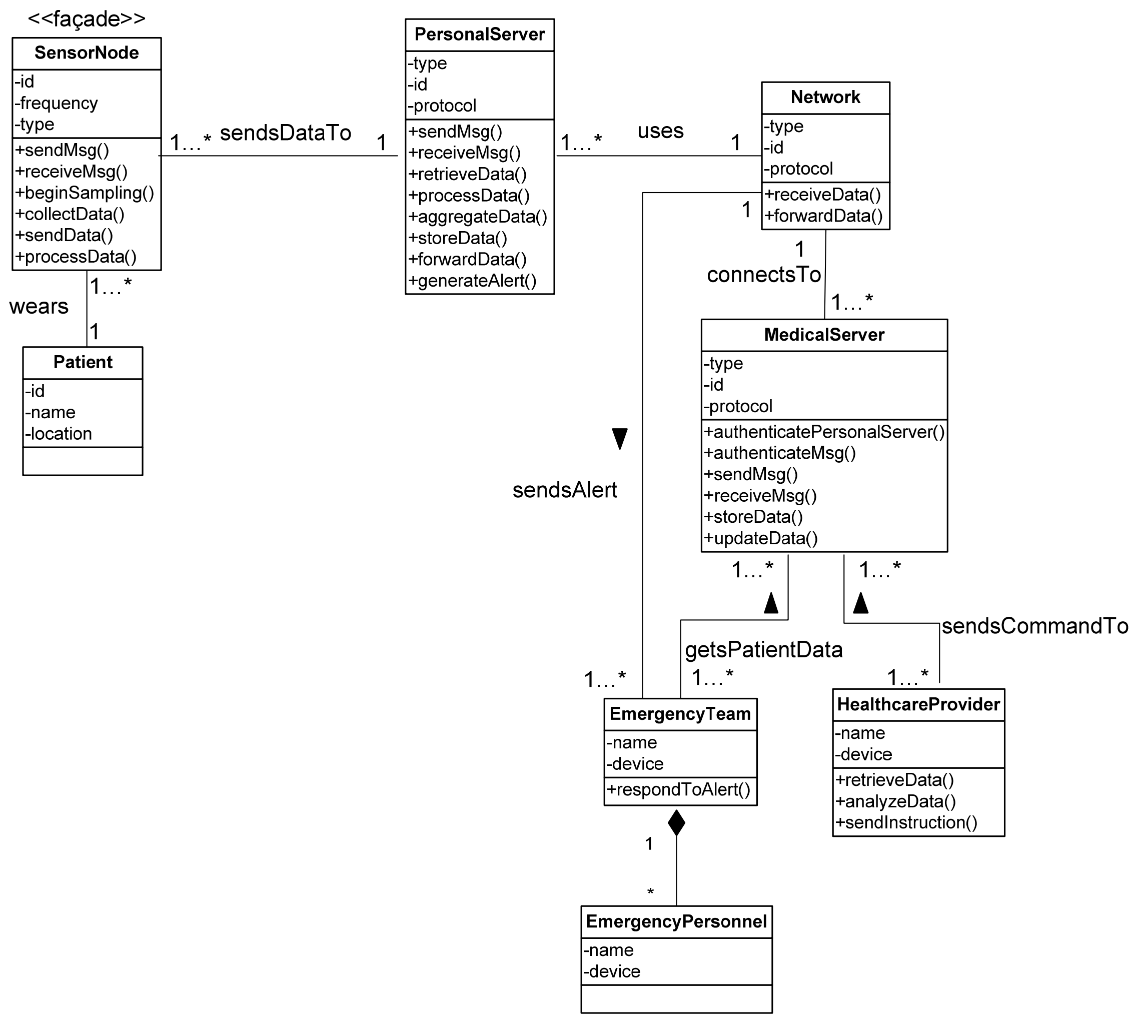

Figure 5.2 Class Diagram of a Remote Patient Monitoring System

5.2.7 Dynamics

Figure 5.3 describes a sequence diagram for the use case Collect and Transmit Data.

Description:

1. The personal server directs the sensor node to begin sampling vital signs.

2. The sensor node collects the vital signs and sends the collected data to the personal server.
3. The personal server processes the collected data and forwards it to the network.
4. The network then forwards the data to the medical server.

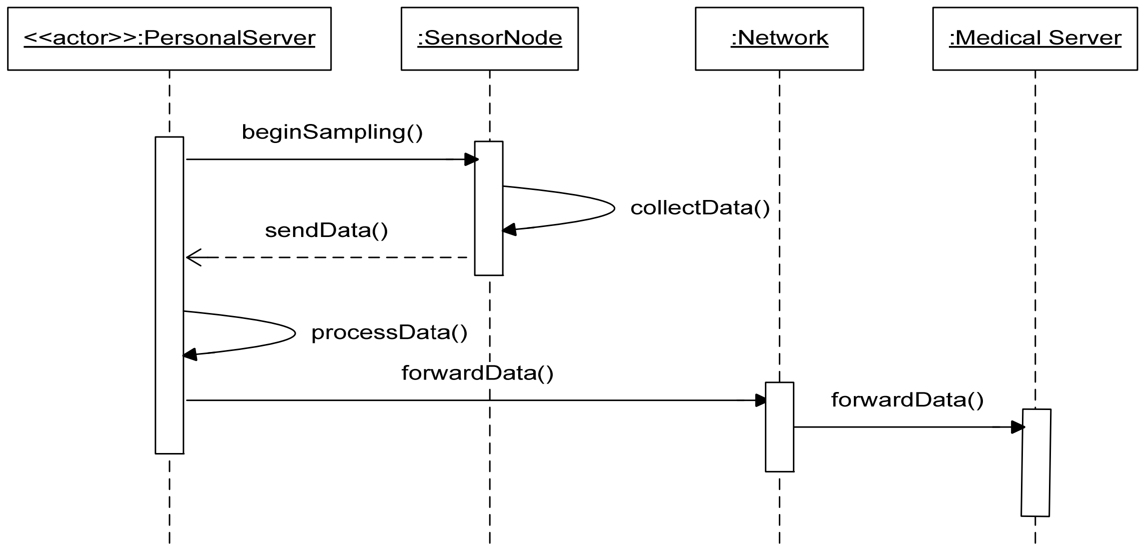

Figure 5.3 Sequence Diagram for Collect and Transmit Data

Alternate Flow:

Figure 5.4 describes a sequence diagram for an exception in use case Collect and Transmit Data.

Description:

1. If the personal server encounters any abnormal findings in the collected data, it generates an alert which is forwarded to the network.
2. The network forwards the alert to the emergency team.

3. The personal server also logs the alert on the medical server for the healthcare provider to analyze later.

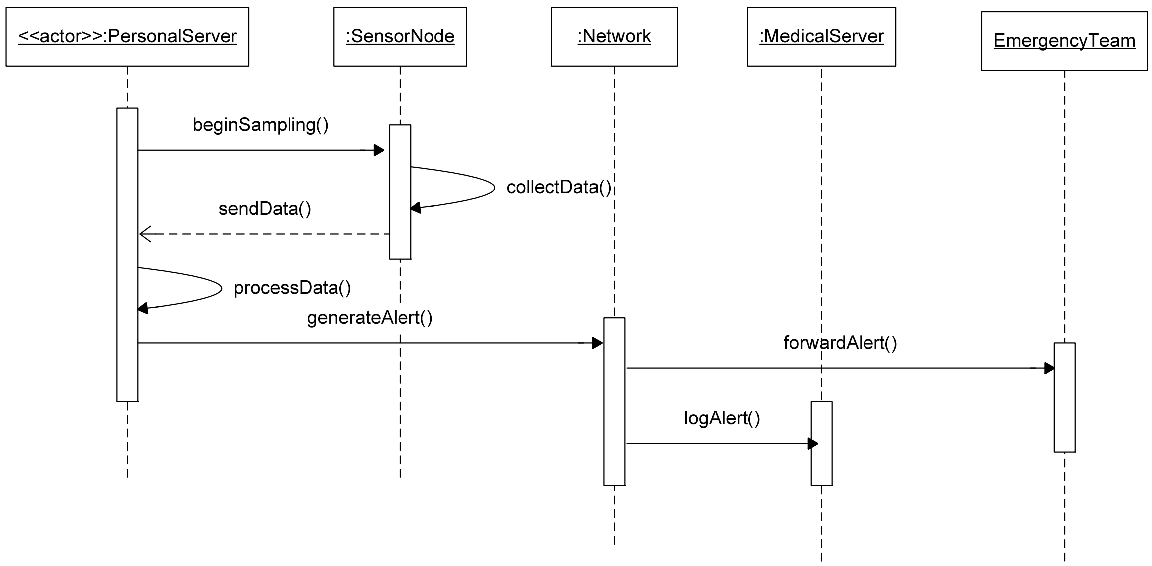

Figure 5.4 Sequence Diagram for Alternate Flow Generate Alert

5.2.8 Known Uses

- A wireless body area sensor network prototype developed by a research group at the University of Alabama [Ott06]. Some of its specifications are:
    - It includes two activity sensors (ActiS), and integrated ECG and tilt sensor (eActiS), and a personal server implemented on a pocket PC having a network coordinator.
    - It uses Zigbee wireless communication and the sensor node and network coordinator software is implemented using a TinyOS environment.

- The CodeBlue prototype which includes the design of sensor node hardware, protocol and middleware framework for medical sensor networks, developed by a research group at Harvard University [Shn05]. Some of its specifications are:
    - It includes pulse oximeter, Telos-based electrocardiogram (EKG) sensor node, and motion capture and electromyographic (EMG) sensor node.
    - It is based on a publish/subscribe routing framework and provides protocols for integrating wireless medical sensors and end user devices. It is implemented using a TinyOS environment.
- The Smart healthcare prototype developed by a research group at the University of Virginia [Vir06]. Some of its specifications are:
    - It includes a body network consisting of pulse oximeter and electrocardiogram (EKG) sensor nodes, bed sensor node, motion sensor node, emplaced sensor network consisting of temperature, humidity, acoustic and luminosity sensor node, and a system backbone consisting of computers, personal digital assistants, databases and graphical user interfaces.
    - It uses a gateway in the system backbone and runs on embedded Linux, the motes use the Zigbee wireless protocol and the database used is MySQL.

5.2.9 Implementation

Users can select from commercially manufactured sensor nodes for medical applications from the market based upon what kind of vital signs they want to monitor [Cro1]. These nodes are pre-programmed and start collecting information once they are strategically placed on the patient body and transmit data to the personal server through Universal

Asynchronous Receiver/ Transmitter (UART). For a personal server the user can buy a pocket PC or a PDA which usually comes with a customized downloadable client program e.g. a post knee surgery monitoring application or a blood sugar level tracking application. In order to connect the sensor network to other network devices and/or databases, the user can buy gateway nodes which come with the operating system and a software development kit. The user can also opt for some off-the-shelf wireless health monitoring platform [Jaf05] which can be easily custom-built for patients by non-engineering staff.

5.2.10 Example resolved

A remote patient monitoring system was installed in the patient's house. The physicians were able to monitor the patient's vital signs and prescribe new medication whenever required and an alert was generated in case of an emergency situation. When the patient did some cardiovascular exercises, he got voice notification on his cell phone regarding the intensity and the duration of the exercise. An alert was generated if the patient felt uncomfortable during the exercise and emergency teams could reach him in case of an emergency situation. Now the patient does not visit the hospital frequently and follows his exercise regime from home. As a result the patient is recovering at a steady rate while leading a healthy lifestyle.

5.2.11 Consequences

The patient monitoring system has the following advantages:

- **Functionality**: This solution can measure the vital signs of a person at regular time intervals and forward them to a medical server.
- **Flexibility**: This solution can support devices such as cell phones, personal digital assistants, laptops, and pagers.
- **Extensibility**: The architecture of the system can accommodate new applications and new network devices for data communication.
- **Storage**: This architecture can store data locally.
- **Communication**: The components of the solution can communicate (send and receive) efficiently with each other co in order to gather or forward medical information.
- **Security**: Although not shown, the communications can be encrypted and an authorization system can be added in the medical server.
- **Availability**: An extra personal server can be used as back up.

The pattern for a remote patient monitoring system has the following disadvantages:

- **Confidentiality**: Even though the system could be designed to be secure, the wireless links could be weak and a person's confidential medical data could be exposed.
- **Denial of service**: The system could be made busy by generating unnecessary traffic so that the user data is unavailable when it is needed the most.

5.2.12 Variants

An important variant is a pattern for a secure remote patient monitoring system.

5.2.13 Related Patterns

A pattern for a sensor node [Sah10] and a pattern for sensor network architectures [Car10] are the two patterns that form the basis for this pattern.

5.3 Conclusion

We have presented a pattern that describes the architecture of a remote patient monitoring system. The Remote Patient Monitoring pattern abstracts the architectural aspects of a patient monitoring system involving wireless sensor network. The various components of a patient monitoring system were studied, including its static and dynamic aspects. Both the advantages and constraints of the system were discussed. In the end the implementation details of the system were also discussed.

6 RELATED WORK AND DISCUSSION

This chapter provides an overview of work done to model sensor nodes, wireless sensor networks and healthcare applications involving wireless sensor networks. This chapter begins by introducing related architectural models for a sensor node. Then some related models for wireless sensor network architecture are described. The next section highlights some related work about healthcare applications involving wireless sensor networks. In the next chapter these models are compared with our work.

6.1 Introduction

Military applications have been the main driving force for research and development in the sensor network technology. An example of early sensor network includes the radar networks used in air traffic control and sensor networks were also used in Cold war to track Soviet submarines. In the 21st century advancement in microelectromechanical system (MEMS) technology lead to the design of small and inexpensive sensor nodes having low-power processors and once again, DARPA spear-headed the research program on sensor networks to leverage the latest technological advances. In the late 1990s, a company called Dust Inc. in Berkeley, CA, envisioned the Smart Dust research project at the University of California, Berkeley, and built MEMS sensor nodes that can sense and communicate and yet are tiny enough to fit inside a cubic millimeter.

6.2 Architectural models for Sensor Nodes

In one of the papers on Smart Dust by [Kah99] the authors have described the architecture of the smart dust sensor node. The smart dust sensor node is designed to have all the components of a regular sensor node packed into a tiny form factor of one cubic millimeter. The motivation behind chasing a small form factor was minimum energy consumption while having all the necessary features. Sensor node runs on finite power supply, and the tiny form factor aimed to consume minimum energy thus prolonging node lifetime. The Smart Dust mote was described to have four subsystems such as sensors and analog signal conditioning, power system, transceiver front end, and the core. The core consisted of all the digital circuits in the system, including the receiver back end, sensor processing circuits, computation circuits, and memory. One of the main criteria of the node design was the extensibility of the core so that it can be reconfigured easily to the changing needs of the application. Though the basic architecture of the mote was kept unaltered, the authors discussed some other factors that affected the design of these nodes. The factors were:

- Determining the exact functional needs of a particular application scenario including necessary signal processing and computation functions. Other than that, the exact amount of node reconfigurability had to be determined as well so that the node could be extended if need arise.
- Mapping of the necessary functionality of the core into various possible architectures.
- Evaluating the choices for achieving the lowest energy solution.

To summarize, the goal of the Smart Dust project was to minimize energy consumption through architecture, while providing the necessary functionality and reconfigurability for a particular scenario. The proposed architecture used a reconfigurable data-driven data path, which facilitated power cycling of the functional units, thereby reducing the standby energy consumption to a minimum.

6.3 Models for types of WSNs

WSNs have been classified into various categories such as flat networks or hierarchical networks, homogenous networks or heterogeneous networks. Before discussing the types of networks it is essential to know why there are different types of network. Whatever may be the classification, each type of network has an objective to achieve which could be energy conservation and maximizing network lifetime, or maximizing throughput or increased coverage. The different architectures are supported by different protocols to achieve the objective. Sensor nodes are autonomous in nature so they would self-configure without any priori information about the network topology. The ultimate goal of a WSN is to detect the specified event of interest in a sensor field. Due to the deployment of large number of sensor nodes, their detection range often overlaps, which means that the same event is usually reported by numerous sensor nodes, which leads to the data redundancy. In-network data aggregation has been proposed as an essential paradigm for routing in WSNs [Int00]. The benefit of data aggregation has been confirmed theoretically in [Kri02] and experimentally in [Hei01]. To ensure the scalability and increased efficiency of network operations, clustering approaches have become an emerging technology for building scalable, robust, energy-efficient WSN applications [Gob05].

In [Hei01] the authors have proposed a clustered architecture in which the nodes organized themselves into local clusters, with one node acting as the local base station or cluster-head. They have also described the method by which the cluster heads alternate in time to maximize the lifetime of the network. The paper concludes by describing some experimental analysis and advantages of this approach.

Heterogeneous WSNs are gaining importance because complex problem settings consist of different environmental conditions and require specific sensor nodes for the individual tasks. [Anw02] have described how to manage activities in a WSN by developing WSN management framework to support common management tasks such as monitoring the WSN, configuration of the WSN, code updates, and managing sensor data. The proposed management architecture consisted of the following infra-structural elements: a management station, a number of management nodes and a high number of heterogeneous sensor nodes. All management tasks in this architecture were controlled by the management station. The paper described several tasks that were required to manage a WSN and its sensor nodes. These tasks were divided into four areas:

(1) Monitoring WSN and the sensor nodes: The monitoring task required that all sensor nodes in the several subnets were displayed at the management station with all necessary information. This included sensor node hardware details, sensor node software details, and dynamic properties. The node ID and other static information were sent when a sensor node joined the network. Additionally the management station could query sensor nodes.

(2) Re-configuring WSN and the sensor nodes: This task included sensor node configuration and network configuration.

(3) Updating sensor nodes: This included code distribution mechanisms and application updates performed on the operating system.

(4) Managing sensor data: This involved handling the data gathered by the sensor nodes.

The structure of the sensor node manager and the protocols used in sensor node monitoring, sensor node re-configuration and sensor node code updating were also described in this paper.

6.4 WSN Models for Health Monitoring

G. Virone et al [Vir06] have designed a system architecture for smart healthcare involving Wireless Sensor Network. This architecture was developed for assisted-living residents and continuous, remote health monitoring applications. An experimental living space was constructed at the Department of Computer Science at UVA for its evaluation. The described architecture was multi-tiered and had heterogeneous devices ranging from lightweight sensors, to mobile components, and to more powerful stationary devices. The main objective of the network was to integrate heterogeneous devices, some wearable on the patient and some placed inside the living space. In the component diagram of the architecture the devices are divided into strata based on their roles and physical interconnections. The authors described each tier of the architecture as follows:

- Body Network and Subsystems: This network comprised of tiny portable devices equipped with a variety of sensors such as heart-rate, heart-rhythm, temperature, oximeter, accelerometer, and performed biophysical monitoring, patient identification, location detection, and other desired tasks. The energy consumption of the nodes was also optimized so that there was no need to change the battery on a regular basis or it could use “kinetic” recharging. The network had sensors and actuators which were able to communicate among themselves. One of the nodes in the body network was designated as the gateway to the emplaced sensor network. Due to size and energy constraints, nodes in this network had little processing and storage capabilities.

- Emplaced Sensor Network: This network included sensor devices deployed in the environment (rooms, hallways, furniture) to support sensing and monitoring, including: temperature, humidity, motion, acoustic and, camera. All devices were connected to a more resourceful backbone. Sensors communicated wirelessly using multi-hop routing and used either wired or battery power. Nodes in this network could vary in their capabilities, but generally did not perform extensive calculation or store much data. The sensor network interfaced to multiple body networks, seamlessly managing handoff of reported data and maintaining patient presence information.
- Backbone: The backbone network connected the traditional systems, such as PDAs, PCs, and databases, to the emplaced sensor network. It also connected discontinuous sensor nodes by a high-speed relay for efficient routing. The backbone could either communicate wirelessly or had to overlay onto an existing wired infrastructure. Nodes in this network possessed significant storage and computation capability, for query processing and location services.

- One or more nodes connected to the backbone were dedicated databases for long-term archiving and data mining. Patients and caregivers interfaced with the network using PDAs, PCs, or wearable devices. Some of the sensor nodes used in this architecture were motion sensor node, temperature and luminosity sensor, bed sensor, pulseoximeter and EKG sensor.

V. Shnayder et al. [Shn05] also developed a combined hardware and software platform for medical sensor networks, called CodeBlue. The CodeBlue sensor network platform provided protocols for device discovery publish/ subscribe multihop routing, as well as a simple query interface that was tailored for medical monitoring. Medical applications involving sensor networks required new hardware designs so the group also developed three mote-based medical sensors such as mote-based pulse oximeter, two-lead electrocardiograph (EKG), and a special-purpose motion-analysis sensor board. They also developed a small form factor variant of the Telos mote called Pluto specifically for wearable applications. However, medical sensor networks and the supporting devices had diverse requirements so it became important to redo the software environment, routing protocols, and query interfaces. The CodeBlue architecture comprised of protocol and middleware framework for medical sensor networks and was intended to act as an “information plane” tying together a wide range of wireless devices used in medical settings.

CodeBlue was implemented using TinyOS and provided protocols for integrating wireless medical sensor nodes and end-user devices such as PDAs and laptops. The architecture was based on publish/subscribe routing framework, that allowed multiple sensor devices to relay data to all receivers that had registered an interest in that data. This communication model turned out to be a perfect fit for the needs of medical applications where a number of caregivers were interested in sensor data from overlapping groups of patients. However a number of considerations had to be taken into account such as the sensor nodes need not publish data at an arbitrary rate. The publishers and subscribers need not be within radio range, hence some form of multihop routing was necessary. In the end, the communication layer should take mobility into account while establishing routing paths.

A discovery protocol was provided to allow end-user devices to determine which sensors should be deployed in a CodeBlue network and for nodes to discover and determine the capabilities of each other while a query interface allowed a receiving device to request data from specific sensors based on type or physical node address. The query interface also provided a filter facility, so that a query could specify a simple predicate on sensor data for e.g. the doctor might request data on a patient only when the vital signs fell outside of a normal range.

7 CONCLUSION AND FUTURE WORK

7.1 Introduction

The goal for this thesis has been to describe the structure of sensor nodes, sensor network architecture and healthcare applications involving wireless sensor networks. We studied the structure of different sensor nodes, sensor architectures and healthcare applications to develop patterns and models built on classes. These classes describe the sensor node and the various operations carried out by them. We have also studied related work and compared them with our patterns. This chapter begins by providing a summary of our research work followed by a comparison with other related work. The chapter ends with some conclusions and future work.

7.2 Summary of research work

Chapter 3 presented a pattern to describe the structure of a sensor node. The structure of the node was first described using an informal block diagram. Then the functions and the relationship between the various components were described using a class diagram. In the end the interactions between the components were described with the help of a sequence diagram. This chapter also discussed three known uses of the pattern and its implementation process.

Chapter 4 presented a pattern to describe the architecture of a sensor network. The basic architecture of the sensor network was described using a block diagram. The class diagram described the structure of the network and the classification of the sensor nodes present in the network. The sequence diagram described the manner in which the data is forwarded in the wireless sensor network. The chapter ended by discussing the implementation aspects of the network and some known uses describing the real life application of sensor networks.

Chapter 5 presented a pattern to describe the architecture a remote patient monitoring system. A block diagram was used to introduce the concept of a patient monitoring system. The class diagram described the functions and the of relationships between the different components in the system. The sequence diagram described the data collection and transmission process in the system as well as the sequence of events that would take place in case an alert was triggered.

7.3 Comparison with other related work

The architectural model for sensor node described in [Kah99] uses conceptual diagram and block diagram to explain the node structure which does not clearly indicate the connections between the components. The functions and interactions between the components are simply enumerated and not explained by using some kind of data flow diagram. This thesis focused more on describing the structure of a node with the help of UML diagrams. A block diagram was used to show the various parts of the node. In order to have better understanding of the node, a class diagram was used to describe the attributes and functions of each component. The class diagram highlighted the relationship between the various components and the way they are interconnected. To understand the behavior of the components in real time, a sequence diagram was used to describe the interactions, dataflow and control flow between the components. The advantages and disadvantages as well as the hardware and software implementation of the node architecture were discussed.

The related works on sensor network models mentioned in the thesis described the network architecture with respect to achieving a particular objective. Some of them described mechanisms to manage a heterogeneous WSN by employing a network manager node. This thesis presented an abstract view of the structure and general architecture of the network models by using a block and class diagram. The class diagram presented a hierarchical classification of the sensor nodes based upon their functions in the network. The sequence diagram described a real time data forwarding interaction between the various nodes in the network. While the related work emphasizes more on achieving the objective for which the network was designed, this research concentrated on describing the various network architectures and sensor node classification.

The WSN model for healthcare monitoring described in [Vir06] was an architecture proposed for assisted living residents consisting of body sensor network that interfaces with another sensor network monitoring the living space. All the collected information was forwarded to a main system which consisted of other supporting devices like computers and PDAs having storage and computational capabilities. Hence the architecture was confined to a particular living area. [Shy05] developed a combined hardware and software platform for medical monitoring which concentrated more on developing protocols for integrating various kinds of network devices. This research presented an abstract view of the structure and general architecture of WSN based patient monitoring system using a block diagram and class diagram. However the architecture proposed in this research could be localized and confined to a closed living space or could be widespread covering a vast area and was extended to explore the option of generating alerts in emergency situations.

7.4 Conclusions

In this research, a pattern was developed which described the structure and operations of a sensor node. This approach would guide the designer to choose different hardware components to build sensor nodes for different applications. After knowing the basic components of a sensor node, their functions and their interconnections, a designer could add new components to support new features or replace a legacy component with an advanced one to achieve some objective such as tiny form factor or minimum energy consumption [Sah10].

Based upon the sensor node pattern, a second pattern was developed that presented an abstract view of the structure and general architecture of wireless sensor network. This approach described the organization of sensor nodes and other wireless devices and the way they are connected with each other to achieve some objective, e.g. signal reach, performance, security, reliability, or other quality factors [Car10]. Finally, a third pattern was developed for a medical application involving a WSN implementing a remote patient monitoring system. This pattern describes how to select and connect sensors, medical devices and other wireless devices with each other to form a patient monitoring system.

Describing sensor nodes and WSNs as patterns provides an overall design and implementation structure sufficient to design any new application involving sensor nodes. With the help of this approach, new sensor applications could be designed more conveniently as the patterns would serve as a reference guide for selecting different sensor nodes, network architectures and implementation platforms for any application. The WSN can then be combined with a complete IT system.

7.5 Future Work

Designing a wireless sensor network is a daunting task because the designer has to select the right kind of sensor nodes, the appropriate number of sensor nodes, the right kind of protocols, the right kind of architecture and last but not the least appropriate security mechanisms for a network. Sensor networks pose unique security challenges because of their inherent limitations in communication and computing. Data is sensitive and always prone to malicious attacks and more so in a wireless environment. Future work in this area includes:

- Designing patterns for a secure sensor network architecture
- Designing patterns for a secure patient monitoring system involving sensor nodes.

REFERENCES

[Aky02] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-116, Aug. 2002.

[Ber01] B. Berkowitz, Technology catches up to runners, Washington Post, sec. E, p. 1., April 20, 2001.

[Bra02] D. Braginsky and d. Estrin, “Rumor routing algorithm for sensor networks”, Intl. orkshop on Wireless Sensor Networks and Applications, 2002.

[Bro99] F. L. Brown, J. DeVietri, G. Diaz, and E. B. Fernandez, “The Authenticator Pattern”, Proceedings of Pattern Language of Programs (PloP’99), 1999

[Bus96] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerland, and M. Stal, “Pattern-oriented Software Architecture”, Wiley, 1996.

[Car10] M. Cardei, E. B. Fernandez, and A. Sahu, “A pattern for Sensor Network Architecture”, submitted for publication, 2010.

[Cho03] C. Y. Chong, and S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," Proc. IEEE, Aug. 2003.

[Cro10] Crossbow Technology, http://www.xbow.com, last accessed on May 28, 2010.

[Fer08] E. B. Fernandez, “Software Architecture and Patterns”, Class notes. Fall 2008.

[Fer10] E. B. Fernandez, "Wireless network security for health applications", in Pervasive Communication Handbook, (M. Ilyas, Editor), CRC Press, 2010.

[Gar01] J.W. Gardner, V. K Varadan, and O. O. Awadelkarim, Microsensors,” MEMS and Smart Devices”, New York: Wiley, 2001.

[Gib03] P. B. Gibbons, B. Karp, Y. Ke, S. Nath, and S. Seshan, “IrisNet: An Architecture for a Worldwide Sensor Web”, IEEE Pervasive Computing, pp. 22-33, Oct.-Dec. 2003.

[Gob05] P. Gober, A. Ziviani, P. Todorova, M.D. Amorim, P. Hunerberg, S. Fdida, “Topology control and localization in wireless ad hoc and sensor networks”, Ad Hoc and Sensor Networks, 301–322, 1 2005.

[Gov99] E. R. Govindan, J. Heidermann, S. Kumar, “Next Century Challenges: Scalable Coordination in Sensor Networks”, Mobicom 1999.

[Hed88] S. Hedetniemi, S. Hedetniemi, and A. Liestman, “A Survey of Gossiping and Broadcasting in Communication Networks,” Networks, vol. 18, 1988.

[Hef09] M. Hefeeda and M. Bagheri, “Forest Fire Modeling and Early Detection using Wireless Sensor Networks”, Ad Hoc and Sensor Wireless Networks, Vol. 7, No. 3-4, pp.169-224, Apr. 2009.

[Hei00] W. W. Heinzelman, A. Chandrakasan, H. Balakrishnan, “Energy- Efficient Communication Protocol for Wireless Microsensor Networks”, HICS 2000.

[IEEE03] http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf., IEEE 802.15.4 specification, May 2003.

[Int00] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks”, Proc. ACM MobiCom’00, pp. 56-67, 2000.

[Jaf05] R. Jafari, A. Encarnacao, A. Zahoory, F. Dabiri, H. Noshadi, M. Sarrafzadeh, “Wireless Sensor Network for Health Monitoring”, Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous, pp 479 – 481, Jul 2005.

[Kar05] H. Karl, A. Willig, “Protocols and architectures for wireless sensor networks” Wiley, TK 7872.D48K37, 2005.

[Kim07] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, “Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks”, Procs. of the 6th International Conference on Information Processing in Sensor Networks (IPSN ’07), pp. 254-263, Apr. 2007

[Lin02] S. Lindsey, C. S. Raghavendra, “PEGASIS: Power Efficient GAthering in Sensor Information Systems”, IEEE Aerospace Conference, March 2002.

[Lub02] O. Boric-Lubecke and V. M. Lubecke, “Wireless house calls: using communications technology for health care monitoring”, IEEE Microwave Mag., v. 3, n. 3, pp. 43–48, September 2002.

[Luk07] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, “MiniSec: A Secure Sensor Network Communication Architecture”, Sixth International Conference on Information Processing in Sensor Networks (IPSN 2007), Apr. 2007.

[Mai02] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, “Wireless sensor networks for habitat monitoring”, Proc. of the 1st ACM International Workshop on Wireless Sensor Networks and Application, 2002.

[Ng06] H. S. Ng, M. L. Sim , and C.M. Tan, “ Security issues of wireless sensor networks in healthcare applications”, BT Technology Journal, Vol 24. No.2, April 2006.

[Ott06] C.Otto, A. Milenkovic, C. Sanders, and E. Jovanov, “System Architecture Of A Wireless Body Area Sensor Network For Ubiquitous Health Monitoring”, Journal of Mobile Multimedia, Vol.1, No.4, pp 307-326, Jan 2006.

[Par00] J. Pärkkä et. al., “A wireless wellness monitor for personal weight management”, Proc. IEEE EMBS Intl. Conf. on Information Technology Applications in Biomedicine, pp. 83–88, 2000.

[Per04] A. Perrig, D. Wagner, and J. Stankovic, “Security in Wireless Sensor Networks”, Communications of the ACM, Vol. 47, No. 6, pp. 53-57, Jun. 2004.

[Sah10]A. Sahu, E. B. Fernandez, and M. Cardei, “The Sensor Node Pattern”, accepted to the 17th Conf. on Pattern Languages of Programs, 2010.

[Sch06] M. Schumacher, E. B.Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, “Security Patterns: Integrating Security and Systems Engineering”, Wiley 2006.

[Shn05] V. Shnayder, B. Chen, K. Lorincz, T. R. F. FulfordJones, and Matt Welsh, “Sensor Networks for Medical Care”, Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2005.

[Vir06] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, R. Stoleru, S. Lin, and J. A. Stankovic, “An Advanced Wireless Sensor Network for Health Monitoring," at Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2), April 2006.

[Wal06] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless Sensor Network Security: A Survey”, Chapter 17 in Security in Distributed, Grid, and Pervasive Computing, Yang Xiao (Ed.), Auerbach Publications, CRC Press, 2006.

[Wer06] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. B. Johnson, J. Lees, and M. Welsh, “Deploying a Wireless Sensor Network on an Active Volcano”, IEEE Internet Computing, pp. 18-25, Mar.-Apr. 2006.

[Wir10] Wireless Sensor Networks Security, Website: http://www.wsnsecurity.info, 2010.

[Yan02] Y. Yang, U. Lu, and B. C. P. Hu, Prescription chips, IEEE Circuits Devices Mag., v. 18, n. 5, pp. 8–16, September 2002.