UNIT-I

WIRELESS SENSOR NETWORKS & ARCHITECTURES

1.1 KEY DEFINITIONS OF SENSOR NETWORKS:

Definition: A Sensor Network is composed of a large number of sensor nodes, which are tightly positioned either inside the phenomenon or very close to it.

Sensor networks have the contribution from signal processing, networking and protocols, databases and information management, distributed algorithms, and embedded systems and architecture.

A wireless sensor network (WSN) can be defined as a network of low-size and low-complex devices denoted as nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links.

The following are the *Key terms and concepts* that will be used in sensor network development techniques.

- *Sensor:* A transducer that converts a physical phenomenon such as heat, light, sound, or motion into electrical or other signals that may be further operated by other apparatus.
- *Sensor node:* A basic unit in a sensor network, with on-board sensors, processor, memory, wireless modem, and power supply. It is often abbreviated as *node*. When a node has only a single sensor on board, the node is sometimes referred as a *sensor*.
- *Network topology:* A connectivity graph where nodes are sensor nodes and edges are communication links. In a wireless network, the link represents a one-hop connection, and the neighbors of a node are those within the radio range of the node.
- *Routing:* The process of determining a network path from a packet source node to its destination.
- *Date-centric:* Approaches that name, route, or access a piece of data via properties, such as physical location, that are external to a communication network. This is to be contrasted with addresscentric approaches which use logical properties of nodes related to the network structure.
- *Geographic routing:* Routing of data based on geographical features such as locations or regions. This is an example of datecentric networking.
- *In-network:* A style of processing in which the data is processed and combined near where the data is generated.
- *Collaborative processing:* Sensors cooperatively processing data from multiple sources in order to serve a high-level task. This typically requires communication among a set of nodes.
- *State:* A snapshot about a physical environment (e.g., the number of signal sources, their locations or spatial extent, speed of movement), or a snapshot of the system itself (e.g.,the network state).
- *Uncertainty:* A condition of the information caused by noise in sensor measurements, or lack of knowledge in models. The uncertainty affects the system’s ability to estimate the state accurately and must be carefully modeled. Because of the ubiquity of uncertainty in the data, many sensor network estimation problems are cast in a statistical framework. For example, one may use a covariance matrix to characterize the uncertainty in a Gaussian-like process or more general probability distributions for non-Gaussian processes.

- *Task:* Either high-level system tasks which may include sensing, communication, processing, and resource allocation, or application tasks which may include detection, classification, localization, or tracking.

- *Detection:* The process of discovering the existence of a physical phenomenon. A threshold- based detector may flag a detection whenever the signature of a physical phenomenon is determined to be significant enough compared with the threshold.
- *Classification:* The assignment of class labels to a set of physical phenomena being observed.
- *Localization and tracking:* The estimation of the state of a physical entity such as a physical phenomenon or a sensor node from a set of measurements. Tracking produces a series of estimates over time.
- *Value of information or information utility:* A mapping of data to a scalar number, in the context of the overall system task and knowledge. For example, information utility of a piece of sensor data may be characterized by its relevance to an estimation task at hand and computed by a mutual information function.
- *Resource:* Resources include sensors, communication links, processors, on-board memory, and node energy reserves. Resource allocation assigns resources to tasks, typically optimizing some performance objective.
- *Sensor tasking:* The assignment of sensors to a particular task and the control of sensor state (e.g., on/off, pan/tilt) for accomplishing the task.
- *Node services:* Services such as time synchronization and node localization that enable applications to discover properties of a node and the nodes to organize themselves into a useful network.
- *Data storage:* Sensor information is stored, indexed, and accessed by applications. Storage may be local to the node where the data is generated, load-balanced across a network, or anchored at a few points (warehouses).
- *Embedded operating system (OS):* The run-time system support for sensor network applications. An embedded OS typically provides an abstraction of system resources and a set of utilities.
- *System performance goal:* The abstract characterization of system properties. Examples include scalability, robustness, and network longevity, each of which may be measured by a set of evaluation metrics.
- *Evaluation metric:* A measurable quantity that describes how well the system is performing on some absolute scale. Examples include packet loss (system), network dwell time (system), track loss (application), false alarm rate (application), probability of correct association (application), location error (application), or processing latency (application/system). An evaluation method is a process for comparing the value of applying the metrics on an experimental system with that of some other benchmark system.

1.2 ADVANTAGES OF SENSOR NETWORKS:

Networked sensing offers unique advantages over traditional centralized approaches. Dense/ compressed networks of distributed communicating sensors can improve signal-to-noise ratio (SNR) by reducing average distances from sensor to source of signal, or target. Increased energy efficiency in communications is enabled by the multi-hop topology of the network. A decentralized sensing system is inherently more strong against individual sensor node or link failures, because of redundancy in the network.

1.2.1 Energy Advantage:

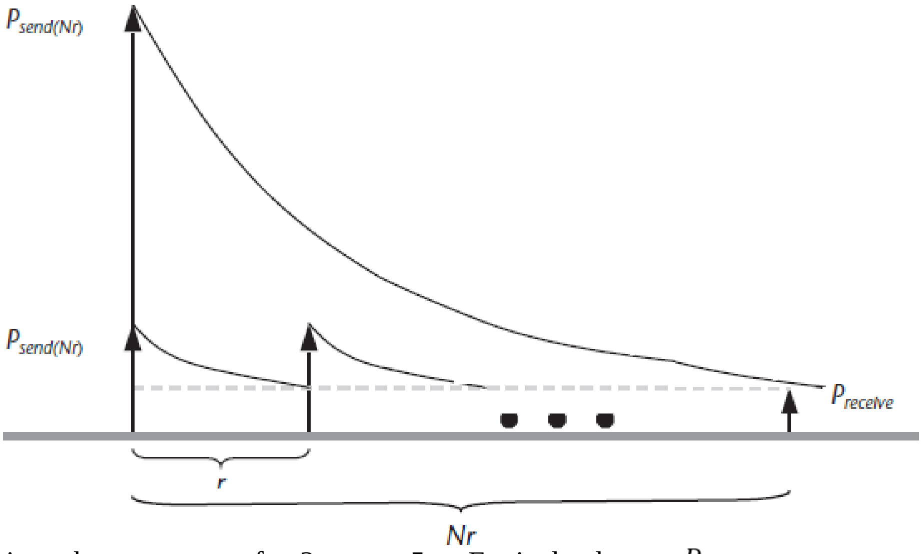
Because of the unique attenuation characteristics of radio-frequency (RF) signals, a multi-hop RF network provides a significant energy saving over a single-hop network for the same distance. Consider the following simple example of an *N*-hop network. Assume the overall distance for transmission is *Nr*, where *r* is the one-hop distance. The minimum receiving power at a node for a given transmission error rate is *Preceive*, and the power at a transmission node is

Psend. Then, the RF attenuation model near the ground is given by $P_{receive} \propto \frac{P_{send}}{r^{\propto}}$, where *r* is the transmission distance and *α* is the RF attenuation exponent. Due to multipath and other interference effects, *α* Therefore, the power advantage of an *N*-hop transmission versus a single-hop transmission over the same distance *Nr* is

$$\eta_{rf} = \frac{P_{send(Nr)}}{N.P_{send(r)}} = \frac{(Nr)^{\propto}P_{receive}}{N.r^{\propto}P_{receive}} = N^{\propto -1} \qquad \propto r^{\propto}P_{receive}$$

=-- (1)

Figure 1.1 illustrates the power attenuation for the multi-hop and single-hop networks. A larger *N* gives a larger power saving due to the consideration of RF energy alone. However, this analysis ignores the power usage by other components of an RF circuitry. Using more nodes increases not only the cost, but also the power consumption of these other RF components. In practice, an optimal design seeks to balance the two conflicting factors for an overall cost and energy efficiency. Latency and robustness considerations may also



is typically in the range of 2 to 5. Equivalently, P_{send} .

argue against an unduly large number of relay nodes.

Figure 1.1: The power advantage of using a multi-hop RF communication over a distance of *Nr*

1.2.2 Detection Advantage:

Each sensor has a finite sensing range, determined by the noise floor at the sensor.A denser sensor field improves the odds of detecting a signal source within the range. Once a signal source is inside the sensing range of a sensor, further increasing the sensor density decreases the average distance from a sensor to the signal source, hence improving the signal-to-noise ratio (SNR). Let us consider the acoustic sensing case in a two-dimensional plane, where the

acoustic power received at a distance *r* is $P_{receive} \propto \frac{P_{source}}{r^2}$, which assumes an inverse distance squared attenuation. The SNR is given by

$$SNR_r = 10\log\frac{P_{receive}}{P_{Noise}} = 10\log\ P_{Source} - 10\log\ P_{Noise} - 20\log r \text{-----------------------------} (2)$$

Increasing the sensor density by a factor of *k* reduces the average distance to a target by a factor of Thus, the $\frac{1}{k}$ SNR advantage of the denser sensor network is

$$\eta_{snr} = SNR_{\frac{r}{k}} - SNR_r = 20\log\ \frac{r}{\frac{r}{k}} = 10\log k \text{----------------------------} (3)$$

Hence, an increase in sensor density by a factor of *k* improves the SNR at a sensor by 10 log *k* db.

1.3 UNIQUE CONSTRAINTS AND CHALLENGES:

1.3.1 Constraints: A sensor network has a unique set of resource constraints problems such as finite on-board battery power and limited network communication bandwidth. A sensor network consists of circulated self-governing sensors to monitor physical or environmental conditions. WSN consist of an array of sensors, each sensor network node has typically several parts such as radio, transceiver, antenna and microcontroller. A Base station links the sensor network to another network to advertise the data sensed for future processing. Each sensor node communicates wirelessly with a few other local nodes within its radio communication range. Sensor networks extend the existing Internet deep into the physical environment.

One of the biggest Constraint/problem of sensor network is power consumption. To solve this issue two methods are defined. First method is to introduce aggregation points(An aggregation is a collection, or the gathering of things together). This reduces total number of messages exchanged between nodes and saves some energy. Usually aggregation points are ordinary nodes that receive data from neighbouring nodes, execute processing and then forward the filtered data to next hop.

Real-time is a very important constraint in WSNs, because real-world conditions can introduce explicit or implicit time constraints. These networks are supposed to sense signals in the environment, and concepts like “data freshness” are important in its applications. This way, in some application, time-based/temporal validity in data collect by nodes can expire very quickly.

1.3.2 Challenges: The challenges we face in designing sensor network systems and applications include Limited hardware, Limited support for networking, Limited support for software development.

- *Limited hardware:* Each node has limited processing, storage, and communication capabilities, and limited energy supply and bandwidth.
- *Limited support for networking:* The network is peer-to-peer, with a mesh topology and dynamic, mobile, and unreliable connectivity. There are no universal routing protocols or central registry services. Each node acts both as a router and as an application host.
- *Limited support for software development:* The tasks are typically real-time and massively distributed, involve dynamic teamwork among nodes, and must handle multiple competing events. Global properties can be specified only via local instructions. Because of the coupling between applications and system layers, the software architecture must be codesigned with the information processing architecture

1.4. DRIVING APPLICATIONS:

Sensor networks may consist of many different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of conditions. These sensor nodes can be put for continuous sensing, location sensing, motion sensing and event detection. The idea of micro-sensing and wireless connection of these sensor nodes promises many new application areas. A few examples of their applications are as follows:

A. Area monitoring applications

Area monitoring is a very common application of WSNs. In area monitoring, the WSN is deployed over a region where some physical activity or phenomenon is to be monitored. When the sensors detect the event being monitored (sound, vibration), the event is reported to the base station, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can be deployed in security systems to detect motion of the unwanted, traffic control system to detect the presence of high-speed vehicles. Also WSNs finds huge application in military area for battleeld surveillance, monitoring friendly forces, equipment and ammunition, reconnaissance of opposing forces and terrain, targeting and battle damage assessment .

B. Environmental applications

A few environmental applications of sensor networks include forest fire detection, green house monitoring, landslide detection, air pollution detection and flood detection. They can also be used for tracking the movement of insects, birds and small animals, planetary exploration, monitoring conditions that affect crops and livestock and facilitating irrigation.

C. Health applications

Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, monitoring the movements and internal processes of insects or other small animals, telemonitoring of human physiological data, and tracking and monitoring doctors and patients inside a hospital.

D. Industrial applications

WSNs are now widely used in industries, for example in machinery condition-based maintenance. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors. They can also be used to measure and monitor the water levels within all ground wells and monitor leachate accumulation and removal.

E. Other applications

Sensor networks now find huge application in our day-to-day appliances like vacuum cleaners, micro-wave ovens, VCRs and refrigerators. Other commercial applications includes constructing smart office spaces, monitoring product quality, managing inventory, factory instrumentation and many more.

1.5 ENABLING TECHNOLOGIES FOR WIRELESS SENSOR NETWORKS:

Building such wireless sensor networks has only become possible with some fundamental advances in enabling technologies.

First technology is the miniaturization of hardware. Smaller feature sizes in chips have driven down the power consumption of the basic components of a sensor node to a level that the constructions of WSNs can be planned. This is particularly relevant to microcontrollers and memory chips and the radio modems which are responsible for wireless communication have become much more energy efficient. Reduced chip size and improved energy efficiency is accompanied by reduced cost.

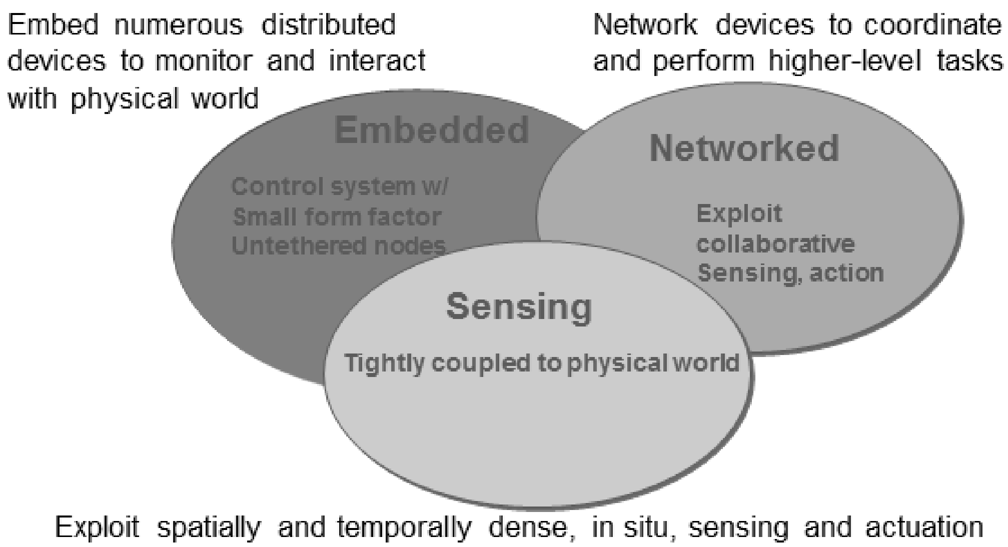

Embed numerous distributed devices to monitor and interact with physical world
Network devices to coordinate and perform higher-level tasks
Embedded
Control system w/ Small form factor Untethered nodes
Networked
Exploit collaborative Sensing, action
Sensing
Tightly coupled to physical world
Exploit spatially and temporally dense, in situ, sensing and actuation

Figure 1.2: Enabling Technologies

Second one is processing and communication and the actual sensing equipment is the third relevant technology. Here, however, it is difficult to generalize because of the vast range of possible sensors.

These three basic parts of a sensor node have to accompanied by power supply. This requires, depending on application, high capacity batteries that last for long times, that is, have only a negligible self-discharge rate, and that can efficiently provide small amounts of current. Ideally, a sensor node also has a device for **energy scavenging**, recharging the battery with energy gathered from the environment – solar cells or vibration-based power generation are conceivable options. Such a concept requires the battery to be efficiently chargeable with small amounts of current, which is not a standard ability. Both batteries and energy scavenging are still objects of ongoing research.

The counterpart to the basic hardware technologies is software. This software architecture on a single node has to be extended to a network architecture, where the division of tasks between nodes, not only on a single node, becomes the relevant question-for example, how to structure interfaces for application programmers. The third part to solve then is the question of how to design appropriate communication protocols.

SINGLE-NODE ARCHITECTURE:

1.6 **HARDWARE COMPONENTS:** Choosing the hardware components for a wireless sensor node, obviously the applications has to consider size, costs, and energy consumption of the nodes. A basic sensor node comprises five main components such as Controller, Memory, Sensors and Actuators, Communication devices and Power supply Unit.

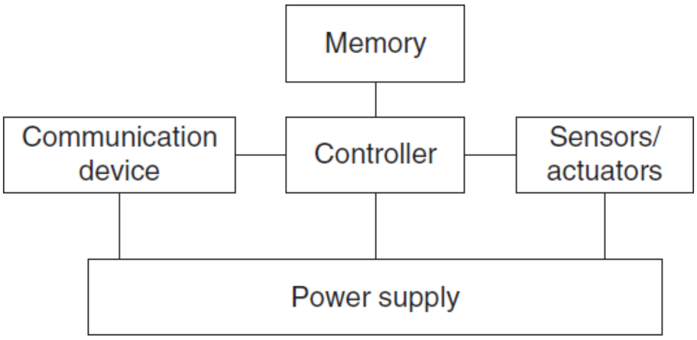


Figure 1.3: Sensor node Hardware components

1.6.1 Controller: A controller to process all the relevant data, capable of executing arbitrary code. The controller is the core of a wireless sensor node. It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes, and decides on the actuator’s behavior. It has to execute various programs, ranging from time- critical signal processing and communication protocols to application programs; it is the Central Processing Unit (CPU) of the node.

For General-purpose processors applications microcontrollers are used. These are highly overpowered, and their energy consumption is excessive. These are used in embedded systems. Some of the key characteristics of microcontrollers are particularly suited to embedded systems are their flexibility in connecting with other devices like sensors and they are also convenient in that they often have memory built in.

A specialized case of programmable processors are Digital Signal Processors (DSPs). They are specifically geared, with respect to their architecture and their instruction set, for processing large amounts of vectorial data, as is typically the case in signal processing applications. In a wireless sensor node, such a DSP could be used to process data coming from a simple analog, wireless communication device to extract a digital data stream. In broadband wireless communication, DSPs are an appropriate and successfully used platform.

An FPGA can be reprogrammed (or rather reconfigured) “in the field” to adapt to a changing set of requirements; however, this can take time and energy – it is not practical to reprogram an FPGA at the same frequency as a microcontroller could change between different programs.

An ASIC is a specialized processor, custom designed for a given application such as, for example, high-speed routers and switches. The typical trade-off here is loss of flexibility in return for a considerably better energy efficiency and performance. On the other hand, where a microcontroller requires software development, ASICs provide the same functionality in hardware, resulting in potentially more costly hardware development.

Examples: Intel Strong ARM, Texas Instruments MSP 430, Atmel ATmega.

1.6.2 Memory: Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data. In WSN there is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on. While RAM is fast, its main disadvantage is that it loses its content if power supply is interrupted. Program code can be stored in Read-Only Memory (ROM) or, more typically, in Electrically Erasable Programmable Read-Only Memory (EEPROM) or flash memory (the later being similar to EEPROM but allowing data to be erased or written in blocks instead of only a byte at a time). Flash memory can also serve as intermediate storage of data in case RAM is insufficient or when the power supply of RAM should be shut down for some time.

1.6.3 Communication Device: Turning nodes into a network requires a device for sending and receiving information over a wireless channel.

Choice of transmission medium: The communication device is used to exchange data between individual nodes. In some cases, wired communication can actually be the method of choice and is frequently applied in many sensor networks. The case of wireless communication is considerably more interesting because it include radio frequencies. Radio Frequency (RF)- based communication is by far the most relevant one as it best fits the requirements of most WSN applications.

Transceivers: For Communication, both transmitter and receiver are required in a sensor node to convert a bit stream coming from a microcontroller and convert them to and from radio waves. For two tasks a combined device called transceiver is used.

Transceiver structure has two parts as Radio Frequency (RF) front end and the baseband part.

1. The radio frequency front end performs analog signal processing in the actual radio frequency Band.
2. The baseband processor performs all signal processing in the digital domain and communicates with a sensor node's processor or other digital circuitry.

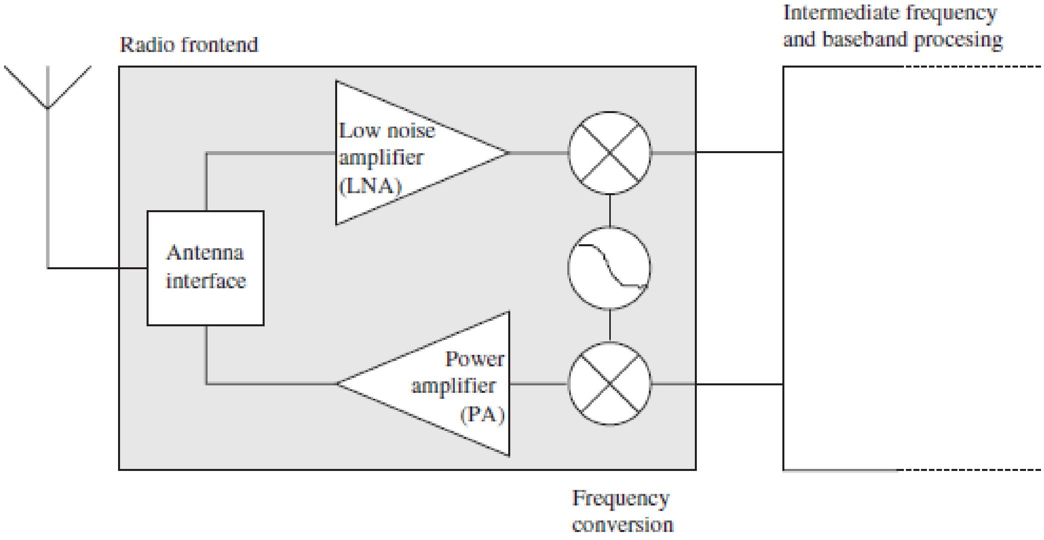


Figure 1.4: RF front end

- ✓ The Power Amplifier (PA) accepts upconverted signals from the IF or baseband part and amplifies them for transmission over the antenna.
- ✓ The Low Noise Amplifier (LNA) amplifies incoming signals up to levels suitable for further processing without significantly reducing the SNR. The range of powers of the incoming signals

varies from very weak signals from nodes close to the reception boundary to strong signals from nearby nodes; this range can be up to 100 dB.

- ✓ Elements like local oscillators or voltage-controlled oscillators and mixers are used for frequency conversion from the RF spectrum to intermediate frequencies or to the baseband. The incoming signal at RF frequencies f_{RF} is multiplied in a mixer with a fixed- frequency signal from the local oscillator (frequency f_{LO}). The resulting intermediate- frequency signal has frequency $f_{LO} - f_{RF}$. Depending on the RF front end architecture, other elements like filters are also present.

Transceiver tasks and characteristics:

- *Service to upper layer:* A receiver has to offer certain services to the upper layers, most notably to the Medium Access Control (MAC) layer. Sometimes, this service is packet oriented; sometimes, a transceiver only provides a byte interface or even only a bit interface to the microcontroller.
- *Power consumption and energy efficiency:* The simplest interpretation of energy efficiency is the energy required to transmit and receive a single bit.
- *Carrier frequency and multiple channels:* Transceivers are available for different carrier frequencies; evidently, it must match application requirements and regulatory restrictions.
- *State change times and energy:* A transceiver can operate in different modes: sending or receiving, use different channels, or be in different power-safe states.
- *Data rates:* Carrier frequency and used bandwidth together with modulation and coding determine the gross data rate.
- *Modulations:* The transceivers typically support one or several of on/off-keying, ASK, FSK, or similar modulations.
- *Coding:* Some transceivers allow various coding schemes to be selected.
- *Transmission power control:* Some transceivers can directly provide control over the transmission power to be used; some require some external circuitry for that purpose. Usually, only a discrete number of power levels are available from which the actual transmission power can be chosen. Maximum output power is usually determined by regulations.
- *Noise figure:* The noise figure NF of an element is defined as the ratio of the Signal-to- Noise Ratio (SNR) ratio SNR_I at the input of the element to the SNR ratio SNR_O at the element's output: NF= $\frac{SNR_I}{SNR_O}$. It describes the degradation of SNR due to the element's

  operation and is typically given in dB: NF dB= SNR_I dB − SNR_O dB.
- *Gain:* The gain is the ratio of the output signal power to the input signal power and is typically given in dB. Amplifiers with high gain are desirable to achieve good energy efficiency.
- *Power efficiency*: The efficiency of the radio front end is given as the ratio of the radiated power to the overall power consumed by the front end; for a power amplifier, the efficiency describes the ratio of the output signal's power to the power consumed by the overall power amplifier.
- *Receiver sensitivity*: The receiver sensitivity (given in dBm) specifies the minimum signal power at the receiver needed to achieve a prescribed E_b/N_0 or a prescribed bit/packet error rate.
- *Range:* The range of a transmitter is clear. The range is considered in absence of interference; it evidently depends on the maximum transmission power, on the antenna characteristics.
- *Blocking performance:* The blocking performance of a receiver is its achieved bit error rate in the presence of an interferer.
- *Out of band emission:* The inverse to adjacent channel suppression is the out of band emission of a transmitter. To limit disturbance of other systems, or of the WSN itself in a multichannel setup, the transmitter should produce as little as possible of transmission power outside of its prescribed bandwidth, centered around the carrier frequency.

- *Carrier sense and RSSI*: In many medium access control protocols, sensing whether the wireless channel, the carrier, is busy (another node is transmitting) is a critical information. The receiver has to be able to provide that information. the signal strength at which an incoming data packet has been received can provide useful information a receiver has to provide this information in the Received Signal Strength Indicator (RSSI).
- *Frequency stability*: The frequency stability denotes the degree of variation from nominal center frequencies when environmental conditions of oscillators like temperature or pressure change.
- *Voltage range***:** Transceivers should operate reliably over a range of supply voltages.

  Otherwise, inefficient voltage stabilization circuitry is required.

1.6.4 Sensors and actuators: The actual interface to the physical world: devices that can observe or control physical parameters of the environment.

Sensors can be roughly categorized into three categories as

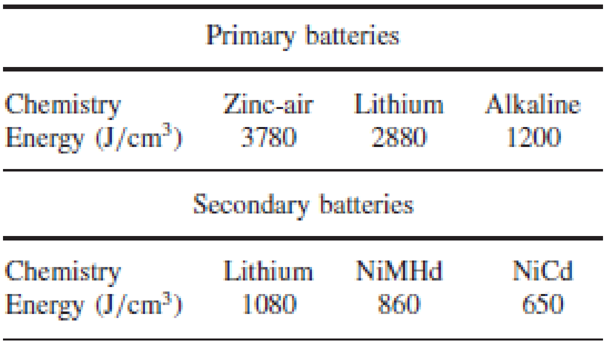
- *Passive, omnidirectional sensors***:** These sensors can measure a physical quantity at the point of the sensor node without actually manipulating the environment by active probing – in this sense, they are passive. Moreover, some of these sensors actually are self-powered in the sense that they obtain the energy they need from the environment – energy is only needed to amplify their analog signal.
- **Passive, narrow-beam sensors** These sensors are passive as well, but have a well- defined notion of direction of measurement.
- **Active sensors** This last group of sensors actively probes the environment, for example, a sonar or radar sensor or some types of seismic sensors, which generate shock waves by small explosions. These are quite specific – triggering an explosion is certainly not a lightly undertaken action – and require quite special attention.

Actuators: Actuators are just about as diverse as sensors, yet for the purposes of designing a WSN that converts electrical signals into physical phenomenon.

1.6.5 Power supply: As usually no tethered power supply is available, some form of batteries are necessary to provide energy. Sometimes, some form of recharging by obtaining energy from the environment is available as well (e.g. solar cells). There are essentially two aspects: Storing energy and Energy scavenging.

Storing energy: Batteries

- *Traditional batteries:* The power source of a sensor node is a battery, either non- rechargeable ("primary batteries") or, if an energy scavenging device is present on the node, also rechargeable



Primary batteries			
Chemistry	Zinc-air	Lithium	Alkaline
Energy (J/cm^3)	3780	2880	1200
Secondary batteries			
Chemistry	Lithium	NiMHd	NiCd
Energy (J/cm^3)	1080	860	650

(“secondary batteries”).

TABLE 1.1: Energy densities for various primary and secondary battery types

Upon these batteries the requirements are

- *Capacity:* They should have high capacity at a small weight, small volume, and low price. The main metric is energy per volume, J/cm^3.
- Capacity under load: They should withstand various usage patterns as a sensor node can consume quite different levels of power over time and actually draw high current in certain operation modes.
- *Self-discharge:* Their self-discharge should be low. Zinc-air batteries, for example, have only a very short lifetime (on the order of weeks).
- *Efficient recharging:* Recharging should be efficient even at low and intermittently available recharge power.
- *Relaxation*: Their relaxation effect – the seeming self-recharging of an empty or almost empty battery when no current is drawn from it, based on chemical diffusion processes within the cell – should be clearly understood. Battery lifetime and usable capacity is considerably extended if this effect is leveraged.
- *DC–DC Conversion:* Unfortunately, batteries alone are not sufficient as a direct power source for a sensor node. One typical problem is the reduction of a battery's voltage as its capacity drops. A DC – DC converter can be used to overcome this problem by regulating the voltage delivered to the node's circuitry. To ensure a constant voltage even though the battery's supply voltage drops, the DC – DC converter has to draw increasingly higher current from the battery when the battery is already becoming weak, speeding up battery death. The DC – DC converter does consume energy for its own operation, reducing overall efficiency.

Energy scavenging: Depending on application, high capacity batteries that last for long times, that is, have only a negligible self-discharge rate, and that can efficiently provide small amounts of current. Ideally, a sensor node also has a device for **energy scavenging**, recharging the battery with energy gathered from the environment – solar cells or vibration-based power generation are conceivable options.

- *Photovoltaics:* The well-known solar cells can be used to power sensor nodes. The available power depends on whether nodes are used outdoors or indoors, and on time of day and whether for outdoor usage. The resulting power is somewhere between 10 μW/cm^2 indoors and 15 mW/cm^2 outdoors. Single cells achieve a fairly stable output voltage of about 0.6 V (and have therefore to be used in series) as long as the drawn current does not exceed a critical threshold, which depends on the light intensity. Hence, solar cells are usually used to recharge secondary batteries.
- *Temperature gradients*: Differences in temperature can be directly converted to electrical energy.
- *Vibrations:* One almost pervasive form of mechanical energy is vibrations: walls or windows in buildings are resonating with cars or trucks passing in the streets, machinery often has low frequency vibrations. both amplitude and frequency of the vibration and ranges from about 0.1 μW/cm^3 up to 10, 000 μW/cm^3 for some extreme cases. Converting vibrations to electrical energy can be undertaken by various means, based on electromagnetic, electrostatic, or piezoelectric principles.
- *Pressure variations:* Somewhat akin to vibrations, a variation of pressure can also be used as a power source.
- *Flow of air/liquid:* Another often-used power source is the flow of air or liquid in wind mills or

turbines. The challenge here is again the miniaturization, but some of the work on millimeter scale MEMS gas turbines might be reusable.

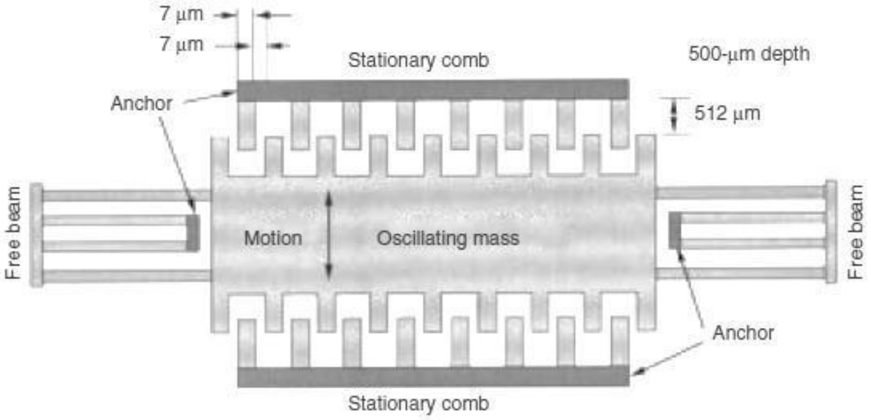
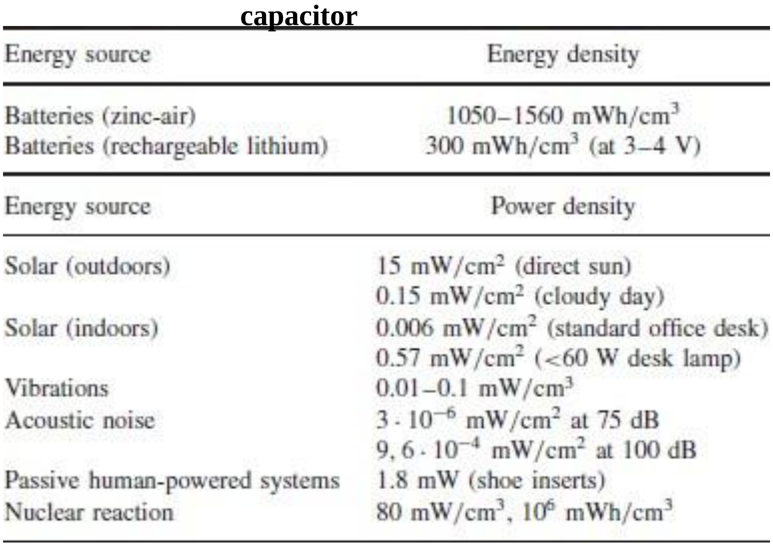


Figure 1.5 A MEMS device for converting vibrations to electrical energy, based on a variable capacitor



Energy source	Energy density
Batteries (zinc-air) Batteries (rechargeable lithium)	1050–1560 mWh/cm^3 300 mWh/cm^3 (at 3–4 V)
Energy source	Power density
Solar (outdoors)	15 mW/cm^2 (direct sun) 0.15 mW/cm^2 (cloudy day)
Solar (indoors)	0.006 mW/cm^2 (standard office desk) 0.57 mW/cm^2 (<60 W desk lamp)
Vibrations	0.01–0.1 mW/cm^3
Acoustic noise	$3 \cdot 10^{-6}$ mW/cm^2 at 75 dB $9,6 \cdot 10^{-4}$ mW/cm^2 at 100 dB
Passive human-powered systems	1.8 mW (shoe inserts)
Nuclear reaction	80 mW/cm^3, 10^6 mWh/cm^3

TABLE 1.2: Comparison of energy sources

1.7 ENERGY CONSUMPTION OF SENSOR NODES:

In previous section we discussed about energy supply for a sensor node through batteries that have small capacity, and recharging by energy scavenging is complicated and volatile. Hence, the energy consumption of a sensor node must be tightly controlled. The main consumers of energy are the controller, the radio front ends, the memory, and type of the sensors. One method to reduce power consumption of these components is designing low- power chips, it is the best starting point for an energy-efficient sensor node. But any advantages gained by such designs can easily be squandered/ wasted when the components are improperly operated. Second method for energy efficiency in wireless sensor node is reduced functionality by using multiple states of operation with reduced energy consumption. These modes can be introduced for all components of a sensor node, in particular, for controller, radio front end, memory, and sensors.

1.7.1 Microcontroller energy consumption: For a controller, typical states are "active", "idle", and "sleep". A radio modem could turn transmitter, receiver, or both on or off. At time t_1, the microcontroller is to be put into sleep mode should be taken to reduce power consumption from P_{active} to P_{sleep}. If it remains active and the next event occurs at time t_{event}, then a total energy is $E_{active} = P_{active} (t_{event} - t_1)$. On the other hand, requires a time τ_{down} until sleep mode has been reached. Let the average power consumption during this phase is $(P_{active} + P_{sleep})/2$. Then, P_{sleep} is consumed until t_{event}. The energy saving is given by

$$E_{saved} = (t_{event} - t_1)P_{active} - (\tau_{down} (P_{active} + P_{sleep})/2 + (t_{event} - t_1 - \tau_{down})P_{sleep}) \text{ -----} (4)$$

Once the event to be processed occurs, however, an additional overhead of $E_{overhead}$

$$= \tau_{Up} (P_{active} + P_{sleep})/2 \text{ -----------------------------------} (5)$$

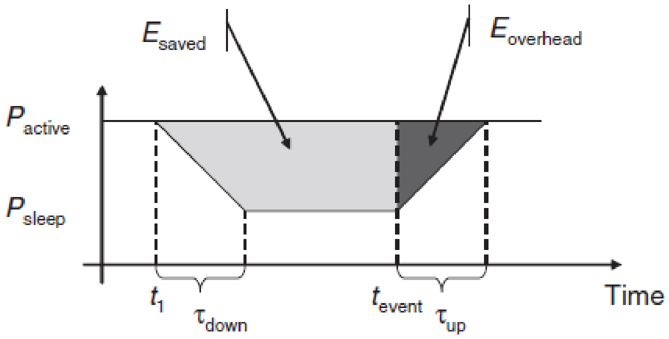


Figure 1.6 Energy savings and overheads for sleep modes

Switching to a sleep mode is only beneficial if $E_{overhead} < E_{saved}$ or, equivalently, if the time to the next event is sufficiently large: ------------------------------- $(t_{event} - t_1) > \frac{1}{2}\left(\tau_{down} + \frac{P_{active} + P_{sleep}}{P_{active} - P_{sleep}}\tau_{up}\right)$ ----------------- (6)

Examples:

Intel StrongARM

The Intel StrongARM provides three sleep modes:

- ✓ In *normal mode*, all parts of the processor are fully powered. Power consumption is up to 400 mW.
- ✓ In *idle mode*, clocks to the CPU are stopped; clocks that pertain to peripherals are active. Any interrupt will cause return to normal mode. Power consumption is up to 100 mW.
- ✓ In *sleep mode*, only the real-time clock remains active. Wakeup occurs after a timer interrupt and takes up to 160 ms. Power consumption is up to 50 µW.

Texas Instruments MSP 430

The MSP430 family features a wider range of operation modes: One fully operational mode, which consumes about 1.2 mW (all power values given at 1 MHz and 3 V). There are four sleep modes in total. The deepest sleep mode, LPM4, only consumes 0.3 µW, but the controller is only woken up by external interrupts in this mode. In the next higher mode, LPM3, a clock is also till running, which can be used for scheduled wake ups, and still consumes only about 6 µW. **Atmel ATmega**

The Atmel ATmega 128L has six different modes of power consumption, which are in principle similar to the MSP 430 but differ in some details. Its power consumption varies between 6 mW and 15 mW in idle and active modes and is about 75 µW in power-down modes.

1.7.2 Memory energy consumption: The most relevant kinds of memory are on-chip memory and FLASH memory. Off-chip RAM is rarely used. In fact, the power needed to drive on-chip memory is usually included in the power consumption numbers given for the controllers. Hence, the most relevant part is FLASH memory. In fact, the construction and usage of FLASH memory can heavily influence node lifetime. The relevant metrics are the read and write times and energy consumption. Read times and read energy consumption tend to be quite similar between different types of FLASH memory. Energy consumption necessary for reading and writing to the Flash memory is used on the Mica nodes. Hence, writing to FLASH memory can be a time- and energy-consuming task that is best avoided if somehow possible.

1.7.3 Radio transceivers energy consumption: A radio transceiver has essentially two tasks: transmitting and receiving data between a pair of nodes. Similar to microcontrollers, radio transceivers can operate in different modes, the simplest ones are being turned on or turned off. To accommodate the necessary low total energy consumption, the transceivers should be turned off most of the time and only be activated when necessary – they work at a low duty cycle.

The energy consumed by a transmitter is due to two sources one part is due to RF signal generation, which mostly depends on chosen modulation and target distance. Second part is due to electronic components necessary for frequency synthesis, frequency conversion, filters, and so on. The transmitted power is generated by the amplifier of a transmitter. Its own power consumption P_{amp} depends on its architecture $P_{amp} = \alpha_{amp} + \beta_{amp}P_{tx}$. where α_{amp} and β_{amp} are constants depending on process technology and amplifier architecture. The energy to transmit a packet *n*-bits long (including all headers) then depends on how long it takes to send the packet, determined by the nominal bit rate *R* and the coding rate R_{code}, and on the total consumed power during transmission.

$$E_{tx}(n, R_{code}, P_{amp}) = T_{start}P_{start} + \frac{n}{RR_{code}}(P_{txElec} + P_{amp})$$ --------- (7)

Similar to the transmitter, the receiver can be either turned off or turned on. While being turned on, it can either actively receive a packet or can be idle, observing the channel and ready to receive. Evidently, the power consumption while it is turned off is negligible. Even the difference between idling and actually receiving is very small and can, for most purposes, be assumed to be zero. To elucidate, the energy E_{rcvd} required to receive a packet has a startup component $T_{start}P_{start}$ similar to the transmission case when the receiver had been turned off (startup times are considered equal for transmission and receiving here); it also has a component that is proportional to the packet time $\frac{n}{RR_{code}}$. During this time of actual reception, receiver circuitry has to be powered up, requiring a (more or less constant) power of P_{rxElec}.

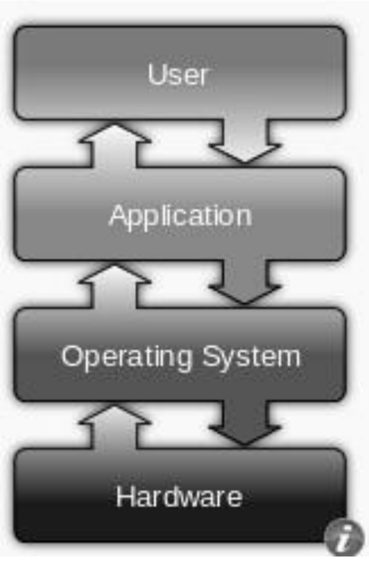
$$E_{rcvd} = T_{start}P_{start} + \frac{n}{RR_{code}}P_{rxElec} + nE_{decBit}$$ ------------ (8)

1.7.4 Power consumption of sensor and actuators:

Providing any guidelines about the power consumption of the actual sensors and actuators is impossible because of the wide variety of these devices. For example, passive light or temperature sensors – the power consumption can possibly be ignored in comparison to other devices on a wireless node. For others, active devices like sonar(A measuring instrument that sends out an acoustic pulse in water and measures distances in terms of time for the echo of the pulse to return), power consumption can be quite considerable in the dimensioning of power sources on the sensor node, not to overstress batteries.

1.8 OPERATING SYSTEMS AND EXECUTION ENVIRONMENTS:

1.8.1 Embedded operating systems:



- ✓ An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.
- ✓ For hardware functions such as input and output and memory allocation, the operating system acts as an intermediary between programs and the computer hardware.
- ✓ An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, that is specifically designed for a particular function.
- ✓ Embedded operating systems are designed to be used in embedded computer systems. They are able to operate with a limited number of

resources. They are very compact and extremely efficient by design.

Figure 1.7 Operating Systems

1.8.2 TinyOS:

- ✓ TinyOS is an open-source, flexible and application-specific operating system for wireless sensor networks.
- ✓ Wireless sensor network consists of a large number of tiny and low-power nodes, each of which executes simultaneous and reactive programs that must work with strict memory and power constraints.

- ✓ TinyOS meets these challenges and has become the platform of choice for sensor network such as limited resources and low-power operation.
- ✓ Salient features of TinyOS are
  - A simple event-based concurrency model and split-phase operations that influence the development phases and techniques when writing application code.
  - It has a component-based architecture which provides rapid innovation and implementation while reducing code size as required by the difficult memory constraints inherent in wireless sensor networks.
  - TinyOS's component library includes network protocols, distributed services, sensor drivers, and data acquisition tools.
  - TinyOS's event-driven execution model enables fine grained power management, yet allows the scheduling flexibility made necessary by the unpredictable nature of wireless communication and physical world interfaces.

1.8.3 Programming paradigms and application programming interfaces:

- ❖ **Concurrent Programming:** Concurrent processing is a computing model in which multiple processors execute instructions simultaneously for better performance. Concurrent means something that happens at the same time as something else. Tasks are broken down into subtasks that are then assigned to separate processors to perform simultaneously, instead of sequentially as they would have to be carried out by a single processor. Concurrent processing is sometimes said to be synonymous with parallel processing.

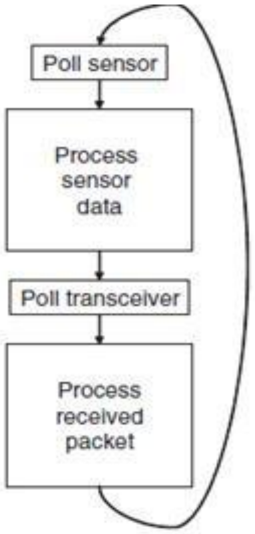


Figure 1.8 Sequential programming model

- ❖ **Process-based concurrency:** Most modern, general-purpose operating systems support concurrent (seemingly parallel) execution of multiple processes on a single CPU. Using processes you are forced to deal with communication through messages, which is the Erlang(A unit of traffic intensity in telephone system) way of doing communication. Data is not shared, so there is no risk of data corruption. Fault-tolerance and scalability is the main advantages of using processes vs. threads. Another advantage of processes is that they can crash and you are perfectly ok with that, because you just restart them (even across network hosts). If thread crashes, it may crash the entire process, which may bring down you application.

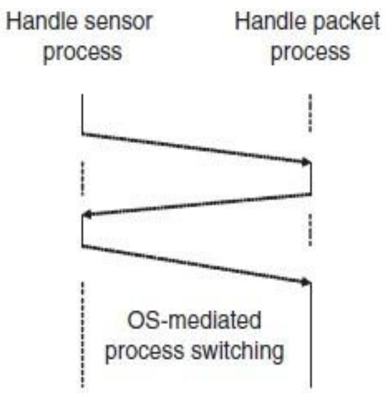
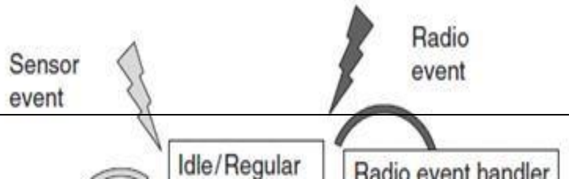


Figure 1.9 Process-based programming model



- **Event-based programming:** In computer programming, event-driven programming is a programming paradigm in which the flow of the program is determined by events such as user actions (mouse clicks, key presses), sensor outputs, or messages from other programs/threads. Event-driven programming is the dominant paradigm used in Graphical User Interfaces (GUI-type of user interface that allows users to interact with electronic devices through graphical icons) and other applications. The system essentially waits for any event to happen, where an event typically can be the availability of data from a sensor, the arrival of a packet, or the expiration of a timer. Such an event is then handled by a short sequence of instructions that only stores the fact that this event has occurred and stores the necessary information.

- **Interfaces to the operating system:** A boundary across which two independent systems meet and act on or communicate with each other. In computer technology, there are several types of interfaces. User interface - the keyboard, mouse, menus of a computer system. The user interface allows the user to communicate with the operating system. Stands for "Application Programming Interface." An API is a set of commands, functions, protocols, and objects (wireless links, nodes) that programmers can use to create software or interact with an external system (sensors, actuators, transceivers). It provides developers with standard commands for performing common operations so they do not have to write the code from scratch.

1.8.4 Structure of operating system and protocol stack: The traditional approach to communication protocol structuring is to use layering: individual protocols are stacked on top of each other, each layer only using functions of the layer directly. This layered approach has great benefits in keeping the entire protocol stack manageable, in containing complexity, and in promoting modularity and reuse. For the purposes of a WSN, however, it is not clear whether such a strictly layered approach will serve. A protocol stack refers to a group of protocols that are running concurrently that are employed for the implementation of network protocol suite. The protocols in a stack determine the interconnectivity rules for a layered network model such as in the OSI or TCP/IP models.

1.8.5 Dynamic energy and power management: Switching individual components into various sleep states or reducing their performance by scaling down frequency and supply voltage and selecting particular modulation and coding are prominent examples for improving energy efficiency. To control these possibilities, decisions have to be made by the operating system, by the protocol stack, or potentially by an application when to switch into one of these states. Dynamic Power Management (DPM) on a system level is the problem at hand. One of the complicating factors to DPM is the energy and time required for the transition of a component between any two states. If these factors were negligible, clearly it would be optimal to always & immediately go into the mode with the lowest power consumption possible.

NETWORK ARCHITECTURE: It introduces the basic principles of turning individual sensor nodes into a wireless sensor network. In this optimization goals of how a network should function are discussed as

- ✓ Sensor network scenarios
- ✓ Optimization goals and figures of merit
- ✓ Gateway concepts

1.9 SENSOR NETWORK SCENARIOS:

1.9.1 Types of sources and sinks: Source is any unit in the network that can provide information (sensor node). A sink is the unit where information is required, it could belong to the sensor network or outside this network to interact with another network or a gateway to another larger Internet**.** Sinks are illustrated by Figure 1.11, showing sources and sinks in direct communication.

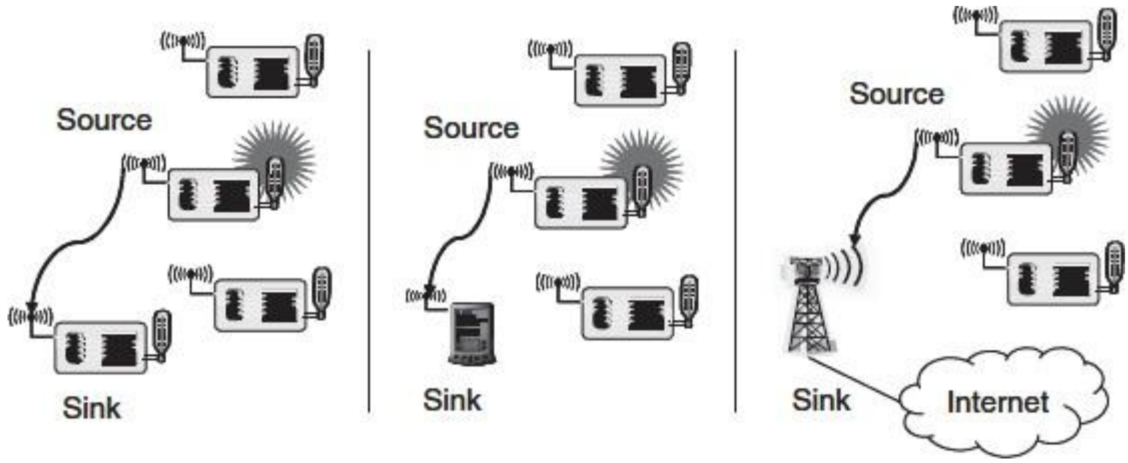


Figure 1.11 Three types of sinks in a very simple, single-hop sensor network

1.9.2 Single-hop versus multi-hop networks:

Because of limited distance the direct communication between source and sink is not always possible. In WSNs, to cover a lot of environment the data packets taking multi hops from source to the sink. To overcome such limited distances it better to use relay stations, The data packets taking multi hops from source to the sink as shown in Figure 1.12, Depending on the particular application of having an intermediate sensor node at the right place is high.

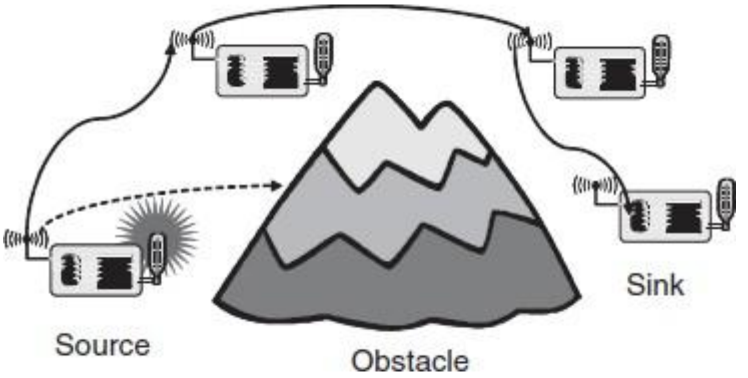


Figure 1.12 Multi-hop networks: As direct communication is impossible because of distance and/or obstacles

Multi-hopping also to improves the energy efficiency of communication as it consumes less energy to use relays instead of direct communication, the radiated energy required for direct communication over a distance d is cd^{α} (c some constant, $\alpha \geq 2$ the path loss coefficient) and using a relay at distance d/2 reduces this energy to $2c(d/2)^{\alpha}$

This calculation considers only the radiated energy. It should be pointed out that only multi- hop networks operating in a store and forward fashion are considered here. In such a network, a node has to correctly receive a packet before it can forward it somewhere. Cooperative relaying (reconstruction in case of erroneous packet reception) techniques are not considered here.

1.9.3 Multiple sinks and sources: In many cases, multiple sources and multiple sinks present. Multiple sources should send information to multiple sinks. Either all or some of the information has to reach all or some of the sinks. This is illustrated in figure 1.13.

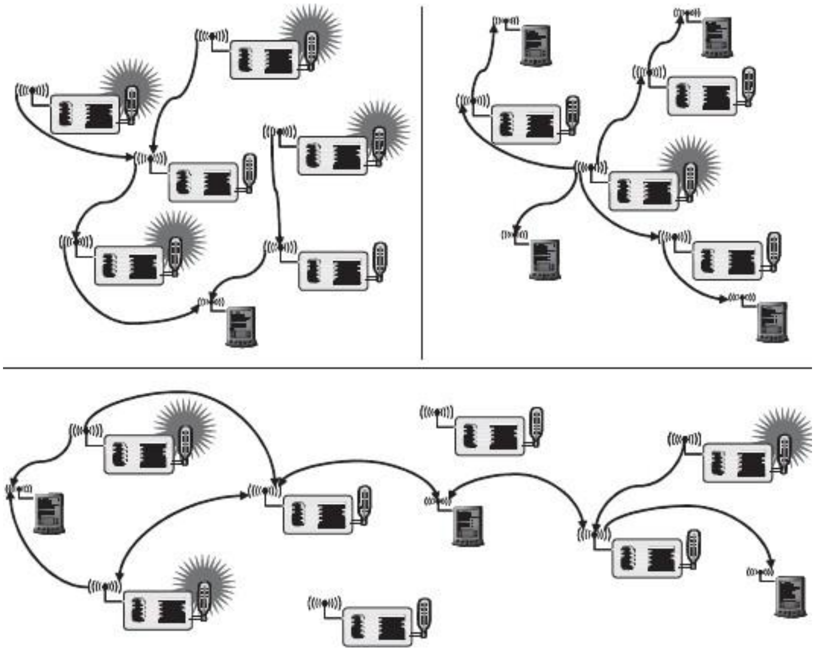


Figure 1.13 Multiple sources and/or multiple sinks.

Note how in the scenario in the lower half, both sinks and active sources are used to forward data to the sinks at the left and right end of the network.

1.9.4 Three types of mobility: In the scenarios discussed above, all participants were stationary. But one of the main virtues of wireless communication is its ability to support mobile participants In wireless sensor networks, mobility can appear in three main forms

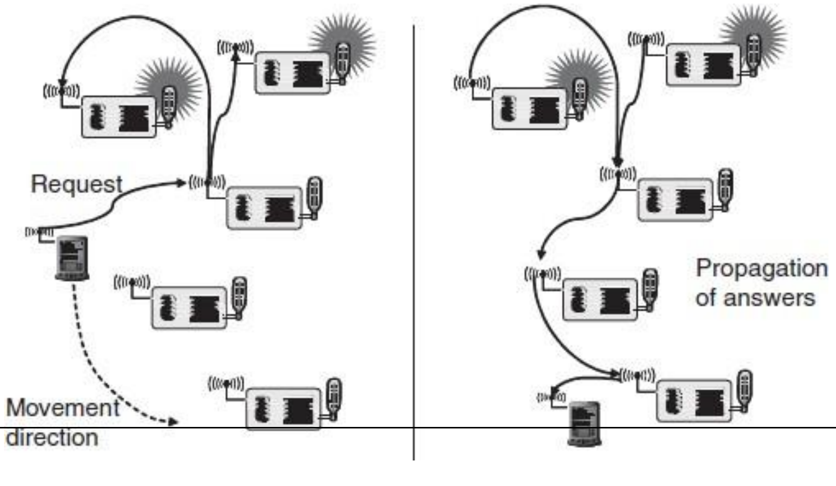
a. Node mobility

b. Sink mobility

c. Event mobility

1.9.4(a) Node Mobility: The wireless sensor nodes themselves can be mobile. The meaning of such mobility is highly application dependent. In examples like environmental control, node mobility should not happen; in livestock surveillance (sensor nodes attached to cattle, for example), it is the common rule. In the face of node mobility, the network has to reorganize to function correctly.

1.9.4(b) Sink Mobility: The information sinks can be mobile. For example, a human user requested information via a PDA while walking in an intelligent building. In a simple case, such a requester can interact with the WSN at one point and complete its interactions before moving on, In many cases, consecutive



interactions can be treated as separate, unrelated requests.

Figure 1.14 Sink mobility: A mobile sink moves through a sensor network as information is being retrieved *on its behalf*

1.9.4(c) Event Mobility: In tracking applications, the cause of the events or the objects to be tracked can be mobile. In such scenarios, it is (usually) important that the observed event is covered by a sufficient number of sensors at all time. As the event source moves through the network, it is accompanied by an area of activity within the network – this has been called the frisbee model. This notion is described by Figure 1.15, where the task is to detect a moving elephant and to observe it as it moves around

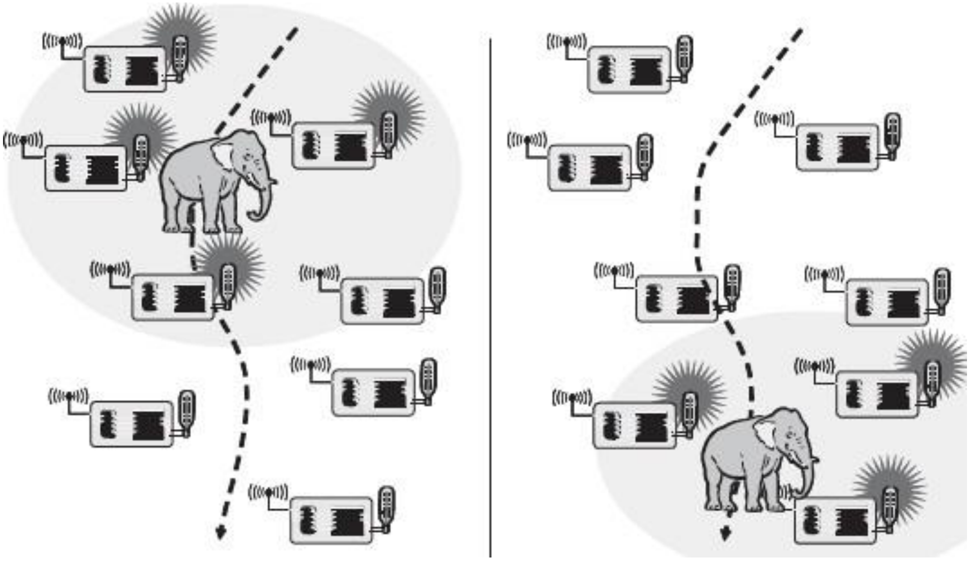


Figure 1.15 Area of sensor nodes detecting an event – an elephant– that moves through the network along with the event source (dashed line indicate the elephant's trajectory; shaded ellipse the activity area following or even preceding the elephant)

<u>1.10</u> OPTIMIZATION GOALS AND FIGURES OF MERIT:

For all WSN scenarios and application types have to face the challenges such as

- ✓ How to optimize a network and How to compare these solutions?
- ✓ How to decide which approach is better?
- ✓ How to turn relatively inaccurate optimization goals into measurable figures of merit? For all the above questions the general answer is obtained from

- ❖ Quality of service
- ❖ Energy efficiency
- ❖ Scalability
- ❖ Robustness

1.10.1 Quality of service: WSNs differ from other conventional communication networks in the type of service they offer. These networks essentially only move bits from one place to another. Some generic possibilities are

- ✓ **Event detection/reporting probability-** The probability that an event that actually occurred is not detected or not reported to an information sink that is interested in such an event For example, not reporting a fire alarm to a surveillance station would be a severe shortcoming.
- ✓ **Event classification error-** If events are not only to be detected but also to be classified, the error in classification must be small
- ✓ **Event detection delay -**It is the delay between detecting an event and reporting it to any/all interested

sinks

- ✓ **Missing reports -**In applications that require periodic reporting, the probability of undelivered reports should be small
- ✓ **Approximation accuracy-** For function approximation applications, the average/maximum absolute or relative error with respect to the actual function.
- ✓ **Tracking accuracy** Tracking applications must not miss an object to be tracked, the reported position should be as close to the real position as possible, and the error should be small.

1.10.2 Energy efficiency: Energy efficiency should be optimization goal. The most commonly considered aspects are:

- ✓ **Energy per correctly received bit-**How much energy is spent on average to transport one bit of information (payload) from the transmitter to the receiver.
- ✓ **Energy per reported (unique) event-**What is the average energy spent to report one event
- ✓ **Delay/energy trade-offs-**"urgent" events increases energy investment for a speedy reporting events. Here, the trade-off between delay and energy overhead is interesting
- ✓ **Network lifetime** The time for which the network is operational
- ✓ **Time to first node death-**When does the first node in the network run out of energy or fail and stop operating?
- ✓ **Network half-life-**When have 50 % of the nodes run out of energy and stopped operating
- ✓ **Time to partition-**When does the first partition of the network in two (or more) disconnected parts occur?
- ✓ **Time to loss of coverage** the time when for the first time any spot in the deployment region is no longer covered by any node's observations.
- ✓ **Time to failure of first event notification** A network partition can be seen as irrelevant if the unreachable part of the network does not want to report any events in the first place.

1.10.3 Scalability: The ability to maintain performance characteristics irrespective of the size of the network is referred to as scalability. With WSN potentially consisting of thousands of nodes, scalability is an obviously essential requirement. The need for extreme scalability has direct consequences for the protocol design. Often, a penalty in performance or complexity has to be paid for small networks. Architectures and protocols should implement appropriate scalability support rather than trying to be as scalable as possible. Applications with a few dozen nodes might admit more-efficient solutions than applications with thousands of nodes.

1.10.4 Robustness: Wireless sensor networks should also exhibit an appropriate robustness. They should not fail just because a limited number of nodes run out of energy, or because their environment changes and severs existing radio links between two nodes. If possible, these failures have to be compensated by finding other routes.

1.11 GATE WAY CONCEPTS:

1.11.1 Need for gateways:

- ✓ For practical deployment, a sensor network only concerned with itself is insufficient.
- ✓ The network rather has to be able to interact with other information devices for example to read the temperature sensors in one's home while traveling and accessing the Internet via a wireless.
- ✓ Wireless sensor networks should also exhibit an appropriate robustness
- ✓ They should not fail just because of a limited number of nodes run out of energy or because of their environment changes and breaks existing radio links between two nodes.
- ✓ If possible, these failures have to be compensated by finding other routes.

Figure 1.16 shows this networking scenario, The WSN first of all has to be able to exchange data with such a mobile device or with some sort of gateway, which provides the physical connection to the Internet. The WSN support standard wireless communication technologies such as IEEE 802.11. The design of gateways becomes much more challenging when considering their logical design. One option is to regard a gateway as a simple router between Internet and sensor network.

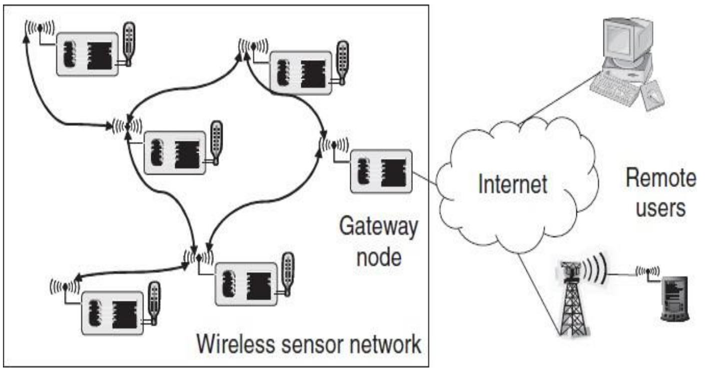


Figure 1.16 A wireless sensor network with gateway node, enabling access to remote clients via the Internet

1.11.2 WSN to Internet communication:

Assume that the initiator of a WSN – Internet communication resides in the WSN.

- ✓ For example, a sensor node wants to deliver an alarm message to some Internet host.
- ✓ The first problem to solve is how to find the gateway from within the network
- ✓ Basically, a routing problem to a node that offers a specific service has to be solved, integrating routing and service discovery
- ✓ If several such gateways are available, how to choose between them?
- ✓ In particular, if not all Internet hosts are reachable via each gateway or at least if some gateway should be preferred for a given destination host?
- ✓ How to handle several gateways, each capable of IP networking, and the communication among them?
- ✓ One option is to build an IP overlay network on top of the sensor network
- ✓ How to map a semantic notion ("Alert Alice") to a concrete IP address?
- ✓ Even if the sensor node does not need to be able to process the IP protocol, it has to include sufficient information (IP address and port number, for example) in its own packets;
- ✓ the gateway then has to extract this information and translate it into IP packets.
- ✓ An ensuing question is which source address to use here – the gateway in a sense has to perform tasks similar to that of a Network Address Translation (NAT) device.

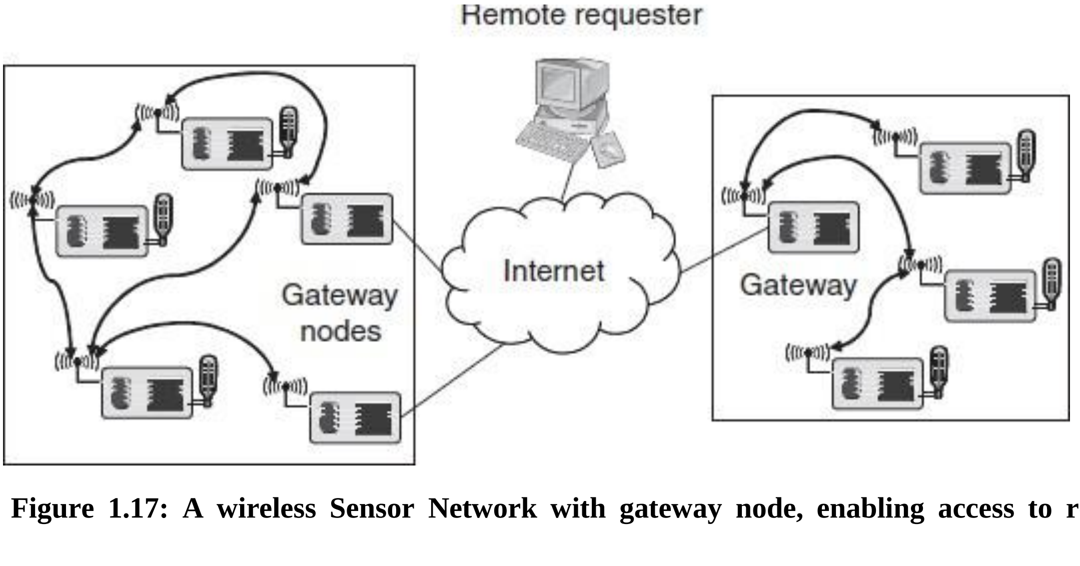


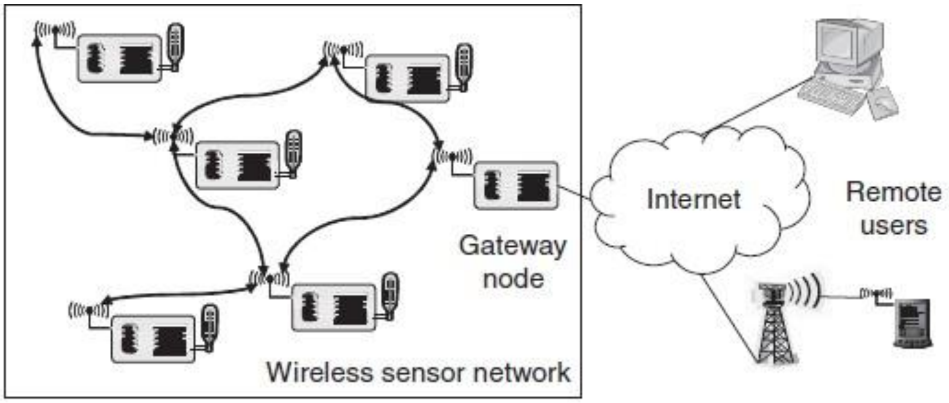
Figure 1.17: A wireless Sensor Network with gateway node, enabling access to remote

clients via the WSN

1.11.3 Internet to WSN communication: The case of an Internet-based entity trying to access services of a WSN is even more challenging.

- ✓ This is fairly simple if this requesting terminal is able to directly communicate with the WSN.
- ✓ The more general case is, however, a terminal "far away" requesting theservice, not immediately able to communicate with any sensor node and thus requiring the assistance of a gateway node

- ✓ First of all, again the question is how to find out that there actually is a sensor network in the desired location, and how to find out about the existence of a gateway node?
- ✓ Once the requesting terminal has obtained this information, how to access the actual services.
- ✓ The requesting terminal can instead send a properly formatted request to this gateway, which acts as an application-level gateway
- ✓ The gateway translates this request into the proper intra sensor network protocol interactions
- ✓ The gateway can then mask, for example, a data-centric data exchange within the network behind an identity-centric exchange used in the Internet
- ✓ It is by no means clear that such an application-level protocol exists that represents an actual simplification over just extending the actual sensor network protocols to the remote terminal
- ✓ In addition, there are some clear parallels for such an application-level protocol with so- called Web Service Protocols, which can explicitly describe services and the way they can be accessed



A wireless sensor network with gateway node, enabling access to remote clients via the Internet

Figure 1.18: A wireless Sensor Network with gateway node, enabling access to remote clients via the internet

1.11.4 WSN tunnelling:

- ✓ The gateways can also act as simple extensions of one WSN to another WSN The idea is to build a larger, “virtual” WSN out of separate parts, transparently “tunneling” all protocol messages between these two networks and simply using the Internet as a transport network.
- ✓ This can be attractive, but care has to be taken not to confuse the virtual link between two gateway nodes with a real link;

- ✓ Otherwise, protocols that rely on physical properties of a communication link can get quite confused (e.g. time synchronization or localization protocols).

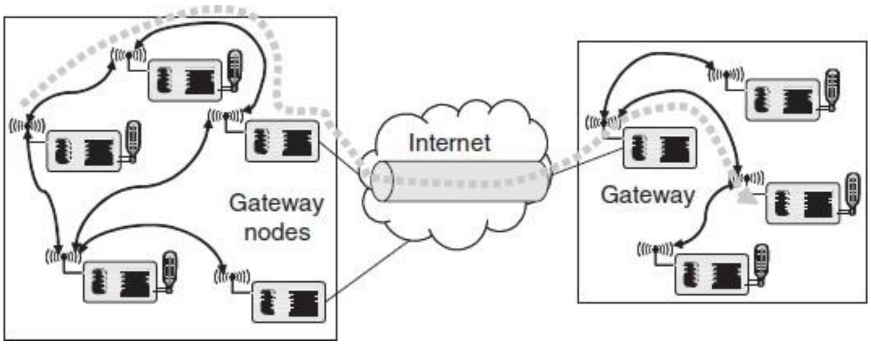


Figure 1.19 Connecting two WSNs with a tunnel over the Internet

CHAPTER II

OVERVIEW OF WIRELESS SENSOR NETWORK

This chapter provides the overview of details of WSN, sensor network classes, wireless sensor network architecture, homogeneous and heterogeneous, wireless networking control systems, routing and advantages of wireless sensor network describes research challenges and sensible concerns that are often overlooked in theoretical study.

Introduction

Wireless Sensor Network (WSNs) [69] have emerged as research areas with a great effect on practical application developments. They permit fine grain observation of the ambient environment at an economical cost much lower than currently possible. In hostile environments where human participation may be too dangerous sensor network may provide a robust service. Sensor network are designed to transmit data from an array of sensor nodes to a data repository on a server [41], [60]. The advances in the integration of micro-electro-mechanical system (MEMS), microprocessor and wireless communication technology have enabled the deployment of large-scale wireless sensor network. WSN [4-5] has potential to design many new applications [159-165] for handling emergency, military and disaster relief operations that requires real time information for efficient coordination and planning. Sensors are devices that produce a measurable response to a change in a physical condition like temperature, humidity, pressure etc. WSNs [90] may consist of many different types of sensors such as seismic, magnetic, thermal, visual, infrared, acoustic and radar, capable to monitor a wide variety of ambient conditions. Though each individual sensor may have severe resource constraint in terms of energy, memory, communication and computation capabilities; large number of them may collectively monitor the physical world, disseminate information upon critical environmental events and process the information.

The emerging field of wireless sensor network combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path by hopping data from node to node in search of its destination. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities. The power of wireless sensor network lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real- time tracking, to monitoring of environmental conditions, to ubiquitous computing environments, to monitoring of the health of structures or equipment. While often referred to as wireless sensor network, they can also control actuators that extend control from cyberspace into the physical world.

Recent technological advances in hardware have enabled the deployment of tiny, low- power sensors with limited on-board signal processing and wireless communication capacities. Wireless sensor network (WSN) become increasingly useful in variety critical applications, such as environmental monitoring, smart offices, battlefield surveillance, and transportation traffic monitoring. In order to achieve high quality and fault-tolerant capability, a sensor network can be composed of hundreds or thousands of unattended sensor nodes, which are often randomly deployed inside the interested area or very close to it [69].

A wireless sensor network consists of a large number of tiny, low-power sensor nodes. The node has sensing, data processing and wireless communication components. Sensor nodes are deployed randomly in the deployment region under examination and collect sensor data. Wireless sensor network have attracted much attention because of their wide range of application, such as military, environmental monitoring, and health care industry. Unlike wired and mobile Ad hoc network, wireless sensor network are infrastructure-less and can operate in any environment as compared to the traditional network. When sensor network are deployed in hostile environments security becomes more important as they are prone to different types of malicious attacks. In order to provide security for sensor network, key management is applied. Although many protocols and algorithms have been proposed for traditional wireless ad hoc network, they are not well suited for the unique features and application requirements of wireless sensor network. To illustrate this point, the differences between wireless sensor network and ad-hoc network are outlined below: The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network [20]. Sensor nodes are densely deployed. Sensor nodes are prone to failures.

Sensors facilitate the instrumenting and controlling of factories, offices, homes, vehicles, cities and the ambiance, especially as commercial off-the-shelf technology becomes available. With sensor network technology ships, aircraft and buildings can “self-detect” structural faults. Places of public assembly can be instrumented to detect airborne agents such as toxins and to trace the contamination which is present. Earthquake-oriented sensors in buildings can locate potential survivors and can help assess structural damage; tsunami-alerting sensors are useful for nations with extensive coastlines. Sensors also find extensive applicability on the battlefield for reconnaissance and surveillance.

Currently, wireless sensor network are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor network with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defence, and smart spaces.

Since a wireless sensor network is a distributed [37] real-time system a natural question is how many solutions from distributed and real-time systems can be used in these new systems? Unfortunately, very little prior work can be applied and new solutions are necessary in all areas of the system. The main reason is that the set of assumptions underlying previous work has changed dramatically. Most past distributed systems research has assumed that the systems are wired, have unlimited power, are not real-time, have user interfaces such as screens and mice, have a fixed set of resources, treat each node in the system as very important and are location independent. In contrast, for wireless sensor network, the systems are wireless, have scarce power, are real-time, utilize sensors and actuators as interfaces, have dynamically changing sets of resources, aggregate behaviour is important and location is critical. Many wireless sensor network also utilize minimal capacity devices which places a further strain on the ability to use past solutions. Since WSN is usually exposed to atrocious and dynamic environments, it is possible for the loss of connectivity of individual nodes. Conventional centralized algorithms need to operate with global knowledge of the whole net work, and an error in transmission or a failure of a critical node will potentially cause a serious protocol failure [90]. On the contrary, distributed algorithms [72-74] are only executed locally within partial nodes, thus can prevent the failure caused by a single node. It is realized that localized algorithms are more scalable and robust than centralized algorithms.

Improving the lifetime in wireless sensor network is important because the sensor nodes in wireless sensor network are constrained by limited energy. The way to improve a WSN lifetime is to develop energy efficient protocols for reducing energy consumption. One of the well known energy efficient methods is the clustering based algorithm which is designed for homogeneous wireless sensor network. The clustering algorithms were also improved and applied to the heterogeneous wireless sensor network. Recent advances in wireless communication technologies have enabled the development of large-scale wireless sensor network that consist of many low-powers, low-cost and small-size sensor nodes. Sensor network hold the promise of facilitating large-scale and real-time data processing in complex environments.

Key management is crucial to the secure operation of wireless sensor network. A large number of keys must be managed in order to encrypt and authenticate all sensitive data. The objective of key management is to dynamically establish and maintain secure channels among communicating parties. Typically, key management solutions use administrative keys to securely and efficiently re-distribute and at times, generate the secure channel session keys to the communicating parties. Session keys may be pair-wise keys used to secure a communication channel between two nodes that are in direct or indirect communication or they may be group keys shared by multiple nodes. Network keys may need to be changed to maintain secrecy and resiliency to attacks, failures, or network topology changes. Key management entails the basic functions of generation, assignment, and distribution of network keys. It is to be noted that re-keying is comprised essentially of these basic functions. As each sensor node is tightly power-constrained and one-off, the lifetime of WSN is limited. In order to prolong the network lifetime, energy-efficient protocols should be designed for the characteristic of WSN. Efficiently organizing sensor nodes into clusters is useful in reducing energy consumption. Many energy-efficient routing protocols are designed based on the clustering structure [118], [120]. The clustering technique can also used to perform data aggregation [110], [73], which combines the data from source nodes into a small set of meaningful information. Under the condition of achieving sufficient data rate specified by applications, the fewer messages are transmitted, the more energy is saved. Localized algorithms can efficiently operate within clusters and need not to wait for control messages propagating across the whole network. Therefore localized algorithms bring better scalability to large network than centralized algorithms, which are executed in global structure. Clustering technique can be extremely effective in broadcast and data query [135], [82]. Cluster-heads will help to broadcast messages and collect interested data within their own clusters.

The rise of informatics drives the rapid development of network and wireless communication technologies [107]. Wireless Sensor Network (WSNs) are increasingly useful [18], [148] and are applied to many applications, such as smart living, environmental monitoring, automatic measurement, healthcare, and traffic monitoring.

Wireless Sensor Network

In a wireless sensor network, it is an important task to collect the data periodically from various sensor nodes for monitoring and recording the physical conditions of the environment. The sensed data must be transmitted and received between the nodes in the network.

The Wireless sensor network (WSN) is a broadcast network; it consists of a large number of sensors that are effective for gathering data in a variety of environments. Since the sensors operate on battery power, it is a great challenging aim to design the energy efficient routing protocols. A Wireless Sensor Network structure is shown in Figure 2.1.

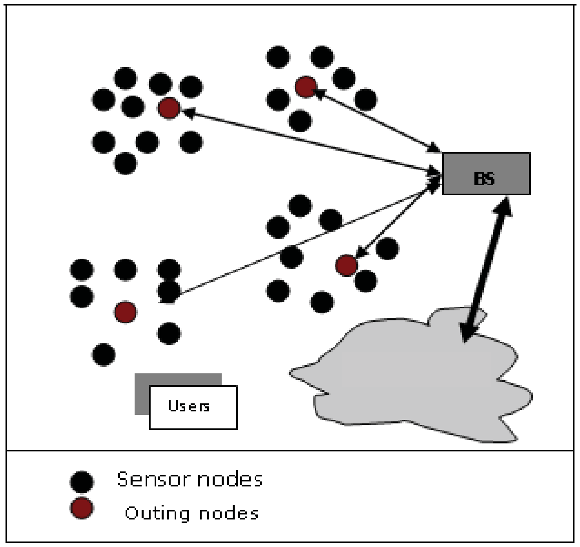


Figure 2.1 Wireless Sensor Network Structure

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni- directional antenna), have a power source [57] (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work.

Network: The network is a set of device connected by communication link.

Sensors: Sensor is used to monitor the environment. Sensor network are used for collecting, storing and sharing the sensed data. They can also be defined as a system comprised of a set of sensor nodes and a communication system that allows automatic data collection and sharing. They allow monitoring remote, hazardous, dangerous or unwired areas, for example in the monitoring and warning systems for tsunamis, volcanoes, or seismologic phenomena. Since sensor network contains large amount of data for the end user, methods of combining or aggregating data into small set of information is necessary and contributes to energy savings.

As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing. Several sources of power consumption in sensors are: (a) signal sampling and conversion of physical signals to electrical ones; (b) signal conditioning, and (c) analog-to-digital conversion.

There are three categories of sensor nodes: Active, Passive and Omni Directional Sensors: passive sensor nodes sense the environment without manipulating it by active probing. In this case, the energy is needed only to amplify their analog signals. There is no notion of “direction” in measuring the environment. Passive, narrow-beam sensors: these sensors are passive and they are concerned about the direction when sensing the environment. Active Sensors: these sensors actively probe the environment. The hardware platform is listed below.

Mica Nodes: The Mica2 (MPR400) and MicaZ (MPR2400) nodes, manufactured by Crossbow Technologies, are typical third-generation wireless sensor nodes. They are compatible with the open-source TinyOS embedded operating system which provides a component-based protocol implemented in the nesC concurrent extension to the C language. The Mica2 and MicaZ feature an Atmel ATmega128L 8-bit processor running at 7MHz. The modular design allows external sensor boards to be attached to a main processing and transceiver board, decoupling sensing and allowing application exibility via the integration of custom sensors to meet specific scenario objectives. Power is supplied via either an external connector or onboard mounting for two AA batteries, which typically provide a current capacity of 2000 mAh, although lithium ion (Li-On) batteries can provide a maximum of 2800mAh. The Mica nodes, with attached battery connector, and an associated base station with power and connectivity to a management computer supplied over Universal Serial Bus (USB). The Chipcon CC1000 transceiver of the Mica2 operates on the 868/915 MHz band. Its data rate of 38.4 kbps provides for messaging applications, and the choice of simple and robust modulation techniques, such as frequency- shift keying (FSK) and on-off keying (OOK), giving good error tolerance and imposing little in terms of synchronisation and channel estimation demands, with consequent power efficiency. The Chipcon CC2420 radio transceiver of the MicaZ operates on the 2.4 GHz Industrial, Scientific and Medical band, on which users may operate licence-free in the UK. It is compliant with the IEEE 802.15.4 standard [64], and operates at the increased data rate of 250kbps, with more complex modulation scheme of direct sequence spread spectrum (DSSS) with Offset Quaternary Phase-Shift Keying (O- QPSK). The increased data rate enables higher data rates from the end source, enabling continuous reporting scenarios that encroach upon the field of ad-hoc networking.

Jennic Nodes: A more recent development in WSN technology is provided by the Jennic nodes from NXP Semiconductor. The JN5148 nodes provide a richer computing environment than the Mica nodes, with 32-bit RISC processors and 128 kB of RAM and ROM. Specialist physical interfaces also allow significantly more data to be sampled, with a digital audio interface allowing audio sampling for phenomena detection. Peak data rates of up to 500 kbps and 667 kbps allow the potential for transmission of low-rate multimedia data such as audio and (with hardware assistance) video. The protocol environment employed is also focused upon enabling higher-layer solutions, with no direct official support for the de-facto standard TinyOS environment in favour of a custom JenNet suite. Accordingly, the nodes and associated technologies are typically marketed at system integrator usage, for example, industrial applications, rather than for direct research. The JenNet protocols provide application integrators with custom higher layer abstractions built upon Zigbee. For example, routing is handled automatically via a tree-healing protocol, which implicitly assumes a relatively small and static network (theoretical maximum of 500 nodes with addressing scheme employed) directed by the sink as coordinator. There is also a centralised channel allocation scheme that selects a single channel for the entire network to use. This exemplifies a recent trend for commercial WSN nodes to over low-configuration applications for logistical control applications. Out of the box, the nodes operate a demonstration application for local temperature monitoring to a base station. With the Jennic nodes, it is possible to bypass the JenNet protocols and to operate directly upon IEEE 802.15.4 , providing significantly increased functionality, such as forming arbitrary mesh topologies and implementing custom MAC and routing protocols. This is important for the ability to implement research protocols upon the nodes.

Spec Motes - Smart Dust: An ultimate destination for WSN technology is provided by the Smart Dust project. The ambitious vision of Smart Dust is to build WSN concepts on a technology foundation of MEMS (micro-electro-mechanical systems). MEMS postulate physical technologies for communication and power at the millimetre scale and below, allowing the extension of WSNs to encompass ultra-high resolution monitoring. Such approaches could include destructive stress testing of physical systems and industrial prototypes during breakdown, medical and military espionage applications.

The concept of wireless sensor network is based on a simple equation

Sensing + CPU + Radio = Thousands of potential applications

As soon as people understand the capabilities of a wireless sensor network, hundreds of applications spring to mind. It seems like a straightforward combination of modern technology.

However, actually combining sensors, radios, and CPU's into an effective wireless sensor network requires a detailed understanding of both the capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption. A core challenge is to map the overall system requirements down to individual device capabilities, requirements and actions. To make the wireless sensor network vision a reality, architecture must be developed that synthesizes the envisioned applications out of the underlying hardware capabilities.

Architecture of WSN

The WSN architecture is shown in figure 2.2. It consists of a large number of sensor nodes, which include small volume, low cost, limited computation and limited power capacity [55]. The sensor node collects the sensed data by the sensor and transmits the data to an external base station (BS) by wireless communication components. Once the sensor nodes set up to form a WSN, the network continues carrying out the data while the node battery power is sufficient. Minimizing energy consumption for maximizing WSN lifetime becomes a key challenge [85].

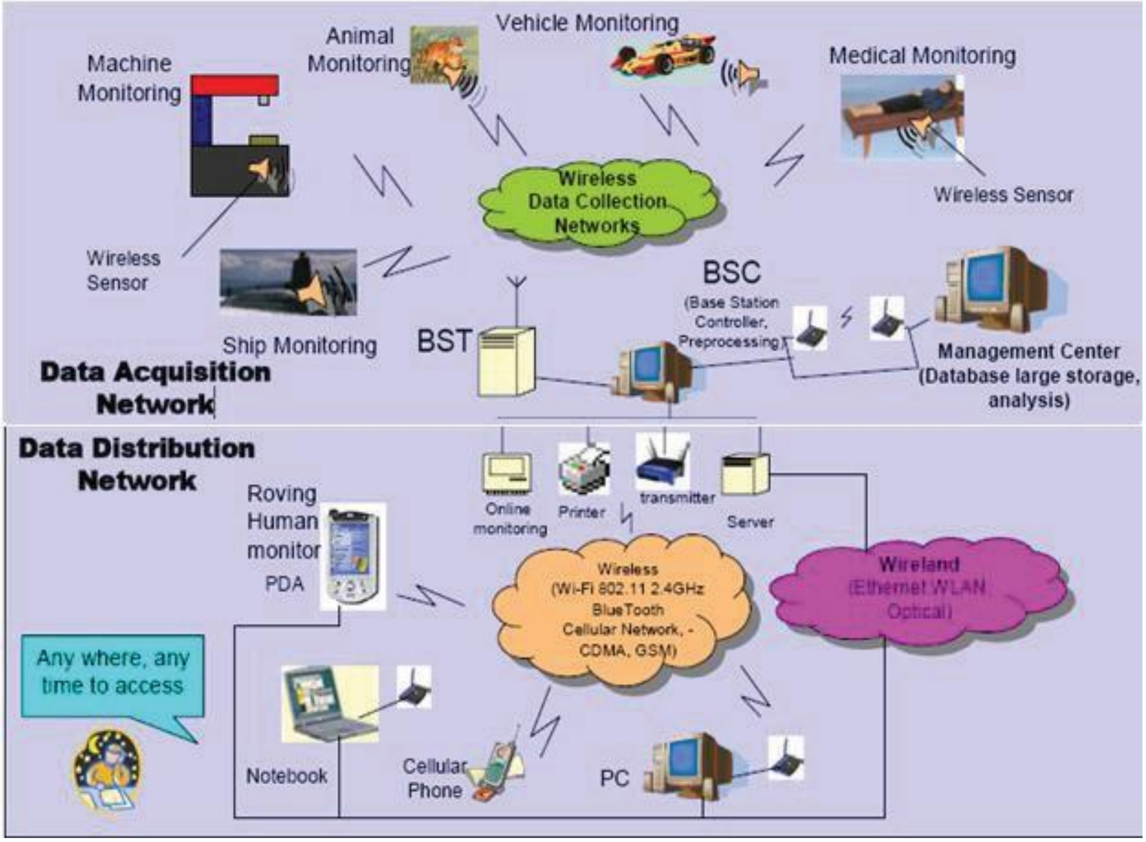

Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Sensor
Wireless Data Collection Networks
Wireless Sensor
Ship Monitoring
BST
BSC (Base Station Controller, Preprocessing)
Management Center (Database large storage, analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Figure 2.2 Wireless Sensor Network

A wireless sensor network is a network of many tiny disposable low power devices, called nodes, which are spatially distributed in order to perform an application-oriented global task. These nodes form a network by communicating with each other either directly or through other nodes. One or more nodes among them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired network. The primary component of the network is the sensor, essential for monitoring real world physical conditions such as sound, temperature, humidity, intensity, vibration, pressure, motion, pollutants etc. at different locations. The tiny sensor nodes, which consist of sensing, on board processor for data processing, and communicating components, leverage the idea of sensor network based on collaborative effort of a large number of nodes [51].

The main design goal of wireless sensor network is to transmit data by increasing the lifetime of the network and by employing energy efficient routing protocols[100,101]. Depending on the applications used, different architectures and designs have been applied in sensor network. Again, the performance of a routing protocol depends on the architecture and design of the network, so the architecture and design of the network is very important features in WSNs. The design of the wireless sensor network is affected by many challenging factors which must be overcome before an efficient network can be achieved in WSNs.

Node Distribution: Node distribution [39] in WSNs is either deterministic or self-organizing and application dependant. The uniformity of the node distribution directly affects the performance of the routing protocol used for this network. In the case of deterministic node distribution, the sensor nodes are mutually placed and gathered data is transmitted through pre- determined paths. In the other case, the sensor nodes are spread over the area of interest randomly thus creating an infrastructure in an *ad hoc* manner.

Network Dynamicity: Since the nodes in WSNs may be static or dynamic, dynamicity of the network is a challenging issue. Most of the routing protocols assume that the sensor nodes and the base stations are fixed *i.e*., they are static, but in the case of dynamic BS or nodes routes from one node to another must be reported periodically within the network so that all nodes can transmit data via the reported route. Again depending on the application, the sensed event can be dynamic or static. For example, in target detection/tracking applications, the event is dynamic, whereas forest monitoring for early fire prevention is an example of a static event.

Monitoring static events works in reactive mode. On the other hand, dynamic events work in proactive mode.

Energy efficiency: The sensor nodes in WSNs have limited energy and they use their energy for computation, communication and sensing, so energy consumption is an important issue in WSNs. According to some routing protocols nodes take part in data fusion and expend more energy. Since the transmission power is proportional to distance squared, multi-hop routing consumes less energy than direct communication, but it has some route management overhead. In this regard, direct communication is efficient. Since most of the times sensor nodes are distributed randomly, multi-hop routing is preferable. In some applications nodes sense environment periodically and lose more energy than the nodes used in some applications where they sense environment when some event occurs.

Scalability: A WSN consists of hundreds to thousands of sensor nodes. Routing protocols must be workable with this huge number of nodes *i.e.*, these protocols can be able to handle all of the functionalities of the sensor nodes so that the lifetime of the network can be stable.

Data Transmission: Data transmission in WSNs is application specific. It may be continuous or event driven or query-based or hybrid. In case of continuous data transmission, sensor nodes send data to the base station periodically. In event driven and query-based transmission they send data to the base station when some event occurs or a specific query is generated by the base station. Hybrid transmission uses a combination of continuous, event driven and query- based transmission, so for architecture and design of WSNs data transmission is a very significant issue.

Data Fusion: Data fusion [45] is a process of combining of data from different sources according to some function. This is achieved by signal processing methods. This technique is used by some routing protocols for energy efficiency and data transfer optimization. Since sensor nodes get data from multiple nodes, similar packets may be fused generating redundant data. In data fusion or data aggregation process awareness is needed to avoid this redundant data.

WSNs are application-specific, so the design requirements of WSNs change according to the application. Hence, routing protocols requirements are changed from one application to another. For instance, the requirements of a routing protocol designed for environmental applications is different from that designed for military or health applications in many aspects. As a result, routing protocols' requirements are as diverse as applications. Some of these are: Scalability, Latency, Throughput, Recourse Awareness, Data Aggregation, Optimal Route, over-head, and other metrics. Some applications need some of these metrics to be provided and other applications need others to be provided. However, routing protocols of all Wireless Sensor network, regardless of the application, must try to maximize the network life time and minimize the energy consumption of the overall network. For these reasons, the energy consumption parameter has higher priority than other factors.

Importance of Energy Efficiency: Some wireless sensor network concepts have explored ideas for energy gathering from the environment, through mechanisms such as solar cells or piezoelectric charging. However, the power source assumed for WSN devices is conventionally assumed to be a limited resource such as a non-rechargeable chemical battery. Furthermore, it is often assumed that the environment for the application scenario is inaccessible or inhospitable, and therefore manual replacement of batteries is not feasible. Therefore, initial energy available at deployment normally limits the lifetime of WSN nodes, mandating the conservation of energy at all levels of the protocol stack where possible.

Wireless sensor network supports the heterogeneous network efficiently then homogeneous network. The Heterogeneous network [87] perform environmental watching and sensor nodes watch a multiplicity of objects, and each data have different levels of energy. In Homogeneous network [87-89,91] each data have same levels of energy. In multi-level heterogeneous network [110], the clustering algorithm should consider the discrepancy of initial energy. In the heterogeneous network, the reference value of each node should be different to the initial energy. In the Leach-Heterogeneous system, the energy efficient[98-99] and life time is increased near to 60% than Leach homogeneous system; Leach- heterogeneous[10] system considerably reduces dissipation which increases the total life time of wireless sensor network.

Generations of Sensor Network

In a similar fashion to the evolution of other technologies, it is possible to describe the Evolution of sensor network in terms of generations.

First Generation Sensor Network - 1GSN

A sensor network consists of individual sensor devices. Deployment is via manual emplacement. The network is fully preconfigured. Access to information is via manual retrieval of the device itself or long-range point-to-point communication links.

Second Generation Sensor Network -2GSN

Sensors work in collaboration to cover an area. The network typically consists of a small number of sensors communicating with a control node equipped with a reach-back link. They are typically manually deployed, relying heavily on pre-configuration.

Third Generation Sensor Network - 3GSN

The third generation of sensors encompasses self-organizing, flexible and scalable network. Sensors communicate with one another for two purposes: communications services (e.g. automatic relaying of messages to a network gateway) and in-network processing (data aggregation and data fusion).

Design Issues of a Wireless Sensor Network

There are a lot of challenges placed by the deployment of sensor network which are a superset of those found in wireless ad hoc network. Sensor nodes communicate over wireless, lossy lines with no infrastructure. An additional challenge is related to the limited, usually non- renewable energy supply of the sensor nodes. In order to maximize the lifetime of the network, the protocols need to be designed from the beginning with the objective of efficient management of the energy resources.

Fault Tolerance

Sensor nodes are vulnerable and frequently deployed in dangerous environment. Nodes can fail due to hardware problems or physical damage or by exhausting their energy supply. We expect the node failures to be much higher than the one normally considered in wired or infrastructure-based wireless network. The protocols deployed in a sensor network should be able to detect these failures as soon as possible and be robust enough to handle a relatively large number of failures while maintaining the overall functionality of the network. Different deployment environments pose different fault tolerance requirements.

Scalability

Sensor network vary in scale from several nodes to potentially several hundred thousand. In addition, the deployment density is also variable. For collecting high-resolution data, the node density might reach the level where a node has several thousand neighbors in their transmission range. The protocols deployed in sensor network need to be scalable to these levels and be able to maintain adequate performance.

Production Costs

Because many deployment models consider the sensor nodes to be disposable devices, sensor network can compete with traditional information gathering approaches only if the individual sensor nodes can be produced very cheaply. The target price envisioned for a sensor node should ideally be less than $1.

Hardware Constraints

At minimum, every sensor node needs to have a sensing unit, a processing unit, a transmission unit, and a power supply. Optionally, the nodes may have several built-in sensors or additional devices such as a localization system to enable location-aware routing. However, every additional functionality comes with additional cost and increases the power consumption and physical size of the node. Thus, additional functionality needs to be always balanced against cost and low-power requirements.

Sensor Network Topology

Although WSNs have evolved in many aspects, they continue to be network with constrained resources in terms of energy, computing power, memory, and communications capabilities. Of these constraints, energy consumption is of paramount importance, which is demonstrated by the large number of algorithms, techniques, and protocols that have been developed to save energy, and thereby extend the lifetime of the network.

Transmission Media

The communication between the nodes is normally implemented using radio communication over the popular ISM bands. However, some sensor network use optical or infrared communication, with the latter having the advantage of being robust and virtually interference free

Power Consumption

As we have already seen, many of the challenges of sensor network revolve around the limited power resources. The size of the nodes limits the size of the battery. The software and hardware design needs to carefully consider the issues of efficient energy use. For instance, data compression might reduce the amount of energy used for radio transmission, but uses additional energy for computation and/or filtering. The energy policy also depends on the application; in some applications, it might be acceptable to turn off a subset of nodes in order to conserve energy while other applications require all nodes operating simultaneously.

Challenges in Wireless Sensor Network

In order to design good applications for wireless micro-sensor network, it is essential to understand factors important to the sensor network applications. Although WSNs share some commonalities with existing wireless ad-hoc network they pose a number of technical challenges different from traditional wireless ad-hoc network [4] [20]. The protocols and algorithms that have been proposed for traditional wireless ad-hoc network are therefore not well suited for the application requirements of the sensor network. To illustrate this point, differences between sensor network and traditional network are outlined below:

Energy

The sensor nodes are generally inaccessible after deployment and normally they have a finite source of energy that must be optimally used for processing and communication to extend their lifetime. It is a well known fact that communication requires significant energy. In order to make optimal use of energy, therefore communication should be minimized as much as possible.

Redundancy

Due to the frequent node failures and inaccessibility of failed nodes, WSNs are required to have high redundancy of nodes so that the failure of few nodes can be negligible.

System Lifetime

The WSNs should function as long as possible. Their system lifetime can be measured by using generic parameters such as time until the nodes die or by using application specific parameters like time until the sensor network is no longer providing acceptable quality results.

Scalability

In WSNs, each sensor node obtains a specific view of the environment. A given sensor's view of the environment is limited both in range and accuracy; it can only cover a limited physical area of the environment. The WSNs therefore, deploys sensor nodes that have a short transmission distance in large numbers to monitor the entire area.

Adaptability

The WSN system should be adaptable to changes such as addition of more nodes, failure of nodes, environmental conditions and thus unlike traditional network, where the focus is on maximizing channel throughput or minimizing node deployment, the major consideration in a sensor network is to extend the network lifetime besides system robustness.

Application Awareness

A WSN is not a general purpose network. In order to deploy it for specific application, the WSN protocols should consider application-specific trade-offs in terms of complexity, resource usage and communication patterns to improve network efficiency.

Lack of Global Identification

Due to large number of sensor nodes in a sensor network the global identification (GID) is generally not possible. Although in some cases, the Global Positioning System (GPS) provides positioning information to sensor nodes but it requires line of sight to several satellites, which is generally not available inside of buildings, beneath dense foliage, underwater, when jammed by an enemy or during MARS exploration etc.

Storage, Search and Retrieval

The sensor network can produce a large volume of raw data such as continuous time series of observations over all points in space covered by the network. Since the data source is continuous traditional databases are not suitable for WSNs.

Data Centric Processing

The naming schemes in WSNs are often data-oriented for example an environmental monitoring system may requests temperature readings through a query like “collect temperature readings in the region bounded by the rectangle (x1,y1,x2,y2)”, instead of a query “collect temperature readings from a set of nodes having addresses x, y and z.”

Production Cost

The cost of a single node is very important to justify overall cost of the network; since the sensor network consist of a large number of sensor nodes therefore cost of each sensor node has to be kept low.

Node Deployment

Node deployment is application dependent and affects performance of the protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths. However, in self organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an ad- hoc manner.

In-Network Processing

In general transport protocols used in wired and wireless network have assumed end-to end approach guaranteeing that data from the senders have not been modified by intermediate nodes until it reaches a receiver. However, in WSNs data can be modified or aggregated by intermediate nodes in order to remove redundancy of information. The previous solutions did not accommodate concept of in-network processing, called data aggregation or diffusion [58] in WSNs.

Latency

Latency refers to delay from when a sender sends a packet until the packet is successfully received by the receiver. The sensor data has a temporal time interval in which it is valid, since the nature of the environment changes constantly, it is therefore important to receive the data in a timely manner.

Fault tolerance

Sensor nodes are fragile and they may fail due to depletion of batteries or destruction by an external event. Realizing a fault-tolerant operation is critical, for successful working of the WSN, since faulty components in a network leads to reduced throughput, thereby decreasing efficiency and performance of the network.

Desired Security Services from the WSNs Perspective

WSNs protocols and applications, three performance metrics are pertinent when providing security services for WSNs. These performance metrics are independent of the chosen encryption mechanism. One is the storage, another is the communication, and the last is computational cost. For WSNs, the communication cost is the costliest among all the others and the chosen security mechanism implemented should try to use these scare resources efficiently.

Confidentiality

WSN Perspective Definition: Confidentiality refers to the protection of the exchanged content (e.g., gathered data, reports, and commands) among the sink(s) and the sensors. An adversary, who has the privilege to access the content, should not be able to decode the exchanged messages in the network.

Current Approaches

Providing a confidential service to WSN applications requires the usage of cryptographic measures like encryption techniques. In general, two distinct forms of encryption approaches are in common use: symmetric and asymmetric key based schemes. Symmetric key based encryption uses the same key at both ends of the communication to encrypt and decrypt the in-formation from cipher text to plaintext and vice verse. On the other hand, with asymmetric key based encryption, a different key (one private and one public) are utilized to convert and recover the information.

The general important observation about encryption mechanisms is that one cannot claim that one encryption method is superior to another as it is essentially a matter of the key size and the computational effort in breaking the encryption algorithm. The second aspect to confidentiality research in WSNs entails designing efficient key management schemes because regardless of the encryption mechanism chosen for WSNs, the keys must be made available to the communicating nodes (e.g., sources, sink(s)) to maintain the privacy of the channels. The key management process involves two fundamental steps: generation (after an analysis) and distribution of keys; and it is triggered by keying events (e.g., due to node addition or an attack) in the network. Nonetheless, it is not an easy task and even in some applications it may be daunting operation to visit a large number of sensors and update their keys (e.g., for underwater sensor applications). Thus, intelligent key management schemes are necessary for WSN.

There are two further observations for confidentiality research in WSNs. First, the research mainly focuses on different keying mechanisms rather than Current Approaches: Providing a confidential service to WSN applications requires the usage of cryptographic measures like encryption techniques. In general, two distinct forms of encryption approaches are in common use: symmetric and asymmetric key based schemes. Symmetric key based encryption uses the same key at both ends of the communication to encrypt and decrypt the information from cipher text to plaintext and vice verse. On the other hand, with asymmetric key based encryption, a different key (one private and one public) are utilized to convert and recover the information.

The following list gives an overview of the research for both the encryption and key management mechanisms for WSNs.

Encryption Mechanisms

In recent works, the feasibility of two encryption techniques has been well scrutinized and understood for the WSN do- main. With the current technological advances in the field of micro-electro- mechanical systems, symmetric encryption techniques are more tailored to WSNs. There are several reasons for this. First of all, using the same key at both ends saves the storage space. For instance in a simple worst case scenario assume that there are N number of nodes in the network. While for symmetric encryption, a given node must posses N-1 number of keys in order to communicate to the other N-1 nodes, for asymmetric encryption, the same node must have N keys, N-1 for others' public keys, one for its own private key. Considering the fact that the key sizes for symmetric algorithms (e.g., 128 bits for AES) are generally smaller than those of asymmetric ones (e.g., recommended 1024 bits for RSA and 160 bits for Elliptic Curve Cryptography (ECC) Based Public Key Scheme), one can conclude that depending on the specified key size of the particular algorithm chosen, the symmetric encryption algorithms may help save from the per-node storage space. Secondly, the symmetric encryption algorithms have been known to utilize the resources more efficiently than their asymmetric counterparts as their cryptographic operations take lesser time and require much less energy consumption than that of asymmetric cryptographic ones. This is primarily due to the fact that the symmetric encryption algorithms are faster in computation as they employ more primitive operations in their algorithms like substitution and permutation of symbols, which are implemented at the hardware level via shifts and XORs, rather than operations applying mathematical functions like modular arithmetic and exponentiation, which are the basis of public key encryption mechanisms. Lastly, the exchange of smaller size keys, when needed in a WSN application, consumes less communication resources, which favours symmetric schemes. A detailed discussion of key mechanisms is given below.

Key Management Mechanisms

As mentioned above, there are two fundamental steps in the key management process: generation and distribution of keys. The key generation step deals with generation of the keys. Depending on the key type that is going to be deployed in the WSN, the keys can be generated once or multiple times during the lifetime of the WSN. The practical approach adopted so far in this avenue of research has been to generate one time different keys such as session, network-wise, master, and group-wise keys depending on the topology and on the application requirements of WSNs. While this helps decrease the computation cost for WSNs, it may increase the storage over nodes depending on the key distribution scheme. The second step is the distribution of keys. The keys should be made available to the nodes without allowing others to see the keys. Traditionally, the keys have been exchanged between the end-points of the communication directly or indirectly through trusted intermediaries (e.g., Key Distribution Centre). The keys could be distributed to the sensors before the network is deployed or they could be re-distributed to nodes on demand as triggered by keying events. In the jargon of security research for WSNs, the former is phrased as Static Key management whereas the latter is as Dynamic Key management. For WSNs, the communication cost dominates other critical cost parameters, i.e., storage and computation. Thus, the research for key distribution has focused more on static key management schemes. Static key management schemes perform key management functions statically prior to or shortly after network deployment. One famous pioneering work in this avenue is by Eschenauer and Gligor, where each sensor in the WSN is pre-configured with a random subset of keys from a large key pool. To agree on a key for communication, two sensor nodes find one common key within their subsets and use this key as their shared secret key. On the other hand, dynamic key management schemes perform the key management steps either periodically or on demand due to keying events in the network. The leading approach in dynamic keying schemes involves exclusion-based systems, the basic notion of which requires each node to have k keys out of k + m keys. m keys are disguised from the attackers and are used only when new keys need to be created once keying events are triggered in the network.

Authentication

Authentication service involves genuineness of the communication. An authentication

[18] mechanism verifies if the exchanged information is emanating from the legitimate participant of the WSN because a malicious entity (e.g., a compromised node) may be able to inject counterfeit content or resend the same content into the network. Moreover, the X.800 specification recommends two sub-cases for authentication. The first involves the authentication of the peer entity and the second deals with the authentication of the origin of the data. For WSNs, the former means authentication of all the nodes that participate in the communication. Authentication can be done between two nodes communicating or one node (e.g., cluster head) and several other nodes around that node (i.e, broadcast authentication). The latter can be implemented at the sink or at an intermediary sensor node where data aggregation takes place.

Current Approaches

There are several traditional methods of authentication in the literature [120]. One is password based method depending on the premise of showing that one knows a secret. The node sends a password with its login information. The receiver verifies that the node is legitimate node by checking that the password is associated with the sender node.

The other one is cryptographic-based method, which is also called challenge- response. A classic technique to provide authentication would be to utilize Message Authentication Codes (MAC). The authenticated sensor node is required to provide the MAC code to be authenticated by the authenticator sensor node. For MACs, hashes, symmetric key-based encryption, and asymmetric key-based encryption methods may all be utilized. Thus, there are several practical ways of creating MACs, but simply creating a MAC involves possessing the same secret at both ends and either encrypting the hash of the content with that key or hashing both the key and the content together. However, as discussed in the confidentiality subsection above, the encryption mechanisms have their associated costs, thus they should be employed with caution.

The last authentication method is address-based or identity-based. For this, the authenticator sensor node can check the identity or the location of the sender node. The password is not sent across the network with these schemes. In comparison to the previous two mechanisms, this method would be very practical for WSNs but would not provide a strong authentication mechanism because it is trivial to spoof a sensor ID. Two of the former leading works include SPINS [12,102-106] and TinySec. They both employ symmetric encryption algorithms and work at the link layer.

Integrity

The recipients in the WSN should be able to detect if the exchanged content between the communicating participants of the WSN have been altered. Furthermore, for the WSN, the integrity service should also ensure that the exchanged content is not deleted, replication of old data, counterfeit, or stale.

Current Approaches

Integrity of the exchanged content is usually provided with the digest of the content appended to the content itself. When the recipient sensor node receives the message it checks to see if the digest of the content that it computes and the digest received equals each other. If they are, then it accepts it as a legitimate message.

Content digests in integrity are created with the usage of hashing algorithms. There are many hashing algorithms in use today. Usually, hashing algorithms do not require the presence of keys unless they are specifically designed to work with keys like keyed-hashing (e.g., HMAC, CMAC). Thus, their impact on a sensor node is only confined with their computational efficiencies. However, as for the keyed-hashing algorithms, previously discussed issues emanating from key generation, key storage, and key exchange are also pertinent here; hence the keyed-hashing techniques must utilize the resources (computation, communication, and storage) efficiently Staleness of the data is of utmost significance in the integrity checking because decision processes of some applications may especially depend on if the data is recent or not. For example, in one very specific WSN application, a certain territory (e.g., territorial waters) could be protected with mines that are detonated by sinks. The freshness and the correct timing of the messages from the sensor nodes in this type of application is very important. A simple solution for these types of applications would be to use counters for the exchanged content. Lastly, another desired aspect of the integrity service may involve providing a recovery mechanism from the altered content.

Access Control

With access control, unauthorized use of a resource is prevented in WSNs. It addresses which participant of the network reaches which content or service. For instance, sensor nodes should not be allowed to have the privileges of sinks such as changing network-wide parameters of the WSN protocols. Thus, limiting services or functionalities depending on the participant would be appropriate.

Current Approaches

One of the most challenging security services for WSNs is access control; hence, this is perhaps why access control for WSNs is one of the security services that have not been studied well in the literature [45]. Believing that part of this is because it is hard to formulate an access control scenario for WSNs. In practical implementations, normally there is one terminating point (i.e., sink) in the network where all the data collected from the network is collected. Thus, other sensors are not expected to access to any resource that may be hosted by other nodes. This is a reasonable expectation for WSN applications where sensors send their readings based on an event. However, there may be sensor applications where source sensor nodes are queried by other sensor nodes as well. For these circumstances, the access control policies can be used. An access control policy should prevent unauthorized nodes from accessing the important information. Setting access policies may also be practical and instrumental for cluster- based or hierarchical sensor node implementations.

Non Repudiation

Non repudiation is service of ensuring that a sensor cannot refute the reception of a message from the other involving party or the set of a message to the other involving party in the communication. According to the X.800 recommendation, the former is the destination and the latter one is called the origin non repudiation.

Current Approaches

Similar to access control, non repudiation has not been formulated well in the WSNs domain. This could be attributed to the lack of need of such a service for WSNs. Or, it could have been thought inside integrity or authentication services implicitly. Although the need for non repudiation service may not seem to be obvious, thinking that it is an achievable important service to contemplate and that there are some practical advantageous in providing this service. A digital signature scheme (DSS), which is based on utilizing encryption methods, would also address non repudiation. Symmetric and asymmetric encryptions can be utilized for DSS. However, their viabilities should be explored in more detail for WSNs. For instance, on the one hand, using the same key both for signature and verification may be vulnerable to another sensor's impersonation of the original sensor's signature. On the other hand, however, employing asymmetric encryption based algorithms may be costly. Naturally, providing non repudiation service may facilitate the endorsement or proof by another entity for a sent or receipt message in WSN.

Availability

Due to threats to the WSN, some portion of the network or some of the functionalities or services provided by the network could be damaged and unavailable to the participants of the network. For instance, some sensors could die earlier than their expected lifetimes. Thus, availability service ensures that the necessary functionalities or the services provided by the WSN are always carried out, even in the case of attacks.

Current Approaches

Availability is a security service that has not been originally considered as one of the security services inside the X.800 recommendation. It may be claimed that it is independent of the security services. The outcome of the secure services provided by the network should guarantee the operations and functionalities aimed by the WSN application. Availability services for WSNs have been mostly studied from the perspective of Denial-of-Service type attacks in the literature. One other pertinent study regarding availability has focused the connectivity properties of WSNs.

Sensor Network Classes

The three application classes have selected are: environmental data collection, security monitoring, and sensor node tracking. We believe that the majority of wireless sensor network deployments will fall into one of these class templates.

Environmental Data Collection

A canonical environmental data collection application is one where a research scientist wants to collect several sensor readings from a set of points in an environment over a period of time in order to detect trends and interdependencies. This scientist would want to collect data from hundreds of points spread throughout the area and then analyze the data offline. The scientist would be interested in collecting data over several months or years in order to look for long-term and seasonal trends. For the data to be meaningful it would have to be collected at regular intervals and the nodes would remain at known locations. At the network level, the environmental data collection application is characterized by having a large number of nodes continually sensing and transmitting data back to a set of base stations that store the data using traditional methods. These network generally require very low data rates and extremely long lifetimes. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment.

Environmental data collection applications typically use tree-based routing topologies

[59] where each routing tree is rooted at high-capability nodes that sink data. Data is periodically transmitted from child node to parent node up the tree-structure until it reaches the sink. With tree-based data collection each node is responsible for forwarding the data of all its descendants. Nodes with a large number of descendants transmit significantly more data than leaf nodes. These nodes can quickly become energy bottlenecks [110], [73]. Once the network is configured, each node periodically samples its sensors and transmits its data up the routing tree and back to the base station. The typical environment parameters being monitored, such as temperature, light intensity, and humidity, does not change quickly enough to require higher reporting rates.

The most important characteristics of the environmental monitoring requirements are long lifetime, precise synchronization, low data rates and relatively static topologies. Additionally it is not essential that the data be transmitted in real-time back to the central collection point. The data transmissions can be delayed inside the network as necessary in order to improve network efficiency.

Security Monitoring

Security monitoring network are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security network are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. These are “report by exception” network.

In security network reducing the latency of an alarm transmission is significantly more important than reducing the energy cost of the transmissions. This is because alarm events are expected to be rare. In a fire security system alarms would almost never be signaled. In the event that one does occur a significant amount of energy could be dedicated to the transmission. Reducing the transmission latency leads to higher energy consumption because routing nodes must monitor the radio channel more frequently. In security network, a vast majority of the energy will be spend on confirming the functionality of neighbouring nodes and in being prepared to instantly forward alarm announcements. Actual data transmission will consume a small fraction of the network energy.

Node Tracking Scenarios

A third usage scenario commonly discussed for sensor network is the tracking of a tagged object through a region of space monitored by a sensor network. There are many situations where one would like to track the location of valuable assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. However, with these systems it is not possible to determine the current location of an object. For example, UPS tracks every shipment by scanning it with a barcode whenever it passes through a routing centre. The system breaks down when objects do not flow from checkpoint to checkpoint. In typical work environments it is impractical to expect objects to be continually passed through check points. With wireless sensor network, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations.

Instead of sensing environmental data, these nodes will be deployed to sense the RF messages of the nodes attached to various objects. The nodes can be used as active tags that announce the presence of a device. A database can be used to record the location of tracked objects relative to the set of nodes at known locations. With this system, it becomes possible to ask where an object is currently, not simply where it was last scanned [138]. Unlike sensing or security network, node tracking applications will continually have topology changes as nodes move through the network. While the connectivity between the nodes at fixed locations will remain relatively stable, the connectivity to mobile nodes will be continually changing. Additionally the set of nodes being tracked will continually change as objects enter and leave the system. It is essential that the network be able to efficiently detect the presence of new nodes that enter the network.

Characteristics of Wireless Sensor Network

WSNs offer unique benefits and versatility with respect to low-power and low-cost rapid deployment for many applications that do not need human supervision. Some of these applications include disaster recovery, military surveillance, health administration, environmental & habitat monitoring, target- tracking etc. Due to the large numbers of nodes involved in the WSN deployment new benefits to the afore-mentioned sensing applications including extended range of sensing, Robustness and fault-tolerance, Improved accuracy, Lower cost.

Wireless Sensor Network (WSN) can be defined as a self-configured and infra structure less wireless network to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the onboard sensors start collecting information of interest. Wireless sensor devices also respond to queries sent from a "control site" to perform specific instructions or provide sensing samples. The working mode of the sensor nodes may be either continuous or event driven. Global Positioning System (GPS) and local positioning algorithms can be used to obtain location and positioning information. Wireless sensor devices can be equipped with actuators to "act" upon certain conditions.

Wireless sensor network (WSNs) enable new applications and require non-conventional paradigms for protocol design due to several constraints. Owing to the requirement for low device complexity together with low energy consumption (i.e. long network lifetime), a proper balance between communication and signal/data processing capabilities must be found. This motivates a huge effort in research activities, standardization process, and industrial investments on this field since the last decade. At present time, most of the research on WSNs has concentrated on the design of energy- and computationally efficient algorithms and protocols, and the application domain has been restricted to simple data-oriented monitoring and reporting applications. A Cable Mode Transition (CMT) algorithm determines the minimal number of active sensors to maintain K-coverage of a terrain as well as K-connectivity of the network. Specifically, it allocates periods of inactivity for cable sensors without affecting the coverage [53], [24] and connectivity requirements of the network based only on local information. A delay-aware data collection network structure for wireless sensor network is proposed. The objective of the proposed network structure is to minimize delays in the data collection processes of wireless sensor network which extends the lifetime of the network. Later considered relay nodes to mitigate the network geometric deficiencies and used Particle Swarm Optimization (PSO) based algorithms to locate the optimal sink location with respect to those relay nodes to overcome the lifetime challenge.

The geometrical solution for locating the optimum sink placement for maximizing the network lifetime. Most of the time, the research on wireless sensor network have considered homogeneous sensor nodes. But nowadays researchers have focused on heterogeneous sensor network where the sensor nodes are unlike to each other in terms of their energy. The problem of deploying relay nodes to provide fault tolerance with higher network connectivity in heterogeneous wireless sensor network, where sensor nodes possess different transmission radii. New network architectures with heterogeneous devices and the recent advancement in this technology eliminate the current limitations and expand the spectrum of possible applications for WSNs considerably and all these are changing very rapidly.

Storage Management

Storage management is an area of sensor network research that is attracting attention. In such class of sensor network, the data must be stored, at least temporarily; within the network until either it is later collected by an observer or ceases to be useful. For example, consider a sensor network that is deployed in a military scenario collecting information about nearby activity. The data has to be dynamically queried by soldiers to attain the mission goals or avoiding sources of danger and help the commanders to assess progress of the mission. The queried data are real-time as well as long-term about enemy activity (for example, to answer a question: Where the supply lines are located?). The data must be stored to enable queries that span temporally long periods, such as days or even months. One can envision similar applications with sensor network deployed in other contexts that answer questions about the environment using recent or historical data. In such network collected data are later accessed by dynamically generated queries. With the knowledge of relevant application and system characteristics, a set of goals for the sensor network storage management can be determined:

a. Minimizing storage size to maximize coverage/data retention

b. Minimizing energy

c. Supporting efficient query execution on the stored data (note that in the reach-back method where all the data must be sent to the observer, query execution is simply transfer of the data to the observer)

d. Providing efficient data management under constrained storage.

Efficiency of query execution can be measured in terms of retrieval time, communication overhead and energy consumption required in sending requested data to the observer. The storage management can influence the efficiency of query execution by effective data placement and indexing. Several approaches to storage management have been proposed to meet these requirements, with most approaches involving a trade off among these different goals.

Storage Management Components

Specifically, each sensor has a local view of the phenomenon. Each sensor sends sensed data to the cluster head (CH) for collaborative storage. Each CH sends it further to resource rich destination for higher degree of collaboration. Further as a result of coordination, a significant reduction in the data to be stored is achieved.

Indexing and Data Retrieval

Indexing and retrieval are more important issues in military type applications, where data can be queried dynamically for example; a commander may be interested in enemy tank movements. Such network are inherently data-centric; observers often name data in terms of attributes or content that may not be topologically relevant. This characteristic of such sensor network is similar to many peer-to-peer (P2P) environments , which are also often data centric. However, existing solutions of data indexing and retrieval in P2P network are not suitable for sensor network due to excessive communication required.

The Geographic Hash Table (GHT) is one of the approaches which can be applied to sensor network. The GHT is a structured approach to sensor network storage that makes it possible to index data on the basis of content without requiring query flooding. GHT also provides load balancing of storage usage (assuming fairly uniform sensor deployment). GHT implements a distributed hash table by hashing a key *k* into geographic coordinates.

Advantages of Storage Management

Accessing and processing data produced in a wireless sensor network using a database like approach has several advantages. Sensors can be deployed in physical environment and applications that manipulate their data; can be created, refined and modified afterwards without any physical intervention on the sensors themselves. The data management activity performed in the network can be remotely controlled by interactively issuing queries, expressed in a high level language, which specify the data, those are of interest for a specific task and how these should be manipulated.

Homogeneous and Heterogeneous

The WS is used the two types of network homogeneous and heterogeneous. The homogeneous mixture is a mixture where the components that make up the mixture are uniformly distributed throughout the mixture. Homogeneous network are less efficient than the heterogeneous network in WSN. So, develop the heterogeneous network. The heterogeneous mixture is a mixture where the components of the mixture are not uniform or have localized regions with different properties, but heterogeneous network are more efficient than the homogeneous network in WSN.

A heterogeneous wireless sensor network [72] consists of different types of sensor nodes, which might measure different data and perform different tasks. To operate such a (sub) network the following devices are required: one management station, several mesh nodes and a comparatively high number of heterogeneous sensor nodes.

The nodes always have data to transmit to a base station, which is often far from the sensing area. This kind of sensor network can be used to track the military object or monitor remote environment. Without loss of generality, assume that the base station is located at the centre of the square region. The network is organized into a clustering hierarchy, and the cluster-heads execute fusion function to reduce correlated data produced by the sensor nodes within the clusters. The cluster-heads transmit the aggregated data to the base station directly.

In the two-level heterogeneous network, there are two types of sensor nodes, i.e., the advanced nodes and normal nodes. Note E_0 the initial energy of the normal nodes, and m the fraction of the advanced nodes, which own a times more energy than the normal ones. Thus there are mN advanced nodes equipped with initial energy of E_0 (1 + a), and (1 - m)N normal nodes equipped with initial energy of E_0. The total initial energy of the two-level heterogeneous network is given by:

$$E_{totaS} = N(1 - N)E_0 + N_N E_0(1 + a) = NE_0(1 + aN) \tag{2.1}$$

Therefore, the two-level heterogeneous network have am times more energy and virtually ‘am’ more nodes. Lets also consider the multi-level heterogeneous network. For multi-level heterogeneous network, initial energy of sensor nodes is randomly distributed over the close set $[E_0, E_0(1 + a_{Nas})]$, where E_0 is the lower bound and a_{Nas} determine the value of the maximal energy. Initially, the node s_i is equipped with initial energy of $E_0(1 + a_i)$, which is a_i times more energy than the lower bound E_0. The total initial energy of the multi-level heterogeneous network is given by:

$$E_{totaS} \quad =_{i=1} E_0(1 + a_i) = E_0(N + \Sigma^N \quad a_i) \tag{2.2}$$

$$\Sigma^N$$

The network is prepared into a clustering hierarchy, and the cluster-heads execute synthesis function to reduce interrelated data produced by the sensor $i=1$ nodes within the clusters. The cluster-heads transmit the aggregated data to the base station directly. As in two-level heterogeneous network, the clustering algorithm should consider the discrepancy of initial energy in multi-level heterogeneous network.

Heterogeneous Network

A heterogeneous wireless sensor network consists of different types of sensor nodes, which might measure different data and perform different tasks. To operate such a (sub) network the following devices are required: one management station, several mesh nodes and a comparatively high number of heterogeneous sensor nodes.

Heterogeneous model is shown in figure 2.3. The nodes always have data to transmit to a base station, which is often far from the sensing area. This kind of sensor network can be used to track the military object or monitor remote environment. Without loss of generality, assume that the base station is located at the centre of the square region. The network is organized into a clustering hierarchy, and the cluster-heads execute fusion function to reduce correlated data produced by the sensor nodes within the clusters. The cluster-heads transmit the aggregated data to the base station directly.

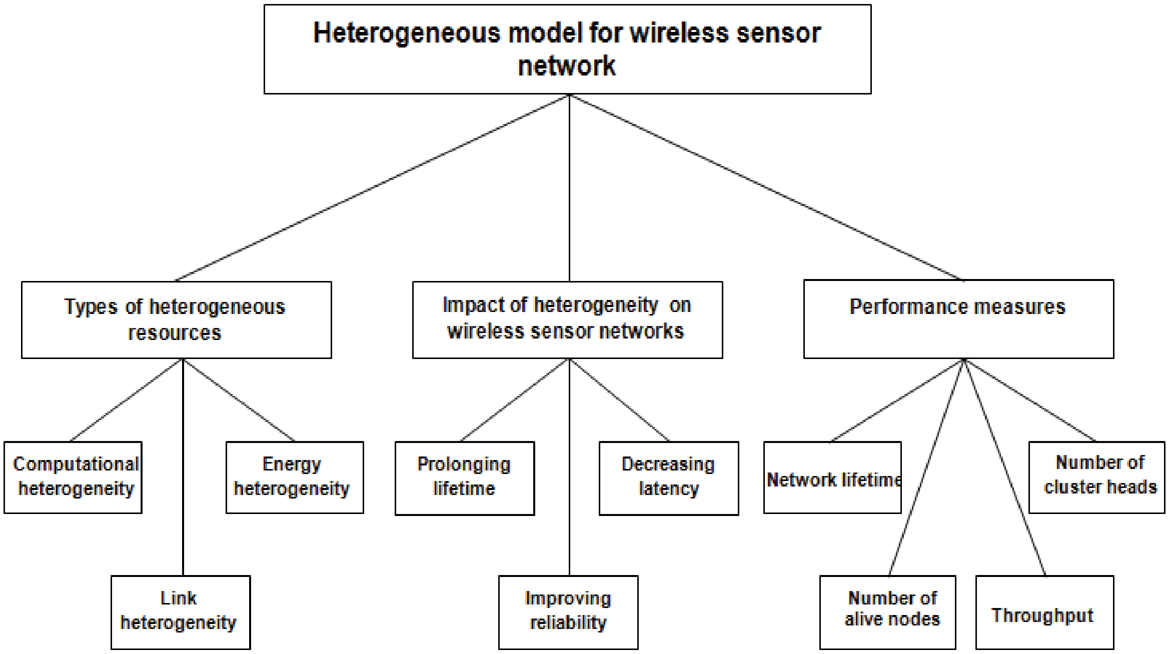


Figure 2.3 Heterogeneous Models for WSN

Types of Heterogeneous Resources

There are three common types of resource heterogeneity in sensor nodes: computational heterogeneity, link heterogeneity and energy heterogeneity.

Computational heterogeneity: It means that the heterogeneous node has a more powerful microprocessor and more memory than the normal node. With the powerful computational resources, the heterogeneous nodes can provide complex data processing and longer-term storage.

Link heterogeneity: It means that the heterogeneous node has high bandwidth and long distance network transceiver than the normal node. Link heterogeneity can provide a more reliable data transmission.

Energy heterogeneity: It means that the heterogeneous node is line powered or its battery is replaceable. Among above three types of resource heterogeneity, the most important resource heterogeneity is the energy heterogeneity because both computational heterogeneity and link heterogeneity will consume more energy resource. If there is no energy heterogeneity, computational heterogeneity and link heterogeneity will bring negative impact to the whole sensor network, i.e., decreasing the network lifetime.

Impact of Heterogeneity on Wireless Sensor Network

Placing few heterogeneous nodes in the sensor network can bring following benefits:

Decreasing latency of data transportation: Computational heterogeneity can decrease the processing latency in immediate nodes and link heterogeneity can decrease the waiting time in the transmitting queue. Fewer hops between sensor nodes and sink node also mean fewer forwarding latency.

Prolonging network lifetime: The average energy consumption for forwarding a packet from the normal nodes to the sink in heterogeneous sensor network will be much less than the energy consumed in homogeneous sensor network.

Improving reliability of data transmission: It is well known that sensor network links tend to have low reliability and each hop significantly lowers the end-to-end delivery rate. With heterogeneous nodes, there will be fewer hops between normal sensor nodes and the sink. So the heterogeneous sensor network can get much higher end-to-end delivery rate than the homogeneous sensor network.

Performance Measures

Some performance measures that are used to evaluate the performance of clustering protocols are listed below

Network Lifetime (stability period): It is the time interval from the start of operation (of the sensor network) until the death of the first alive node.

Number of Cluster Heads Per Round: Instantaneous measure reflects the number of nodes which would send directly to the base station, information aggregated from their cluster members.

Number of Alive Nodes Per Round: This instantaneous measure reflects the total number of nodes and that of each type that has not yet expended all of their energy.

Throughput: This includes the total rate of data sent over the network, the rate of data sent from cluster heads to the base station as well as the rate of data sent from the nodes to their cluster heads.

Homogeneous Network

In homogeneous network all the sensor nodes are identical in terms of battery energy and hardware complexity. With purely static clustering (cluster heads once elected, serve for the entire lifetime of the network) in a homogeneous network, it is evident that the cluster head nodes will be over-loaded with the long range transmissions to the remote base station, and the extra processing necessary for data aggregation and protocol co-ordination. As a result the cluster head nodes expire before other nodes. However it is desirable to ensure that all the nodes run out of their battery at about the same time, so that very little residual energy is wasted when the system expires. One way to ensure this is to rotate the role of a cluster head randomly and periodically over all the nodes as proposed in LEACH [110]. However the downside of using a homogeneous network and role rotation is that all the nodes should be capable of acting as cluster heads, and therefore should possess the necessary hardware capabilities.

Single Hop Homogeneous Network: Following are some of the salient features of a single hop homogeneous sensor network. Since all the nodes are identical, the main design objective is to guarantee a certain network lifetime (in terms of number of data gathering [76] cycles), and at the same time ensure that all the nodes expire at about the same time so that there is very little residual energy left behind when the network expires. Since each node has to be capable of acting as a cluster head, it is necessary for each node to have the hardware capable of performing long range transmissions to the remote base station, complex data computations (if required), and co-ordination of MAC and routing within a cluster. Thus the system is robust to node failures.

Routing

Beyond the basics of WSN routing just presented, there are many additional key issues including: Reliability, Integrating with wake/sleep schedules, Unicast, multicast and anycast semantics, Real-time, Mobility, Voids, Security, and Congestion.

Key issues of Routing

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 “errors,” and packet delivery ratio. Significant empirical evidence indicates that the packet delivery ratio is the best metric, but it can be expensive to collect. Empirical data also show 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 MANET routing algorithms such as DSR and AODV do not work well in WSN because those 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 WSN.

Integration with Wake/Sleep Schedules

To save power many WSNs place nodes into sleep states. Obviously, an awake node should not choose an asleep node as the next hop (unless it first awakens that node).

Unicast, Multicast and Anycast Semantics: As mentioned above, in most cases a WSN rout messages to a geographic destination. What happens when it arrives at this destination? There are several possibilities. First, the message may also include an ID with a specific unicast node in this area as the target, or the semantics may be that a single node closest to the geographic destination is to be the unicast node. Second, the semantics could be that all nodes within some area around the destination address should receive the message. This is an area multicast. Third, it may only be necessary for any node, called any cast, in the destination area to receive the message.

Real-Time

For some applications, messages must arrive at a destination by a deadline. Due to the high degree of uncertainty in WSN it is difficult to develop routing algorithms with any guarantees.

Some protocol uses a notion of velocity to prioritize packet transmissions. Velocity is a nice metric that combines the deadline and distance that a message must travel.

Voids

Since WSN nodes have a limited transmission range, it is possible that for some node in the routing path there are no forwarding nodes in the direction a message is supposed to travel. Protocols like GPSR [64] solve this problem by choosing some other node "not" in the correct direction in an effort to find a path around the void.

Security and Congestion

If adversaries exist, they can perpetrate a wide variety of attacks on the routing algorithm including selective forwarding, black hole, Sybil, replays, wormhole and denial of service attacks. Unfortunately, almost all WSN routing algorithms have ignored security and are vulnerable to these attacks. Today, many WSN has periodic or infrequent traffic. Congestion does not seem to be a big problem for such network. However, congestion is a problem for more demanding WSN 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 use back pressure, reducing source node transmission rates, throwing out less important messages, and using scheduling to avoid as many collisions as possible which only exacerbate the congestion problem.

Reduce Costs

The sensor network consist of a large number of sensor nodes. To identify the overall cost of the network, a single node cost is very important. So, the cost of each sensor node has to be low in cost, Reduce Installation costs and time, Reduce maintenance costs

Increasing Efficiency: Optimize measurement processes, Access data almost anywhere and anytime, Decrease Downtime.

Wireless Sensor Network Routing Protocols

The survey of different routing protocols that have been developed for secure sensor network and find their capabilities and deficiencies and suggest the most efficient among them. A wireless sensor network (WSN) consists of numerous tiny autonomous sensing nodes that are deployed across a wide geographical area. Routing in WSN differs according to the type of its network structure. The figure 2.4 below shows the different network architectures and routing techniques used by the protocols to work.

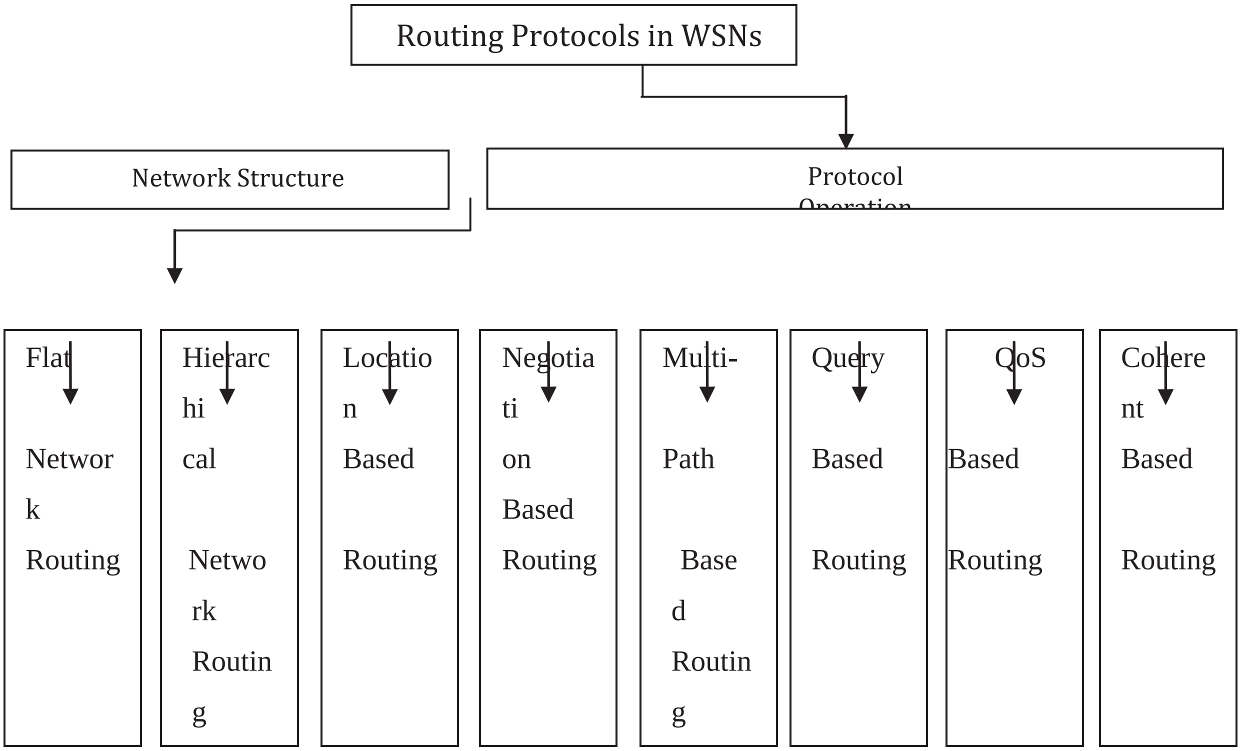


Figure 2.4 Routing protocols in WSN

Current routing techniques are Flat-routing, Hierarchical-routing and Location-based routing.

Flat based Routing

Each sensor node behaves the same way and co-operates with other nodes to perform the sensing task. The network contains a large number of such nodes and a Base Station (BS) sends queries to certain regions and waits for data from the sensors located in the selected regions. Data-centric routing is used where there is no global identifier for nodes; instead data are identified using attribute based naming.

Advantages

The advantages of at routing protocols are scalability and simplicity. Flat network are scalable because each node participates equally in the routing task and the nodes only need information about their direct neighbours for routing. New nodes can easily be added to the network that use at routing protocols.

Disadvantage

The main disadvantage of at routing protocols is the creation of hotspots. The nodes around the base station will deplete their energy sources faster than the other nodes. This cannot be avoided because all the packets have to be routed to the base station eventually. This might not be a problem in network that have more than one base station. Network disconnectivity is another problem where certain sections of the network can become unreachable. If there is only node connecting a part of the network to the rest and if it fails, then that section would be cut off from rest of the network.

Hierarchical Routing

Hierarchical routing protocols are based on cluster heads and the process by which the nodes decide which clusters to join. Routing path establishment is usually not considered because the nodes are one hop away from the cluster head and they always send data to the cluster head. Since most of the hierarchical routing protocols follow the same procedure, only the important hierarchical protocols are explained the following section. This routing method has special advantages related to scalability and efficient communication; they also provide energy-efficient routing in WSNs.

Advantages

The advantages of hierarchical routing are data aggregation and localized power consumption. Data from the entire cluster can be combined with the cluster head and then sent to the base station in a single packet. The amount of power consumed in a cluster is less than the network as a whole.

Disadvantages

The disadvantages of hierarchical routing are the creation of hotspots, special hardware requirements, complexity and non-scalable. Hotspots are created because the nodes elected as cluster heads consume more energy than other nodes in the network. If the cluster heads are not rotated regularly, the network becomes partitioned and this causes areas to become cut off from the network.

Most of the hierarchical routing protocols require the cluster heads to have special hardware requirements like better radio equipments, higher processing power, more energy resources and etc. In network that rotate the cluster heads, the cluster head selection is very complex and requires high processing capability.

Hierarchical protocols are not very scalable because the number of cluster heads increases as the network size increases. The message overhead also increases as the number of nodes in the network increase.

Location-based Routing

Sensor nodes are addressed depending on their locations. Relative coordinates of neighboring nodes are obtained either by exchanging information between neighbor nodes or by directly communicating with a Global Positioning System (GPS) [80].

The Hierarchal routing is the routine that operates in the hierarchal structures of WSNs. The main goal of the hierarchal routing protocols is to save the energy of sensor nodes as much as possible, and hence it prolongs the WSN lifetime. To design energy aware hierarchal routing protocol.

Protocol Operation based Routing Protocols

Routing protocols [80] taxonomy has another basic and important classification, namely operation based routing protocols. They are Multipath based, Query-based, Negotiation based Quality-of-service based and Coherent-based routing protocols.

Multipath-Based

These protocols are efficient in handling multiple paths. Nodes send the collected data on multiple paths rather than using a single path. The reliability and fault tolerance of the network increases as there is, as long as it is possible, an alternative path when the primary path fails.

Query-Based

Query-based routing propagates the use of queries issued by the base station. The base station sends queries requesting for certain information from the nodes in the network. A node, which is responsible for sensing and collecting data, reads these queries and if there is a match with the data requested in the query it starts sending the data to the requested node or the base station. This process is known as Directed Diffusion [57] where the base station sends interest messages on to the network. These interest messages, which move in the network, create a path while passing through all the sensor nodes. Any sensor node, which has the data suitable to the interest message, sends collected data along with the interest message towards the base station. Thus, less energy is consumed and data aggregation is performed on a route.

Negotiation-Based

These protocols use high-level descriptions coded in high level so as to eliminate the redundant data transmissions. Flooding is used to disseminate data, due to the fact that flooding data are overlapped and collisions occur during transmissions. Nodes receive duplicate copies of data during transmission. The same data content is sent or exchanged again and again between the same set of nodes, and a lot of energy is utilized during this process. Negotiation protocols like SPIN [123] are used to suppress duplicate information and prevent redundant data from being sent to the next neighbouring nodes or towards the base station by performing several negotiation messages on the real data that has to be transmitted.

Quality of Service (QoS)-Based

In this type of routing protocol, both quality and energy have to be maintained within the network. Whenever a sink requests for data from the sensed nodes in the network, the transmission has to satisfy certain quality-of-service parameters, such as, for example, bounded latency (data has to be sent as soon as it is sensed without delaying any further) and bandwidth consumed. Sequential Assignment Routing (SAR) [115] is one of the first routing protocols that use the notion of QoS in routing decisions. Routing decision in SAR depends on three factors: energy consumption within the network by the sink and the nodes, QoS of each path in the network, and priority level of each packet sent.

Coherent-Based

In a WSN, the sensor nodes collect data and send it to the nearest neighbours or the sink within the network. In this process, the processing of the collected data is the most important event. There are two types of data-processing techniques followed within the network structure: coherent and non-coherent data processing based routing. All the nodes within the network collect the data and process it before sending to the next nearest node for further processing. This technique is called non-coherent data process routing and the nodes that perform further processing on the data are called aggregators. In coherent routing, after minimum processing, the data is forwarded to the aggregators. This minimum processing includes functions like time stamping or duplicate suppression. This technique is energy efficient as all the processing is done by the nodes, which reduces the total time and energy consumption.

Routing Challenges and Design Issues in WSN

Despite the innumerable applications of WSNs, these network have several restrictions, e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSNs is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. The design of routing protocols in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs. In the following, we summarize some of the routing challenges and design issues that affect routing process in WSNs.

Node Deployment

Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized.

In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter-sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

Energy Consumption without Losing Accuracy

Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime [45]. In a multihop WSN [28], each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Data Reporting Model

Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. Data reporting categorizes [144]; Time-driven (continuous), Event-driven, Query-driven and Hybrid. The time-driven delivery model is suitable for applications that require periodic data monitoring. As such, sensor nodes will periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest at constant periodic time intervals. In event-driven and query-driven models, sensor nodes react immediately to sudden and drastic changes in the value of a sensed attribute due to the occurrence of a certain event or a query is generated by the BS. As such, these are well suited for time critical applications. A combination of the previous models is also possible. The routing protocol is highly influenced by the data reporting model with regard to energy consumption and route stability.

Node/Link Heterogeneity

In many studies, all sensor nodes were assumed to be homogeneous, i.e. having equal capacity in terms of computation, communication, and power. However, depending on the application a sensor node can have different role or capability. The existence of heterogeneous set of sensors raises many technical issues related to data routing. For example, some applications might require a diverse mixture of sensors for monitoring temperature, pressure and humidity of the surrounding environment, detecting motion via acoustic signatures, and capturing the image or video tracking of moving objects. These special sensors can be either deployed independently or the different functionalities can be included in the same sensor nodes. Even data reading and reporting can be generated from these sensors at different rates, subject to diverse quality of service constraints, and can follow multiple data reporting models. For example, hierarchical protocols designate a cluster-head node different from the normal sensors. These cluster heads can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth, and memory. Hence, the burden of transmission to the BS is handled by the set of cluster-heads.

Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signalling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

Network Dynamics

Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's and sensor nodes is sometimes necessary in many applications [145]. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS.

Transmission Media

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. In general, the required bandwidth of sensor data will be low, on the order of 1-100 kb/s. Related to the transmission media is the design of medium access control (MAC). One approach of MAC design for sensor network is to use

TDMA based protocols that conserve more energy compared to contention based protocols like CSMA (e.g., IEEE 802.11).

Connectivity

High node density in sensor network precludes them from being completely isolated from each other. Therefore, sensor nodes are expected to be highly connected. This, however, may not prevent the network topology from being variable and the network size from being shrinking due to sensor node failures. In addition, connectivity depends on the, possibly random, distribution of nodes.

Coverage

In WSNs, each sensor node obtains a certain view of the environment. A given sensor's view of the environment is limited both in range and in accuracy; it can only cover a limited physical area of the environment. Hence, area coverage is also an important design parameter in WSNs.

Data Aggregation

Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. This technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols. Signal processing methods can also be used for data aggregation. In this case, it is referred to as data fusion where a node is capable of producing a more accurate output signal by using some techniques such as beam forming to combine the incoming signals and reducing the noise in these signals.

Quality of Service

In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime.

Energy Awareness

Every node uses some energy for activities like sensing, processing, storage and transmission. A node in the network should know how much energy will be utilized to perform a new task that is submitted, the amount of energy that is dissipated can vary from high, moderate to low depending upon the type of functionality or activity it has to perform.

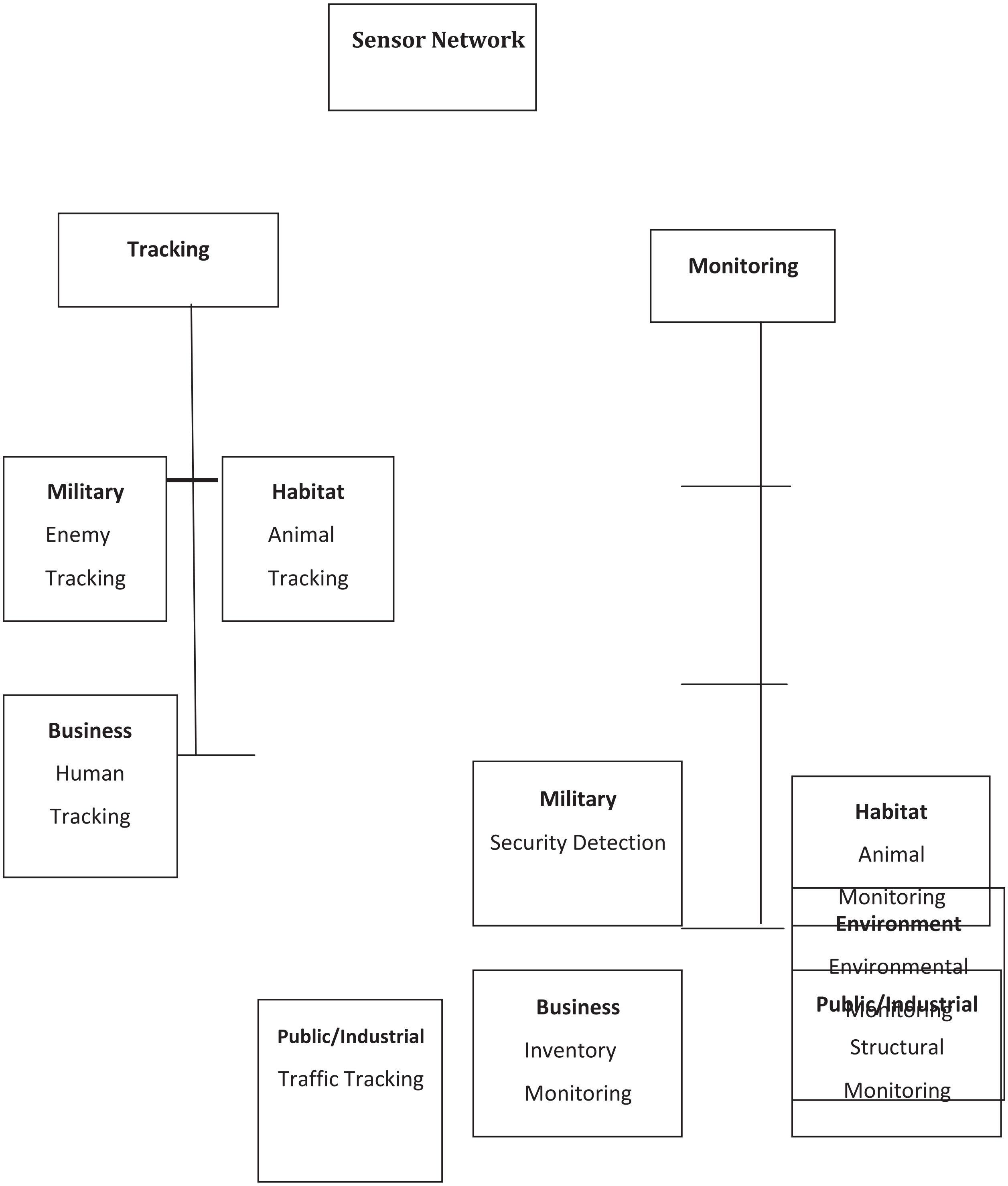
Transmission Scheme

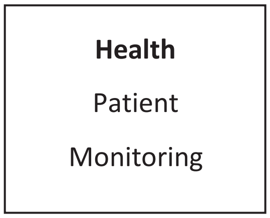
Sensor nodes which collect the data transmit it to the sink or the base station either using the hierarchical routing schemes.

Network Power Usage

All the sensor nodes in the network use a certain amount of network power which helps them to perform certain activities like sensing or processing or even forming groups within the network area. The amount of energy or power utilized by the sensor nodes or a group of sensors within the network is known as network power usage.

Applications of Wireless Sensor Network





Health

Patient

Monitoring

Figure 2.5 Overview of Sensor Applications

Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.

Health Applications: Some of the health applications for sensor network are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.

Environmental Sensing: The term Environmental Sensor Network has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc. Some other major areas are listed below: Air pollution monitoring , Forest fires detection ,Greenhouse monitoring, Landslide detection.

Structural Monitoring: Wireless sensors can be utilized to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc enabling Engineering practices to monitor assets remotely without the need for costly site visits.

Industrial Monitoring: Wireless sensor network have been developed for machinery condition- based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.

Agricultural sector: using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Irrigation automation enables more efficient water use and reduces waste.

Health Applications

Some of the health applications for sensor network are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals;

telemonitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.

Tele Monitoring of Human Physiological Data: The physiological data collected by the sensor network can be stored for a long period of time, and can be used for medical exploration. The installed sensor network can also monitor and detect elderly people's behaviour, e.g., a fall. These small sensor nodes allow the subject a greater freedom of movement and allow doctors to identify pre-defined symptoms earlier. Also, they facilitate a higher quality of life for the subjects compared to the treatment centres. A ''Health Smart Home'' is designed in the Faculty of Medicine in Grenoble—France to validate the feasibility of such system.

Tracking and Monitoring Doctors and Patients Inside a Hospital: Each patient has small and light weight sensor nodes attached to them. Each sensor node has its specific task. For example, one sensor node may be detecting the heart rate while another is detecting the blood pressure. Doctors may also carry a sensor node, which allows other doctors to locate them within the hospital.

Drug Administration in Hospitals**:** If sensor nodes being attached to medications, the chance of getting and prescribing the wrong medication to patients can be minimized. Because, patients will have sensor nodes that identify their allergies and required medications can be made. Computerized systems as described in have shown that they can help minimize adverse drug events.

Home Applications

Home automation: As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs. These sensor nodes inside the domestic devices can interact with each other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily.

Smart environment: The design of smart environment can have two different perspectives, that is, human-centered and technology-centered. For human-centered, a smart environment has to adapt to the needs of the end users in terms of input/ output capabilities. For technology- centered, new hardware technologies, networking solutions, and middleware services have to be developed. A scenario of how sensor nodes can be used to create a smart environment is described in. The sensor nodes can be embedded into furniture and appliances, and they can communicate with each other and the room server. The room server can also communicate with other room servers to learn about the services they offered, e.g., printing, scanning, and faxing. These room servers and sensor nodes can be integrated with existing embedded devices to become self-organizing, self regulated, and adaptive systems based on control theory models as described in. Another example of smart environment is the ‘‘Residential Laboratory’’ at Georgia Institute of Technology. The computing and sensing in this environment has to be reliable, persistent, and transparent.

Other Commercial Applications

Some of the commercial applications are monitoring material fatigue; building virtual keyboards; managing inventory; monitoring product quality; constructing smart office spaces; environmental control in office buildings; robot control and guidance in automatic manufacturing environments; interactive toys; interactive museums; factory process control and automation; monitoring disaster area; smart structures with sensor nodes embedded inside; machine diagnosis; transportation; factory instrumentation; local control of actuators; detecting and monitoring car thefts; vehicle tracking and detection; and instrumentation of semiconductor processing chambers, rotating machinery, wind tunnels, and anechoic chambers.

Environmental Control in Office Buildings: The air conditioning and heat of most buildings are centrally controlled. Therefore, the temperature inside a room can vary by few degrees; one side might be warmer than the other because there is only one control in the room and the air flow from the central system is not evenly distributed. A distributed wireless sensor network system can be installed to control the air flow and temperature in different parts of the room. It is estimated that such distributed technology can reduce energy consumption by two quadrillion British Thermal Units (BTUs) in the US, which amounts to saving of $55 billion per year and reducing 35 million metric tons of carbon emissions.

Interactive Museums: In the future, children will be able to interact with objects in museums to learn more about them. These objects will be able to respond to their touch and speech. Also, children can participate in real time cause-and-effect experiments, which can teach them about science and environment. In addition, the wireless sensor network can provide paging and localization inside the museum. An example of such museums is the San Francisco Exploratorium that features a combination of data measurements and cause and- effect experiments.

Detecting and Monitoring Car Thefts: Sensor nodes are being deployed to detect and identify threats within a geographic region and report these threats to remote end users by the Internet for analysis.

Managing Inventory Control: Each item in a warehouse may have a sensor node attached. The end users can find out the exact location of the item and tally the number of items in the same category. If the end users want to insert new inventories, all the users need to do is to attach the appropriate sensor nodes to the inventories. The end users can track and locate where the inventories are at all times.

Vehicle Tracking and Detection: There are two approaches as described in to track and detect the vehicle: first, the line of bearing of the vehicle is determined locally within the clusters and then it is forwarded to the base station, and second, the raw data collected by the sensor nodes are forwarded to the base station to determine the location of the vehicle.

Traditional WSNs Applications

Monitoring needs a high probability of success in the packet delivery (reliability). In addition to reliability, control applications ask also for timely packet delivery (latency). If reliability and latency constraints are not met, the correct execution of control decisions may be severely compromised, thus creating unstable control loops. High reliability and low latency may demand significant energy expenditure, thus reducing the WSN lifetime. Controllers can usually tolerate a certain degree of packet losses and delay : For example, the stability of a closed loop control system may be ensured by high reliable communications and large delays, or by low delays when the packet loss is high. In contrast to monitoring applications, for control applications there is no need to maximize the reliability. A trade-off between latency, packet losses, and stability requirements can be exploited for the benefit of the energy consumption, as proposed by the system level design approach. Therefore, claimed that the protocol design for control needs a system-level approach whereby the need of a parsimonious use of energy and the typical requirements of the control applications are jointly taken into account and control and WSNs protocols are co-designed. Exploiting such a trade-off poses extra challenges when designing WSNs protocols for control applications when compared to more traditional communication network, namely:

Advantages of Wireless Sensor Network

The WSNs has revolutionized the world around us. They are becoming integral part of our lives, more so than the present-day computers because of their numerous advantages as mentioned below

Ease of Deployment

A sensor network contains hundreds or even thousands of nodes and can be deployed in remote or dangerous environments. Since these nodes are small and economical, throwing of hundreds or thousands of micro-sensors from a plane flying over a remote or dangerous area allows extracting information in ways that could not have been possible otherwise.

Extended Range of Sensing

Single macro-sensor nodes can only extract data about events in a limited physical range. In contrast, a micro-sensor network uses large numbers of nodes enabling them to cover a wide area.

Improved Lifetime

The nodes located close to each other will have correlated data therefore they can be grouped together. Only one of the nodes in a round robin fashion from the group therefore needs to be in active state at any instance of time keeping other nodes in sleep state. It will enhance the network life time.

Fault Tolerance

In WSN several sensor nodes are close to each other and have correlated data, it makes these systems much more fault tolerant than single macro-sensor system. The macro-sensor system cannot function if macro-sensor node fails, whereas in case of micro-senor network even if smaller number of micro-sensor nodes fails, the system may still produce acceptable qualitative information.

Improved Accuracy

While an individual micro-sensor's data might be less accurate than a macro-sensor's data. The data from nodes located close to each other can be combined since they are gathering information about the same event. It will result in better accuracy of the sensed data and reduced uncorrelated noise.

Lower Cost

Even though, to replace each macro-sensor node several micro-sensor nodes are required they will still be collectively much cheaper than their macro-sensor counterpart due to their reduced size, simple as well as cheap circuitry and lesser accuracy constraints. As a result, protocols that enable micro-sensor network to provide necessary support in sensing applications are becoming more popular.

Summary

A brief introduction about Wireless Sensor Network, illustrating the different fundamental aspects and components of Wireless Sensor Network, the architecture, issues and challenges in Wireless Sensor Network, classes of sensor network and various Wireless sensor network applications was provided. The crucial energy and security problem which is a cause of concern in the field of wireless sensor network was also discussed.