Principle of Wireless Sensor Network

Wireless Sensor Network is a network of autonomous sensor nodes that are capable of collecting, processing and transmitting data wirelessly. WSNs are used in a wide range of applications, including environmental monitoring, surveillance, industrial automation and healthcare. The principles of WSNs can be summarized as follows:

- Resource constraints: Sensor nodes in a WSN are typically low-power, and have limited computational and storage capabilities. They rely on battery power and are expected to operate for extended periods without maintenance or battery replacement.
- Communication: Sensor nodes communicate with each other wirelessly, typically using radio frequency (RF) transmissions. The communication range of each node is limited, and nodes must cooperate to rely data over longer distances.
- Data aggregation: To conserve energy and reduce bandwidth requirements, sensor nodes often perform local data aggregation before transmitting data to the base station or sink node.
- Routing: Sensor nodes must determine the best route for data transmission to the base station, taking into account the network topology, communication range, and energy constraints of each node
- Security: Sensor networks can be vulnerable to security threats, including eavesdropping, tampering and node compromise. Security mechanisms such as encryption, authentication and access control are necessary to orotect the network and its data.
- Data Processing: Sensor nodes may perform basic processing of the collected data, such as filtering or compression, before transmitting it to the base station. Data processing algorithms may also be distributed across multiple nodes to improve efficiency and reduce latency
- Application-specific functionality: WSN are designed for specific applications and the functionality of the network is tailored to meet the requirements of the application. Examples of applications include environmental monitoring, surveillance and industrial automation.

Application Types

Application of wireless sensor networks can be classified based on the interaction pattern between sources and sinks. The classification is as follows:

- Event detection : In this category of application, Sensor nodes should report to the sink once they have detected the occurrence of a specified event. The simplest event scan be detected locally by a single sensor node in isolation (e.g a temperature threshold is exceeded). If several different events can occur, event classification is necessary.
- Periodic Measurements: In this type of applications sensor has to periodically report the measured values. The reporting period is application dependent.
- Function Approximation and edge detection: Physical values like temperature which changes from one place to another can be regarded as a function of location. A WSN can be used to approximate this unknown function using a limited number of samples taken at each individual sensor node this is function approximation. Similarly, finding edges or structures in such functions along the boundaries of patterns is called edge detection.
- Tracking: This includes applications where the source of an event is mobile (e.g an intruder in surveillance scenarios). The WSN can be used to report updates on the event source's position to the sink, like speed and direction.
- Deployment option
    1. Fixed Deployment: Well planned deployment of sensor nodes
    2. Random Deployment: By dropping a large number of nodes from an aircraft over a forest fire.

Challenges For Wireless Sensor Networks

Major challenges for WSN is in its characteristic requirements and required mechanisms

- Characteristic Requirements
  - Types of service: WSN is expected to provide meaningful information or actions about a given task. The concept like scoping of interactions to specific geographic regions or to time intervals will become important. Hence, new paradigms of using such a network are required, along with new interfaces and new ways of thinking about the service of a network.
  - Quality of service: The amount and quality of information that can be extracted at given sinks about the observed objects or area so adapted quality concepts like reliable detection of events or the approximation quality is important
  - Fault Tolerance: Since nodes may run out of energy or might be damaged or since the wireless communication between two nodes can be permanently interrupted it is important that the WSN as a whole is able to tolerate such faults. To tolerate node failure, redundant deployment is necessary, using more nodes than would be strictly necessary if all nodes functioned correctly.
  - Lifetime: WSN must operate at least for a given mission time or as long as possible. Hence, the lifetime of a WSN becomes a very important figure of merit. Evidently an energy efficient way of operation of the WSN is necessary. An alternative energy supplies might also be a available on a sensor node. Typically, these sources are not powerful enough to ensure continuous operation but can provide some recharging of batteries. Under such conditions, the lifetime of the network should ideally be infinite. When quality of service investing more energy can increase quality but decrease lifetime. Concepts to harmonize these trade-offs are required.
  - Scalability: Since a WSN might include a large number of nodes, the employed architectures and protocols must be able scale to these numbers.
  - Wide range of densities: In a WSN, the number of nodes per unit area the density of the network can vary considerably. Different applications will have very different node densities. The density can vary over time and space because nodes fail or move, the density also does not have to homogeneous in the entire network and the network should adapt to such variations.
  - Programmable: These nodes should be programmable and their programming must be changeable during operation when new tasks become important.
  - Maintainability: The WSN has to monitor its own health and status to change operational parameters or to choose different trade-offs. In this sense the network has to maintain itself. It could also be able to interact with external maintenance mechanisms to ensure its extended operation at a required quality.
- Required mechanisms

  To realize these requirements, innovative mechanisms for a communication network have to be found as well as new architectures and protocol concepts
  - Multihop wireless communication: Communication over long distances is only possible using prohibitively high transmission power. The use of intermediate nodes as relays can reduce the total required power. Hence for many forms of WSNs, multihop communication will be a necessary ingredient.
  - Energy-efficient operation: To support long lifetimes, energy-efficient operation is a key technique. Options to look into include energy-efficient data transport between two nodes or more importantly the energy- efficient determination of a requested information.
  - Auto-Configuration: A WSN will have no configure most of its operational parameters autonomously, independent of external configuration- the sheer number of nodes and simplified deployment will require that capability in most applications.
  - Collaboration and in-network processing: in some applications, a single sensor is not able to decide whether an event has happened but several sensors provide enough information. Information is processed in the network itself in various forms to achieve this collaboration as opposed to having every node transmit all data to an external network and process it at the edge of the network.
  - Locality: Nodes which are very limited in resources like memory, should attempt to limit the state that they accumulate during protocol processing to only information about their direct neighbors.

- Exploit trade-offs: WSNs will have to rely to a large degree on exploiting various inherent trade-offs between mutually contradictory goals, both during system/protocol design and at runtime. Another important trade-off is node density: depending on application, deployment and node failures at runtime, the density of the network can change considerably the protocols will have to handle very different situations possibly present at different places of a single network.

Comparison with AD HOC network vs Wireless Sensor Networks

An ad hoc network is a network that is setup, literally for a specific purpose to meet a quickly