**Lecture One**

**Wireless Sensor Networks**

**1.1 Sensor's Background with Challenges and Constraints**

**1.1.1 Sensing and Sensors**

***Sensing***is a technique used to gather information about a physical object or process, including the occurrence of events (i.e., changes in state such as a drop in temperature or pressure). An object performing such a sensing task is called a *sensor*. For example, the human body is equipped with sensors that are able to capture optical information from the environment (eyes), acoustic information such as sounds (ears), and smells (nose). These are examples of *remote sensors*, that is, they do not need to touch the monitored object to gather information.

A ***sensor*** is a device that translates parameters or events in the physical world into signals that can be measured and analyzed. Another commonly used term is ***transducer*,** which is often used to describe a device that converts energy from one form into another. A sensor, then, is a type of transducer that converts energy in the physical world into electrical energy that can be passed to a computing system or controller.

An example of the steps performed in a sensing (or ***data acquisition***) task is shown in Figure 1.1. Phenomena in the physical world (often referred to as *process*, *system*, or *plant*) are observed by a sensor device. The resulting electrical signals are often not ready for immediate processing; therefore they pass through a *signal conditioning* stage. Here, a variety of operations can be applied to the sensor signal to prepare it for further use. For example, signals often require ***amplification*** (or attenuation) to change the signal magnitude to better match the range of the following analog-to-digital conversion. Further, signal conditioning often applies ***filters***to the signal to remove unwanted noise within certain frequency ranges (e.g., high pass filters can be used to remove 50 or 60 Hz noise picked up by surrounding power lines). After conditioning, the analog signal is transformed into a digital signal using an ***analog-to-digital converter (ADC).*** The signal is now available in a digital form and ready for further ***processing, storing, or visualization***.



Many wireless sensor networks also include ***actuators***which allow them to directly control the physical world. For example, an actuator can be a ***valve*** controlling the flow of hot water, a ***motor*** that opens or closes a door or window, or a ***pump*** that controls the amount of fuel injected into an engine. Such a *wireless sensor and actuator network* (WSAN) takes commands from the processing device (controller) and transforms these commands into input signals for the actuator, which then interacts with a physical process, thereby forming a closed control loop (also shown in Figure 1.1).

**1.1.1.1 Sensor Classifications**

**Which sensors should be chosen for an application?**

Depends on the physical property to be monitored, for example, such properties include temperature, pressure, light, or humidity. Table 1.1 summarizes some common physical properties, including examples of sensing technologies that are used to capture them. Besides physical properties, the classification of sensors can be based on a variety of other methods, for example:

1. Whether they require an ***external power supply***. If the sensors require external power, they are referred to as ***active sensors***. That is, they must emit some kind of energy (e.g., microwaves, light, sound) to trigger a response or to detect a change in the energy of the transmitted signal. On the other hand, ***passive sensors*** detect energy in the environment and derive their power from this energy input – for example, passive infrared (PIR) sensors measure infrared light radiating from objects in the proximity.



1. Electrical phenomena they utilize to convert physical properties into electrical signals. ***Resistive sensors*** rely on changes to a conductor’s electrical resistivity, ρ, based on physical properties such as temperature. The resistance, R, of a conductor can be determined as:



Where

( l ) Is the **length** of the conductor

(A) Is the **area** of the cross-section.

For example,

***Wheatstone bridge*** (Figure 1.2) is a simple circuit that can be used to **convert a physical property into an observable electric effect**. In this bridge, *R*1, *R*2, and *R*3 are resistors of known resistance (where the resistance of *R*2 is adjustable) and *Rx* is a resistor of unknown value. If the ratio*R*2*/R*1 is identical to the ratio *Rx/R*3, the measured voltage *V*OUT will be zero. However, if the resistance of *Rx* changes (e.g., due to changes in temperature), there will be an imbalance, which will be reflected by a change in voltage *V*OUT. In general, the relationship between the measured voltage *V*OUT, the resistors, and the supply voltage (VCC) can be expressed as:





1. A similar principle can be applied to ***capacitive* sensors**, which can be used to measure motion, proximity, acceleration, pressure, electric fields, chemical compositions, and liquid depth.

For example, in the parallel plate model, that is, a capacitor consisting of two parallel conductive plates separated by a dielectric with a certain **permittivity *ε***, the capacitance is determined as:



where

*A* is the plate area and *.*

*d* is the distance between the two plates.

Similar to the resistive model, changes in any of these parameters will change the ***capacitance***. For example,

if pressure is applied to one of the two plates, the separation *d* can be reduced, thereby increasing the capacitance. Similarly, a change in the permittivity of the dielectric can be caused by an increase in temperature or humidity, thereby resulting in a change in capacitance.

1. **Inductive sensors** are based on the electrical principle of inductance, that is, where an electromagnetic force is induced by a fluctuating current Change in any of these parameters (e.g., caused by movements of the core within the coil) change the inductance. Inductive sensors are often used to measure **proximity, position, force, pressure, temperature, and acceleration.**

**1.2 Challenges and Constraints**

**1.2.1 Energy**

The constraint most often associated with sensor network design is that sensor nodes operate with limited energy budgets. Typically, they are powered through batteries, which must be either replaced or recharged

Therefore, some MAC protocols for sensor networks are ***contention-free***,

that is, access to the medium is strictly regulated, eliminating collisions and allowing sensor nodes to shut down their radios when no communications are expected

**1.2.2 Self-Management**

It is the nature of many sensor network applications that they must operate in remote areas and harsh environments, without infrastructure support or the possibility for maintenance and repair. Therefore, sensor nodes must be *self-managing* in that they configure themselves, operate and collaborate with other nodes, and adapt to failures, changes in the environment, and changes in the environmental stimuli without human intervention.

**1.2.3 Wireless Networking**

The reliance on wireless networks and communications poses a number of challenges to a sensor network designer. For example, *attenuation* limits the range of radio signals, that is, a radio frequency (RF) signals fades (i.e., decreases in power) while it propagates through a medium and while it passes through obstacles. The relationship between the received power and transmitted power of an RF signal can be expressed using the *inverse-square law*:



As a consequence, an increasing distance between a sensor node and a base station rapidly increases the required transmission power. Therefore, it is more energy-efficient to split a large distance into several shorter distances, leading to the challenge of supporting *multi-hop* communications and routing.

**1.2.4 Decentralized Management**

The *large scale* and the *energy constraints* of many wireless sensor networks make it infeasible to rely on *centralized* algorithms (e.g., executed at the base station) to implement network management solutions such as topology management or routing. A decentralized approach allows each node to make routing decisions based on limited local information (e.g., a list of the node’s neighbors, including their distances to the base station and nodes energy). While this decentralized approach may lead to nonoptimal routes and the management overheads can be reduced significantly.

**1.2.5 Design Constraints (p13, Waltenegus Dargie)**

The primary goal of wireless sensor design is to create smaller, cheaper, and more efficient devices. Driven by the need to execute dedicated applications with little energy consumption, typical sensor nodes have the processing speeds and storage capacities of computer systems from several decades ago.

The need for small form factor and low energy consumption also prohibits the integration of many desirable components, such as GPS receivers. These constraints and requirements also impact the *software design at various levels*, for example, operating systems must have small memory footprints and must be efficient in their resource management tasks.

A sensor’s hardware constraints also affect the design of many *protocols and algorithms executed in a WSN*. For example, routing tables that contain entries for each potential destination in a network may be too large to fit into a sensor’s memory. Instead, only a small amount of data (such as a list of neighbors) can be stored in a sensor node’s memory

Further, while in-network processing can be employed to eliminate redundant information, some sensor fusion and aggregation algorithms may require more computational power and storage capacities than can be provided by low-cost sensor nodes

Therefore, many software architectures and solutions (operating system, middleware, and network protocols) must be designed to operate efficiently on very resource-constrained hardware.

**1.2.6 Security**

Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. Further, wireless communications make it easy for an adversary to eavesdrop on sensor transmissions

For example, one of the most challenging threats is a ***denial-of-service attack***, whose goal is to disrupt the correct operation of a sensor network. This can beachieved using a variety of attacks, including a ***jamming attack***, where high-powered wirelesssignals are used to prevent successful sensor communications.

While there are numerous techniques and solutions for distributed systems that ***prevent attacks*** or contain the extent and damage of such attacks, many of these incur significant computational, communication, and storage requirements, which often cannot be satisfied by resource-constrained sensor nodes.

From the discussion so far, it becomes clear that many design choices in a WSN differ from the design choices of other systems and networks. Table 1.2 summarizes some of the key differences between traditional networks and wireless sensor networks



**Example**

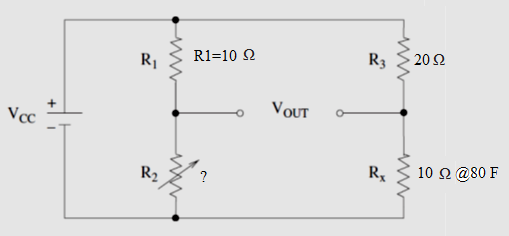
Consider a Wheatstone bridge circuit using a resistive temperature sensor *Rx* as shown In Figure. Further assume that *R*1 = 10Ωand *R*3 = 20Ω. Assume that the current temperature is F and *Rx (*80*)* = 10*Ω*. You wish to calibrate the sensor such that the output voltage *V*OUT is zero whenever the temperature is F.

(a) What is the desired value of *R*2?

(b) What is the output voltage (as a function of the supply voltage) at a temperature of

90 ◦F, when this increase in temperature leads to an increase in resistance of 20% for *Rx*?

Ans.

(a)

At balance condition,

At balance conditions,

(b)