Chapter 1: Introduction

1.1 Basics

You may have seen “sensors” in many occasions. This book targets tiny sensors that have RF (Radio Frequency) communication capabilities. Those sensors could form a wireless network, called wireless sensor networks (WSNs). Then a natural question is: why do WSN technologies advance so quickly?

WSNs become a reality because of the integration of three technologies: (1) Micro-electro-mechanical systems (MEMS), which could make sensors’ mechanic parts fit into a very tiny chip (even less than a Quarter!); (2) digital electronics, which make a tiny chip (with microcontroller) powerful enough to handle the incoming sensor data (such as data compression, data fusion, networking operations); (3) Wireless (RF) communications, which relay the sensor data among many sensors.

As shown in Figure 1.1, a WSN sensor typically includes an analog sensing chip to sense environmental parameters (such as temperature, lights, etc), a microcontroller to perform local data processing (such as data compression) and networking operations (such as communicating with a neighbor sensor), and a radio transceiver to wirelessly send / receive sensed data. The entire sensor can be powered by batteries or other power sources (such as solar) with a lifetime of several months to a few years.
In Chapter 2, we will discuss about the details of each WSN sensor component. Here please pay attention to a few important things:

(1) Figure 1.1 just lists the most important components of a WSN sensor. There could be other circuit parts depending on practical application requirements. For instance, we may put GPS receiver in a sensor to make it keep track of accurate positions. A solar panel could be used to absorb solar energy, which avoids the use of AA batteries.

(2) Do not call any device that can sense environmental parameters as “WSN sensor” due to the following facts:

Analog sensor, digital sensor, and WSN sensor: An analog sensor detects environmental parameters and changes its voltage level or other signals. Its output is a continuous, weak, noisy analog signal. A digital sensor has internal ADC (Analog-to-digital converter) and a low-capacity CPU (or called microcontroller). It can interface to a computer to display the sensed data. A WSN sensor adds RF communication capability to a digital sensor. Its CPU runs wireless network protocols such as hop-to-hop routing protocols. Moreover, the design of a WSN sensor emphasizes the tiny size, low cost and low energy consumption.

To build a practical WSN application, a WSN sensor should have the following features: tiny size, low cost and low energy consumption.

(1) Tiny size: A WSN sensor should be made very portable in order to achieve a large-
scale, convenient deployment. For instance, we may ask each patient in a nursing home to carry a few medical sensors in order to achieve anytime, anyplace monitoring. If medical sensors are large (say, larger than a cell phone), it is not convenient for a patient to carry them. As another example, if we want to achieve environmental surveillance in a large city, many tiny sensors could be dropped from a plane. If the sensors are large, it may not be easy to deploy. Moreover, it is better to make the sensors look more “hidden” in order to achieve a safe, “clean” sensing in the environment.

(2) Low cost: A WSN should be able to operate well even though there are numerous sensors (>1000s) in the network. Therefore, each sensor should have low cost for popular applications. In the future the unit price could be less than $1 each [Akyildiz02].

(3) Low energy consumption: Because each sensor is designed to be disposable, we shouldn’t expect to replace sensors’ batteries one by one, especially in a large-scale network. If we wish a WSN to operate for a long time, it should have low energy consumption.

In the future discussion, unless we specially point out which type of sensor (analog sensor, digital sensor or WSN sensor), when we use “sensors”, we mean “WSN sensors”. A “WSN sensor” is often called “mote”.

WSNs have a wide range of applications in health, military, homeland security, and others. For example, the physiological data about a patient can be monitored remotely by a doctor through a medical sensor network. While this brings lots of conveniences to the patient, it also allows the doctor to better understand the patient’s 7/24 condition. Sensor networks can also be used to detect chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. We can envision that, in future,
wireless sensor networks will be an integral part of our lives, just like the present personal computers.

Mobile ad hoc networks (MANET) [CPERKINS00] have attracted many attentions. A typical example is the wireless network among some laptops carried by mobile people. Because of the nodes’ mobility, the design objective of a MANET is to make the routing protocols adapt to quickly changing network topology.

So, what are the differences between WSN and MANET?

<table>
<thead>
<tr>
<th>WSNs and MANETs [Akyildiz02]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The number of sensors in a WSN can be several orders of magnitude higher than the nodes in a MANET. Therefore, sensors are more densely deployed.</td>
</tr>
<tr>
<td>• Due to the low cost design objective, sensors are prone to failures. But the MANET nodes (such as laptops) could be designed to have strong calculation capability.</td>
</tr>
<tr>
<td>• Most typical WSN applications do not require mobility, i.e., the sensors are stationary. But a MANET node has high mobility.</td>
</tr>
<tr>
<td>• Sensors are limited in power (typically battery-driven), computational capacities (its CPU has slow operation frequency), and memory (typically less than 100K bytes).</td>
</tr>
</tbody>
</table>

Similar to MANET, in a WSN hop-to-hop communications are necessary because of the limited RF communication distance of each sensor. For instance, most of current WSN sensors can only transmit data for less than 300 feet. It is not possible to ask a remote sensor to directly (i.e., using a single hop) communicate with a server.

Besides the limited wireless signal broadcasting distance, from energy consumption
viewpoint, a multi-hop approach is better than a single-hop case. This is because the signal energy level fades away quickly when the distance goes on:

\[ RSS \propto \frac{1}{d^\alpha} \tag{1.1} \]

Where \( RSS \) is Received Signal Strength in a receiver, \( d \) is the radio signal propagation distance between a sender and a receiver, and \( \alpha \) is the path loss ratio. Its value is typically between 2 to 5. The larger it is, the smaller the \( RSS \) is. The path loss ratio \( \alpha \) varies in different radio propagation terrains and weather conditions.

Suppose \( \alpha=2 \), if we increase the distance \( d \) for 10 times longer, the RSS will be 100 times weaker than original value. Therefore,

In WSNs, multi-hop, relay-based data communications can generally save more energy (and make the received signal stronger) than direct sender-receiver (1-hop) communications. Also remember: in WSNs, one of the top concerns is energy consumption. That is why so many WSNs communication mechanisms are proposed with energy-efficiency as the main target.

Since a WSN is a distributed system, a natural question is: how many solutions from distributed systems can be used in WSNs? Unfortunately, very little prior work can be applied and new solutions are necessary in all areas of the WSNs. Most past distributed systems research has assumed that the systems are wired, have unlimited power, have user interfaces such as screens and mice, have a fixed set of resources, treat each node in the system as very important and location independent. In contrast, for WSNs, the systems are wireless, have scarce power, utilize sensors and actuators as interfaces, have dynamically changing sets of resources, aggregate behavior is more important than individuals, and sensor location is critical. Many
WSNs also utilize minimal capacity devices to reduce manufacturing cost. This places a further strain on the ability to use past solutions.

In WSNs, a variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment. Depending on the applications and the type of sensors used, actuators may be incorporated in the sensors. However, if the sensors communicate through other strong hardware components such as an actuator, the common WSN design concerns (such as low power, low cost, short communication range, etc.) may not exist anymore. This book will focus on common WSNs with those resource constrains.

As a matter of fact, a WSN has very serious design and resource constraints [Akyildiz02] [CPERKINS00]. Resource constraints refer to a limited amount of energy, short communication range, low bandwidth, and limited processing and storage in each node. Design constraints are application dependent and depend on the monitored environment. The environment plays a key role in determining the size of the network, the deployment scheme, and the network topology. The size of the network varies with the monitored environment. For indoor environments, fewer nodes are required to form a network in a limited space. However, outdoor environments may require more nodes to cover a larger area. An ad hoc (random) deployment is preferred over pre-planned deployment when the environment is inaccessible by humans or when the network is composed of hundreds to thousands of nodes. Obstructions in the environment can also limit communication between nodes, which in turn affects the network connectivity (or topology). Research in WSNs aim to meet the above constraints by introducing new design concepts, creating or improving existing protocols, building new applications, and developing new algorithms.
Can we call a *multi-camera network* (using wireless signals) as a WSN since each camera uses light sensor(s) to capture picture pixels? If a camera does not have serious resource constraints (for instance, its memory could be over 1G bytes and its CPU could operate with more than 16 bits of bus width), we normally call such a network as ad hoc network or a general wireless network (instead of calling it a WSN). However, if each camera has serious resource constraints (for instance, it has an 8-bit CPU, <100K storage, limited radio communication distance), we could call it a WSN. Recently, people have proposed the concept of video sensor network (VSN), which consists of many low-cost video sensors. VSN is a special type of WSN. Remember: the design of WSN is so challenging because of such serious resource constraints. Without such constraints, we could easily borrow the design ideas from traditional wireless networks.

Can we call a *multi-robot system* as a WSN since each robot could have one or multiple sensors? Normally we do not call such a multi-robot network as a WSN due to the following reasons: (1) Although each robot has tiny, low-memory, slow-CPU sensor(s), it also has other circuit components that may achieve powerful CPU calculations and/or long-distance RF communications. Therefore, we cannot say that all wireless networking functionalities are achieved by those tiny sensors. In this case, we would call it as a MANET.

Can we call a *multi-vehicle network* as a WSN since each vehicle has hundreds of tiny sensors? If we limit our research in the wireless networking achieved by the tiny, RF-capable sensors in different vehicles, we may call such a case as a WSN. However, normally vehicles use strong RF antennas to keep their communications. The main challenge is the highly dynamic network topology due to vehicles’ mobility. Therefore, we call such a scenario as a vehicle ad hoc network (VANET) instead of a WSN.
After we understand general WSN concepts, a natural question is: how challenging is it to design networking protocols among tiny sensors with serious resource constraints? To answer this question, first we simply review the network protocol concepts. Later on, we will explain the design challenges in each protocol layer. If you want to know more details on protocols, please refer to other course materials such as “Computer Networks”, “Wireless Networks”, “Digital / Data Communications”, and so on.

Place Figure 1.2 here.

**Figure 1.2** WSN network protocol stack

As shown in Figure 1.2, assume a sender (sensor) reports the event data (such as fire) to a remote server (receiver). The sender needs to use multi-hop communications to relay its data through some intermediate sensors. Based on OSI standard, we have 7 layers of network protocols, i.e. Application layer, Session layer, Presentation layer, Transport layer, Routing layer, Data Link layer, and Physical layer. However, in WSNs, typically we do not need Session layer and Presentation layer. As shown in Figure 1.2, in the receiver side, we do need all 5 layers to achieve successful sensed data collections:

1. **Application Layer**: The receiver needs to display the data on the screen. The Application layer defines the sensor data display format and performs sensor database management. If the sensor data needs to be displayed in Internet web pages, the Application layer needs to understand Internet application layer protocols such as HTTP.

2. **Transport Layer**: TCP is a typical Transport layer protocol. The main functionalities of
Transport layer are to (a) achieve end-to-end (E2E) reliable data transmission; (b) reduce network congestion. TCP achieves E2E reliable transmission through packet retransmission and timeout check. TCP also reduces network congestion through data rate control. However, in WSNs, TCP is not suitable to transport layer protocol due to its high overhead. In Chapter 5 we will discuss WSNs Transport layer in details.

(3) Routing layer: It achieves hop-to-hop data forwarding among numerous sensors. It searches the optimal path that has low energy consumption, or low delay, or other good features. Once the optimal path is established, the sensed data can be relayed one-by-one by sensors. The routing layer also maintains the route in case that the network conditions change from time to time (for instance, a sensor in the path may drain its batteries).

(4) Data Link layer: While Transport layer is responsible for “end-to-end” transmission control, Data Link layer only handles neighboring (1-hop away) nodes’ communication issues. For instance, a sensor may determine whether or not it should adjust its sending rate based on its upstream and downstream sensors’ buffer setups. Sometimes Data link layer is called Medium Access Control (MAC) layer. Actually MAC is part of Data link layer tasks since MAC only takes care of the wireless medium sharing issues among 1-hop neighbors. MAC ensures that all neighboring sensors do not cause signal transmission conflicts. While a Data link layer may handles error detection, data framing, and other tasks.

(5) Physical layer: It converts meaningful data to wireless signals through encoding / modulation and other wireless communication modules. Since this layer only sees “signals” such as voltage levels (“0” or “1”), it cannot understand any higher layer issues (such as routing, data content, reliability, etc.).
In the following discussion, we will provide an overview on the design issues in different WSNs layers. [Akyildiz02] has more comprehensive review on those layers. Moreover, we will cover other important issues such as sensor localization.

1.2 MAC Layer

A medium access control (MAC) protocol coordinates signal transmissions over a shared Radio Frequency (RF) channel. When a group of sensors communicate using a radio frequency, the MAC protocol determines the communication schedules and rules since at any time only one pair of users can use the frequency to send out data to each other. The MAC protocol determines the wireless channel occupancy durations and many other things.

The most commonly used channel sharing solutions are *contention-based* scheme. In general contention-based scheme, a sensor that has a message to transmit tests the channel to see if it is busy or not. If not busy then it transmits; if it is busy it waits and tries again later. After colliding, sensors wait random amounts of time to avoid re-colliding. If two or more sensors transmit at the same time, there is a collision, and all the sensors under collision try to access the channel again later.

Many wireless MAC protocols also have a *doze* mode where sensors not involved with sending or receiving a packet in a given timeframe go into *sleep* mode to save energy. Many
variations exist on this basic scheme. An effective MAC protocol for WSNs must consume low power, avoid collisions, be implemented with a small code size and memory requirements, be efficient for a single application, and be tolerant to changing radio frequency and networking conditions.

1.3 Routing

Multi-hop route search and data forwarding are critical services required for WSN. Because of this, there has been a large amount of work on this topic. Internet and MANET routing techniques do not perform well in WSNs. For instance, most Internet routing protocols assume highly reliable wired connections (such as fiber optics or cable) where packet errors are rare; this is not true in WSNs because wireless links have high bit error rates. Many MANET routing solutions are optimized for highly mobile nodes, and they often assume symmetric links between neighbors (i.e., if node A can reliably reach node B, then B can reach A). This is often not true for WSNs. These differences have necessitated the invention and deployment of new routing solutions.

For WSNs, which are often deployed in an ad hoc (random) fashion, the routing protocol typically begins with neighbor discovery. Sensors send out rounds of messages (packets) and build local neighbor tables. These tables include the minimum information such as each neighbor’s ID. Other typical information in these tables could be sensors’ location, remaining energy, delay via that sensor, and an estimate of link quality. Once the tables are established, messages are directed from a source location to a destination address based on geographic coordinates, or IDs.

1.4 Other communication issues

Beyond the basics of WSN protocols just presented, there are many additional key issues.
In the following we list a few examples:

**Reliability**: Since messages travel multiple hops, it is important to have a high reliability on each link, otherwise the probability of a message transiting the entire network would be unacceptably low. Significant work is being done to identify reliable links using metrics such as received signal strength, link quality index (which is based on bit errors), and packet delivery ratio. Significant empirical evidence indicates that packet delivery ratio is the best metric, but it can be expensive to collect. Empirical data also shows that many links in a WSN are *asymmetric*, meaning that while node A can successfully transmit a message to node B, the reverse link from B to A may not be reliable. Asymmetric links are one reason that MANET routing algorithms do not work well in WSNs because their protocols send a discovery message from source to destination and then use the reverse path for acknowledgements. This reverse path is not likely to be reliable due to the high occurrence of asymmetry found in WSNs.

**Integration with wake / sleep schedules**: To save power many WSNs place sensors into sleep states. However, it is challenging to determine the wake / sleep schedule for a group of neighboring sensors based on the practical data transmission timing conditions.
Unicast, multicast and any cast semantics: In some cases a WSN server routes messages to a geographic destination area with a group of sensors. Should the server talk with one specific sensor in that area or all area sensors? There are several possibilities. First, the message may include a sensor ID with a specific unicast node in this area as the target. Second, the semantics could be that all sensors within the area should receive the message. This is called multicast communications. Third, it could be any sensor, called anycast, in the destination area to receive the message. There is also often a need to flood (broadcast) a command message to the entire network. Many routing schemes exist to support the above unicast, multicast, anycast or broadcast communications.

Real-Time: For some applications, messages must arrive at a destination by a deadline. Due to the high degree of uncertainty in WSNs it is difficult to develop routing algorithms with latency guarantees. WSN protocols may prioritize packet transmissions for some time-critical applications.

Mobility: Routing design becomes more challenging if either the message source or destination or both are moving. Solutions include continuously updating local neighbor tables or identifying proxy sensors which are responsible for keeping track of where sensors are. Proxy sensors for a given sensor may also change as a sensor moves further and further away from its original location.

Broken links: Since WSN sensors have a limited RF transmission range, it is possible that there are no forwarding sensors in the path where a message is supposed to travel. Or, the sensors may drain their batteries and do not work anymore. The routing protocols should be able to deal with such broken wireless links.

Security: If adversaries exist, they can perpetrate a wide variety of attacks on the WSN
protocols. Typical attacks include selective forwarding, black hole, Sybil, replays, wormhole and denial of service attacks. Security is an important area in any wireless networks due to the unreliable, broadcast-based radio signal transmissions.

Congestion: Today, many WSNs have periodic or infrequent traffic. Congestion does not seem to be a big problem for such networks. However, congestion is a problem for more demanding WSNs and is expected to be a more prominent issue with larger systems that might process audio, video and have multiple base stations (creating more cross traffic). Even in systems with a single base station, congestion near the base station is a serious problem since traffic converges at the base station. Solutions to reduce network congestion include backpressure, reducing source node transmission rates, throwing out less important messages, and using scheduling to avoid as many transmission collisions as possible.

1.5 Sensor localization

Node Localization: Node localization is the problem of determining the geographical location of each node in a WSN. If an event is detected, we need to know the exact sensor location. Localization is one of the most fundamental and difficult problems that must be solved for WSNs. Many issues need to be considered in node localization. For example, what are the pros and cons of using beacons (nodes which know their locations)? If using beacon nodes, how many and what are their communication ranges? What degree of location accuracy is required, <5 meters or <1 meter? Is the system indoors or outdoors? Is it a 2-dimentional (2D) or 3D localization problem? What is the algorithm’s communication overhead (how many command messages does it use in unit time)? How long should it take to localize a sensor? And many other issues.
For outdoor systems, equipping each node with GPS is a simple answer. However, the sensor’s cost will go up and thus such a scheme becomes unacceptable in most WSN applications. Most other solutions for localization in WSNs are either range-based or range-free. Range-based schemes use various techniques to first determine distances between nodes (range) and then compute locations using geometric principles. To determine distances, extra hardware is usually employed, e.g., using special circuit to detect the time difference between arrivals of sound and radio waves. The difference can then be converted to a distance measurement. In range-free schemes distances are not determined directly, but hop counts are used. Once the hop counts are determined, distances between nodes are estimated using an average distance per hop and then geometric principles are used to compute the location. Range-free solutions are not as accurate as range-based solutions and often require more network messages. However, they do not require extra hardware on every node.

When you propose a new WSN protocol, always keep in mind about the low-cost requirements of sensors / systems. For example, adding GPS to each sensor could solve many problems easily. However, GPS needs to use expensive satellite communication systems to receive timing /position information. Currently many commercialized sensors still cost more than $100 each unit. However, our long-term goal is to make each sensor cheaper than $1. Thus large-scale deployment becomes feasible.

1.5 Clock Synchronization

The clocks of each node in a WSN should have the same time control scheme. Clock synchronization is important for many reasons. When an event occurs in a WSN, it is often necessary to know where and when it occurred. Clocks are also used for many system and
Since clocks drift over time, they must be periodically re-synchronized. In some instances when very high accuracy is required, it is even important for nodes to account for clock drift between synchronization periods.

The NTP protocol [DLM91] used to synchronize clocks or the Internet has too heavy weight for WSNs since they require frequent message exchanges. Placing GPS on every node is too costly. Representative clock synchronization protocols that have been developed for WSNs are: RBS [JELSON02], TPSN [SGANERIWal03] and FTSP [MMAROTI04]. In RBS a reference time message is flooded to neighbors. Receivers record the time when the message is received. Nodes exchange their recorded times and adjust their clocks to achieve synchronization. Accuracies are around 30 microseconds for 1 hop. This work did not address multi-hop systems, but it could be extended to such a case.

In TPSN a spanning tree is created for the entire network. This solution assumes that all links in the spanning trees are symmetric. Then pairwise synchronization is performed along the edges of the tree starting at the root. Since there is no broadcasting as in RBS, TPSN is expensive. A key attribute of this protocol is that the timestamps are inserted into outgoing messages in the MAC layer thereby reducing non-determinism. Accuracy is in the range of 17 microseconds.

In FTSP, there are radio-layer timestamps, skew compensation with linear regression, and periodic flooding to make the protocol robust to failures and topology changes. Both transmission and reception of messages are time stamped, and differences are used to compute
and adjust clock offsets. Accuracy is in the range of 1-2 microseconds. Considerations in using a clock synchronization protocol include choosing the frequency of resynchronization, determining if clock drift between synchronization times is required, how to handle the multi-hop / network problem, and minimizing overhead costs in terms of energy and added network traffic congestion.

1.7 Power Management

Many devices such as Mica2 and MicaZ [Crossbow08] that are used in WSN run on two AA batteries. Depending on the activity level of a node, its lifetime may only be a few days if no efficient power management schemes are used. Since most systems require much longer network lifetime (a few months or even longer than 1 year), significant research has been undertaken to increase lifetime while still meeting functional requirements.

At the hardware level it is possible to add solar cells or just scavenge energy from motion or wind. For example, underwater sensors can storage energy from water current. Batteries and low power circuits are improving each year. Most hardware platforms allow multiple power saving states (off, idle, on) for each component of the device (such as the analog sensor chip, the radio transceiver, and the microcontroller). Only the components required at a particular time need to be active.

At the software level power management solutions are targeted at (i) minimizing communications since transmitting and listening for messages is energy expensive, and (ii) creating sleep/wake-up schedules for nodes or particular components of nodes. Minimizing the number of messages is a cross-cutting problem. For example, with a good MAC protocol there are fewer collisions and retries. With good routing schemes, short paths and congestion
avoidance can be achieved. Those effects reduce the number of messages sent. Efficient neighbor discovery, time synchronization, localization, query dissemination and flooding can all reduce the number of network messages thereby increasing system lifetime.

Solutions to sleep/wake-up patterns vary considerably. Many solutions attempt to keep awake the minimum number of nodes, called sentries, to provide the required sensing coverage while permitting all the others to sleep. To balance energy consumption a rotation is performed periodically where new sentries are selected for the next period of time. Another common technique is to control the duty-cycles of nodes. As an example, a node may be awake for 200 milliseconds out of each second for a 20% duty cycle. The chosen duty cycle percentage depends on application requirements, but the end result is usually a very significant savings in energy.

1.8 Special WSNs

There are many types of WSNs. For instance, if the sensors have video capture capability, the WSN is called a *video sensor network*. In the following two sections, we highlight two special WSNs: Multimedia WSNs and Underwater WSNs.

1.8.1 Wireless Multimedia Sensor Networks [Akyildiz07] [Purushottam07]

A special type of WSN technologies is called *wireless multimedia sensor network* (WMSN). Such an application poses many challenges to the traditional WSN design. As the term suggests, it collects multimedia (or video / audio) data from its sensors. Multimedia data needs quite large storage compared to the traditional data (such as floating-point value) collected by wireless sensor networks, and thus the demand for bandwidth is increased, and additional processing power is required for such networks. Despite the additional resources required for
such networks, the applications are of great interest and are used in many military and civil applications.

WMSNs will not only enhance existing sensor network applications such as tracking, home automation, and environmental monitoring, but will also enable several new applications such as:

- **Storage of potentially relevant activities.** For instance, a WMSN may be utilized to capture a criminal act in progress such as a robbery.

- **Traffic avoidance, enforcement and control systems.** For instance, a traffic light camera may watch for a license plate of a getaway car and report, to nearby police office of its recent location.

- **Advanced health care delivery.** Telemedicine sensor networks [HU03] can be integrated with 3G multimedia networks to enable health care services that can receive a distress alert and locate the distressed patients. A patient carries sensors to allow remote doctors to monitor his/her various bodily factors including temperature, blood pressure, glucose levels, ECG, breathing. Additionally, remote medical staff can monitor their patients via video and audio sensors, location sensors, motion or activity sensors, all of which can be embedded in wrist devices [HU03].

- **Automated assistance for the elderly.** WMSNs can be used to monitor, record, and study the behavior of the elderly as to identify the causes of their ailments. Networks of worn video and audio sensors can detect emergency situations and immediately connect the elderly with remote assistance services or nearby relatives.

- **Environmental monitoring.** Many projects utilizing acoustic and video sensors for habitat monitoring are being developed, in which information has to be conveyed in a time-critical
fashion. For example, oceanographers can use sets of video sensors to capture the process of sandbars evolving via image processing techniques [HOLMAN 03].

- **Person locator services.** Multimedia such as live video streams and images, along with techniques for advanced signal processing, can be used to determine the location of a missing person, or identify suspects and criminals.

- **Industrial process control.** Multimedia information such as image, temperature, pressure, as well as other parameters, could be used to direct a time-critical industrial process. Machine vision is the act of applying computer vision techniques to industry and manufacturing. Such information can be analyzed by sensor networks to support a manufacturing process such as those used in semiconductor chips, automobiles, food or pharmaceutical products. For example, in the quality control aspect of manufacturing processes, details or final products are inspected rapidly by sensors to detect defects. Also, machine vision systems are able to determine the location and orientation of parts of the product to be grasped by a robotic arm. Integrating machine vision systems with wireless multimedia sensor networks allow for the simplification of visual inspection systems and add additional flexibility for those that require continuous, high-velocity, and high-resolution operations.

WMSNs require a design approach that accounts for several important factors including bandwidth demand, power consumption, application-specific QoS requirements, ability to support heterogeneous applications, multimedia coverage, multimedia in-network processing, and integration into other network technologies. With ever increasing demand for higher resolution, and higher quality in the data collected by the sensor network, it translates into an ever increasing demand for bandwidth.

There are several approaches to the design of a WMSN [Purushottam07]. One is to use a
single-tier flat, homogeneous design with central storage. This design allows a network to expand easily with the simple addition of another sensor. Disadvantages of such a design include single-point (the central storage) failure, poor scalability (due to single-tier, centralized architecture), the limited processing capability and the limited scope of a single sensor, which disallows on-demand network utilization. For example, a surveillance network using this design would not be able to utilize multiple cameras to recognize an object and wake up on demand to perform object recognition. Another design approach is to utilize a multi-tier network, where the higher tiers include some form of central processing. This design has better scalability and can meet different cost/performance trade-off requirements. For instance, the higher capacity cameras may perform less frequent, but more powerful image processing operations. Some people propose the single-tier clustered design approach where each cluster contains a variety of sensors. This approach provides slightly more processing capability and visibility, yet one cluster cannot utilize another cluster's collected data.

1.8.2 Underwater Acoustic Sensor Networks [Akyildiz04a]

While the traditional terrestrial WSNs have many applications within population centers, several factors prevent such networks from being utilized offshore. Offshore networks (also called underwater WSNs) would require traditional WSNs have the ability to survive underwater, low-maintenance and a protocol that is tolerant of high transmission delay (due to the use of acoustic signals instead of RF ones under the water) and high bit error rates. Underwater acoustic sensor networks present many design challenges primarily due to the medium (water) in which they are placed, sensor corrosion by water, lack of sunlight, the propagation delay of acoustic signals (~1500 m/s) being $10^5$ times longer than the delay of radio
transmission (light speed), common loss of connectivity, and high packet loss. Despite these challenges, such networks do perform well for applications such as assisted navigation, disaster prevention (namely tsunami threats), environmental monitoring, mine reconnaissance, tactical surveillance, and the exploration of the depths of the sea.

Underwater acoustic networks primarily come in three distinct flavors [Akyildiz04a]:

- Static two-dimensional underwater WSNs for ocean bottom monitoring. Such networks consist of sensor nodes that anchor to the bottom of the seabed.

- Static three-dimensional underwater WSNs for ocean-column monitoring. These include networks of sensors whose depth into the water can be controlled, and may be utilized for monitoring applications of several ocean phenomena (pollution, ocean bio-activity, chemical processes, etc).

- Three-dimensional networks of autonomous underwater vehicles (AUVs). These networks include fixed portions composed of anchored sensors and additional sensors attached to autonomous vehicles to guide the piloting thereof. (As we discussed before, this type of networks are typically called MANET since the vehicles may have strong communication / data processing capabilities).

Three dimensional underwater networks are used as a means of detecting, observing, and capturing underwater phenomena that cannot be effectively observed via ocean bottom sensor nodes. In such networks, sensor nodes suspend at different depths to observe a certain phenomenon. Of the possible solutions, one would be to attach each underwater sensor to a surface buoy via wires whose length can be adjusted to control the depth of each sensor node. Although such a solution allows for ease of deployment of the sensor network, such buoys can interfere with ships passing by, or additionally they are susceptible to being located and disabled.
by enemies in military applications. Floating buoys are also vulnerable to changes in the weather, and random tampering.

With these reasons in mind, another approach would be to anchor sensor devices to the bottom rather than the top. In such an approach, each sensor device is attached to the ocean bottom and consists of a floating buoy that can be inflated by a pump. As a result of pressure, the buoy is able to push the sensor upwards to the surface. The sensor's depth can be adjusted by constricting or relaxing the length of the wire that is connected to the sensor and the anchor via an electronically controlled engine that resides on the sensor device. One challenge to such an approach is that the ocean currents can sway the devices. There are various challenges with such an architecture that needs to be resolved to enable 3D monitoring, including:

- **Sensing coverage.** Sensors should collaboratively regulate their depth to fully cover the ocean column with their sensing ranges in consideration. Thus, the network must be capable of sampling the desired phenomenon at all depths.

- **Communication coverage.** In 3D underwater networks it may be possible that the sink is not immediately reachable, therefore sensors should be able to relay data to the surface station by means of multi-hop paths. As a result, network devices must coordinate their depths to ensure that the network topology is always connected so that at least one path exists between each sensor and the sink.

AUVs, or autonomous underwater vehicles, can function without the need for tethers, cables, or remote control, thus they have a plethora of applications in the field of oceanography, environmental monitoring, as well as underwater resource study. The feasibility of inexpensive AUV submarines equipped with multiple underwater sensors that can reach any depth in the ocean has been demonstrated by prior experiments. Thus, it can be utilized to improve the
abilities of underwater sensor networks in many ways. An area of research, the integration and enhancement of fixed underwater sensor networks with AUVs, calls for new network coordination algorithms such as:

- **Adaptive sampling.** This includes control techniques to direct the mobile vehicles to locations where their collected data will be of most use. Such an approach is known as adaptive sampling. For instance, the density of sensor nodes can be adjusted in an area when a higher sampling rate is requested for a certain monitored phenomenon.

- **Self-configuration.** It involves control procedures to automatically detect connectivity gaps due to node failures or channel impairment. Moreover, AUVs may either be utilized to install and maintain the sensor network infrastructure or to install new sensors into the network. AUVs additionally may be used as temporary relay sensor nodes to restore connectivity, if only temporarily.

Although underwater sensor networks also use “wireless” media to transmit the data, it is different from terrestrial WSNs where RF signals are used. The typical unlicensed RF spectrum could be 433MHz or 2.4GHz. Underwater WSNs use “acoustic signals” as wireless media. Acoustic signals have much lower frequency than RF ones. For instance, it could be only 11KHz. However, such acoustic signals can propagate for a much longer distance than RF ones in water environments.

### 1.9 WSN Applications

In this section, we list some typical WSN applications. Many important applications are environmental monitoring. Environmental applications, such as tracking the movements of birds, insects and small animals, chemical or biological detection, large-scale earth monitoring and
planetary exploration, flood detection, forest fire detection, and pollution study, are all extremely important to protect our living environments.

Sensor networks can be strategically deployed in a forest to detect the origin of forest fires. Since these sensor networks may be unattended for large periods, efficient energy saving mechanisms and solar cell technologies may be used. The sensors perform distributed collaboration and overcome obstacles (such as trees and rocks) that block the line-of-sight of the sensors. Researchers from the University of California, Berkeley demonstrated the feasibility of sensor networking technology in a fire environment with their FireBug application [DOOLIN05]. They deployed a 10-node network in a field and successfully measured important environmental conditions such as relative humidity and temperature as a flame front passed during a prescribed burn. The fire community currently utilizes high-tech airborne infrared sensors to track flame fronts and intensities over very large scale areas.

Internet can be used by remote users to control, monitor and observe the bio-complexity of the environment. Satellite and airborne sensors are useful in observing large biodiversity, but they are not fine grain enough to observe small size biodiversity, which makes up most of the biodiversity in an ecosystem. So there is a need for ground level deployment of sensor nodes to observe the bio-complexity. Figure 1.3 below shows an Internet/WSN integrated application scenario.

Place Figure 1.3 here.

**Figure 1.3** Connect WSN to Internet

Deployments in rugged terrain and under extremely harsh conditions have just begun. A
A group of researchers from Harvard recently deployed a sensor network on an active volcano in South America to monitor seismic activity using vibration sensors. Though they only used a single-hop deployment strategy, they implemented a fairly tight time synchronization protocol to accurately correlate their data. With this system they hope to be able to monitor and help predict volcanic eruptions, earthquakes, and other similar volcanic activities [JOHNSON05].

On a smaller scale, a sensor network can be deployed on a single redwood tree using nodes to cover roughly 50 meters. With this unique deployment researchers were able to map the differences in the microclimate over a single tree.

Sensor networks deployed in natural parks and wildlife reserves closely monitor and aggregate data from animal and plant life. Earlier methods of field monitoring were error prone, tedious and potentially dangerous to plant and animal life. Data gathered from sensor networks can be studied, and useful information such as nesting patterns, flowering seasons, effects of different micro-environments can be inferred without harm to plant or animal lives. In one of the first successful demonstrations of a sensor network deployment, researchers at the University of California, Berkeley deployed a sensor network at Great Duck Island off the coast of Maine [ANDERSON02]. They placed their sensors in burrows and used heat to detect the presence of nesting birds, providing invaluable data to biological researchers. Additionally, their work provided helpful observations about many deployment aspects such as performance, routing, and topology construction. In this application, UC Berkeley Mica motes are used. The sensor uses an Atmega-103 microcontroller running at 4M Hz, 916M Hz radio from RF monolithic to provide bidirectional communication at 40kbps. 32 motes were placed at area of interest. These motes transmit sensor data to a gateway, which is responsible for forwarding the data to a remote base station. Figure 1.4 below represents the simulation scaling for the motes vs. the time delay for
busy, quiet, and inactive networks.

Place Figure 1.4 here.

**Figure 1.4** WSN delay performance [ANDERSON02]

Researchers from the UC Berkeley *Center for Embedded Networked Sensing* deployed a sensor network into the James Reserve Forest in California with purposes from soil temperature monitoring to wildlife tracking [CERPA 01]. They have used multi-hop routing and multiple, heterogeneous nodes.

Other habitat monitoring deployments that have been used for monitoring specific species include a system to monitor Cane Toad populations [BULUSU 05], and a system for tracking the movements of Zebras [JUANG 02].

WSNs have proved to be very useful in both offensive and defensive military applications. Sensor networks can be used to gather data about the existing state of a military troop. The data gathered may include the amount of equipment at hand, the ammunition and troop strength, and the location of troops. These reports are gathered and can be sent to higher levels in the clustering hierarchy of troop leaders, where an appropriate command can be taken depending on the current state of affairs. Sensors being used for battlefield surveillance are randomly deployed in inaccessible regions and critical areas for closely watching the presence of opposing forces. Moreover these networks can also be deployed to discover new approach routes and paths in scenarios without human intervention.

Target tracking is another useful military application. Sensor networks may be used to track the path of enemy troops for targeting. The analyzed data can be fed to an intelligent
ammunition system. When the target such as a vehicle is moving in sensor field, target state histories (such as spatial trajectory) have to be estimated on the basis of sensor measurements. Each sensor node provides a local measurement useful in estimating the target state. Just before or after an attack, sensor networks can be deployed in the target area to gather the battle damage assessment. Sensor networks can also be deployed in friendly detection to detect an alarm against potential nuclear, biological, or chemical attacks. The networks can be incorporated the ability to take counter measures against such attacks as well.

Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring diagnostics, drug administration in hospitals, tele-monitoring of human physiological data, and tracking and monitoring patients inside a hospital. The physiological data collected from sensors can be used for medical exploration. This data can also be stored for a long period of time. The sensor networks detect elderly people’s behavior. These small sensor nodes allow the doctors to identify pre-defined symptoms. Each sensor node has its specific task, for example, one sensor node may detect the heart rate and another detects the blood pressure. Sensor networks used for drug administration in hospitals help to minimize the chance of getting and prescribing the wrong medication to patients.

WSNs are envisioned to be ubiquitous, integrating themselves to all homes, offices and household appliances. Such devices can be connected to actuators which take an action when the environment changes to a particular state. End users could communicate with these devices to make control decisions remotely. In smart homes, the sensors make intelligent decisions such as what changes to make, what actuations to be performed based on the transforming states of the environment. The lights automatically turn on when a person enters the room at night. The temperature inside an office can vary by a few degrees. If the air flow of the room is not evenly
distributed, a distributed sensor network can be used to control the air flow and temperature. Smart sensor nodes and actuators can be placed in appliances, such as refrigerators, oven and air-conditioners so the end users can manage home via Internet or Satellite. In a warehouse, each item in the warehouse may have a sensor node attached. Thus by querying the network details of an item, the type, price, and serial number can be collected and stored in a backend database. New items are added to the inventory by attaching a new sensor to the inventories.

There are many other applications for these sensor networks. One such application is monitoring a nuclear reactor. WSNs can control the chain reaction in nuclear reactors. The sensors monitor the reaction by observing parameters like radiation and temperature. The observer uses data from sensors and maintains the nuclear reactor in a stable state. The sensor node senses information and sends to the control node. The control node aggregates the data and sends to the observer, and also checks abnormal conditions like drastic changes in radiation or temperature. If abnormal condition occurs, the control node sends information to the observer, as well as to an alarm.

Another sensor network application is suspicious individual detection. Consider a scenario in which a person is making frequent trips to a shop that sells chemicals and then also makes visits to a shop that sells firearms. Detecting such persons and placing them on a suspicious individuals list can help to determine that person’s connections and motivations. With appropriate mining of the data collected from sensors placed in the various shops, connections, links and associations, we could detect suspicious groups or individuals.

WSNs also have many applications in underground mines. The first application example is environmental data collection, where some nodes operate with a sensor module to take measurements of physical phenomena in the mine, such as temperature, luminosity or oxygen
The second example is security monitoring. For this class of applications, the nodes are placed at known positions to supervise and to detect a possible anomaly such as fire and toxic gas. The third example is the localization of an object in a supervised area. With wireless sensor networks, the objects (or persons) can be localized by simply labeling them with a small node. This task is important for many applications such as traffic management in underground mines, tracking or rescue operations.

In summary, WSNs are certainly a promising approach for a variety of applications, such as offensive and defensive military applications, environmental applications, security of buildings and spaces, measuring traffic flows, industrial sensing and diagnostics, critical infrastructure protection, and target tracking and personal location. The motivation for using wireless sensors in areas (especially areas with difficult access) is generally two-fold: cost, because wiring typically accounts for 80% of the cost of sensor installations, and safety, since we can take measurements in locations where the wiring is very difficult or impossible to install [LEGG].

The advantages of WSNs come from not only its self-organized nature (i.e. after deployment numerous sensors could automatically form a connected network), but also its “wireless” communication capabilities under harsh environments. This book does not target “wired” sensor networks since wireless media make protocol design much more challenging than wires.
1.1 Multi-choice questions:

(1) The differences between “analog sensors” and the sensors in WSNs do NOT include which of the following:

A. WSN sensors have ADC (analog-to-digital) capabilities.
B. WSN sensors have CPU (or called microcontroller) to do some local data processing.
C. Traditional analog sensors typically do not need power input.
D. Traditional analog sensors cannot self-organize themselves into a wireless network.

(2) The differences between WSNs and MANETs do NOT include which of the following:

A. WSNs typically have larger scale (more nodes) than MANETs.
B. MANETs have more mobility behaviors.
C. MANETs nodes are typically have more power storage than WSNs nodes.
D. WSNs have higher design/deployment cost than MANETs.

(3) Underwater sensor networks are different from terrestrial sensor networks due to its main feature as follows:
A. Underwater sensors typically do not use RF communications. Acoustic communications are used instead.

B. Underwater sensors are mobile while terrestrial sensors are fixed.

C. Underwater sensors are more expensive than terrestrial ones.

D. Underwater sensors typically use solar power.

(4) Wireless Multimedia Sensor networks have the following concerns:

A. They need large storage due to video/audio data.

B. They need strict QoS (quality-of-service) considerations.

C. They need large bandwidth.

D. All of the above.

(5) On WSN localization, which of the follow items is true?

A. WSN localization typically uses GPS.

B. WSN localization can easily achieve <0.1 meter accuracy.

C. WSN localization can use triangle theory to localize a node.

D. WSN localization does not need clock synchronization.

1.2 Explain the hardware architecture of a WSN sensor node. What type of CPUs can it use? List some examples after doing some web research.
1.3 What kinds of design and resource constrains does a WSN have?

1.4 Why cannot underwater sensor networks use RF communications?

1.5 Assume we use WSNs for vineyard monitoring. Conduct some web research and draw a feasible WSN system diagram (including sensors, sink, Internet server, etc.) to achieve such an application.