Wireless Sensor Networks

Introduction

A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity.

The environment can be the physical world, a biological system, or an information technology (IT) framework. Network(ed) sensor systems are seen by observers as an important technology that will experience major deployment in the next few years for a plethora of applications, not the least being national security. Typical applications include, but are not limited to, data collection,monitoring, surveillance, and medical telemetry. In addition to sensing, one is often also interested in control and activation.

There are four basic components in a sensor network:

1. an assembly of distributed or localized sensors
2. an interconnecting network (usually, but not always,wireless-based)
3. a central point of information clustering; and
4. a set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining.

In this context, the sensing and computation nodes are considered part of the sensor network; in fact, some of the computing may be done in the network itself. Because of the potentially large quantity of data collected, algorithmic methods for data management play an important role in sensor networks. The computation and communication infrastructure associated with sensor networks is often specific to this environment and rooted in the device and application-based nature of these networks.

Constraints and challenges.

Individual sensor node in WSN is a resource constrained. They have limited processing capability, storage capacity, and communication bandwidth. It is necessary to consider the hardware constraints of the sensor nodes.

A. **Energy** In WSN Energy is the biggest constraint. Energy consumption in sensor nodes can be divided into three parts:

1. Energy for the transducer.
2. Energy for communication among sensor nodes.
3. Energy for microprocessor computation. It was found that each bit transmitted in WSNs consumes about as much power as executing 800–1000 instructions. Thus, communication is more costly than computation in WSN's.

B. **Power Consumption** The wireless sensor node are micro-electronic device that can be equipped with very limited power source (<0.5 Ah, 1.2 V). In some application, replenishment of power resources might be impossible. Sensor node lifetime, therefore, shows a strong dependence on battery lifetime.

C. **Memory** Memory of sensor nodes usually consists of flash memory and RAM. Flash memory is used to store downloaded application code and RAM is used for storing application programs, sensor data, and intermediate computations. There is limited space to run complicated algorithms and functions after loading OS and application code [5].

D. **Transmission Range** Range of communication in sensor nodes is very limited for both technically and by the need to conserve energy. The actual range achieved from a given transmission signal strength is dependent on various environmental factors such as weather, vibration, humidity, pressure and terrain etc.

E. **Communication** A sensor node utilize maximum energy in data communication. This involves both data transmission and reception. It can be seen that for short-range communication with low radiation power, transmission and reception energy costs are nearly the same. Mixers, frequency synthesizers, phase locked loops (PLL), voltage control oscillators (VCO) and power amplifiers, all consume valuable power in the transceiver circuitry.

F. **Higher Latency In Communication** Network congestion, Multi-hop routing and processing in the intermediate nodes of WSN may give rise to higher latency in packet transmission. So, it is very difficult to achieve synchronization. Such synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution.

G. **Unattended Operation Of Networks** Generally, the nodes in a WSN are deployed in remote regions like mountain, terrain and are left unattended. The likelihood that a sensor experiences a physical attack in such an environment is therefore, very high. Detection of physical tampering is virtually impossible due to remote management of a WSN.

Applications of Sensor Networks.

Wireless sensor network are deployed widely and they give an economical solution to many problems. In this section we give a survey on applications of Wireless Sensor Networks. Here are some typical and promising applications of WSNs are: A. **Military Applications** It can be used as commanders to monitor the status (position, quantity, availability) of their troops, equipment and battlefield surveillance or reconnaissance of opposing forces and terrain to target the enemy, to detect attack etc. B. **The Medical Application** Sensors can be extremely useful in patient diagnosis and monitoring. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure [8]. C. **Commercial Applications** It can be used to detect/track/monitor a vehicle, to support interactive devices, or to control environmental condition of a building. D. **Environmental Monitoring** It can be used to monitor the condition/status of environment such as humidity, temperature, pressure, and pollution in soil, marine, and atmosphere. It also includes traffic, habitat, Wild fire etc. E. **Infrastructure Protection Application** It includes water distribution monitoring power grids monitoring, etc. [8]. F. Scientific Exploration WSNs can be deployed under the water or on the land surface of a planet for scientific research purpose. G. **Public Safety** WSNs can be applied to monitor the chemical, biological or other environmental threats, it is important that the availability of the network is never threatened.

Advantages of WSN

1. Network setups can be carried out without fixed infrastructure.
2. Suitable for the non-reachable places such as over the sea, mountains, rural areas or deep forests.
3. Flexible if there is random situation when additional workstation is needed.
4. Implementation pricing is cheap.

5. It avoids plenty of wiring.
6. It might accommodate new devices at any time.
7. It's flexible to undergo physical partitions.
8. It can be accessed by using a centralized monitor.

Mobile Ad hoc NETworks or MANET's

An ad hoc network is a network that is setup, literally, for a specific purpose, to meet a quickly appearing communication need. The simplest example of an ad hoc network is perhaps a set of computers connected together via cables to form a small network, like a few laptops in a meeting room. In this example, the aspect of self-configuration is crucial – the network is expected to work without manual management or configuration.Usually, however, the notion of a MANET is associated with wireless communication and specifically wireless multihop communication; also, the name indicates the mobility of participating nodes as a typical ingredient. Examples for such networks are disaster relief operations – firefighters communicate with each other – or networks in difficult locations like large construction sites, where the deployment of wireless infrastructure (access points etc.), let alone cables, is not a feasible option. In such networks, the individual nodes together form a network that relays packets between nodes to extend the reach of a single node, allowing the network to span larger geographical areas than would be possible with direct sender – receiver communication.

MANET	WSN
diversity, although present, is not quite as large in MANETs.	WSNs are conceivable with very different network densities, from very sparse to very dense deployments, which will require different or at least adaptive protocols.
MANETs, on the other hand, are used to support more conventional applications (Web, voice, and so on) with their comparably well understood traffic characteristics.	WSNs have to interact with the environment, their traffic charateristics can be expected to be very different from other, human-driven forms of networks. A typical consequence is that WSNs are likely to exhibit very low data rates over a large timescale, but can have very bursty traffic when something happens (a phenomenon known from real-time systems as event showers or alarm storms). Long periods (months) of inactivity can alternate with short periods (seconds or minutes) of very high activity in the network, pushing its capacity to the limits.
MANETs also have scarce energy but compared to WSN they have large resources.	WSNs have tighter requirements on network lifetime, and recharging or replacing WSN node batteries is much less an option than in MANETs
In a MANET, each individual node should be fairly reliable	in a WSN, an individual node is next to irrelevant.in a WSN, an individual node is next to irrelevant

Issues	MANET	WSN
Standards	IEEE 802.11	IEEE 802.15.4
Number of nodes	Less than WSN	Very large
Node movement	Decentralized	Centralized
Node works	Nodes act both as host & router	Nodes separately
Interaction	"Closed" to humans	With environment
Main purpose	Distributed computing	Information gathering
Application-equipment	More expensive	Less than MANET
Application-specific	Comparably uniform	Much stronger on application specifics
Scale	Larger	Much larger
Bandwidth	Deficient more than WSN	Sometimes deficiency
Failure in nodes	Less than WSN	prone to failure
Data rate	Designed to carry rich multimedia data	Very low
Data redundancy	No	Yes
Power	-	Limited
Population of nodes	Sparsely	Densely
Deployed by	Several unrelated entities	Single owner
Application node	-	stationary nodes
Communication mode	Point-to-Point	Broadcast
Routing Protocols	Pro-active, Reactive, Hybrid	Flooding, Gossiping, Flat Routing, Hierarchical, Location based
Memory constrained	Less than WSN	Very high
	[illegible]	Depends on

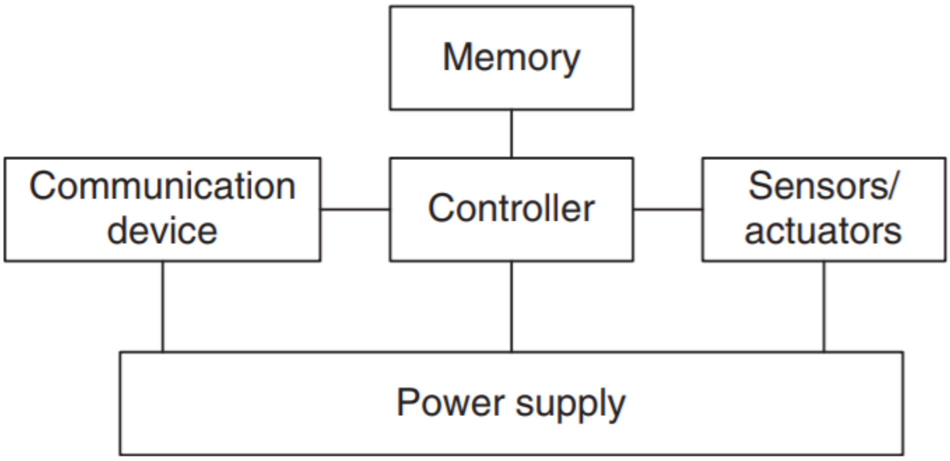
Network size	Depends on active users	Depends on extension of the observed area

Enabling technologies for wireless sensor networks.

Building such wireless sensor networks has only become possible with some fundamental advances in enabling technologies. First and foremost among these technologies 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 contemplated. This is particularly relevant to microcontrollers and memory chips as such, but also, the radio modems, responsible for wireless communication, have become much more energy efficient. Reduced chip size and improved energy efficiency is accompanied by reduced cost, which is necessary to make redundant deployment of nodes affordable.

Energy supply for a sensor node is at a premium: batteries have small capacity, and recharging by energy scavenging is complicated and volatile. Hence, the energy consumption of a sensor node must be tightly controlled. Newer Advancements in technologies have introduced new battery optimization paradigms which have greatly contributed to growth of WSN. Most newly designed chips have low power consumption which in turn make a power efficient sensor node.

Single Node Architecture



A basic sensor node comprises five main components:

1. **Controller** A controller to process all the relevant data, capable of executing arbitrary code.
2. **Memory** Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.
3. **Sensors and actuators** The actual interface to the physical world: devices that can observe or control physical parameters of the environment.
4. **Communication** Turning nodes into a network requires a device for sending and receiving information over a wireless channel.

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).

Each of these components has to operate balancing the trade-off between as small an energy consumption as possible on the one hand and the need to fulfill their tasks on the other hand. For example, both the communication device and the controller should be turned off as long as possible. To wake up again, the controller could, for example, use a preprogrammed timer to be reactivated after some time. Alternatively, the sensors could be programmed to raise an interrupt if a given event occurs – say, a temperature value exceeds a given threshold or the communication device detects an incoming transmission.

Components:

1. **Controller**

   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

2. **Memory**

   The memory component is fairly straightforward. Evidently, 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. The long read and write access delays of flash memory should be taken into account, as well as the high required energy.

3. **Sensors and actuators**

   Sensors Sensors can be roughly categorized into three categories:

   - **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. There is no notion of "direction" involved in these measurements. Typical examples for such sensors include thermometer, light sensors, vibration, microphones, humidity, mechanical stress or tension in materials, chemical sensors sensitive for given substances, smoke detectors, air pressure, and so on.
   - **Passive, narrow-beam sensors** These sensors are passive as well, but have a well-defined notion of direction of measurement. A typical example is a camera, which can "take measurements" in a given direction, but has to be rotated if need be.
   - **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.

   Actuator

- In the context of sensor networks, any output device. **Actuator**s allow a WSN node to influence its environment, providing a feedback channel through which its decisions can be enacted.
- It is something, typically a mechanism, which converts energy to motion. The most common example is a motor, but it can be a pump, switch or valve.
- A motor which is installed in the control system of a vibrating mechanism to adjust the response. An **actuator** actually converts the imposed energy into motion.
- A device that converts energy into motion. It also can be used to apply a force.
- A mechanical device for moving or controlling something.
- A device used to produce a motion or action. The major **actuator**s in industrial applications are electric motors, hydraulic and pneumatic cylinders.
- An effecting unit that agents can use to manipulate their environment.

4. **Communication Devices**

   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 network like settings (using field buses like Profibus, LON, CAN, or others). The communication devices for these networks are custom off-the-shelf components. The case of wireless communication is considerably more interesting. The first choice to make is that of the transmission medium – the usual choices include radio frequencies, optical communication, and ultrasound; other media like magnetic inductance are only used in very specific cases. Of these choices, Radio Frequency (RF)-based communication is by far the most relevant one as it best fits the requirements of most WSN applications: It provides relatively long range and high data rates, acceptable error rates at reasonable energy expenditure, and does not require line of sight between sender and receiver.

5. **Power Supply**

   For untethered wireless sensor nodes, the power supply is a crucial system component. There are essentially two aspects: First, storing energy and providing power in the required form; second, attempting to replenish consumed energy by "scavenging" it from some node-external power source over time.

   Storing power is conventionally done using batteries. As a rough orientation, a normal AA battery stores about 2.2–2.5 Ah at 1.5 V. Battery design is a science and industry in itself, and energy scavenging has attracted a lot of attention in research