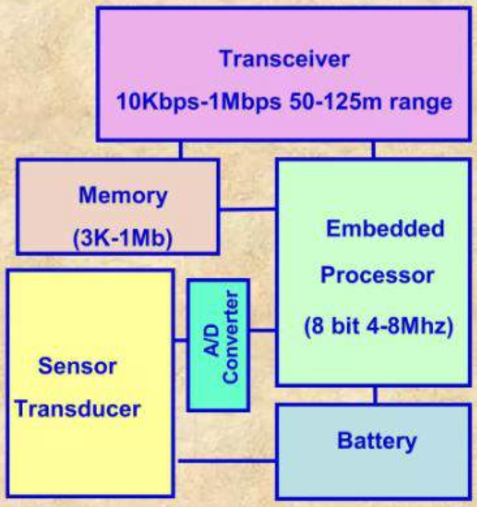
Chapter 8: Wireless Sensor Networks

Table of Contents

Introduction

- Wireless Sensor Networks can be considered as a special case of ad hoc networks with reduced or no mobility
- WSNs enable reliable monitoring and analysis of unknown and untested environments
- These networks are "data centric", i.e., unlike traditional ad hoc networks where data is requested from a specific node, data is requested based on certain attributes such as, "which area has temperature over 35°C or 95°F"
- A sensor has many functional components as shown in Figure 8.1
- A typical sensor consists of a transducer to sense a given physical quantity, an embedded processor, small memory and a wireless transceiver to transmit or receive data and an attached battery

Functional Components: A Sensor



The Mica Mote

Mica Motes-2

Mica Board

Applications

- Thousands of sensors over strategic locations are used in a structure such as an automobile or an airplane, so that conditions can be constantly monitored both from the inside and the outside and a real-time warning can be issued whenever a major problem is forthcoming in the monitored entity
- These wired sensors are large (and expensive) to cover as much area is desirable
- Each of these need a continuous power supply and communicates their data to the end-user using a wired network
- The organization of such a network should be pre-planned to find strategic position to place these nodes and then should be installed appropriately
- The failure of a single node might bring down the whole network or leave that region completely un-monitored

Applications

- Unattendability and some degree of fault tolerance in these networks are desirable in those applications where the sensors may be embedded in the structure or places in an inhospitable terrain and could be inaccessible for any service
- Undoubtedly, wireless sensor networks have been conceived with military applications in mind, including battlefield surveillance and tracking of enemy activities
- However, civil applications considerably outnumber the military ones and are applicable to many practical situations
- Judging by the interest shown by military, academia, and the media, innumerable applications do exist for sensor networks
- Examples include weather monitoring, security and tactical surveillance, distributed computing, fault detection and diagnosis in machinery, large bridges and tall structures, detecting ambient conditions such as temperature, movement, sound, light, radiation, vibration, smoke, gases, or the presence of certain biological and chemical objects

Applications

- Under the civil category, envisioned applications can be classified into environment observation and forecast system, habitat monitoring equipment and human health, large structures and other commercial applications

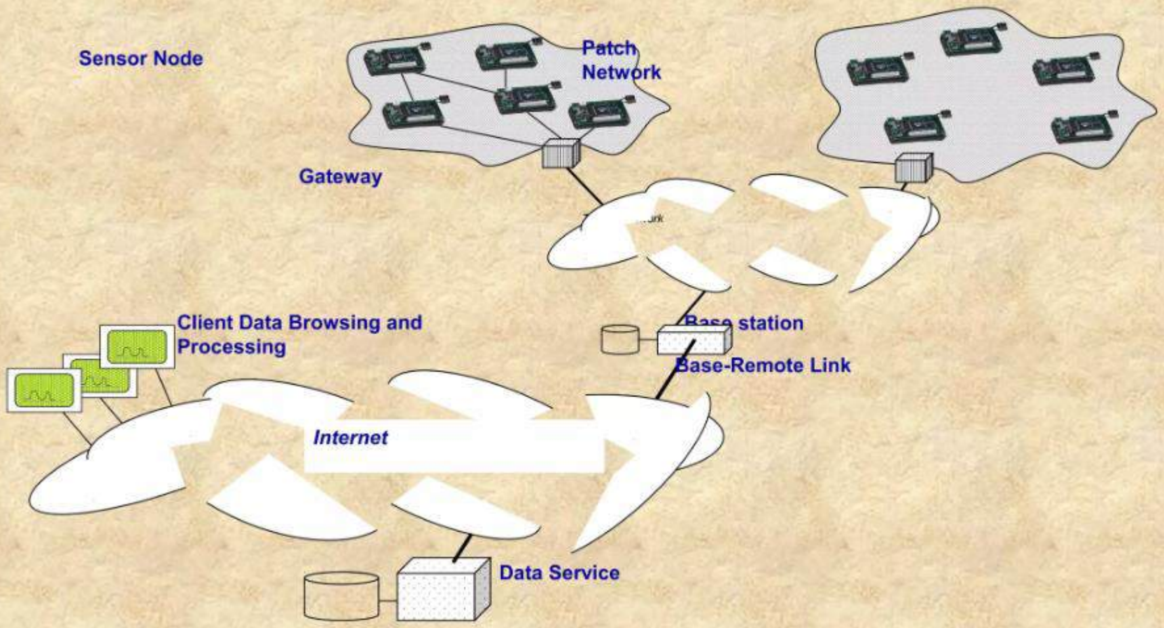
Habitat Monitoring

- A prototype test bed consisting of iPAQs (i.e., a type of handheld device) has been built to evaluate the performance of these target classification and localization methods
- As expected, energy efficiency is one of the design goals at every level: hardware, local processing (compressing, filtering, etc.), MAC and topology control, data aggregation, data-centric routing and storage
- Preprocessing is proposed in for habitat monitoring applications, where it is argued that the tiered network in GDI is solely used for communication
- The proposed 2-tier network architecture consists of micro nodes and macro nodes, wherein the micro nodes perform local filtering and data to significantly reduce the amount of data transmitted to macro nodes

Applications The Grand Duck Island Monitoring Network

- Researchers from the University of California at Berkeley (UCB) and Intel Research Laboratory deployed in August 2002 a mote-based tiered sensor network in Great Duck Island (GDI), Maine, aimed at monitoring the behavior of storm petrel
- The overall system architecture is depicted in Figure 8.13
- A total of 32 motes have been placed in the area to be sensed grouped into sensor patches to transmit sensed data to a gateway which is responsible for forwarding the information from the sensor patch to a remote base station through a local transit network
- The base station then provides data logging and replicates the data every 15 minutes to a database in Berkeley over a satellite link
- Remote users can access the replica database server in Berkeley, while local users make use of a small PDA-size device to perform local interactions such as adjusting the sampling rates, power management parameters, etc.

The Grand Duck Island Monitoring Netwo



Applications: Remote Ecological Micro-Sensor Network

- PODS is a research project undertaken at the University of Hawaii that has built a wireless network of environmental sensors to investigate why endangered species of plants will grow in one area but not in neighboring areas
- They deployed camouflaged sensor nodes, (called PODS), in the Hawaii Volcanoes National Park
- The PODS consist of a computer, radio transceiver and environmental sensors, sometimes including a high resolution digital camera, relaying sensed data via wireless link back to the Internet
- Bluetooth and 802.11b are chosen as the MAC layer, while data packets are delivered through the IP
- In PODS, energy efficiency is identified as one of the design goals and an ad hoc routing protocols called Multi-Path On-demand Routing (MOR) has been developed

Applications: Remote Ecological Micro-Sensor Network

- Weather data are collected every ten minutes and image data are collected once per hour
- Users employ the Internet to access the data from a server in University of Hawaii at Manoa
- The placement strategy for the sensor nodes is then investigated
- Topologies of 1-dimensional and 2-dimensional regions such as triangle tile, square tile, hexagon tile, ring, star, and linear are discussed
- The sensor placement strategy evaluation is based on three goals: resilience to single point of failure, the area of interest has to be covered by at least one sensor, and minimum number of nodes
- Finally, it is found that the choice of placement depends on d and r

Environmental Monitoring Application

- Sensors to monitor landfill and the air quality
- Household solid waste and non-hazardous industrial waste such as construction debris and sewer sludge are being disposed off by using over 6000 landfills in USA and associated organic components undergo biological and chemical reaction such as fermentation, biodegradation and oxidation-reduction
- This causes harmful gases like methane, carbon dioxide, nitrogen, sulfide compounds and ammonia to be produced and migration of gases in the landfill causes physical reactions which eventually lead to ozone gases, a primary air pollutant and an irritant to our respiratory systems
- The current method of monitoring landfill employs periodic drilling of collection well, collecting gas samples in airtight bags and analyze off-site, making the process very time consuming

Environmental Monitoring Application

- The idea is to interface gas sensors with custom-made devices and wireless radio and transmit sensed data for further analysis
- Deployment of a large number of sensors allows real-time monitoring of gases being emitted by the waste material or from industrial spills
- Place a large number of sensors throughout the area of interest and appropriate type of sensors can be placed according to the type of pollutant anticipated in a given area
- A large volume of raw data from sensors, can be collected, processed and efficiently retrieval
- A generic set up of a WSN, has been covered and various associated issues have been clearly pointed out
- The scheme can be easily used and adopted for other applications as well

Environment Observation and Forecasting System

- The Environment Observation and Forecasting System (EOFS) is a distributed system that spans large geographic areas and monitors, models and forecasts physical processes such as environmental pollution, flooding, among others
- Usually, it consists of three components: sensor stations, a distribution network, and a centralized processing farm
- Some of the characteristics of EOFS are:
  - Centralized processing: The environment model is computationally very intensive and runs on a central server and process data gathered from the sensor network
  - High data volume: For example, nautical X-band radar can generate megabytes of data per second
  - QoS sensitivity: This defines the utility of the data and there is an engineering trade-off between QoS and energy constraint
  - Extensibility
  - Autonomous operation

Drinking Water Quality

- A sensor based monitoring system with emphasis on placement and utilization of in situ sensing technologies and doing spatial-temporal data mining for water-quality monitoring and modeling
- The main objective is to develop data-mining techniques to water-quality databases and use them for interpreting and using environmental data
- This also helps in controlling addition of chlorine to the treated water before releasing to the distribution system
- Detailed implementation of a bio-sensor for incoming wastewater treatment has been discussed
- A pilot-scale and full scale system has also been described

Disaster Relief Management and Soil Moisture Monitoring

- Novel sensor network architecture has been proposed in that could be useful for major disasters including earthquakes, storms, floods, fires and terrorist attacks
- The SNs are deployed randomly at homes, offices and other places prior to the disaster and data collecting nodes communicate with database server for a given sub area which are in-turn linked to a central database for continuous update

Soil Moisture Monitoring

- A soil moisture monitoring scheme using sensors, over a one hectare outdoor area and various performance parameters measured from an actual system
- A custom made moisture sensor is interfaced with Mica-2 Mote wireless board

Health Care Monitoring

- Telemonitoring of human physiological data, tracking and monitoring of doctors and patients inside a hospital, drug administrator in hospitals, …
- An example: Artificial retina developed within the Smart Sensors and Integrated Microsystems (SSIM) project
- A retina prosthesis chip consisting of one hundred microsensors are built and implanted within the human eye, allowing patients with no vision or limited vision to see at an acceptable level
- Wireless communication is required to suit the need for feedback control, image identification and validation
- The communication pattern is deterministic and periodic like a TDMA scheme

Building, Bridge and Structural Monitoring

- Projects have explored the use of sensors in monitoring the health of buildings, bridges and highways
- A Bluetooth based scatternet has been proposed to monitor stress, vibration, temperature, humidity etc. in civil infrastructures
- Simulation results are given to justify effectiveness of their solution by having a set of rectangular Bluetooth equipped sensor grids to model a portion of bridge span
- Fiber optic based sensors have been proposed for monitoring crack openings in concrete bridge decks, of strain and corrosion of the reinforcement in concrete structures
- Corrosion of steel bars is measured by using special super glue and angular strain sensors

Smart Energy and Home/Office Applications

- Societal-scale sensor networks can greatly improve the efficiency of energy-provision chain, which consists of three components: the energy-generation, distribution, and consumption infrastructure
- It has been reported that 1% load reduction due to demand response can lead to a 10% reduction in wholesale prices, while a 5% load response can cut the wholesale price in half

DARPA Efforts towards Wireless Sensor Networks

- The DARPA has identified networked micro sensors technology as a key application for the future
- On the battlefield of the future, a networked system of smart, inexpensive and plentiful microsensors, combining multiple sensor types, embedded processors, positioning ability and wireless communication, will pervade the environment and provide commanders and soldiers alike with heightened situation awareness

Body Area Network

- Specialized sensors and transducers are being developed to measure human body characterizing parameters
- There has been increased interest in the biomedical area and numerous proposals have recently been introduced
- Micro sensor array is used for artificial retina, glucose level monitoring, organ monitors, cancer detectors and general health monitoring
- A wearable computing network has been suggested to remotely monitor the progress of a physical therapy done at home and an initial prototype has been developed using electroluminescent strips indicating the range of human body's motion
- An indoor/outdoor wearable navigation system has been suggested for blind and visually impaired people through vocal interfaces about surrounding environment and changing the mode from indoor to outdoor and vice-versa using simple vocal command

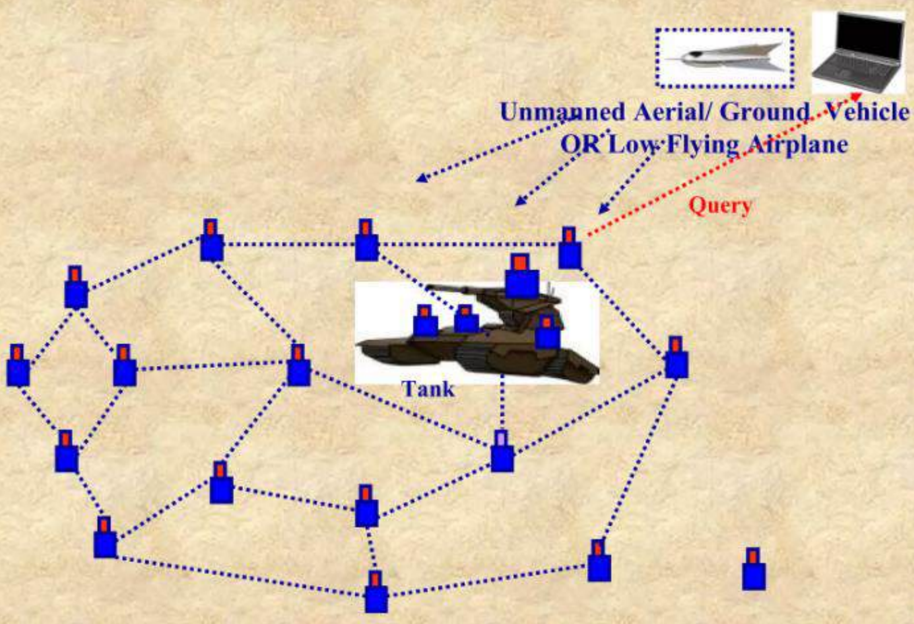
Conclusions and Future Directions

- Sensor networks are perhaps one of the fastest growing areas in the broad wireless ad hoc networking field
- As we could see throughout this chapter, the research in sensor networks is flourishing at a rapid pace and still there are many challenges to be addressed such as:
  - Energy Conservation - Nodes are battery powered with limited resources while still having to perform basic functions such as sensing, transmission and routing
  - Sensing - Many new sensor transducers are being developed to convert physical quantity to equivalent electrical signal and many new development is anticipated
  - Communication - Sensor networks are very bandwidth-limited and how to optimize the use of the scarce resources and how can sensor nodes minimize the amount of communication
  - Computation - Here, there are many open issues in what regards signal processing algorithms and network protocols

Chapter 9: Data Retrieval in Sensor Networks

Table of Contents

Introduction



Introduction

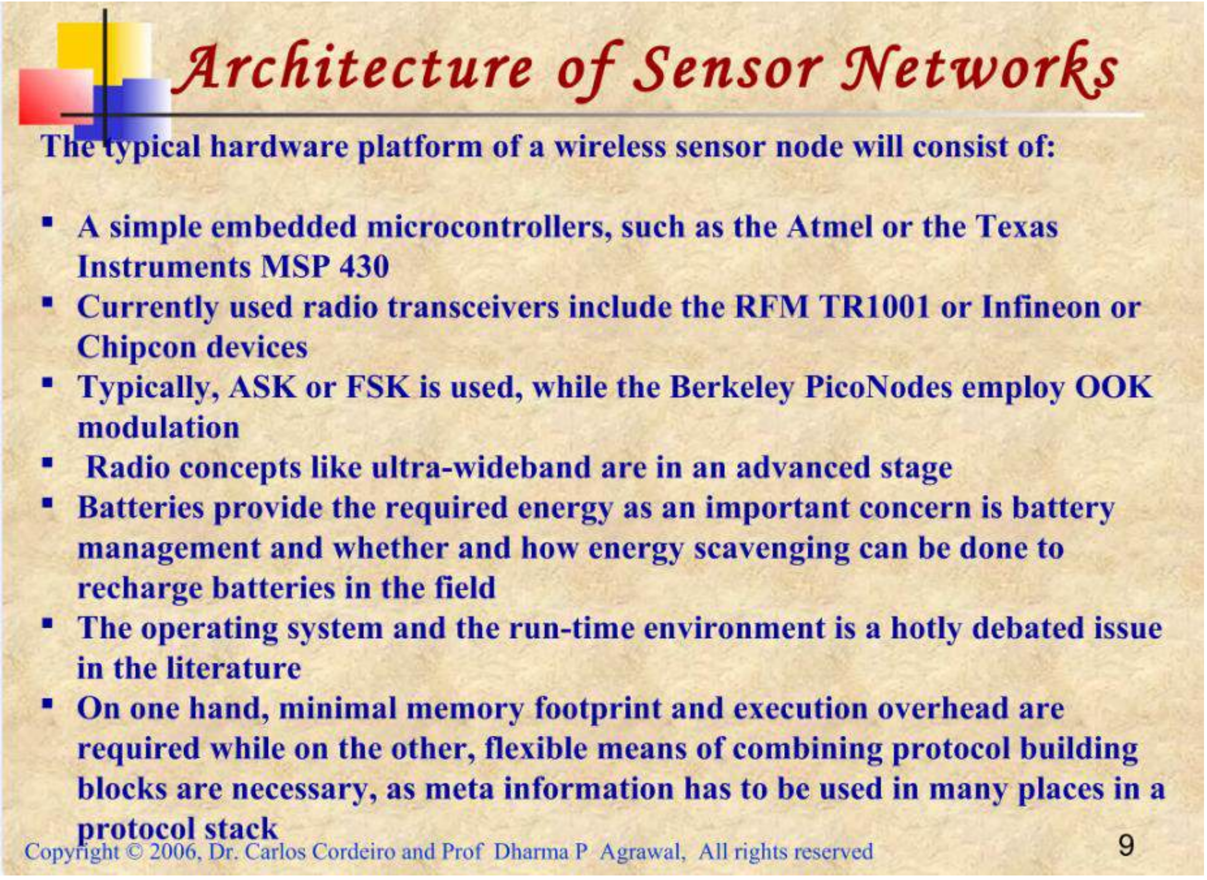
- A typical Sensor Node (SN) of the network contains several transducers to measure many different physical parameters and any one could be selected under the program control at a given time
- The sensed values need to be routed by each SN to the BS either directly or via its CH in a multihop fashion due to power limitations
- In a WSN, the overall objective can be defined by the BS and this process is usually known as injection of the query by the BS
- In real-life, a low-flying airplane, an unmanned aerial or ground vehicle or a powerful laptop can act as a BS or a sink and usually have adequate source of power
- This enables the BS to transmit a query message at a very high power level so as to reach all SNs in a given area simultaneously Such broadcasting is to enable all SNs to start working on the request and the query could also include information about some necessary characteristics of the query

Introduction

- If the BS has limited power to reach just few close-by SNs, then the query need to be forwarded/broadcasted to a given area of interest or possibly to the whole WSN
- The multi-hop routes are to be employed just like the response is forwarded in a multi-hop fashion
- The use of a particular type of query might depend on the application requirements
- Sometime, the query may ask for multiple parameters such as temperature, pressure, humidity, etc., and may be required to sense and transmit the values only once, or over a period of time, or use past history to gain statistical information
- Based on these, the query can be divided into three categories:
  - One time queries
  - Persistent queries
  - Historical queries

Classifications of WSNs

- WSNs can be classified on the basis of their mode of operation or functionality, and the type of target applications
- Accordingly, we classify WSNs into three types:
  - Proactive Networks – The nodes in this network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest and they provide a snapshot of the relevant parameters at regular intervals and are well suited for applications requiring periodic data monitoring
  - Reactive Networks – In this scheme, the nodes react immediately to sudden and drastic changes in the value of a sensed attribute and as such, these are well suited for time critical applications
  - Hybrid Networks – This is a combination of both proactive and reactive networks where sensor nodes not only send data periodically, but also respond to sudden changes in attribute values



The architecture of sensor networks, specifically wireless sensor networks (WSNs), is tailored to accommodate the specific needs of applications and the communication technologies they rely on. This results in significant variations in both individual sensor node hardware and the overall network structure.

1. Sensor Node Hardware Components:

- Microcontrollers:

- Sensor nodes are built using simple embedded microcontrollers (e.g., Atmel or Texas Instruments MSP430). These microcontrollers must balance power consumption with computational power, memory, and sleep modes, which influence energy efficiency and responsiveness.

- Radio Transceivers:

- Common transceivers include RFM TR1001 and Chipcon devices, which use modulation techniques like ASK, FSK, or OOK (as in Berkeley PicoNodes). Emerging technologies, such as ultra-wideband, offer advances in communication efficiency. A potential breakthrough is the **wake-up radio concept**, which allows sensor nodes (SNs) to remain in sleep mode and wake up when a relevant transmission is detected, reducing power consumption.

- Energy Supply (Batteries):

- Batteries are the primary power source, but efficient battery management and energy scavenging (recharging through environmental energy) are critical for long-term operation. Self-discharge and recharge rates, as well as overall battery life, are key concerns.

- Operating Systems & Run-Time Environments:

- The trade-off between minimal memory and flexibility for protocol integration is central to the design of operating systems for SNs. Run-time environments that support structures like blackboards, publish/subscribe, or tuplespaces are suggested as suitable for handling the multi-protocol, meta-information-heavy requirements of WSNs.

2. Network Architecture:

The architecture of WSNs must ensure both sensing coverage and communication connectivity, which relies on the density of the sensor deployment.

- Density and Lifetime:

- The network's lifetime can be defined by either the failure of individual sensors or by a percentage failure rate (e.g., 95% area coverage). Denser sensor deployment provides redundancy, but increasing density can also lead to higher energy consumption and transmission delays due to collisions. The optimal sensor density maximizes sensor lifetime by balancing communication distance and energy consumption.

- Transmission Strategies:

- Energy consumption varies depending on whether data is transmitted directly between two sensors or via intermediate nodes. Using intermediate sensors can save energy compared to long-range transmissions (Figure 9.3 illustrates these strategies).

- Energy-Driven Protocols:

- WSN protocols must be energy-efficient, focusing on data aggregation and reducing unnecessary transmissions. Redundant or correlated sensor readings can be aggregated to minimize the number of packets sent.

- Addressing and QoS:

- Address-free structures may be essential for scalability and energy efficiency, using geographic or data-centric addressing systems. QoS, redundancy, and sensor reading imprecision must be accounted for in the design of the network.

In-Network Processing:

- WSNs often perform in-network processing, such as data aggregation and distributed signal processing, to reduce the number of transmitted packets. The exact nature of WSN services is not fully defined, as they do not simply transmit bits like traditional networks.

- Gateway and Integration:

- WSNs must be integrated into larger networks via a gateway to bridge different communication protocols. Integration into middleware architectures, like CORBA or Web Services, and services described in WSDL or UDDI present challenges in representing the unique functionality of WSNs.

- Reconfiguring Tasks:

- It may be necessary to update the tasks or software of sensor nodes over time, requiring remote reconfiguration capabilities for the WSN.

Physical Layer

The physical layer in the context of wireless sensor networks (WSNs) refers to the hardware and communication technologies used to transmit data between sensor nodes. However, limited research has been conducted on developing protocols specifically tailored to the unique needs of WSNs at the physical layer, particularly in terms of **energy efficiency and handling the overhead related to radio transmission (e.g., retransmissions and communication costs).**

Several points about the physical layer include:

- Energy-Efficient Transmission: A key focus is on how to transmit data with minimal energy consumption while considering potential retransmissions and overhead. Some energy-efficient modulation techniques have been explored in previous research (e.g., Schurgers 2001).

- Modulation Techniques for Sensor Nodes: Research such as that by Gao (2001) addresses the hardware aspects of CDMA (Code Division Multiple Access) and other modulation issues, emphasizing how these impact sensor nodes' performance.

- Communication Protocol Design: Shih (2001b) provides discussions on communication protocol designs that are based on the physical layer, offering insights into how the physical layer impacts overall network performance.

- **Standardization Efforts**: Although specific details are not covered, the work being done by organizations like the IEEE (notably the IEEE 802.15.4 standard) is recognized as relevant. IEEE 802.15.4 focuses on low-rate wireless personal area networks (LR-WPANs), which are critical for many WSN applications due to **their low power consumption and cost-effective communication**.

MAC LAYER

The MAC (Medium Access Control) layer plays a vital role in wireless sensor networks (WSNs), mainly in regulating how sensor nodes **share the communication medium efficiently while minimizing energy consumption**. The main focus of MAC layer research for WSNs is to keep sensor nodes in sleep mode as long as possible to conserve energy, making it a crucial area of study.

Key concepts of MAC layer include:

Channel Allocation Schemes:

- **Static Channel Allocation**: Bandwidth is divided among sensor nodes using techniques like FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access), CDMA (Code Division Multiple Access), or SDMA (Space Division Multiple Access). These methods minimize interference but work best in static, low-node-count environments where nodes have predictable data loads.

- Dynamic Channel Allocation: This is more suited for environments where the number of active nodes varies, and data generation is bursty (i.e., sporadic). Contention-based protocols such as CSMA (Carrier Sense Multiple Access) are used here. Although these can minimize collisions, they may lead to energy wastage and delays due to retransmissions.

Hierarchical Clustering and TDMA:

- In a hierarchical clustering model, TDMA can be used to allocate time slots to each sensor node within a cluster. Nodes transmit data in their designated slots and can sleep during other periods to save energy. This is especially beneficial in both proactive networks (where nodes transmit periodically) and reactive networks (where nodes respond to sudden events).

CDMA and Intra/Inter-Cluster Collisions:

- CDMA can be used to avoid collisions between clusters. Though more energy is required per bit transmitted, CDMA allows multiple transmissions using the same frequency, making it useful for inter-cluster communication.

MAC Design Challenges:

1. **Node Failure**: When sensor nodes fail, MAC protocols must adapt by forming new routes and adjusting power levels to maintain network connectivity.

2. **Energy Consumption Sources**:

   - Collisions: Corrupted packets due to collisions lead to retransmissions, consuming more energy.

   - Overhearing: Nodes may waste energy by listening to transmissions not intended for them.

   - Control Packet Overhead: The need for control packets to manage network operations increases energy usage as the number of nodes rises or nodes fail.

   - Idle Listening: Nodes may waste energy waiting to receive data that is never sent.

Energy Conservation Techniques:

- One of the most effective methods for conserving energy in WSNs is periodic sleeping: nodes turn off their radios and synchronize based on a sleep schedule. This reduces the idle listening problem, a major energy drain in sensor networks.

Scheduling and Reservation vs. Contention-based MAC:

- Scheduling-based MAC protocols (like TDMA) save more energy compared to contention-based protocols (like IEEE 802.11). However, TDMA requires careful management of cluster formation, inter-cluster communication, and dynamic adaptation to changes in the number of nodes in the network.

In summary, the MAC layer in WSNs faces unique challenges related to energy efficiency, node failure, and dynamic network environments. Various strategies, including static and dynamic channel allocation, hierarchical clustering, and scheduled sleeping, are employed to **balance energy conservation with reliable communication.**

The Sensor-MAC (S-MAC) protocol:

1. Energy Efficiency in WSNs:

- WSNs are designed for prolonged operation, making energy conservation crucial since recharging batteries is often impractical.
- Nodes typically spend much of their time in an idle state, consuming similar energy levels in both idle and receiving modes.

2. Low Duty Cycle Operation:

- Nodes in S-MAC operate on a low duty cycle, alternating between listening and sleeping to conserve energy.
- By doing this, S-MAC addresses four primary sources of energy consumption: collision, control overhead, overhearing, and idle listening.

3. Coordinated Sleep Schedules:

- S-MAC nodes communicate and coordinate their sleep schedules to minimize energy waste.
- Each node broadcasts its schedule to neighbors using SYNC packets, helping to prevent clock drift and ensuring nodes follow similar wake and sleep patterns.

4. Handling Different Schedules:

- If two neighboring nodes have different schedules, they can either:
  - Listen to both schedules, or
  - Transmit data according to both schedules.
- Neighbor discovery is periodically performed to ensure nodes are aware of each other's presence and schedules.

5. Communication Process:

- During communication, a node first performs carrier sensing during its neighbor's listening periods.
- If the channel is clear, it sends a Request to Send (RTS) followed by a Clear to Send (CTS) from the receiver, enabling data transfer during their scheduled times.
- Broadcasts do not use RTS/CTS to avoid potential collisions from multiple responses.

6. Adaptive Listening:

- To reduce latency in multi-hop transmissions, nodes that overhear transmissions can briefly wake up to receive data, rather than waiting for their next scheduled listen time.

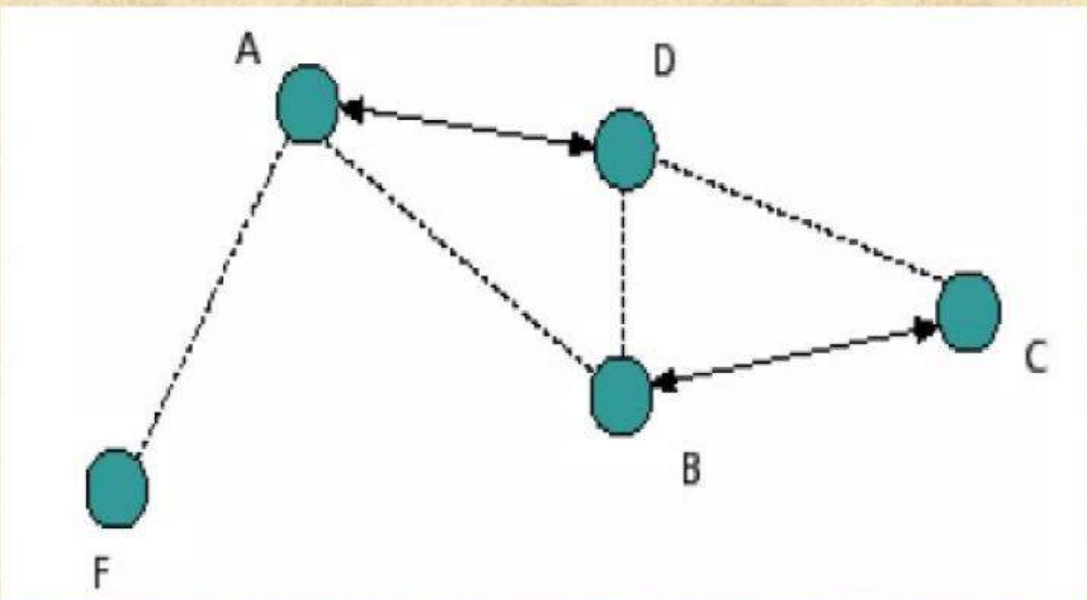
SMACS

- The SMACS is an infrastructure-building protocol that forms a flat topology (as opposed to a cluster hierarchy) for sensor networks
- SMACS is a distributed protocol which enables a collection of SNs to discover their neighbors and establish transmission/reception schedules for communicating with them without the need for any local or global master nodes
- In order to achieve this ease of formation, SMACS combines the neighbor discovery and channel assignment phases
- SMACS assigns a channel to a link immediately after the link's existence is discovered
- This way, links begin to form concurrently throughout the network
- By the time all nodes hear all their neighbors, they would have formed a connected network
- In a connected network, there exists at least one multihop path between any two distinct nodes

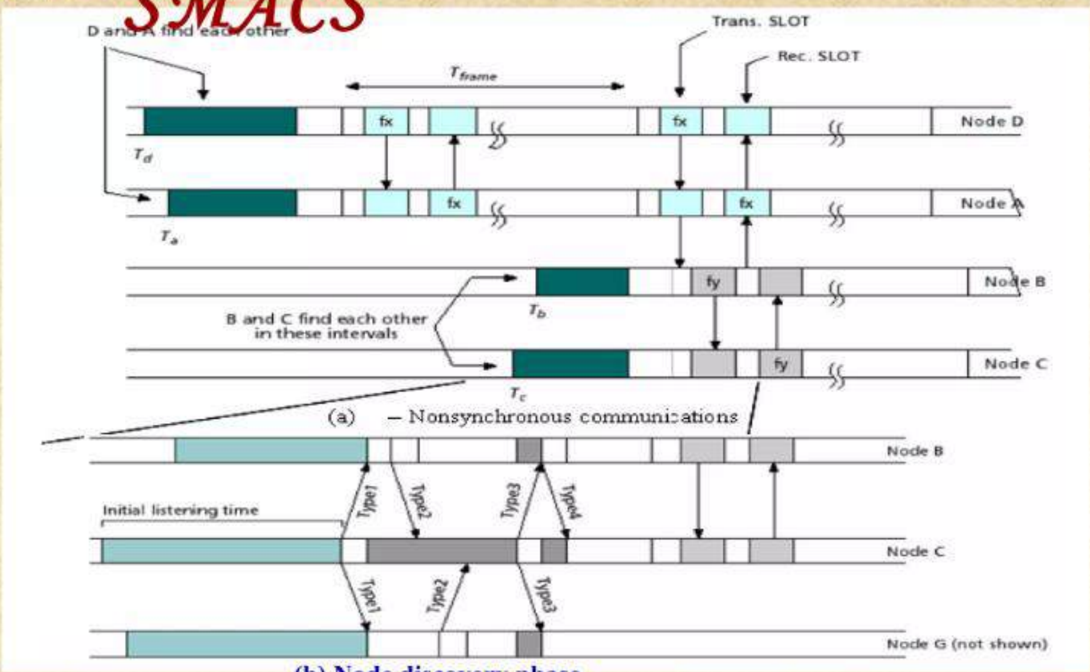
SMACS

- Since only partial information about radio connectivity in the vicinity of a SN is used to assign time intervals to links, there is a potential for time collisions with slots assigned to adjacent links whose existence is not known at the time of channel assignment
- To reduce the likelihood of collisions, each link is required to operate on a different frequency
- This frequency band is chosen at random from a large pool of possible choices when the links are formed
- This idea is described in Figure 9.6(a) for the topology of Figure 9.5
- Here, nodes A and D wake up at times T_a and T_d
- After they find each other, they agree to transmit and receive during a pair of fixed time slots
- This transmission/reception pattern is repeated periodically every T_{frame}
- Nodes B and C, in turn, wake up later at times T_b and T_c, respectively

Network Topology



Node Discovery Phase in SMACS



(b) Node discovery phase

SMACS

- **The method by which SNs find each other and the scheme by which time slots and operating frequencies are determined constitute an important part of SMACS**
- **To illustrate this scheme, consider nodes B, C, and D shown in Figure 9.6(b)**
- **These nodes are engaged in the process of finding neighbors and wake up at random times**
- **Upon waking up, each node listens to the channel on a fixed frequency band for some random time duration**
- **A node decides to transmit an invitation by the end of this initial listening time if it has not heard any invitations from other nodes**
- **This is what happens to node C, which broadcasts an invitation or TYPE1 message**
- **Nodes B and D hear this TYPE1 message and broadcasts a response, or TYPE2, message addressed to node C during a random time following reception of TYPE1**

EAR protocol (Energy and Activity Aware Routing)

It is designed to facilitate communication between mobile and stationary nodes in a wireless sensor network (WSN), particularly where **energy efficiency and bandwidth are concerns**. Here's a breakdown of the key concepts:

1. **Introduction of Mobility**: EAR accommodates mobile nodes that can move through a network primarily composed of stationary sensors. This is particularly useful in scenarios where limited power consumption is crucial.

2. **Low-Power Operation**: The protocol is designed to minimize energy usage by allowing mobile nodes to initiate and control connections with stationary nodes. This reduces the number of messages exchanged, which is important since battery life is a priority for stationary nodes.

3. **Connection Control**: Mobile nodes manage when to connect or disconnect from stationary nodes. They have a registry that tracks nearby stationary nodes, allowing them to make informed decisions about connections based on proximity and signal quality.

4. **Eavesdropping Mechanism**: Mobile nodes listen for periodic "Broadcast Invite" messages sent by stationary nodes. These messages inform them of available connections without requiring immediate responses, allowing mobile nodes to assess the network environment.

5. **Connection Establishment**: The EAR protocol involves several key message types:

- Broadcast Invite (BI): Sent by stationary nodes to invite mobile nodes to connect. Mobile nodes respond by registering the stationary nodes they encounter.
- Mobile Invite (MI): A response from the mobile node to a BI message, indicating its intent to connect.
- Mobile Response (MR): Sent by the stationary node in reply to the MI, confirming the connection and assigning communication slots in the TDMA frame.
- Mobile Disconnect (MD): Sent by the mobile node when it wants to terminate a connection, typically based on the signal quality (SNR).

6. **Efficiency and Transparency**: The EAR protocol is designed to be transparent to the existing stationary nodes' protocols, minimizing the need for specialized messages and ensuring seamless operation within the network.

The Sparse Topology and Energy Management (STEM)

This protocol is designed for sensor networks that spend most of their time in a low-power monitoring state, only becoming active when specific events occur. Here's a breakdown of its main concepts:

1. **Reactive Monitoring**: STEM is particularly suited for applications where the network primarily senses the environment, such as detecting forest fires. The goal is to keep the network operational for long periods while using minimal energy during monitoring.

2. **Energy-Efficient Operation**: During the monitoring state, only the sensors and some preprocessing circuits of the nodes are active. The main processor and communication radio remain off to save energy until an event is detected.

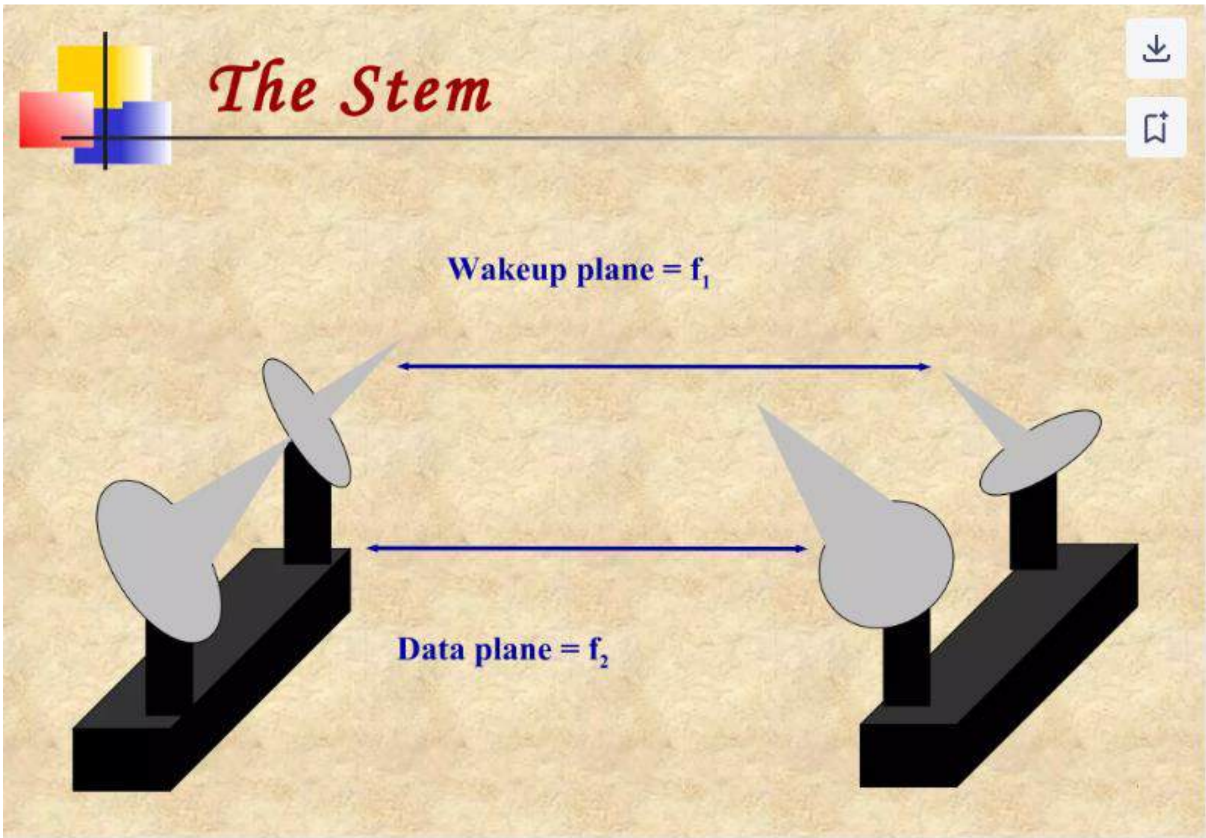
3. **Event Detection**: When a potential event is detected, the node's main processor wakes up to analyze the data and determine if communication with other nodes is necessary. However, the radios of neighboring nodes may remain off if they did not detect the same event.

4. **Beacon Communication:** To initiate communication, a node (the initiator) periodically sends out a beacon signal targeting another node (the target). This beacon alerts the target node to wake up and establish a communication link.

5. **Link Activation**: Upon receiving the beacon, the target node responds, and both nodes keep their radios on. If the data needs to be forwarded, the target becomes the initiator for the next hop, repeating the process.

6. **Separate Frequency Bands**: STEM uses different frequency bands for the wakeup protocol and data transmission to avoid interference. The wakeup messages are sent over one frequency (the "wakeup plane"), while actual data packets are transmitted over another frequency (the "data plane").

7. **Hardware Support**: Some commercially available sensors support this dual-band operation, allowing for effective implementation of the STEM protocol.



ROUTING LAYER

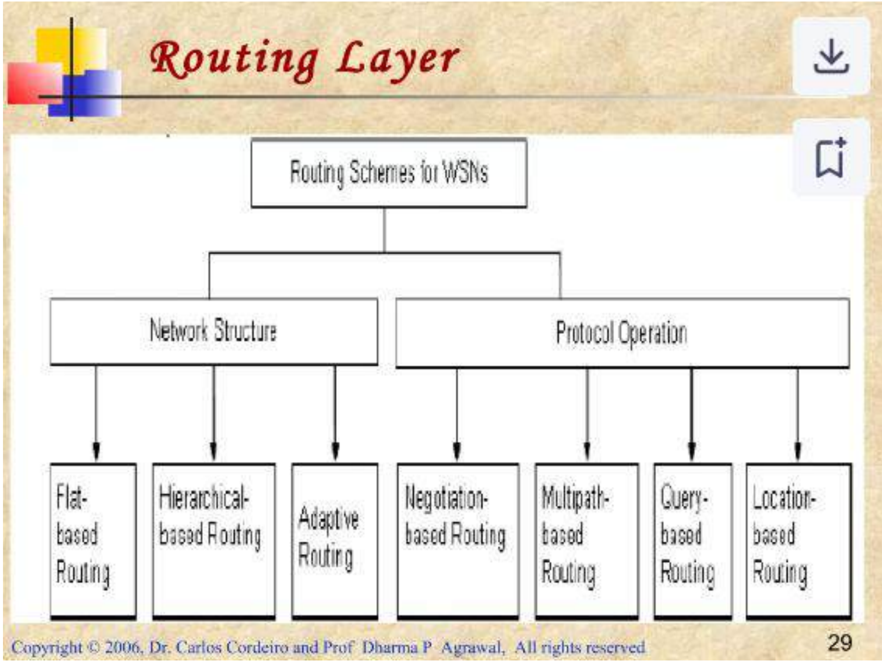
This section explores energy-efficient routing techniques developed specifically for WSNs, focusing on extending network lifetime.

Key concepts of WSN routing include:

Routing Approaches:

1. Multi-Hop Routing: In WSNs, data is usually sent over multiple hops from a source node to the BS. The BS can be fixed or mobile, serving as a gateway between the sensor network and external systems, such as the Internet. Multi-hop routing is energy-efficient, as direct communication with the BS can be energy-intensive for distant nodes.
2. Energy-Efficient Routing Goals: The primary aim is to minimize energy consumption and maximize network lifetime. WSN routing protocols use specific strategies, including **data aggregation, clustering, in-network processing, and data-centric techniques to meet this goal.**

Classification of Routing Protocols for WSNs



Routing protocols in WSNs can be classified based on **network structure and protocol operation.**

By Network Structure:

- **Flat-based Routing**: All nodes have equal roles, and data is typically forwarded based on query responses. This approach is suitable for small networks.
- **Hierarchical-based Routing**: Nodes play distinct roles; some nodes (cluster heads) are designated with additional responsibilities, such as aggregating data and forwarding it to the BS. This approach conserves energy by reducing redundant data Transmission and is commonly used in large WSNs.
- **Adaptive Routing**: Protocols adapt parameters based on current network conditions, such as energy availability, to maintain efficiency.

By Protocol Operation:

- **Multipath-based Routing**: Utilizes multiple paths for data transmission to increase reliability and load balancing.
- **Query-based Routing**: Nodes send data in response to specific queries, saving energy by limiting transmissions to relevant data only.
- **Negotiation-based Routing**: Prevents redundant data transmission through negotiation among nodes before data forwarding.
- **Location-based Routing**: Nodes use location information to route data, optimizing routes and reducing transmission energy costs.

Considerations for WSN Routing:

1. **Energy Conservation Priority**: Energy efficiency is prioritized over data quality to prolong network lifespan.
2. **Stationary Nodes**: Many applications assume nodes are stationary, favoring table-driven routing protocols over reactive schemes to reduce energy spent on route discovery.
3. **Cooperative Routing**: Sensor nodes collaborate by sending data to a cluster head (CH), which aggregates the data and further processes it, reducing overall route cost in terms of energy use.
4. **Use of Timing and Position Information**: Certain protocols leverage time and position data for efficient routing, adapting routes as network conditions and node locations change.

Network Structure Based

Flat Routing

In flat routing based protocols, all nodes play the same role.

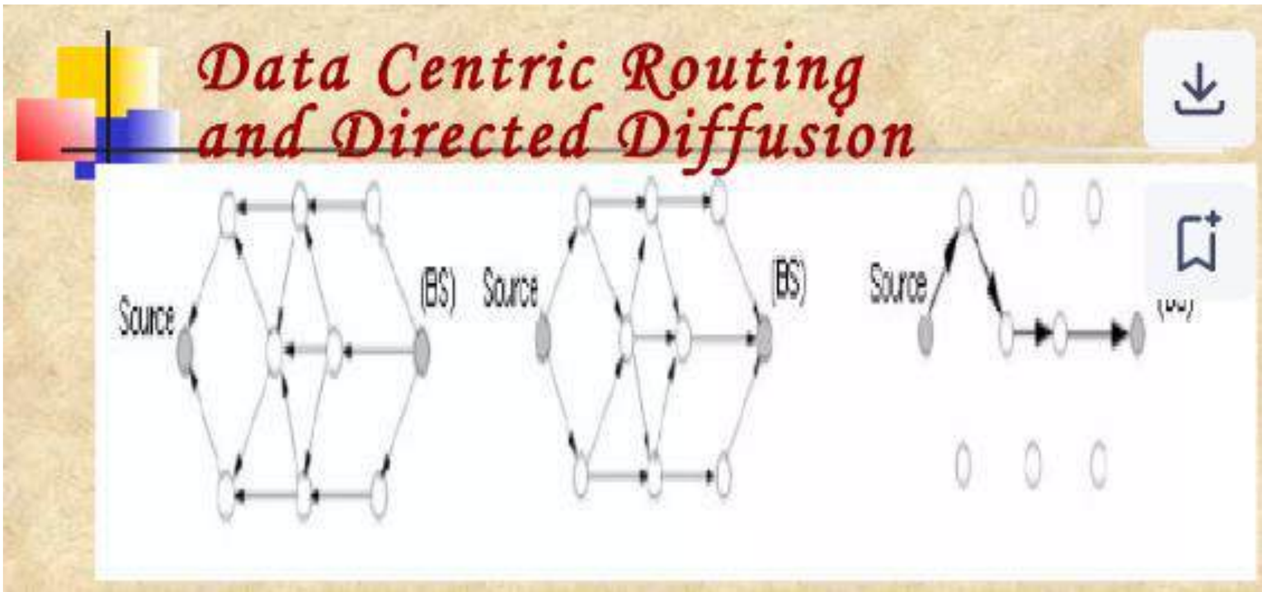
Directed Diffusion

Directed Diffusion operates through a process involving **data aggregation and in-network processing**, which helps reduce redundant transmissions and save energy. Here's an overview of the Directed Diffusion process:

1. **Interest Propagation**: The base station (BS) initiates communication by broadcasting an "interest" that specifies a task to be fulfilled by the network. This interest diffuses through the network hop-by-hop, with each node broadcasting it to its neighbors.
2. **Gradient Setup**: Each node that receives an interest establishes a gradient—a direction of data flow—towards the node from which it received the interest. This gradient setup forms paths from multiple data sources to the BS, allowing data to flow towards the requesting node. Different gradients may be formed to neighbors with varying strengths, affecting data flow.
3. **Data Transmission and Path Reinforcement**: Once data is transmitted, paths are refined by reinforcing the best paths to ensure efficient routing and prevent further flooding. The BS may also periodically refresh the interest to maintain data flow, as the wireless medium can be unreliable.
4. **In-network Aggregation**: As data flows along these gradients, nodes aggregate information from various sources, reducing the number of transmissions and minimizing energy consumption.

5. **Event-Specific Propagation**: Directed Diffusion is well-suited for ongoing or persistent queries, where nodes continuously provide data over time, such as monitoring environmental conditions. However**, it may not be efficient for one-time or historical queries, as setting up gradients for a single-use path can be unnecessary**.

By aggregating data and choosing optimized paths, Directed Diffusion conserves energy, extends network lifetime, and improves robustness.



Hierarchical Routing is a type of cluster-based routing approach in wireless sensor networks (WSNs) aimed at improving energy efficiency and scalability. By organizing nodes into clusters, hierarchical routing protocols achieve a balanced load across the network, where energy-intensive tasks are primarily handled by selected nodes called Cluster Heads (CHs).

Key Concepts of Hierarchical Routing

1. Cluster Formation and Role Assignment: Nodes in a WSN are organized into clusters, with each cluster containing a designated CH. Regular sensor nodes within a cluster perform sensing and data collection tasks and then relay this data to their CH. The CH, typically a higher-energy node, is responsible for aggregating data and sending it either to an upper-level CH or directly to the Base Station (BS).

2. Energy Efficiency: By aggregating data, CHs reduce the number of transmissions and the energy spent in data transfer. Since data is aggregated at the cluster level before reaching the BS, this hierarchical approach minimizes communication cost, conserves node energy, and enhances the network's lifespan.

3. Scalability: Hierarchical routing supports a scalable architecture by limiting communication within clusters and only forwarding processed data to higher layers. This structure is especially beneficial in large networks where a direct transmission from each node to the BS would be inefficient and unsustainable.

Example: **Cluster-Based Routing Protocol (CBRP)**

The Cluster-Based Routing Protocol (CBRP) is a fundamental protocol proposed by Jiang (1998) that segments the network into clusters of two-hop-diameter. Each node only communicates with its CH, which is responsible for further routing data. However, CBRP has some notable limitations for WSNs:

- High Overhead: CBRP requires frequent "hello" messages to establish and maintain clusters, which consumes significant network energy and bandwidth.

- Stationary Nodes: In most WSN applications where nodes are stationary, the overhead created by continuous hello messaging becomes unnecessary and reduces overall efficiency.

Adaptive Routing protocols are designed to dynamically adjust to the available resources and network environment, aiming to conserve energy and improve communication efficiency in Wireless Sensor Networks (WSNs). One prominent family of adaptive routing protocols is the

Sensor Protocols for Information via Negotiation (SPIN)

Key Concepts of Adaptive Routing with SPIN

1. **Data-Centric Communication**: SPIN protocols assign high-level metadata to data packets, allowing nodes to negotiate the data before transmission. This data-centric approach prevents the transmission of redundant information since nodes only send data that their neighbors lack.
2. **Energy Adaptation**: SPIN adapts to each node’s available resources, ensuring that low-energy nodes reduce participation when energy is scarce. This energy-awareness prevents nodes from expending energy on unnecessary transmissions, prolonging the network’s operational lifespan.

3. **Three-Stage Communication**: SPIN protocols follow a three-stage communication process using three types of messages:
   - **ADV**: Advertises new data.
   - **REQ**: Requests specific data that the node does not possess.
   - **DATA**: Transmits the actual data when requested.

This process continues iteratively until all nodes in the network have the information they need.

Types of SPIN Protocols

- **SPIN-1 and SPIN-2**: These are the foundational protocols of the SPIN family. SPIN-1 handles basic data negotiation, while SPIN-2 includes a threshold-based energy mechanism. When a node's energy level drops below a certain point, it only participates in data transmission if it can complete the process without falling below the threshold.
- **SPIN-BC (Broadcast Channel)**: SPIN-BC is optimized for broadcast environments. Nodes delay their responses with random timers, avoiding redundant requests when multiple nodes request the same data.
- **SPIN-PP (Point-to-Point)**: For point-to-point communication, SPIN-PP operates with a three-way handshake similar to SPIN-1 but requires only single-hop neighbor awareness. This protocol is effective for networks where energy and data reliability are less of a concern.
- **SPIN-EC (Energy-Constrained)**: This variant uses an energy threshold heuristic. Nodes participate only if they can complete all stages without reducing energy below a predefined threshold.
- **SPIN-RL (Reliable)**: In error-prone environments, SPIN-RL adds mechanisms to SPIN-PP to manage lossy channels. Nodes track received ADV messages and can request retransmissions for data not received within a time window, ensuring reliable data transfer.

Advantages of SPIN

- **Energy Efficiency**: By negotiating metadata before full data transfer, SPIN reduces unnecessary data exchanges and conserves energy.
- **Adaptability**: SPIN adjusts to the network’s energy levels and only participates when feasible, extending node life.
- **Reduced Redundancy**: By eliminating redundant data transfers and only transmitting unique data, SPIN conserves bandwidth and energy.

Limitations

SPIN protocols, while energy efficient and suitable for mobile WSNs, are not always ideal for networks with strict latency requirements or real-time demands. **The delay from negotiation and the overhead from ADV and REQ messaging can be excessive in dense networks** or environments where rapid data dissemination is needed.