SRINIVASAN COLLEGE OF ARTS & SCIENCE

(Affiliated Bharathidasan University, Tiruchirappalli)

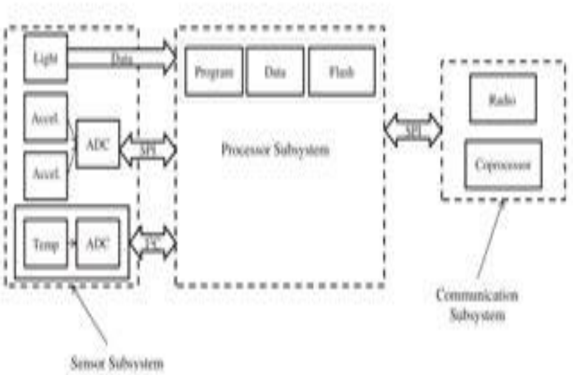
PERAMBALUR – 621 212

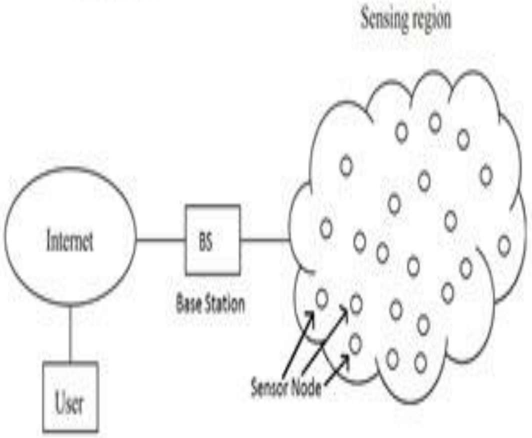
Department of Computer Science & Information Technology

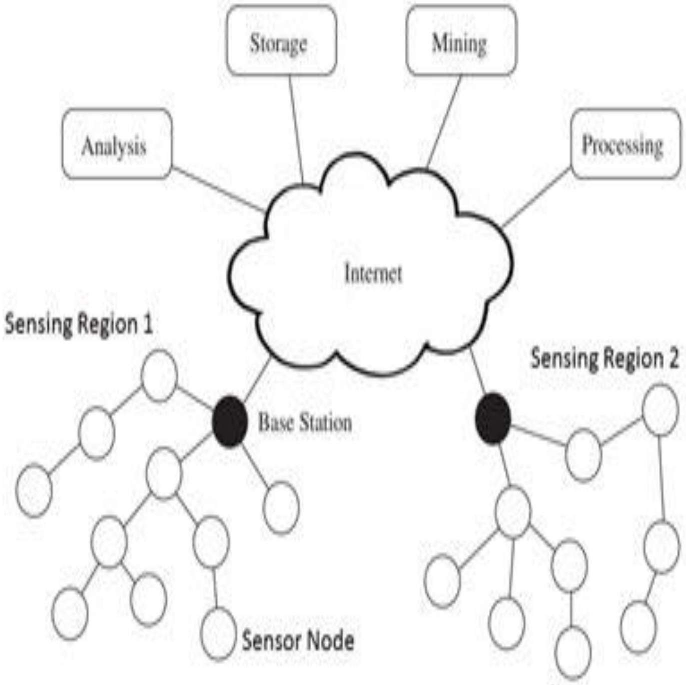
COURSE MATERIAL

Subject	**:**	**WIRELESS SENSOR NETWORKS**
Subject Code	**:**	**P16CS42**
Class	**:**	**II M.Sc., COMPUTER SCIENCE**
Semester	**:**	**IV**

WIRELESS SENSOR NETWORKS (WSN)







Unit - I

INTRODUCTION

A Wireless Sensor Network (WSN) is a distributed network and it comprises a large number of distributed, self-directed, tiny, low powered devices called sensor nodes alias motes. WSN naturally encompasses a large number of spatially dispersed, petite, battery-operated, embedded devices that are networked to supportively collect, process, and convey data to the users, and it has restricted computing and processing capabilities. Motes are the small computers, which work collectively to form the networks. Motes are energy efficient, multi-functional wireless device . The necessities for motes in industrial applications are widespread. A group of motes collects the information from the environment to accomplish particular application objectives. They make links with each other in different configurations to get the maximum performance. Motes communicate with each other using transceivers. In WSN the number of sensor nodes can be in the order of hundreds or even thousands. In comparison with sensor networks, Ad Hoc networks will have less number of nodes without any infrastructure. The differences between WSN and Ad hoc Networks are presented in the Table given.

Now a days wireless network is the most popular services utilized in industrial and commercial applications, because of its technical advancement in processor, communication, and usage of low power embedded computing devices. Sensor nodes are used to monitor environmental conditions like temperature, pressure, humidity, sound, vibration, position etc. In many real time applications the sensor nodes are performing different tasks like neighbor node discovery, smart sensing, data storage and processing, data aggregation, target tracking, control and monitoring, node localization, synchronization and efficient routing between nodes and base station.

Table 1.1 Wireless Sensor Networks Vs Ad hoc Networks

Parameters	**Wireless Sensor Networks**	**Ad Hoc Networks**
Number of sensor nodes	Large	Medium
Deployment	Densely deployed	Scattered
Failure rate	Prone to failures	Very rare
Topology	Changes very frequently	Very rare
Communication paradigm	Broadcast communication	Point-to-Point communications
Battery	Not replaceable/ Notrechargeable	Replaceable
Identifiers	No unique identifiers	Unique identifiers
Centric	Data centric	Address centric
Fusion / aggregation	Possible	Not suitable
Computational capacities, and memory	Limited	Not limited
Data rate	Low	High
Redundancy	High	Low

Wireless sensor nodes are equipped with sensing unit, a processing unit, communication unit and power unit. Each and every node is capable to perform data gathering, sensing, processing and communicating with other nodes. The sensing unit senses the environment, the processing unit computes the confined permutations of the sensed data, and the communication unit performs exchange of processed information among neighboring sensor nodes. The basic building block of a sensor node is shown in Figure 1.1.

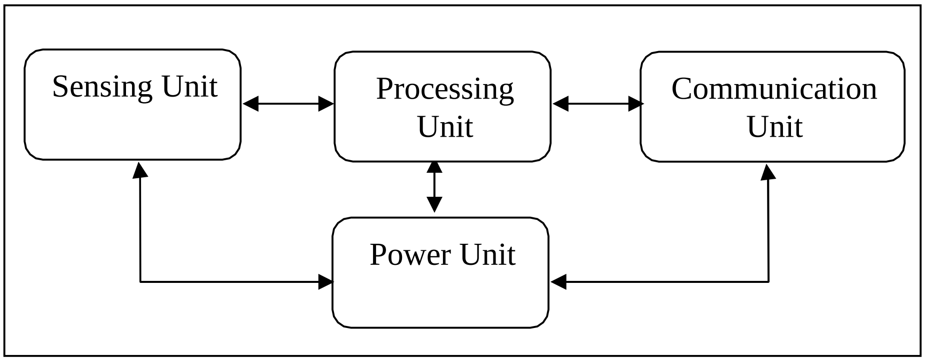


Figure 1.1 Basic Building Blocks of Sensor Node

The sensing unit of sensor nodes integrates different types of sensors like thermal sensors, magnetic sensors, vibration sensors, chemical sensors, bio sensors, and light sensors. The measured parameters from the external environment by sensing unit of sensor node are fed into the processing unit. The analog signal generated by the sensors are digitized by using Analog to Digital converter (ADC) and sent to controller for furtherprocessing.

The processing unit is the important core unit of the sensor node. The processor executes different tasks and controls the functionality of other components. The required services for the processing unit are pre-programmed and loaded into the processor of sensor nodes. The energy utilization rate of the processor varies depending upon the functionality of the nodes. The variation in the performance of the processor is identified by the evaluating factors like processing speed, data rate, memory and peripherals supported by the processors. Mostly ATMEGA 16, ATMEGA 128L, MSP 430 controllers [7] are used in commercial motes. The computations are performed in the processing unit and the acquired result is transmitted to the base station through the communication unit.

In communication unit, a common transceiver act as a communication unit and it is mainly used to transmit and receive the information among the nodes and base station and vice versa. There are four states in the communication unit: transmit, receive, idle and sleep. In general the functionality of the sensor node is shown in Figure1.2.

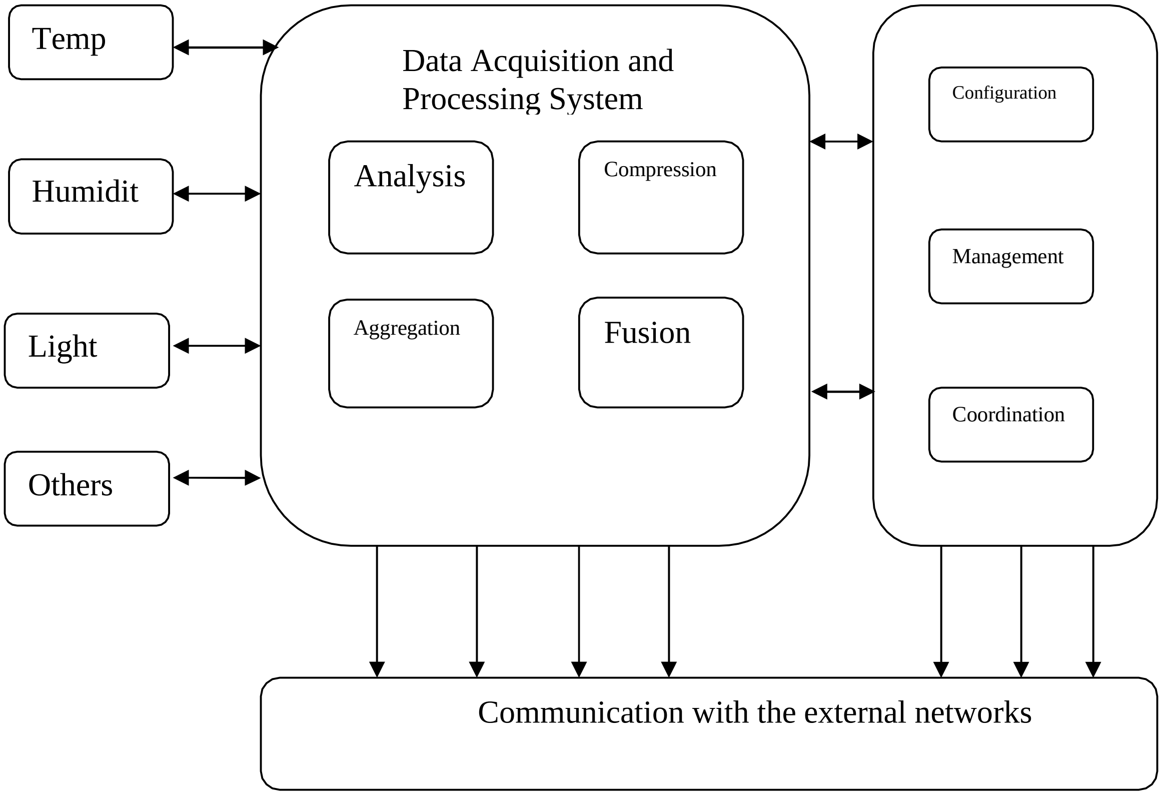


Figure 1.2 Functionality of A Sensor Node

The major characteristics of the sensor node used to evaluate the performance of WSN are[6]

1. **Fault tolerance**: Each node in the network is prone to unanticipated failure. Fault tolerance is the capability to maintain sensor network functionalities without any break due to sensor nodefailures.
2. **Mobility of nodes**: In order to increase the communication efficiency, the nodes can move anywhere within the sensor field based on the type ofapplications.
3. **Dynamic network topology**: Connection between sensor nodes follows some standard topology. The WSN should have the capability to work in the dynamic topology.
4. **Communication failures**: If any node in the WSN fails to exchange data with other nodes, it should be informed without delay to the base station or gateway node.
5. **Heterogeneity of nodes:** The sensor nodes deployed in the WSN may be of various types and need to work in a cooperativefashion.
6. **Scalability**: The number of sensor nodes in a sensor network can be in the order of hundreds or even thousands. Hence, WSN designed for sensor networks is supposed to be highlyscalable.
7. **Independency:** The WSN should have the capability to work without any central controlpoint.
8. **Programmability:** The option for reprogramming or reconfiguring should be available for the WSN to become adaptive for any dynamic changes in the network.
9. **Utilization of sensors:** The sensors should be utilized in a way that produces the maximum performance with lessenergy.

10. **Impracticality of public key cryptosystems:** The limited computation and power resources of sensor nodes often make it undesirable to use public keyalgorithms.
11. **Lack of aprior knowledge of post-deployment configuration:** If a sensor network is deployed via random distribution, the protocols will not be aware of the communication status between each nodes afterdeployment.

The following metrics are used to evaluate the performance of a WSN [8]: network coverage, node coverage, efficiency in terms of system lifetime, effortless deployment, data accuracy, system response time, fault tolerance, scalability, network throughput, sample rate, security, the cost of the network and network architecture used. The individual sensor node in the WSN is evaluated using flexibility, robustness, computation, communication, security, synchronization, node size and cost.

The components of WSN system are sensor node, rely node, actor node, cluster head, gateway and base station which are explained below [2].

Sensor node: Capable of executing data processing, data gathering and communicating with additional associated nodes in the network. A distinctive sensor node capability is about 4-8 MHz, having 4 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Relay node: It is a midway node used to communicate with the adjacent node. It is used to enhance the network reliability. A rely node is a special type of field device that does nothaveprocesssensororcontrolequipmentandassuchdoesnotinterfacewiththe process itself. A distinctive rely node processor speed is about 8 MHz, having 8 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Actor node: It is a high end node used to perform and construct a decision depending upon the application requirements. Typically these nodes are resource rich devices which are outfitted with high quality processing capabilities, greater transmission powers and greater battery life. A distinctive actor node processor capability is about 8 MHz, having 16 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency [7].

Cluster head: It is a high bandwidth sensing node used to perform data fusion and data aggregation functions in WSN. Based on the system requirements and applications, there will be more than one cluster head inside the cluster. A distinctive cluster head processor is about 4-8 MHz, having 512 KB of RAM, 4 MB flash and preferably 2.4 GHz of radio frequency [7]. This node assumed to be highly reliable, secure and is trusted by all the nodes in the sensor network.

Gateway: Gateway is an interface between sensor networks and outside networks. Compared with the sensor node and cluster head the gateway node is most powerful in terms of program and data memory, the processor used, transceiver range and the possibility of expansion through external memory. A distinctive gateway processor speed is about 16 MHz, having 512 KB of RAM, 32 MB flash and preferably 2.4 GHz of radio frequency.

Base station: It is an extraordinary type of nodes having high computational energy and processing capability.

Attractive functionality of sensor nodes in a WSN includes effortlessness installation, fault indication, energy level diagnosis, highly reliablity, easy coordination with other nodes in the network, control protocols and simple network interfaces with other smart devices. In WSN, based on the sensing range and environment, the sensor nodes are classified into four groups, namely specialized sensing node, generic sensing node, high bandwidth sensing node and gateway node. The radio bandwidth for thesensor nodes are <50 Kbps, <100 Kbps, ≈500 Kbps and >500 Kbps respectively. On board processing, computational rate and communication ranges differ from node to node in WSN. Particularly for some dedicated application sensor nodes with different capabilities are used. For example, smart specialized sensing nodes are preferred for special purpose devices, intelligent generic sensing node preferred for generic functions. For interconnectivity functions high end smart bandwidth sensing node and gateway nodes arepreferred.

Sensor networks are clustered with gateway, relay node, actor node and cluster head, and every other node within the communication range. Cluster is a collection of group of sensor nodes in that particular sensor field. There may be more than one cluster in WSN. Based on the parameters like computation rate, processing speed, storage, and communication range, sensor nodes are identified and selected for WSN formation [9]. Based on the node properties the sensor networks are classified into two types, homogenous sensor networks and heterogeneous sensor networks. In homogenous sensor networks, all sensor nodes have the same property in terms of computation, communication, memory, energy level and reliability. In heterogeneous sensor networks, the nodes are of different capabilities in terms of computation, communication, memory, energy level and reliability. If all the sensor nodes within the cluster are having the same properties (homogenous) it is referred as distributed WSN (DWSN). Otherwise if the sensor nodes have different properties (heterogeneous) it is called as hierarchical WSN (HWSN). The distributed and hierarchical WSN is shown in Figure 1.3.

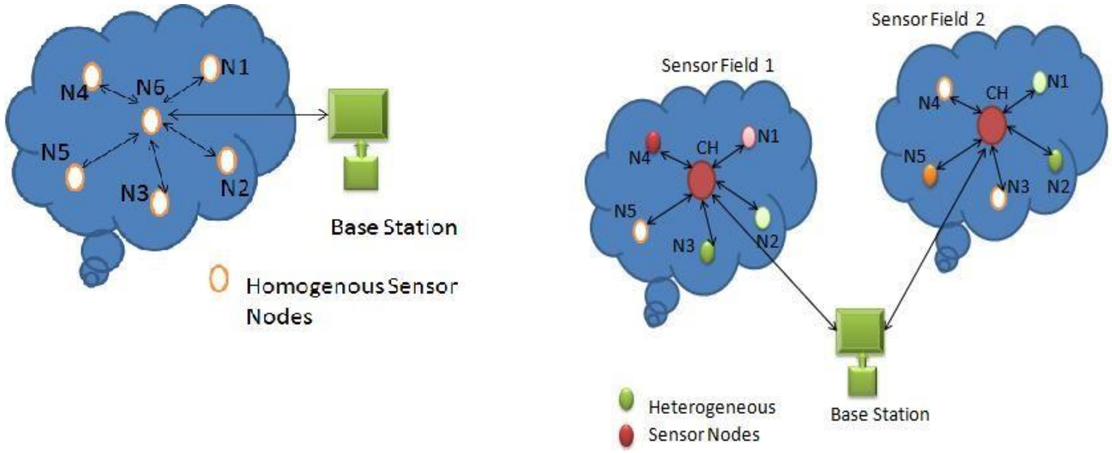


Figure 1.3 Distributed and Hierarchical WSN

Senor nodes in an open environment regularly sense the physical and environmental changes and transmit the information to the centralized server called a gateway. The computational rate and interaction of sensor nodes with the physical environment is different for different nodes in the network. In real time, sensor nodes are more constrained in its computational energy and storage resources.

The sensor nodes are intelligent to observe an extensive diversity of ambient circumstances that includes flow, temperature, pressure, humidity, moisture, noise levels, mechanical stress, speed, etc. Many novel applications are being developed due to the new concept of micro sensing and wireless networking for these smart sensing devices. Some of the possible assorted applications [24] of WSN ’s are temperature control, inventory management, physiological monitoring, habitat monitoring,precision agriculture, forest fire detection, nuclear, chemical, and biological attack detection, military, transportation, disaster relief, and environmental monitoring.

1.2 WSNORGANIZATION

Any WSN can be configured [24] as a five layered architecture as explained below

- The physical layer is responsible for frequency selection, modulation and data encryption.
- The data link layer functions as a pathway for multiplexing of data streams, data frame detection, Medium Access control (MAC) and errorcontrol.
- The network layer is used to route the data supplied by the transport layer using special multi-hop wireless routing protocols between sensor nodes and sinknodes.
- The transport layer maintains the flow of data if the application layer requiresit.
- The application layer makes the hardware and software of the lower layers transparent to the enduser.

1.3 ISSUES AND CHALLENGES IN DESIGNINGWSN

- Sensor networks do not fit into any regular topology, because while deploying the sensor nodes they are scattered [8] [9][10]
- Very limitedresources
  - Limitedmemory,
  - Limitedcomputation

    - Limitedpower
- It comes under fewer infrastructures and also maintenance is verydifficult.
- Unreliablecommunication
    - Unreliable datatransfer
    - Conflicts andlatency
- Sensornodereliesonlyonbatteryanditcannotberechargedorreplaced. Hardware design for sensor node should also be considered.
- Unattendedoperations
    - Exposure to physicalattack
    - Remotelymanaged
    - No central control point
- Achieving synchronization between nodes is also anotherissue.
- Node failure, topology changes and adding of nodes and deletion of nodes is another challengingissue.
- Because of its transmission nature and hostile environment, security is a challengingissue.
- Based on the applications, sensor node has to be chosen with respect to computationrate.

1.4 SECURITY IN WSN

Sensor networks pretence exclusive challenges, so conventional security techniques used in traditional networks cannot be applied directlyforWSN. The sensor devicesare inadequate in their energy, computation, and communication capabilities. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. WSN works together closely with their corporal environments, posing new security troubles [11]. As a result, existing security mechanisms are insufficient, and novel ideas areneeded.

- Sensor nodes are randomly deployed in an open and unattended environment,so security is critical for suchnetworks
- WSN uses wireless communication, which is predominantly easy to eavesdropon.
- An attacker can easily inject malicious node in thenetwork.
- WSN involves a large number of nodes in the network. Enforcing security inall the levels is important and also toocomplex.
- Sensor nodes are resource constraints in terms of memory, energy,transmission range, processing power. Hence asymmetric cryptography is too expensive and symmetric cryptography is used asalternatives.
- Cost of implementing tamper resistant software is veryhigh.

WSN’s general security goals [12] are confidentiality, integrity, authentication, availability, survivability, efficiency, freshness and scalability as described in Table 1.2. WSN is susceptible to many attacks because of its transmission nature, resource restriction on sensor nodes and deployment in uncontrolled environments. To ensure the security services in WSN many crypto mechanisms like symmetric andasymmetric methods are proposed. To achieve security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent between sensor nodes.

Table 1.2 Security Services

Confidentiality	Keeping node information secret from others but authorized users see it.
Integrity	Possible for the receiver node of a message to confirm that it has not been customized in transit.
Device authentication	Justification of the identity of the device.
Message authentication	Justification the source of information
Validation	To provide correctness of authorization to use or manipulate resources.
Access control	Restricting access to resources.
Revocation	Renunciation of certification or authorization.
Survivability	The lifetime of the sensor node must be extended even the node is compromised.
Nonrepudiation	Preventing the denial of a previous commitment.
Availability	High availability systems in sensor node is aim to remain available at all times preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.
Data freshness	Data freshness objective ensures that messages are fresh, meaning that they are in proper order and have not beenreused.

In a distinctive circumstance, any two nodes (A and B) exchange data over an insecure channel. A and B want to make sure that their data exchange remains incomprehensible by anyone who might be listening. Furthermore, because A and B are in remote locations, A must be sure that the information it receives from B is not been modified by anyone during transmission. In addition, it must be sure that the information really does originate from B and not someone impersonating B. Cryptography is used to achieve above mentionedproblems.

The art and science of keeping communication secure is called cryptography, and it is experienced by cryptographers. Cryptography is a process [27] associated with scrambled plain text (ordinary text, or clear text) into cipher text (a process called encryption), then back again (known as decryption). It is a mathematical techniques connected to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The two components required to encrypt data are an algorithm and a key. The algorithm is generally known and the key is kept secret. The key is very large number that should be impossible to guess, and of a size that makes an exhaustive search impractical. In a symmetric cryptosystem [26], the same key is used for encryption and decryption. In an asymmetric cryptosystem, the key used for decryption is different from the key used for encryption. In WSN, cryptographic systems are characterized as which type of operations used for transforming the data, how many numbers of keys used, key size and the way in which the sensor node process thedata.

The possible threats [20] among the sensor nodes in WSN are tabulated in Table 1.3.

Table 1.3 Threat Model of WSN

Threat Model	**Action**
False Node insertion	Feed false data Prevent the true data flow among the nodes
Routing Attack	Alteration of Routing Path Sinkhole, Wormhole Attack
Malicious data	False Observation
Subversion of Node	Extraction of original data from node Misbehavior

The schematic view of crypto functions is shown in Figure 1.4. The taxonomy of cryptographic primitives is shown in Figure 1.5.

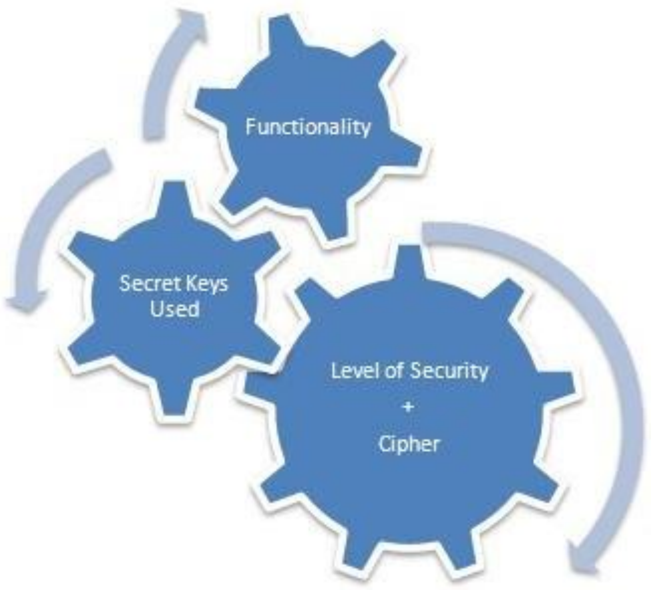


Figure 1.4 Cryptographic Systems

Lars [27] classified and proposed some categories of breaking sensor node information in WSN. These are total break, global deduction, local deduction and information deduction. Total break means, the cryptanalyst finds the key value (K) used in the sensor node, it's very difficult and also time consuming process. Global deduction means cryptanalyst finds the alternate algorithm, local deduction means cryptanalyst finds the equivalent original text and make it try to get the original data from the node. Information deduction means the cryptanalyst gain some information about the key and the data from the sensor node. The security strength of the entire crypto system mainly depends on the secret keys used, not in thealgorithm.

To provide secure communications [13] between the sensor nodes in the WSNs, all the messages should be encrypted and authenticated with different secret keys. The total number of keys processed in the sensor node and the network is too high. For that reason, it is important to design strong and efficient Key Management Schemes (KMS) for WSNs.Inanuncontrolledenvironment,whichenablethesensornodestocommunicate

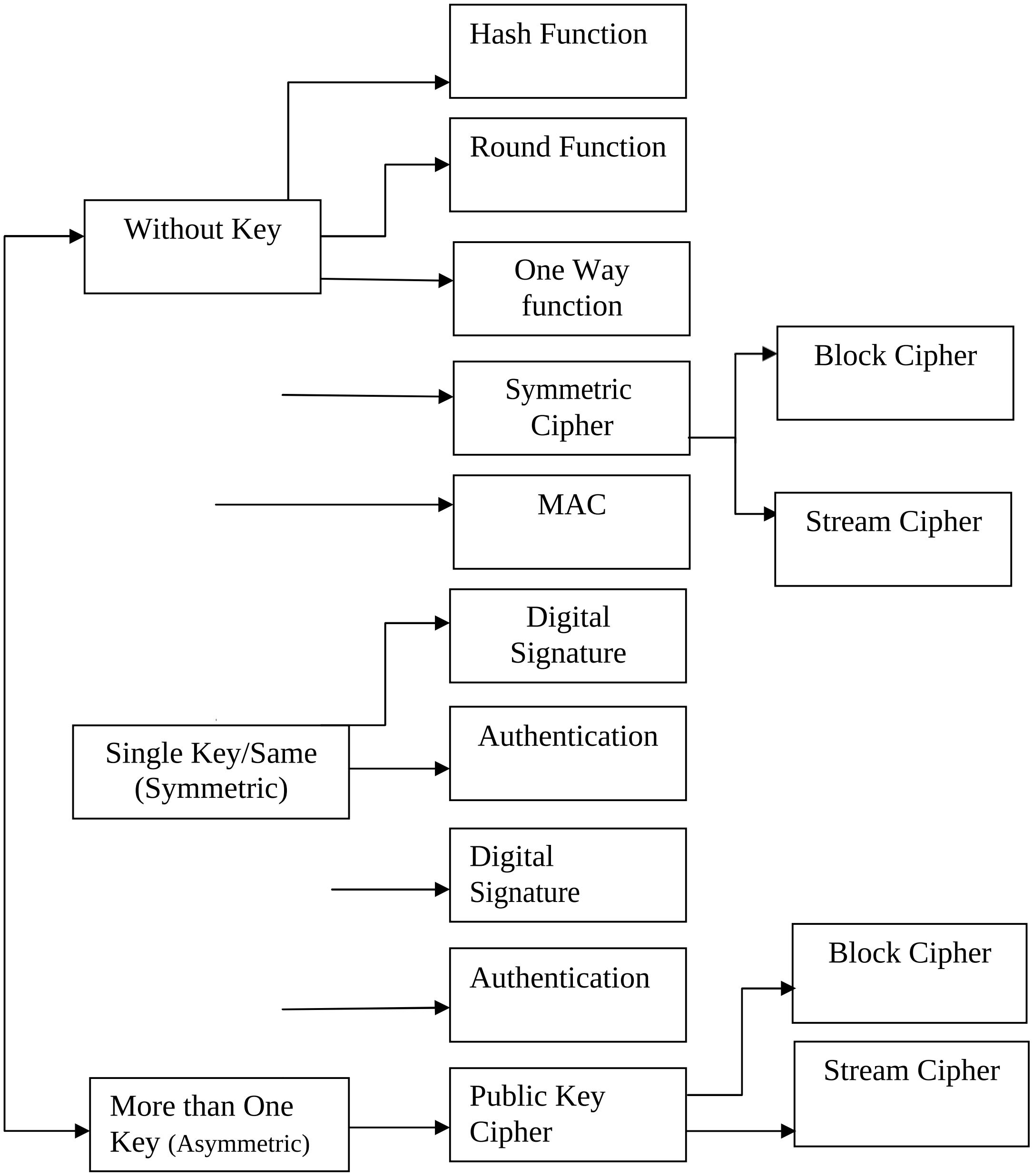


Figure 1.5 Taxonomy of Cryptographic Basics

‘

securely with each other nodes using crypto techniques. The reason of key management [26] for WSN is to load, distribute and handle the secret keys in sensor nodes to establish a secure communication among sensor nodes. Security critical applications depend on the key management scheme because it has to provide high fault tolerance when a node get compromised. Whenever the new node wants to add or leave from the network the key management schemes play a vital role. The key updating process during node addition and node deletion are discussed and shown in Figure1.6.

While designing the key management schemes, the important metrics [35] to be evaluated are 1. **Local / global connectivity:** Each node communicates with every other node in the sensor field region.

2. Resilience: Whenever a sensor node is compromised, the key management scheme assures in securing the remaining communication link against nodecapture.

3. Scalability: Capability to support when large numbers of nodes are added to the sensor network.

4. Efficiency: In terms of storage, communication andcomputation.

Managing efficient cryptographic keys [14] is a difficult problem in case of large dynamic sensor groups. Each time a member is evicted from or added to the group, the group key must be changed. The members of a group must be able to compute a new key efficiently, at the same time forward and backward security must be guaranteed. Forward securing means that any evicted member node cannot determine any future group key, evenwhen

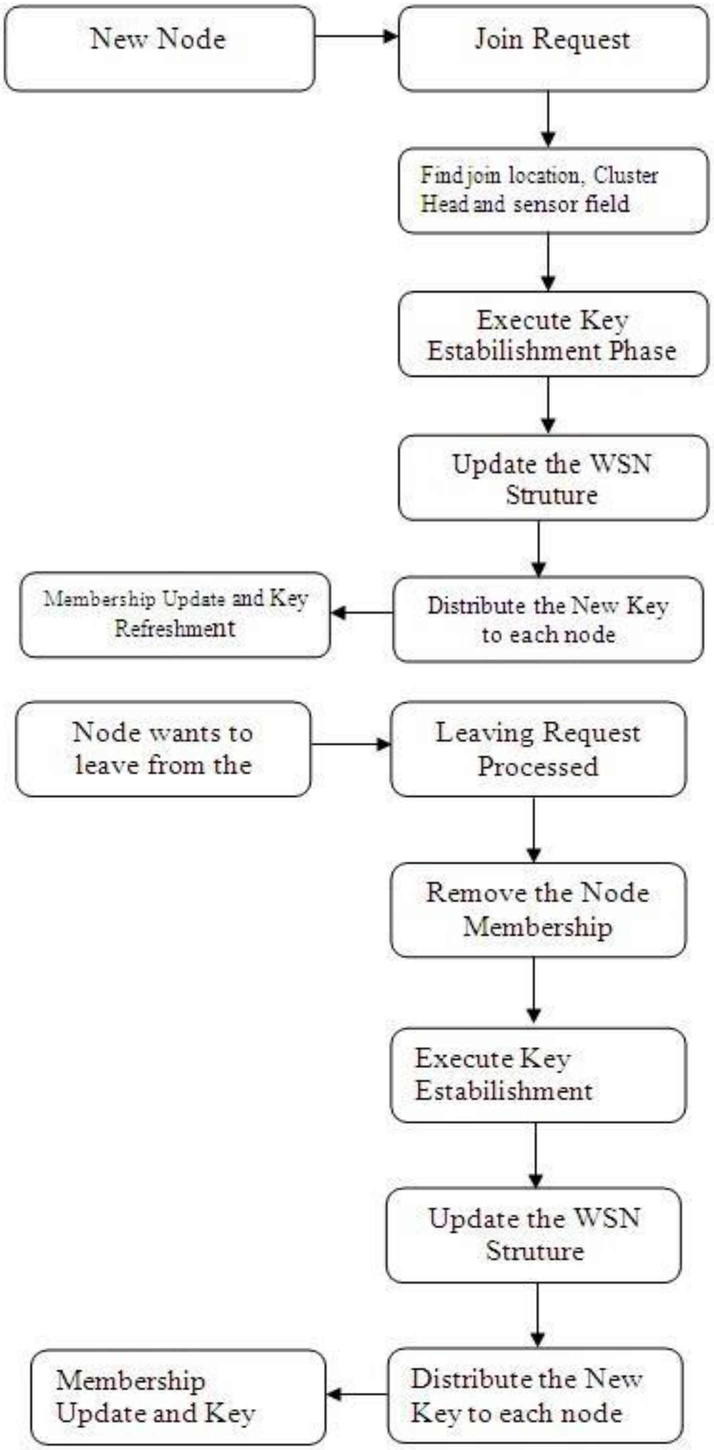

New Node
Join Request
Find join location, Cluster Head and sensor field
Execute Key Estabilishment Phase
Update the WSN Struture
Distribute the New Key to each node
Membership Update and Key Refreshment
Node wants to leave from the
Leaving Request Processed
Remove the Node Membership
Execute Key Estabilishment
Update the WSN Struture
Distribute the New Key to each node
Membership Update and Key

Figure 1.6 Key Refreshment Process In Node Addition and Deletion

performing other tasks. Backward security means that a newly added member node cannot determine any past key, even when working with other new members. Key management for large dynamic group communications raises a problem with scalability. Keys for encryption and authentication purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial. Many key agreement [15] schemes used in general networks, such as Diffie-Hellman and public-key based schemes are not suitable for WSN. Pre-distribution of secret keys for all pairs of nodes is not feasible due to the large amount of memory used when the network size is large. In WSN, keying mechanism is classified into two types, these are static and dynamic keying. The comparison between static and dynamic keying are described in Table 1.4[16]

Table1.4 Static Vs Dynamic Key Management

Parameters	**Static keying**	**Dynamic keying**
Network lifetime	Short	Long
Key pool	Very large	Small size
Key assignment	Once predeployment	Post deployment
Key generation	Once predeployment	Post deployment
Key distribution	All keys are predistributed to nodes prior to deployment	Subsets of keys are re-distributed to some nodes as needed
Handling node capture	Exposed keys are lost	Exposed keys are altered
Communication cost	Not applicable for administrative keys (Key pre distribution).	High
Storage cost	More keys per node	Fewer keys per node
Handling node addition	Hard	Easy
Network resilience	High	High
Network connectivity	Less	More

During node deployment, the sensor node is clustered into different groups. The node that is placed in restricted areas is called a sensor field. Using key generation server, the keys are generated and loaded into each sensor node; the key storage server is used to store the keys. A node deployment process is described in Figure 1.7.

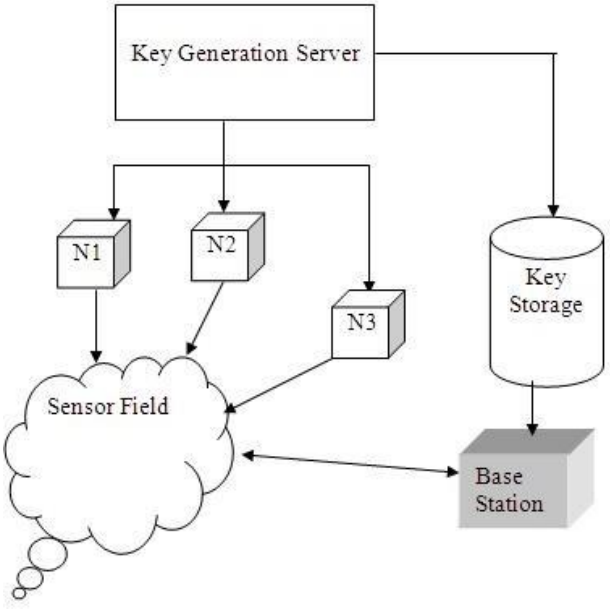


Figure 1.7 Node Deployments

Typical communication pattern in WSN is shown in Table 1.5.

Table 1.5 Communication Pattern in WSN

Source	Purpose
Node to Node	Sensor Readings, Queries
Node to GroupHead, Node to ClusterHead	Sensor Readings, Queries
Node to Base Station	Sensor Readings, Queries
Base Station to all the nodes in the WSN, Cluster Head & Group Head	Queries, Reconfiguration and Routing
Intra Cluster	Among Neighboring Sensor Node, To minimize the total amount of message shared, for Network data processing and data aggregation.

1.5 SCOPE OF THERESEARCH

The research reported in this thesis pertains to authenticated KMS in WSN. From literature survey, the matrix based keying mechanism is suitable for KMS in WSN. All the metrics related to KMS such as key connectivity between nodes, resilience, efficiency and scalability are evaluated against the a proposed work and achieved at an accepted level compared with existing schemes. Authentication at each layer of cluster also implemented using congruence techniques. Depends upon the applications, sensor node has to be incorporated into the network. Various types of sensor nodes are also designed using LPC 2149, LPC 2378 and AT91SAM9263 to set up the efficientWSN.

The research carried out encompasses the following objectives:

- The parameters which affect the quality of key management in WSN are to be identified.
- The problems with existing key management scheme are to beidentified.
- Efficient key management protocol along with its competency with sensor node constraints are to be developed and implemented along with an efficient node to node authentication protocol is designed.
- To develop a WSN in real time using ARM processors and implement the proposed hybrid KMS to achieve maximumthroughput.

The entire process of the thesis work is consolidated and shown in Figure 1.8.

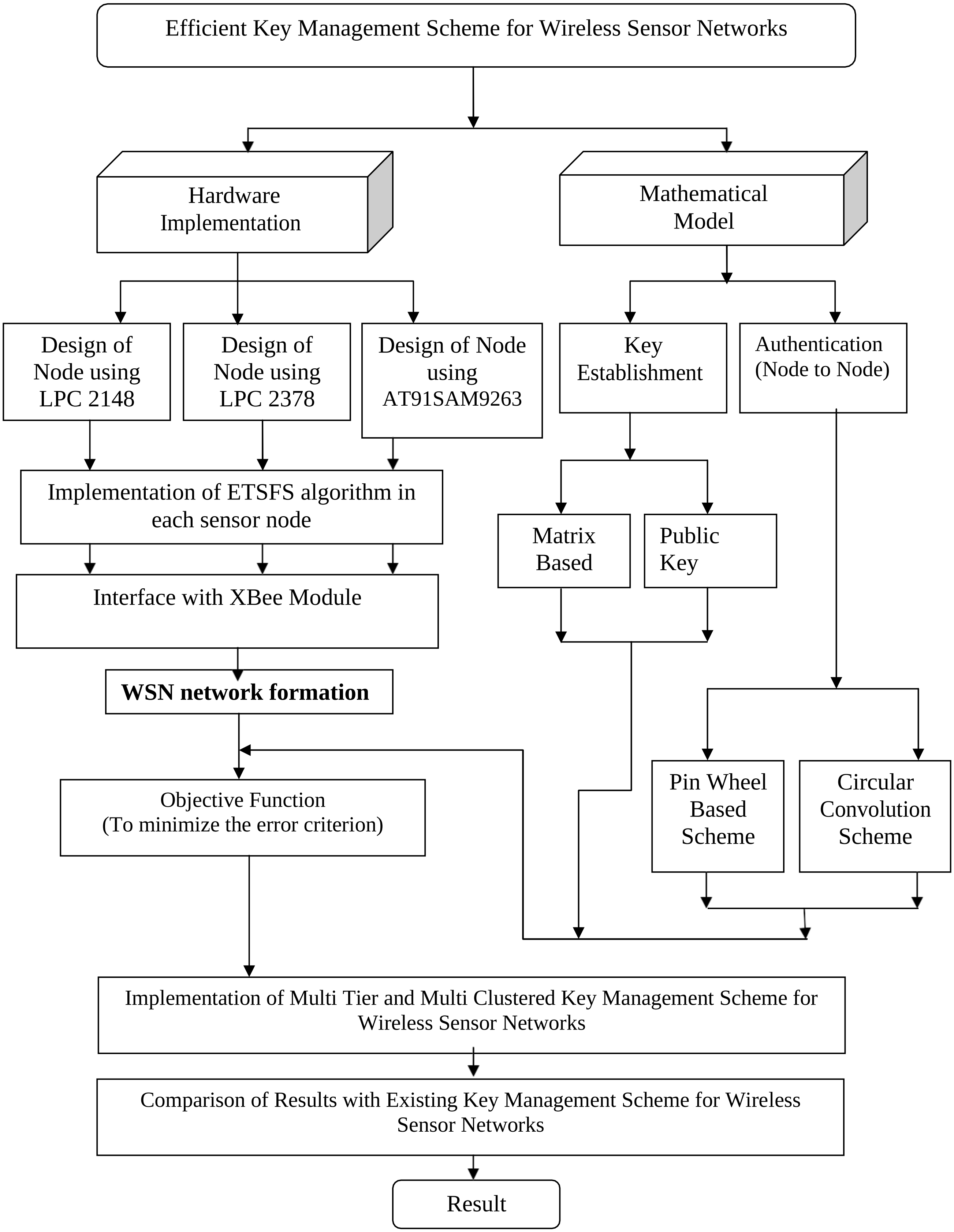

Efficient Key Management Scheme for Wireless Sensor Networks
Hardware Implementation
Mathematical Model
Design of Node using LPC 2148
Design of Node using LPC 2378
Design of Node using AT91SAM9263
Key Establishment
Authentication (Node to Node)
Implementation of ETSFS algorithm in each sensor node
Matrix Based
Public Key
Interface with XBee Module
WSN network formation
Pin Wheel Based Scheme
Circular Convolution Scheme
Objective Function (To minimize the error criterion)
Implementation of Multi Tier and Multi Clustered Key Management Scheme for Wireless Sensor Networks
Comparison of Results with Existing Key Management Scheme for Wireless Sensor Networks
Result

Figure 1.8 Research Scheme

1.6 ORGANIZATION OFTHESIS

Chapter 2 presents the literature review with reference to this work. It also presents the relevant research works in KMS for WSN.

Chapter 3 presents ‘LU decomposition based KMS. It describes the matrix based KMS techniques for WSN and the performance evaluation is done.

Chapter 4 entitled ‘Congruence based pin wheel authentication protocol for WSN’ describes how the node authentication has been employed in the proposed WSN and security analysis is performed.

Chapter 5 entitled ‘Multi Tier & Multi Clustered WSN using LL^T, deals with the analytical model of an integrated KMS with authentication, and provides better optimization using matrix based key distribution approach for providing an efficient KMS for WSN. The results are compared with the existing KMS.

Chapter 6 entitled ‘Implementation of ARM based sensor nodes’ describes the hardware information related to the processing unit of sensor nodes and TSFS implementation in ARM node. The timing analysis for key generating and data encryption are done.

Chapter 7 finally concludes with the contributions of this research work.

Unit – II

SINGLE-NODE ARCHITECTURE:

1.5 HARDWARECOMPONENTS: Choosingthehardwarecomponentsforawirelesssensor node,obviouslytheapplicationshastoconsidersize,costs,andenergyconsumptionofthe nodes.AbasicsensornodecomprisesfivemaincomponentssuchasController,Memory, SensorsandActuators,CommunicationdevicesandPowersupplyUnit.

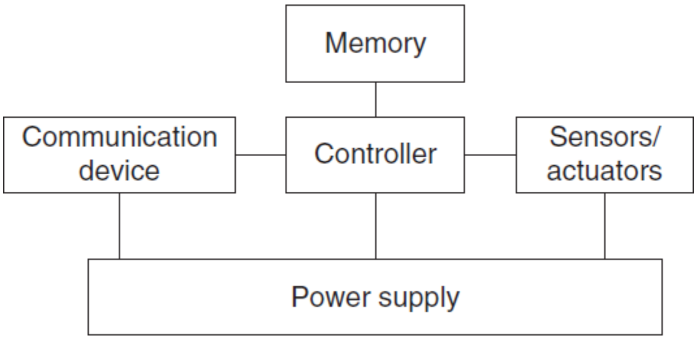


Figure 1.3: Sensor node Hardware components

1.5.1 Controller: Acontrollertoprocessalltherelevantdata,capableofexecutingarbitrary code.Thecontrolleristhecoreofawirelesssensornode.Itcollectsdatafromthesensors, processesthisdata,decideswhenandwheretosendit,receivesdatafromothersensornodes, anddecidesontheactuator'sbehavior.Ithastoexecutevariousprograms,rangingfromtime- critical signal processing and communication protocols to application programs; it is the CentralProcessingUnit(CPU)ofthenode.

For General-purpose processors applications microcontrollers are used. Theseare highlyoverpowered,andtheirenergyconsumptionisexcessive.Theseareusedinembedded systems.Someofthekeycharacteristicsofmicrocontrollersareparticularlysuitedto embeddedsystemsaretheirflexibilityinconnectingwithotherdeviceslikesensorsandthey arealsoconvenientinthattheyoftenhavememorybuiltin.

AspecializedcaseofprogrammableprocessorsareDigitalSignalProcessors(DSPs). Theyarespecificallygeared,withrespecttotheirarchitectureandtheirinstructionset,for processinglargeamountsofvectorialdata,asistypicallythecaseinsignalprocessing applications.Inawirelesssensornode,suchaDSPcouldbeusedtoprocessdatacomingfrom asimpleanalog,wirelesscommunicationdevicetoextractadigitaldatastream.Inbroadband wirelesscommunication,DSPsareanappropriateandsuccessfullyusedplatform.

AnFPGAcanbereprogrammed(orratherreconfigured)"inthefield"toadapttoa changingsetofrequirements;however,thiscantaketimeandenergy–itisnotpracticalto reprogramanFPGAatthesamefrequencyasamicrocontrollercouldchangebetweendifferent programs.

AnASICisaspecializedprocessor,customdesignedforagivenapplicationsuchas,for example,high-speedroutersandswitches.Thetypicaltrade-offhereislossofflexibilityin returnforaconsiderablybetterenergyefficiencyandperformance.Ontheotherhand,wherea microcontroller requires software development, ASICs provide the same functionality in hardware,resultinginpotentiallymorecostlyhardwaredevelopment.

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

1.5.2 Memory: Some memory to store programs and intermediate data; usually, different typesofmemoryareusedforprogramsanddata.InWSNthereisaneedforRandomAccess Memory(RAM)tostoreintermediatesensorreadings,packetsfromothernodes,andsoon. WhileRAMisfast,itsmaindisadvantageisthatitlosesitscontentifpowersupplyis interrupted.ProgramcodecanbestoredinRead-OnlyMemory(ROM)or,moretypically,in ElectricallyErasableProgrammableRead-OnlyMemory(EEPROM)orflashmemory(thelater beingsimilartoEEPROMbutallowingdatatobeerasedorwritteninblocksinsteadofonlya byteatatime).FlashmemorycanalsoserveasintermediatestorageofdataincaseRAMis insufficientorwhenthepowersupplyofRAMshouldbeshutdownforsometime.

1.5.3 CommunicationDevice: Turningnodesintoanetworkrequiresadeviceforsending andreceivinginformationoverawirelesschannel.

*Choiceoftransmissionmedium:*Thecommunicationdeviceisusedtoexchangedatabetween individualnodes.Insomecases,wiredcommunicationcanactuallybethemethodofchoice andisfrequentlyappliedinmanysensornetworks.Thecaseofwirelesscommunicationis considerablymoreinterestingbecauseitincluderadiofrequencies.RadioFrequency(RF)-basedcommunicationisbyfarthemostrelevantoneasitbestfitstherequirementsofmost WSNapplications.

*Transceivers:*ForCommunication,bothtransmitterandreceiverarerequiredinasensornode toconvertabitstreamcomingfromamicrocontrollerandconvertthemtoandfromradio waves.Fortwotasksacombineddevicecalledtransceiverisused. TransceiverstructurehastwopartsasRadioFrequency(RF)frontendandthebasebandpart.

1. Theradiofrequencyfrontendperformsanalogsignalprocessingintheactualradio frequencyBand.
2. The baseband processor performs all signal processing in the digital domain and communicateswithasensornode’sprocessororotherdigitalcircuitry.

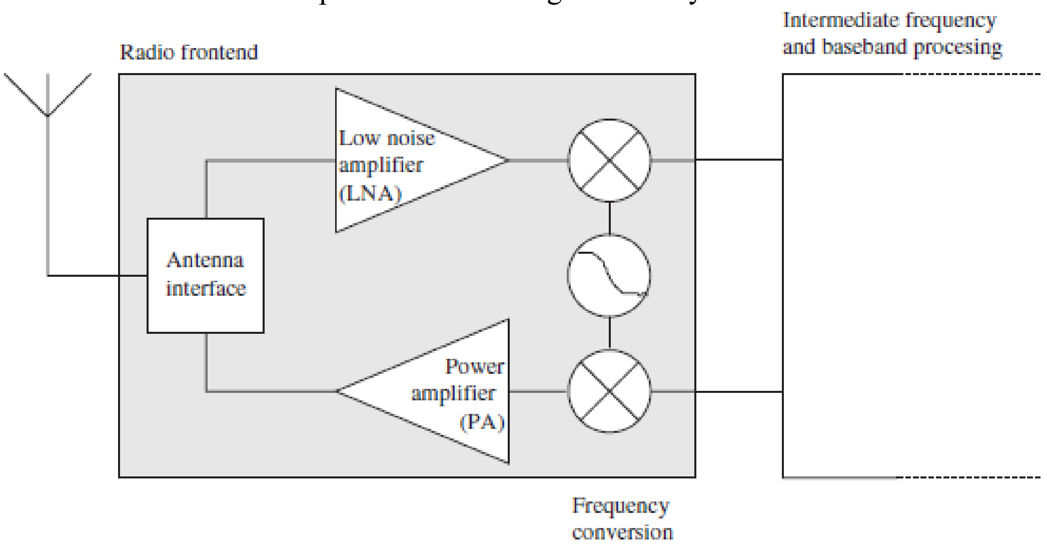


Figure 1.4: RF front end

- ✓ ThePowerAmplifier(PA)acceptsupconvertedsignalsfromtheIForbasebandpartand amplifiesthemfortransmissionovertheantenna.
- ✓ TheLowNoiseAmplifier(LNA)amplifiesincomingsignalsuptolevelssuitablefor furtherprocessingwithoutsignificantlyreducingtheSNR.Therangeofpowersofthe incomingsignalsvariesfromveryweaksignalsfromnodesclosetothereception boundarytostrongsignalsfromnearbynodes;thisrangecanbeupto100dB.
- ✓ Elementslikelocaloscillatorsorvoltage-controlledoscillatorsandmixersareusedfor frequency conversion from the RF spectrum to intermediate frequencies or to thebaseband.TheincomingsignalatRFfrequenciesf_{RF}ismultipliedinamixerwithafixed-frequencysignalfromthelocaloscillator(frequencyf_{LO}).Theresultingintermediate-frequencysignalhasfrequencyf_{LO}−f_{RF}.DependingontheRFfrontendarchitecture,otherelementslikefiltersarealsopresent.

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.

- *CarriersenseandRSSI*:Inmanymediumaccesscontrolprotocols,sensingwhether the wireless channel, the carrier, is busy (another node is transmitting) is a criticalinformation.Thereceiverhastobeabletoprovidethatinformation.thesignal strengthatwhichanincomingdatapackethasbeenreceivedcanprovideuseful information a receiver has to provide this information in the Received Signal Strength Indicator(RSSI).
- *Frequencystability*:Thefrequencystabilitydenotesthedegreeofvariationfrom nominal center frequencies when environmental conditions of oscillators like temperatureorpressurechange.
- *Voltagerange*:Transceiversshouldoperatereliablyoverarangeofsupplyvoltages. Otherwise, inefficient voltage stabilization circuitry is required.

1.5.4 Sensorsandactuators: Theactualinterfacetothephysicalworld:devicesthatcan observeorcontrolphysicalparametersoftheenvironment.

Sensorscan be roughly categorized into three categories as

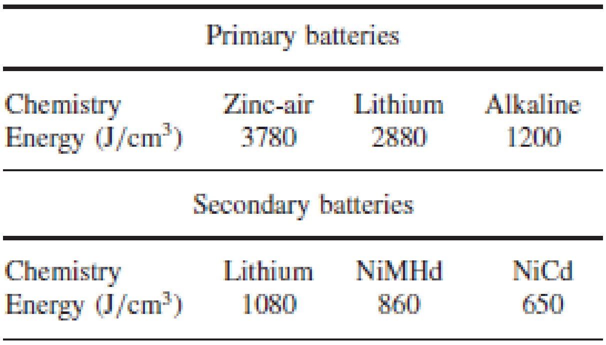
- *Passive,omnidirectionalsensors*:Thesesensorscanmeasureaphysicalquantityat the point of the sensor node without actually manipulating the environment by activeprobing–inthissense,theyarepassive.Moreover,someofthesesensors actuallyareself-poweredinthesensethattheyobtaintheenergytheyneedfromthe environment–energyisonlyneededtoamplifytheiranalogsignal.
- **Passive,narrow-beamsensors**Thesesensorsarepassiveaswell,buthaveawell definednotionofdirectionofmeasurement.
- **Activesensors**Thislastgroupofsensorsactivelyprobestheenvironment,forexample, asonarorradarsensororsometypesofseismicsensors,whichgenerateshockwaves bysmallexplosions.Thesearequitespecific–triggeringanexplosioniscertainlynota lightlyundertakenaction–andrequirequitespecialattention.

Actuators: Actuatorsarejustaboutasdiverseassensors,yetforthepurposesofdesigninga WSNthatconvertselectricalsignalsintophysicalphenomenon.

1.5.5 Powersupply: Asusuallynotetheredpowersupplyisavailable,someformofbatteries arenecessarytoprovideenergy.Sometimes,someformofrechargingbyobtainingenergy fromtheenvironmentisavailableaswell(e.g.solarcells).Thereareessentiallytwoaspects: StoringenergyandEnergyscavenging.

Storing energy: Batteries

- *Traditionalbatteries:*Thepowersourceofasensornodeisabattery,eithernonrechargeable ("primary batteries") or, if an energy scavenging device is present onthe node,alsorechargeable("secondarybatteries").



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

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

Upon these batteries the requirements are

- □ *Capacity:*Theyshouldhavehighcapacityatasmallweight,smallvolume,andlowprice. The main metric is energy per volume, J/cm^3.
- □ *Capacityunderload*:Theyshouldwithstandvarioususagepatternsasasensornodecanconsumequitedifferentlevelsofpowerovertimeandactuallydrawhighcurrentin certain operationmodes.
- □ *Self-discharge:*Theirself-dischargeshouldbelow.Zinc-airbatteries,forexample,have onlyaveryshortlifetime(ontheorderofweeks).
- □ *Efficientrecharging:*Rechargingshouldbeefficientevenatlowandintermittentlyavailable rechargepower.
- □ *Relaxation***:**Theirrelaxationeffect–theseemingself-rechargingofanemptyoralmost emptybatterywhennocurrentisdrawnfromit,basedonchemicaldiffusionprocesses withinthecell–shouldbeclearlyunderstood.Batterylifetimeandusablecapacityis considerablyextendedifthiseffectisleveraged.
- □ *DC–DCConversion:*Unfortunately,batteriesalonearenotsufficientasadirectpowersourceforasensornode.Onetypicalproblemisthereductionofabattery'svoltageas itscapacitydrops.ADC–DCconvertercanbeusedtoovercomethisproblemby regulatingthevoltagedeliveredtothenode'scircuitry.Toensureaconstantvoltage eventhoughthebattery'ssupplyvoltagedrops,theDC–DCconverterhastodraw increasinglyhighercurrentfromthebatterywhenthebatteryisalreadybecoming weak,speedingupbatterydeath.TheDC–DCconverterdoesconsumeenergyforits ownoperation,reducingoverallefficiency.

*Energyscavenging:*Dependingonapplication,highcapacitybatteriesthatlastforlongtimes, thatis,haveonlyanegligibleself-dischargerate,andthatcanefficientlyprovidesmallamounts ofcurrent.Ideally,asensornodealsohasadevicefor**energyscavenging**,rechargingthe batterywithenergygatheredfromtheenvironment–solarcellsorvibration-basedpower generationareconceivableoptions.

- □ *Photovoltaics:*Thewell-knownsolarcellscanbeusedtopowersensornodes.Theavailablepowerdependsonwhethernodesareusedoutdoorsorindoors,andontime ofdayandwhetherforoutdoorusage.Theresultingpowerissomewherebetween10 $\mu W/cm^2$indoorsand15mW/cm^2 outdoors.Singlecellsachieveafairlystableoutput voltageofabout0.6V(andhavethereforetobeusedinseries)aslongasthedrawn current does not exceed a critical threshold, which depends on the light intensity. Hence,solarcellsareusuallyusedtorechargesecondarybatteries.
- □ *Temperaturegradients***:**Differencesintemperaturecanbedirectlyconverted toelectricalenergy.
- □ *Vibrations:*Onealmostpervasiveformofmechanicalenergyisvibrations:walls orwindows in buildings are resonating with cars or trucks passing in the streets, machinery often has low frequency vibrations. both amplitude and frequencyofthevibrationandrangesfromabout0.1$\mu W/cm^3$ upto10,000$\mu W/cm^3$ forsomeextremecases.Convertingvibrationstoelectricalenergycanbeundertaken byvarious means,basedonelectromagnetic,electrostatic,orpiezoelectricprinciples.
- □ *Pressurevariations:*Somewhatakintovibrations,avariationofpressurecanalso beusedasapowersource.
- □ *Flowofair/liquid:*Anotheroften-usedpowersourceistheflowofairorliquidin windmillsorturbines.Thechallengehereisagaintheminiaturization,butsomeofthe workonmillimeterscaleMEMSgasturbinesmightbereusable.

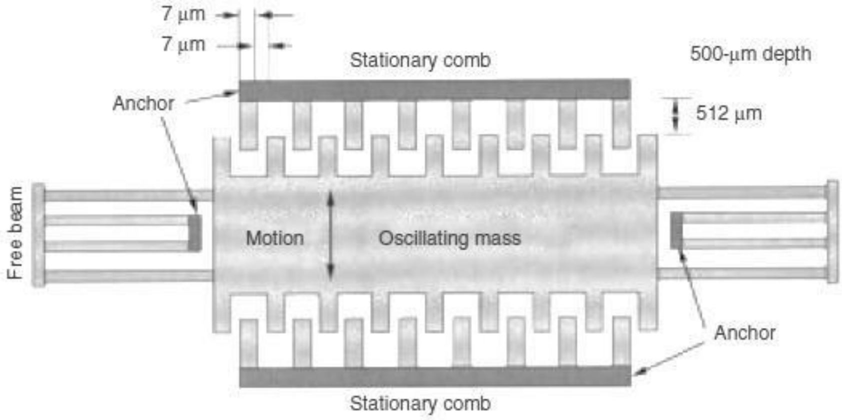
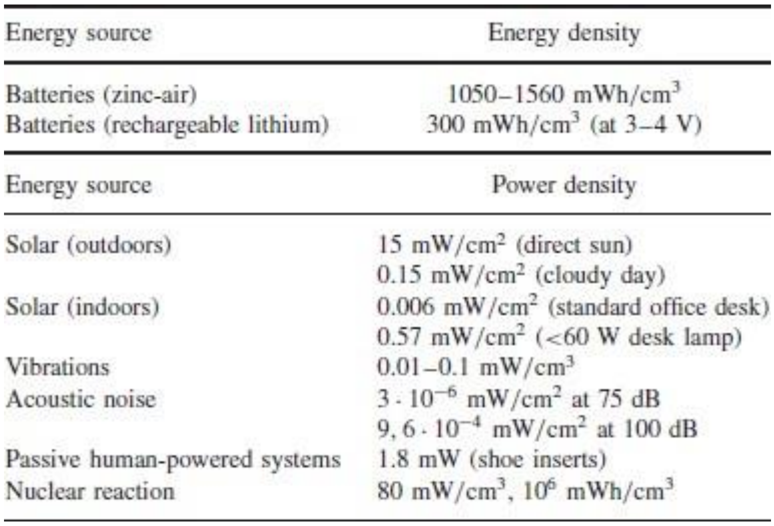


Figure 1.5 A MEMS device for converting vibrations to electrical energy, based on a variable capacitor



Energy source	Energy density
Batteries (zinc-air)	1050–1560 mWh/cm^3
Batteries (rechargeable lithium)	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:

Inprevioussectionwediscussedaboutenergysupplyforasensornodethrough batteriesthathavesmallcapacity,andrechargingbyenergyscavengingiscomplicatedand volatile.Hence,theenergyconsumptionofasensornodemustbetightlycontrolled.Themain consumersofenergyarethecontroller,theradiofrontends,thememory,andtypeofthe sensors.Onemethodtoreducepowerconsumptionofthesecomponentsisdesigninglow-powerchips,itisthebeststartingpointforanenergy-efficientsensornode.Butany advantagesgainedbysuchdesignscaneasilybesquandered/wastedwhenthecomponents are improperly operated. Second method for energy efficiency in wireless sensor node isreduced functionality by using multiple states of operation with reduced energy consumption. Thesemodescanbeintroducedforallcomponentsofasensornode,inparticular,for controller,radiofrontend,memory,andsensors.

1.7.1 Microcontroller energy consumption: For a controller, typical states are “active”,“idle”,and“sleep”.Aradiomodemcouldturntransmitter,receiver,orbothonoroff.Attimet_1, themicrocontrolleristobeputintosleepmodeshouldbetakentoreducepowerconsumptionfromP_{active}toP_{sleep}.Ifitremainsactiveandthenexteventoccursattimet$_{event}$,thenatotal energyis$E_{active}=P_{active}(t_{event}-t_1)$.Ontheotherhand,requiresatimeτ_{down}untilsleepmodehas beenreached.Lettheaveragepowerconsumptionduringthisphaseis$(P_{active}+P_{sleep})/2$.Then, P_{sleep}isconsumeduntilt$_{event.}$Theenergysavingisgivenby

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

Oncetheeventtobeprocessedoccurs,however,anadditionaloverheadof

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

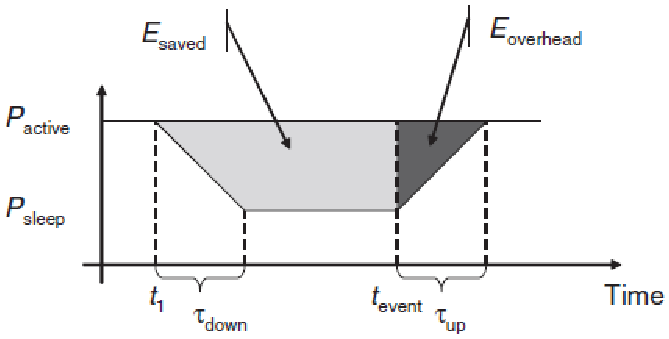


Figure 1.6 Energy savings and overheads for sleep modes

Switchingtoasleepmodeisonlybeneficialif$E_{overhead} < E_{saved}$or,equivalently,ifthetimetothe nexteventissufficientlylarge: --- (6)

$$(t_{event} - t_1) > \frac{1}{2}\left(\tau_{down} + \frac{P_{active} + P_{sleep}}{P_{active} - P_{sleep}}\tau_{up}\right)$$

Examples:

Intel StrongARM

The Intel StrongARM provides three sleep modes:

- ✓ In*normalmode*,allpartsoftheprocessorarefullypowered.Powerconsumptionisup to 400mW.
- ✓ In*idlemode*,clockstotheCPUarestopped;clocksthatpertaintoperipheralsareactive. Anyinterruptwillcausereturntonormalmode.Powerconsumptionisupto100mW.
- ✓ In *sleep mode*, only the real-time clock remains active. Wakeup occurs after a timer interruptandtakesupto160ms.Powerconsumptionisupto50µW.

Texas Instruments MSP 430

TheMSP430familyfeaturesawiderrangeofoperationmodes:Onefullyoperationalmode, whichconsumesabout1.2mW(allpowervaluesgivenat1MHzand3V).Therearefoursleep modesintotal.Thedeepestsleepmode,LPM4,onlyconsumes0.3µW,butthecontrollerisonly wokenupbyexternalinterruptsinthismode.Inthenexthighermode,LPM3,aclockisalso tillrunning,whichcanbeusedforscheduledwakeups,andstillconsumesonlyabout6µW. **AtmelATmega**

TheAtmelATmega128Lhassixdifferentmodesofpowerconsumption,whichareinprinciple similartotheMSP430butdifferinsomedetails.Itspowerconsumptionvariesbetween6mW and15mWinidleandactivemodesandisabout75µWinpower-downmodes.

1.7.2 Memoryenergyconsumption: Themostrelevantkindsofmemoryareon-chipmemory andFLASHmemory.Off-chipRAMisrarelyused.Infact,thepowerneededtodriveon-chip memory is usually included in the power consumption numbers given for thecontrollers. Hence,themostrelevantpartisFLASHmemory.Infact,theconstructionandusageofFLASH memorycanheavilyinfluencenodelifetime.Therelevantmetricsarethereadandwritetimes andenergyconsumption.Readtimesandreadenergyconsumptiontendtobequitesimilar betweendifferenttypesofFLASHmemory.Energyconsumptionnecessaryforreadingand writingtotheFlashmemoryisusedontheMicanodes.Hence,writingtoFLASHmemorycan beatime-andenergy-consumingtaskthatisbestavoidedifsomehowpossible.

1.7.3 Radiotransceiversenergyconsumption: Aradiotransceiverhasessentiallytwotasks: transmittingandreceivingdatabetweenapairofnodes.Similartomicrocontrollers,radio transceiverscanoperateindifferentmodes,thesimplestonesarebeingturnedonorturned off.Toaccommodatethenecessarylowtotalenergyconsumption,thetransceiversshouldbe turnedoffmostofthetimeandonlybeactivatedwhennecessary–theyworkatalowduty cycle.

TheenergyconsumedbyatransmitterisduetotwosourcesonepartisduetoRFsignal generation,whichmostlydependsonchosenmodulationandtargetdistance.Secondpartis duetoelectroniccomponentsnecessaryforfrequencysynthesis,frequencyconversion,filters, andsoon.Thetransmittedpowerisgeneratedbytheamplifierofatransmitter.Itsownpower consumptionP_{amp}dependsonitsarchitecture$P_{amp}=\alpha_{amp}+\beta_{amp}P_{tx}$.where$\alpha_{amp}and\beta_{amp}$are constantsdependingonprocesstechnologyandamplifierarchitecture.Theenergytotransmit apacket$n$-bitslong(includingallheaders)thendependsonhowlongittakestosendthe packet,determinedbythenominalbitrate$R$andthecodingrateR_{code},andonthetotal consumedpowerduringtransmission.

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

Similartothetransmitter,thereceivercanbeeitherturnedofforturnedon.While beingturnedon,itcaneitheractivelyreceiveapacketorcanbeidle,observingthechanneland readytoreceive.Evidently,thepowerconsumptionwhileitisturnedoffisnegligible.Eventhe differencebetweenidlingandactuallyreceivingisverysmallandcan,formostpurposes,be assumedtobezero.Toelucidate,theenergyE_{rcvd}requiredtoreceiveapackethasastartup component$T_{start}P_{start}$similartothetransmissioncasewhenthereceiverhadbeenturnedoff (startuptimesareconsideredequalfortransmissionandreceivinghere);italsohasa componentthatisproportionaltothepackettime.Duringthistime$\frac{n}{RR_{code}}$ofactualreception, receivercircuitryhastobepoweredup, requiringa(moreorlessconstant)powerofP_{rxElec}.

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

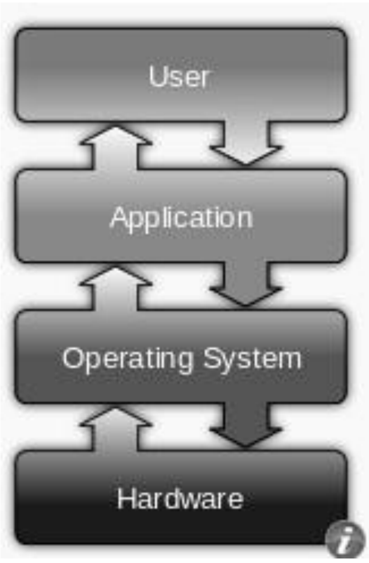
1.7.4 Power consumption of sensor andactuators:

Providinganyguidelinesaboutthepowerconsumptionoftheactualsensorsandactuatorsis impossiblebecauseofthewidevarietyofthesedevices.Forexample,passivelightor temperaturesensors–thepowerconsumptioncanpossiblybeignoredincomparisontoother devicesonawirelessnode.Forothers,activedeviceslikesonar(Ameasuringinstrumentthat sendsoutanacousticpulseinwaterandmeasuresdistancesintermsoftimefortheechoof thepulsetoreturn),powerconsumptioncanbequiteconsiderableinthedimensioningof powersourcesonthesensornode,nottooverstressbatteries.

1.8 OPERATING SYSTEMS AND EXECUTIONENVIRONMENTS:

1.8.1 Embedded operatingsystems:

- ✓ Anoperatingsystem(OS)issystemsoftwarethatmanages computer hardware and software resources andprovides commonservicesforcomputerprograms.
- ✓ For hardware functions such as input and output and memory allocation, the operating system acts as an intermediary between programs and the computer hardware.
- ✓ Anembeddedsystemissomecombinationofcomputer hardware and software, either fixed in capability or programmable,thatisspecificallydesignedforaparticular function.
- ✓ Embedded operating systems are designed to be used in embeddedcomputersystems.Theyareabletooperatewith alimitednumberofresources.Theyareverycompactand extremely efficientbydesign.



1.8.2 TinyOS:

- ✓ TinyOSisanopen-source,flexibleandapplication-specificoperatingsystemforwireless sensornetworks.
- ✓ Wirelesssensornetworkconsistsofalargenumberoftinyandlow-powernodes,each of which executes simultaneous and reactive programs that must work with strict memoryandpowerconstraints.

- ✓ TinyOS meets these challenges and has become the platform of choice for sensor networksuchaslimitedresourcesandlow-poweroperation.
- ✓ SalientfeaturesofTinyOSare
  - □ Asimpleevent-basedconcurrencymodelandsplit-phaseoperations influence the development phases and techniques when writing applicationcode.
  - □ It has a component-based architecture which provides rapid innovationandimplementationwhilereducingcodesizeasrequiredbythedifficultmemory constraintsinherentinwirelesssensornetworks.
  - □ TinyOS'scomponentlibraryincludesnetworkprotocols,distributedservices, sensordrivers,anddataacquisitiontools.
  - □ TinyOS'sevent-drivenexecutionmodelenablesfinegrainedpowermanagement, yetallowstheschedulingflexibilitymadenecessarybytheunpredictablenature ofwirelesscommunicationandphysicalworldinterfaces.

1.8.3 Programming paradigms and application programminginterfaces:

- ❖ **Concurrent Programming:** Concurrent processing isacomputingmodelinwhichmultipleprocessors execute instructions simultaneously for better performance. Concurrent means something that happensatthesametimeassomethingelse.Tasks are broken down into subtasks that are then assigned to separate processors to perform simultaneously, instead of sequentially as they wouldhavetobecarriedoutbyasingleprocessor. Concurrentprocessingissometimessaidtobe synonymouswithparallelprocessing.

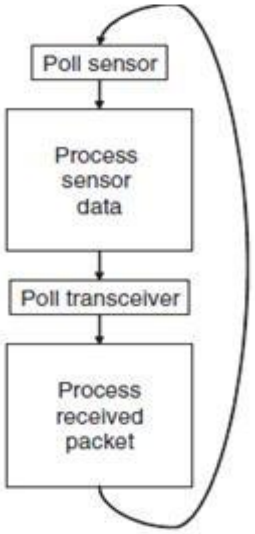


Figure 1.8 Sequential programming model

- ❖ **Process-based concurrency:** Most modern, general-purpose operating systems support concurrent (seemingly parallel) execution of multipleprocessesonasingleCPU.Usingprocesses youareforcedtodealwithcommunicationthrough messages,whichistheErlang(Aunitoftraffic intensity in telephone system) way of doing communication.Dataisnotshared,sothereisno 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 perfectlyokwiththat,becauseyoujustrestart them (even across network hosts). If thread crashes,itmaycrashtheentireprocess,whichmay bringdownyourentireapplication.

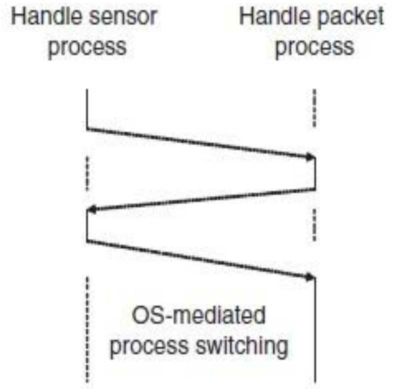


Figure 1.9 Process-based programming model

- ❖ **Event-based programming:** In computer programming, event-driven programming is a programmingparadigm in which the flow ofthe programis determinedbyeventssuchasuseractions (mouse clicks, key presses), sensor outputs, or messages from other programs/threads. Event-driven

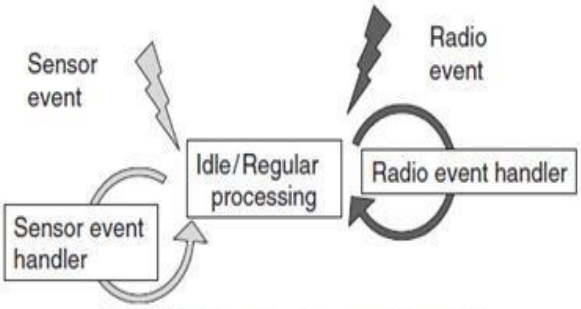


Figure 1.10 Event-based programming model

programmingisthedominantparadigmusedinGraphicalUserInterfaces(GUI-typeof userinterfacethatallowsuserstointeractwithelectronicdevicesthroughgraphical icons)andotherapplications.Thesystemessentiallywaitsforanyeventtohappen, whereaneventtypicallycanbetheavailabilityofdatafromasensor,thearrivalofa packet,ortheexpirationofatimer.Suchaneventisthenhandledbyashortsequenceof instructionsthatonlystoresthefactthatthiseventhasoccurredandstoresthe necessaryinformation.

❖ **Interfaces to the operating system:** A boundary across which two independent systemsmeetandactonorcommunicatewitheachother.Incomputertechnology, thereareseveraltypesofinterfaces.Userinterface-thekeyboard,mouse,menusofa computersystem.Theuserinterfaceallowstheusertocommunicatewiththeoperating system.Standsfor"ApplicationProgrammingInterface."AnAPIisasetofcommands, functions,protocols,andobjects(wirelesslinks,nodes)thatprogrammerscanuseto createsoftwareorinteractwithanexternalsystem(sensors,actuators,transceivers).It providesdeveloperswithstandardcommandsforperformingcommonoperationsso theydonothavetowritethecodefromscratch.

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 ofeachother,eachlayeronlyusingfunctionsofthelayerdirectly.Thislayeredapproachhas greatbenefitsinkeepingtheentireprotocolstackmanageable,incontainingcomplexity,andin promotingmodularityandreuse.ForthepurposesofaWSN,however,itisnotclearwhether suchastrictlylayeredapproachwillserve.Aprotocolstackreferstoagroupofprotocolsthat are running concurrently that are employed for the implementation of network protocol suite. Theprotocolsinastackdeterminetheinterconnectivityrulesforalayerednetworkmodel suchasintheOSIorTCP/IPmodels.

1.8.5 Dynamic energy and power management: Switching individual components into varioussleepstatesorreducingtheirperformancebyscalingdownfrequencyandsupply voltageandselectingparticularmodulationandcodingareprominentexamplesforimproving energyefficiency.Tocontrolthesepossibilities,decisionshavetobemadebytheoperating system,bytheprotocolstack,orpotentiallybyanapplicationwhentoswitchintooneofthese states.DynamicPowerManagement(DPM)onasystemlevelistheproblemathand.Oneofthe complicatingfactorstoDPMistheenergyandtimerequiredforthetransitionofacomponent betweenanytwostates.Ifthesefactorswerenegligible,clearlyitwouldbeoptimaltoalways&immediatelygointothemodew iththelowestpowerconsumptionpossible.

NETWORKARCHITECTURE: Itintroducesthebasicprinciplesofturningindividualsensor nodesintoawirelesssensornetwork.Inthisoptimizationgoalsofhowanetworkshould functionarediscussedas

- ✓ Sensor networkscenarios
- ✓ Optimizationgoalsandfiguresofmerit
- ✓ Gatewayconcepts

1.9 SENSOR NETWORKSCENARIOS:

1.9.1 Types of sources and sinks: Source is any unit in the network that can provide information(sensornode).Asinkistheunitwhereinformationisrequired,itcouldbelongto thesensornetworkoroutsidethisnetworktointeractwithanothernetworkoragatewayto anotherlargerInternet**.**SinksareillustratedbyFigure1.11,showingsourcesandsinksindirect communication.

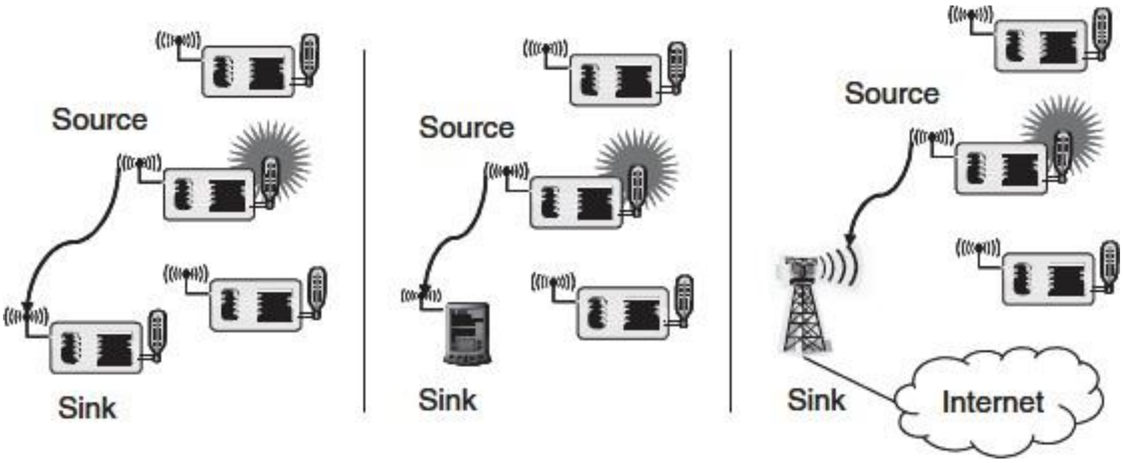


Figure 1.11 Three types of sinks in a very simple, single-hop sensor network

1.9.2 Single-hop versus multi-hopnetworks:

Becauseoflimiteddistancethedirectcommunicationbetweensourceandsinkisnotalways possible.InWSNs,tocoveralotofenvironmentthedatapacketstakingmultihopsfromsource tothesink.Toovercomesuchlimiteddistancesitbettertouserelaystations,Thedata packetstakingmultihopsfromsourcetothesinkasshowninFigure1.12,Dependingonthe particularapplicationofhavinganintermediatesensornodeattherightplaceishigh.

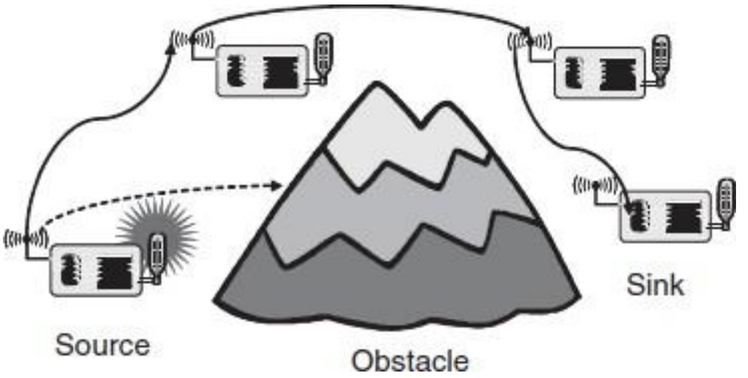


Figure 1.12 Multi-hop networks: As direct communication is impossible because of distance and/or obstacles

Multi-hoppingalsotoimprovestheenergyefficiencyofcommunicationasitconsumesless energytouserelaysinsteadofdirectcommunication,theradiatedenergyrequiredfordirect communicationoveradistancediscd$^{\alpha}$(csomeconstant,$\alpha \geq 2$thepathlosscoefficient)and usingarelayatdistanced/2reducesthisenergyto$2c(d/2)^{\alpha}$

Thiscalculationconsidersonlytheradiatedenergy.Itshouldbepointedoutthatonlymulti-hopnetworksoperatinginastoreandforwardfashionareconsideredhere.Insuchanetwork, anodehastocorrectlyreceiveapacketbeforeitcanforwarditsomewhere. Cooperative relaying(reconstructionincaseoferroneouspacketreception)techniquesarenotconsidered here.

1.9.3 Multiplesinksandsources: Inmanycases,multiplesourcesandmultiplesinkspresent. Multiple sources should send information to multiple sinks. Either all or some ofthe informationhastoreachallorsomeofthesinks.Thisisillustratedinfigure1.13.

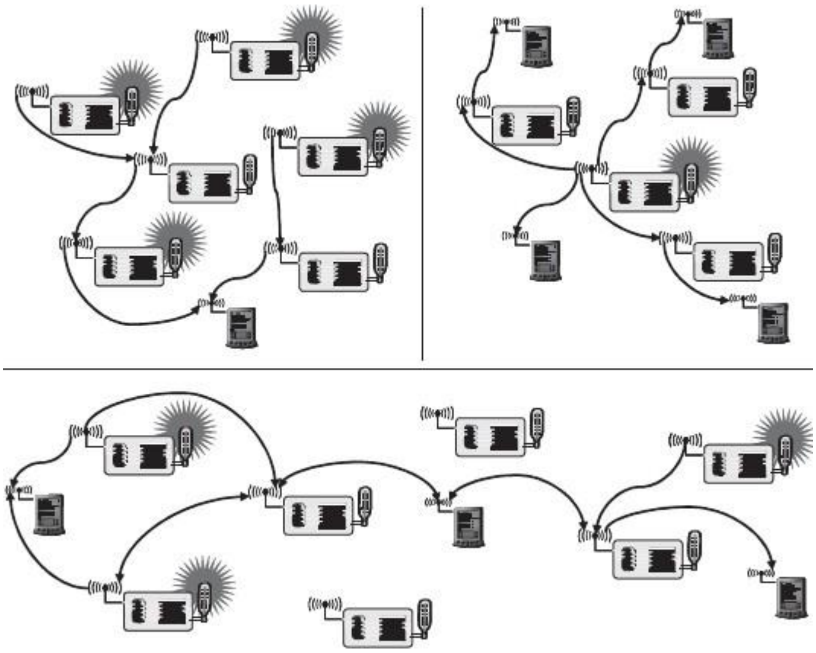


Figure 1.13 Multiple sources and/or multiple sinks.

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 tosupport mobileparticipantsInwirelesssensornetworks,mobilitycanappearinthreemainforms

a. Node mobility
b. Sink mobility
c. Event mobility

1.9.4(a)Node Mobility: Thewirelesssensornodesthemselvescanbemobile.Themeaningof suchmobilityishighlyapplicationdependent.Inexampleslikeenvironmentalcontrol,node mobilityshouldnothappen;inlivestocksurveillance(sensornodesattachedtocattle,for example),itisthecommonrule.Inthefaceofnodemobility,thenetworkhastoreorganizeto functioncorrectly.

1.9.4(b)SinkMobility: Theinformationsinkscanbemobile.Forexample,ahumanuser requestedinformationviaaPDAwhilewalkinginanintelligentbuilding.Inasimplecase,such arequestercaninteractwiththeWSNatonepointandcompleteitsinteractionsbeforemoving on,Inmanycases,consecutiveinteractionscanbetreatedasseparate,unrelatedrequests.

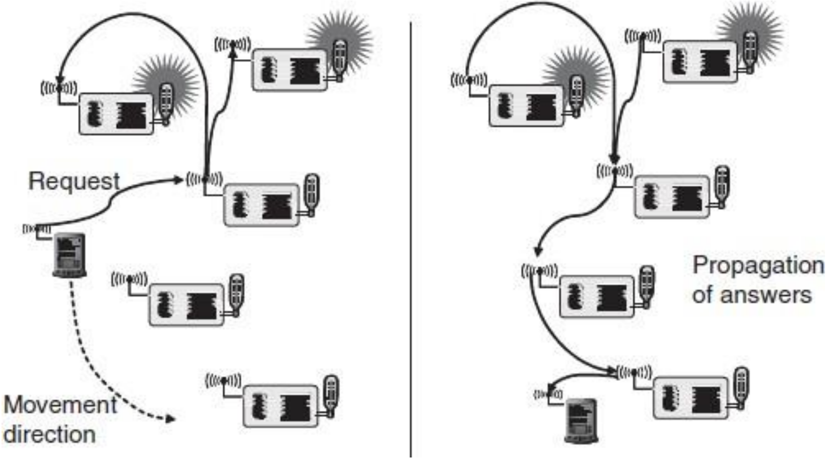


Figure 1.14 Sink mobility: A mobile sink moves through a sensor network as information is being retrieved *on its behalf*

1.9.4(c)EventMobility: Intrackingapplications,thecauseoftheeventsortheobjectstobe trackedcanbemobile.Insuchscenarios,itis(usually)importantthattheobservedeventis coveredbyasufficientnumberofsensorsatalltime.Astheeventsourcemovesthroughthe network,itisaccompaniedbyanareaofactivitywithinthenetwork–thishasbeencalledthe frisbeemodel.ThisnotionisdescribedbyFigure1.15,wherethetaskistodetectamoving elephantandtoobserveitasitmovesaround

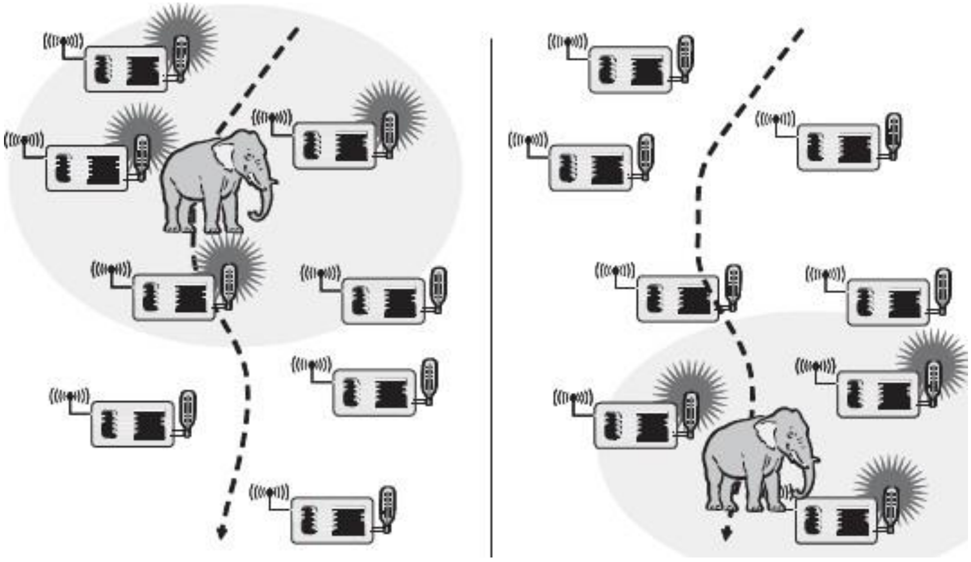


Figure 1.15 Area of sensor nodes detecting an event – an elephant– that moves through the network along with the event source (dashed line indicate the elephant's trajectory; shaded ellipse the activity area following or even preceding the elephant)

1.10 OPTIMIZATION GOALS AND FIGURES OFMERIT:

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

- HowtooptimizeanetworkandHowtocomparethesesolutions?
- Howtodecidewhichapproachisbetter?
- Howtoturnrelativelyinaccurateoptimizationgoalsintomeasurablefiguresofmerit?

Foralltheabovequestionsthegeneralanswerisobtainedfrom

- Quality ofservice
- Energyefficiency
- Scalability
- Robustness

1.10.1Quality of service: WSNs differ from other conventional communication networks in thetypeofservicetheyoffer.Thesenetworksessentiallyonlymovebitsfromoneplaceto another.Somegenericpossibilitiesare

- **Eventdetection/reportingprobability-**Theprobabilitythataneventthatactually occurredisnotdetectedornotreportedtoaninformationsinkthatisinterestedin suchaneventForexample,notreportingafirealarmtoasurveillancestationwouldbe a severeshortcoming.
- **Event classification error-** If events are not only to be detected but also to be classified,theerrorinclassificationmustbesmall
- **Eventdetectiondelay-**Itisthedelaybetweendetectinganeventandreportingitto any/all interestedsinks
- **Missingreports-**Inapplicationsthatrequireperiodicreporting,theprobabilityof undeliveredreportsshouldbesmall
- **Approximation accuracy-** For function approximation applications, the average/maximumabsoluteorrelativeerrorwithrespecttotheactualfunction.
- **Trackingaccuracy**Trackingapplicationsmustnotmissanobjecttobetracked,the reportedpositionshouldbeasclosetotherealpositionaspossible,andtheerror should besmall.

1.10.2 Energyefficiency:Energyefficiencyshouldbeoptimizationgoal.Themostcommonly considered aspectsare:

- ✓ **Energypercorrectlyreceivedbit-**Howmuchenergyisspentonaveragetotransport onebitofinformation(payload)fromthetransmittertothereceiver.
- ✓ **Energyperreported(unique)event-**Whatistheaverageenergyspenttoreportone event
- ✓ **Delay/energy trade-offs-**"urgent" events increases energy investment for a speedy reportingevents.Here,thetrade-offbetweendelayandenergyoverheadisinteresting
- ✓ **Networklifetime**Thetimeforwhichthenetworkisoperational
- ✓ **Timetofirstnodedeath-**Whendoesthefirstnodeinthenetworkrunoutofenergyor failandstopoperating?
- ✓ **Networkhalf-life-**Whenhave50%ofthenodesrunoutofenergyandstopped operating
- ✓ **Time to partition-**When does the first partition of the network in two (or more) disconnected partsoccur?
- ✓ **Timetolossofcoverage**thetimewhenforthefirsttimeanyspotinthedeployment regionisnolongercoveredbyanynode'sobservations.
- ✓ **Time to failure of first event notification** A network partition can be seen as irrelevantiftheunreachablepartofthenetworkdoesnotwanttoreportanyeventsin the firstplace.

1.10.3 Scalability: Theabilitytomaintainperformancecharacteristicsirrespectiveofthesize ofthenetworkisreferredtoasscalability.WithWSNpotentiallyconsistingofthousandsof nodes,scalabilityisanobviouslyessentialrequirement.Theneedforextremescalabilityhas directconsequencesfortheprotocoldesign.Often,apenaltyinperformanceorcomplexityhas tobepaidforsmallnetworks.Architecturesandprotocolsshouldimplementappropriate scalabilitysupportratherthantryingtobeasscalableaspossible.Applicationswithafew dozennodesmightadmitmore-efficientsolutionsthanapplicationswiththousandsofnodes.

1.10.4 Robustness: Wirelesssensornetworksshouldalsoexhibitanappropriaterobustness. Theyshouldnotfailjustbecausealimitednumberofnodesrunoutofenergy,orbecausetheir environmentchangesandseversexistingradiolinksbetweentwonodes.Ifpossible,these failureshavetobecompensatedbyfindingotherroutes.

1.11 GATE WAYCONCEPTS:

1.11.1 Need forgateways:

- ✓ Forpracticaldeployment,asensornetworkonlyconcernedwithitselfisinsufficient.
- ✓ Thenetworkratherhastobeabletointeractwithotherinformationdevicesfor exampletoreadthetemperaturesensorsinone'shomewhiletravelingandaccessing theInternetviaawireless.
- ✓ Wirelesssensornetworksshouldalsoexhibitanappropriaterobustness
- ✓ Theyshouldnotfailjustbecauseofalimitednumberofnodesrunoutofenergyor becauseoftheirenvironmentchangesandbreaksexistingradiolinksbetweentwo nodes.
- ✓ Ifpossible,thesefailureshavetobecompensatedbyfindingotherroutes.

Figure1.16showsthisnetworkingscenario,TheWSNfirstofallhastobeabletoexchange datawithsuchamobiledeviceorwithsomesortofgateway,whichprovidesthephysical connection to the Internet. The WSN support standard wireless communication technologies suchasIEEE802.11.Thedesignofgatewaysbecomesmuchmorechallengingwhen consideringtheirlogicaldesign.Oneoptionistoregardagatewayasasimplerouterbetween Internetandsensornetwork.

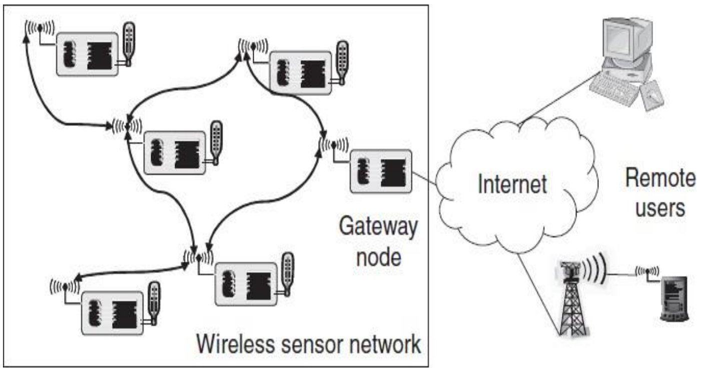


Figure 1.16 A wireless sensor network with gateway node, enabling access to remote clients via the Internet

1.11.2 WSNtoInternetcommunication: AssumethattheinitiatorofaWSN–Internet communicationresidesintheWSN.

- Forexample,asensornodewantstodeliveranalarmmessagetosomeInternethost.
- Thefirstproblemtosolveishowtofindthegatewayfromwithinthenetwork
- Basically,aroutingproblemtoanodethatoffersaspecificservicehastobesolved, integratingroutingandservicediscovery
- Ifseveralsuchgatewaysareavailable,howtochoosebetweenthem?
- Inparticular,ifnotallInternethostsarereachableviaeachgatewayoratleastifsome gatewayshouldbepreferredforagivendestinationhost?
- Howtohandleseveralgateways,eachcapableofIPnetworking,andthecommunication amongthem?
- OneoptionistobuildanIPoverlaynetworkontopofthesensornetwork
- Howtomapasemanticnotion(“AlertAlice”)toaconcreteIPaddress?
- EvenifthesensornodedoesnotneedtobeabletoprocesstheIPprotocol,ithasto includesufficientinformation(IPaddressandportnumber,forexample)initsown packets;
- thegatewaythenhastoextractthisinformationandtranslateitintoIPpackets.
- Anensuingquestioniswhichsourceaddresstousehere–thegatewayinasensehasto performtaskssimilartothatofaNetworkAddressTranslation(NAT)device.

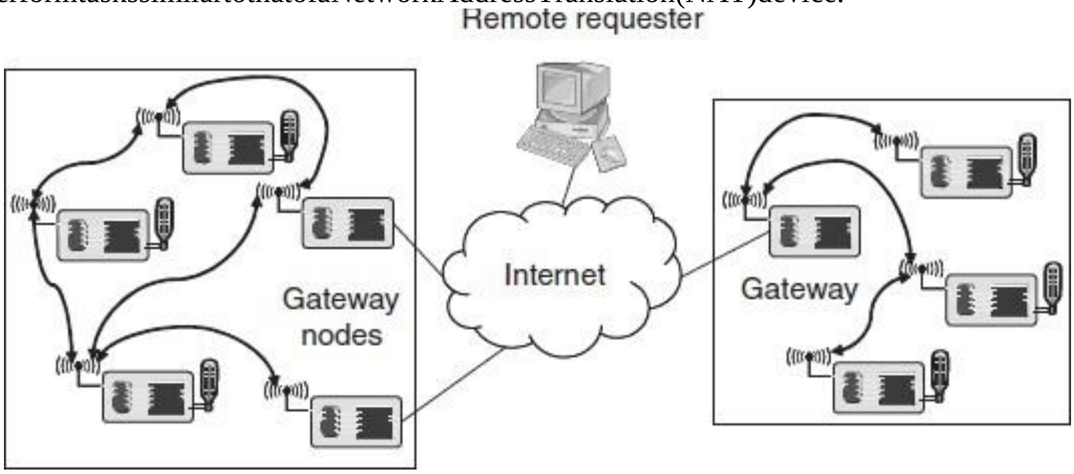
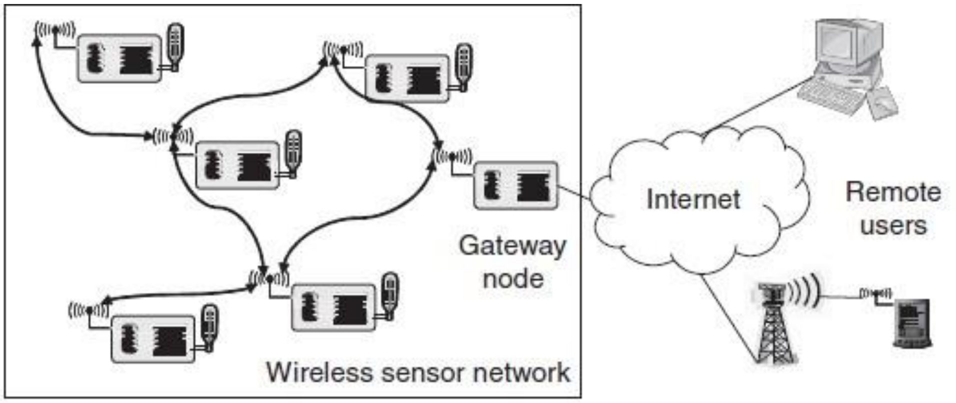


Figure 1.17: A wireless Sensor Network with gateway node, enabling access to remote clients via the WSN

1.11.3 InternettoWSNcommunication: The case of an Internet-based entity trying to access servicesofaWSNisevenmorechallenging.

- Thisisfairlysimpleifthisrequestingterminalisabletodirectlycommunicatewiththe WSN.
- Themoregeneralcaseis,however,aterminal“faraway”requestingtheservice,not immediatelyabletocommunicatewithanysensornodeandthusrequiringthe assistanceofagatewaynode

- ✓ Firstofall,againthequestionishowtofindoutthatthereactuallyisasensornetwork inthedesiredlocation,andhowtofindoutabouttheexistenceofagatewaynode?
- ✓ Oncetherequestingterminalhasobtainedthisinformation,howtoaccesstheactual services.
- ✓ Therequestingterminalcaninsteadsendaproperlyformattedrequesttothisgateway, whichactsasanapplication-levelgateway
- ✓ Thegatewaytranslatesthisrequestintotheproperintrasensornetworkprotocol interactions
- ✓ Thegatewaycanthenmask,forexample,adata-centricdataexchangewithinthe networkbehindanidentity-centricexchangeusedintheInternet
- ✓ Itisbynomeansclearthatsuchanapplication-levelprotocolexiststhatrepresentsan actualsimplificationoverjustextendingtheactualsensornetworkprotocolstothe remoteterminal
- ✓ Inaddition,therearesomeclearparallelsforsuchanapplication-levelprotocolwithso-calledWebServiceProtocols,whichcanexplicitlydescribeservicesandthewaythey can beaccessed



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 WSNtunnelling:

- ✓ ThegatewayscanalsoactassimpleextensionsofoneWSNtoanotherWSNTheideais tobuildalarger,“virtual”WSNoutofseparateparts,transparently“tunneling”all protocolmessagesbetweenthesetwonetworksandsimplyusingtheInternetasa transportnetwork.
- ✓ Thiscanbeattractive,butcarehastobetakennottoconfusethevirtuallinkbetween twogatewaynodeswitharealllink;
- ✓ Otherwise,protocolsthatrelyonphysicalpropertiesofacommunicationlinkcanget quiteconfused(e.g.timesynchronizationorlocalizationprotocols).

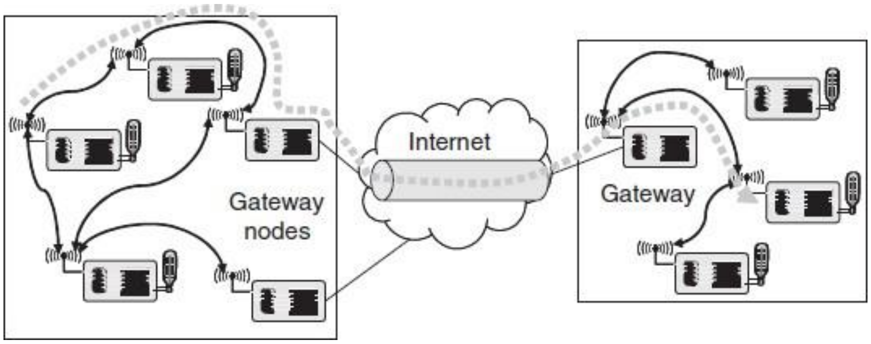


Figure 1.19 Connecting two WSNs with a tunnel over the Internet

UNIT –III

PHYSICAL LAYER AND TRANSCEIVER DESIGN CONSIDERATIONS INWSNs:

Wireless sensor networks have characteristics that are different from traditional wireless networks. For example, nodes have more simple power constraints, although they may transmit at shorter distances and lower data rates. In this Chapter, we consider the specific physical layer requirements of wireless sensor networks, taking into consideration the particular characteristics and usage setups of wireless sensor networks. We find that spread spectrum technologies meet the requirements much better than narrowband technologies. Furthermore, Ultra- Wideband technologies are found to be a promising emergingalternative.

Wireless sensor networks share many of the problems and challenges of traditional wireless networks, such as the nature of the challenges presented by multipath wireless channels, as well as bandwidth and power constraints. There are additional challenges and constraints that are in WSN as size and cost, from which other constraints like power, processing power and memory constraints are derived.

In general, there may be both sensing and non-sensing nodes in a wireless sensor network,

i.e. all sensors are nodes but not all nodes are sensors. The non-sensing nodes assist in communications but don't themselves sense data. The non-sensing nodes may have less power constraints than do the sensing nodes.

2.1.1 Physical Layer Requirements/Considerations:

The physical layer in wireless networked sensors has to be designed with sensor networking requirements in mind. In particular

□ TheCommunicationdevicemustbecontainableinasmallsize,sincethesensornodes asmall.Socheaper,slightlylargerantennasmaybeacceptableinthosecases.

□ TheCommunicationdevicesmustbecheap,sincethesensorswillbeusedinlargenumbersin redundantfashion.

□ Theradiotechnologymustworkwithhigherlayersintheprotocolstacktoconsumevery low powerlevels.

For all the above reasons, the physical layer cannot be too complex. Therefore, *the nature and complexity of the physical layer* processing is an important consideration in selecting a physical layer technology for wireless networked sensors.

Another consideration is *interference from other devices* that are not part of the wireless sensor network. Since nodes are densely deployed in wireless sensor networks, they may interfere more with one another than in traditional wireless networks. Although the lower transmission powers of the devices help reduce the interference they cause to one another, interference is still a problem. Sophisticated noise canceling algorithms such as antenna arrays to be used.

Furthermore, *link layer and physical layer synchronization* is an important issue. For sensor networks, the link and physical layers must be designed to allow relative synchronization between communicating nodes.

Yet another consideration in evaluating physical layers for wireless sensor networks is in the *capability to re-use radio technology*. This applies to sensors where the sensing itself relies on radio waves. Unless excessive interference between sensing and communications signals can be avoided, the benefits of radio reuse may not be realizable.

Next one *is Antenna considerations*, the desired small form factor of the overall sensor nodes restricts the size and the number of antennas. If the antenna is much smaller than the carrier's wavelength, it is hard to achieve good antenna efficiency, that is, with ill-sized antennas one must spend more transmit energy to obtain the same radiated energy. With small sensor node cases, it will be hard to place two antennas with suitable distance to achieve receive diversity. The antennas should be spaced apart at least 40–50% of the wavelength used to achieve good effects fromdiversity.

Finally, the ability to do *physical layer multicasting* is useful. By physical layer multicasting, we mean that a signal can be sent to multiple receivers at the same time, but not necessarily broadcast. The desired receivers are able to receive the desired signal, and the other receivers to filter it out, at the physical layer. Of course, the filtering can be done higher in the protocol stack as well, but that consumes more resources than physical layer multicasting.

2.1.2 Physical layer Evaluation ofTechnologies:

We consider 3 main classes of physical layer technologies for use in wireless sensor networks, based on bandwidth considerations:

a) Narrowbandtechnologies

b) Spread spectrumtechnologies

c) Ultra-Wideband (UWB)technologies.

(a) Narrow band Technologies: Narrow-band technologies employ a radio bandwidth, *W*, that is narrow in the sense that it is on the order of the symbol rate. In fact, if *M-ary* symbols are used (using higher-level modulation schemes), then each symbol conveysbits of information.

Therefore the bandwidth efficiency is — where R is the data rate in bits per unit time. _ is often

described in bits per second per hertz. Note that the Shannon capacity, in bits per second per hertz, can beexpressedas ---(1)

Where

In Majority of traditional systems bandwidth is limited due to regulatory and/or licensing constraintsinnarrowfrequencies.Animportantobjectiveinthedesignofsuchsystemsisto

maximize achievable data rate. Therefore, it becomes desirable to increase , which mayincrease the .Sincerealmodulationschemesdonotachievecapacity,sothemodulationschemeslike

4QAM, 16QAM and 64-QAM are used.

(b) Spread spectrum technologies: The advantages of spread spectrum systems over narrow band systemsincludes

□ Lowprobabilityofdetection

□ Lowprobabilityofinterrupt

□ Ability to communicate with low power

□ Noise-like signals and noise-like interference to other receivers

□ Robustness to narrow-band interference

□ Multiple-access to the same frequency band by several transmitters

□ Robustness to multipath channel impairments

Properly designed spread spectrum systems can achieve higher effective SNR than equal-rate narrowband systems, for the same transmit power. This gain, at the expense of bandwidth, is often quantified as processing gain, which is the ratio of transmission bandwidth to data bandwidth.

Advantages 3 through 5 are especially useful for sensor networks. In addition, spread spectrum is good for physical layer multicasting. There are a variety of spread spectrum technologies, the most widespread of which is Direct-Sequence Spread Spectrum (DS-SS). In DS-SS, a narrowband signal is "spread" into a wideband signal, by modulating it with a high rate chip sequence. The chip sequence is pseudorandom, giving the resultant signal its characteristic properties. Another common variety of spread spectrum is Frequency Hopping Spread Spectrum (FH-SS). In FH-SS, the spreading is achieved by "hopping" the signal over a wide range of frequencies, where the sequence of hopped to frequencies ispseudo-random.

(c) Ultra-Wideband (UWB) technologies: Ultra-Wideband (UWB) technology can hethought of as an extreme case of spread spectrum technology with many proposed applications in communications. Its characteristics include:

(i) Large bandwidths. The transmission bandwidths employed by UWB systems is usually much larger than the transmission bandwidths of typical spread spectrum systems, being on the order of gigahertz rather thanmegahertz.

(ii) Large fractional bandwidths. UWB systems tend to have relatively larger fractional bandwidths than traditional communicationssystems.

The technologies are now compared according to various criteria, and rated. The ratings are collected together in TABLE- 2.1. The ratings are on a scale of 1 to 5, with 1 being the worst rating (very poor) and 5 being the best (very good).

S. No	Criterion	Narrow Band	Spread Spectrum	UWB
1	Device Size	4	4	4
2	Cost	3	3	4
3	Power Consumption	2	4	5
4	Low range, Low data rate	3	4	5
5	Robustness to interference	1	4	5
6	Robustness to Noise	2	4	5
7	Ease of Synchronization	3	5	2
8	Radio Reusability	2	2	4
9	Physical Layer multicast	1	4	5
10	Regularity Issues	2	4	3

Table 2.1: Rating of technologies bye criteria

2.2 PERSONAL AREANETWORKs(PANs):

1. Thomas Zimmerman was the first research scientist to introduce the idea of Personal Area Network(PAN).
2. The communication network established for the purpose of connecting computer devices of personal use is known as PAN (Personal AreaNetwork).
3. When a network is established by connecting phone lines to PDAs (Personal Digital Assistants), this communication is known as PAN (Personal AreaNetwork).
4. PANs can be wired (USB or FireWire) or wireless (infrared, ZigBee, Bluetooth,UWB).
5. Wireless Personal Area Network (WPAN) can perform really efficient operations if we connect them with specializeddevices.
6. The range of a PAN typically is a fewmeters.
7. Examples of wireless PAN, or WPAN, devices include cell phone headsets, wireless keyboards, wireless mice, printers, bar code scanners and gameconsoles.

2.2.1 Examples forPANs:

Examples-1:

1. Blue tooth wirelessPAN:

- ✓ These are referred as Pico nets. Pico nets are Ad hocnetworks.
- ✓ Pico nets work over a range of 200metres and transmit data of about 2100 Kbit/sec.
- ✓ The Bluetooth technology is based on IEEE 802.15standard.
- ✓ The wearable and portable computer devices communicate with eachother.
- ✓ In this process of hand shake, an electric field is generated around people, and they emit Picoamps.
- ✓ These emissions complete the circuit and hence an exchange of information takesplace.

Examples-2:

2. ZigBee:

- ✓ Itisashort-range,low-powercomputernetworkingprotocolthatcomplieswiththeIEEE 802.15.4 standard.
- ✓ In the U.S., ZigBee devices operate in the 902-928 MHz and 2.4 GHz unlicensedbands.
- ✓ ZigBee employs DS-SS modulation with a gross data rate of 40 kb/s in the 900 MHz band and 250 kb/s in the 2.4 GHzband.
- ✓ There are three types of ZigBeedevices:
    - □ *ZigBeeCoordinator(ZC):F*ormingtherootofthenetworktreeandbridgingtoothernetworks,
    - □ *ZigBee Router (ZR):* It can run an application function as well as act as anintermediaterouterbypassingdatafromotherdevices.
    - □ *ZigBee End Device (ZED):* It contains just enough functionality to talk to its parent node. It can sleep most of the time, extending its battery life.

Examples-3:

3. Ultra-WideBand(UWB):

- ✓ It is a radio technology useful for short-range, high-bandwidth communications that does not create harmful interference to users sharing the sameband.
- ✓ A pulse-based UWB method is the basis of the IEEE 802.15.4a draftstandard

Examples-4:

4. Wi-Fi orWiMAX

- ✓ Wi-Fi or WiFi is a technology for wireless local area networking with devices based on the IEEE 802.11standards.

2.3 HIDDEN NODE AND EXPOSED NODEPROBLEM:

In WSN, to exchange data two exchange control frames are used before transmitting data

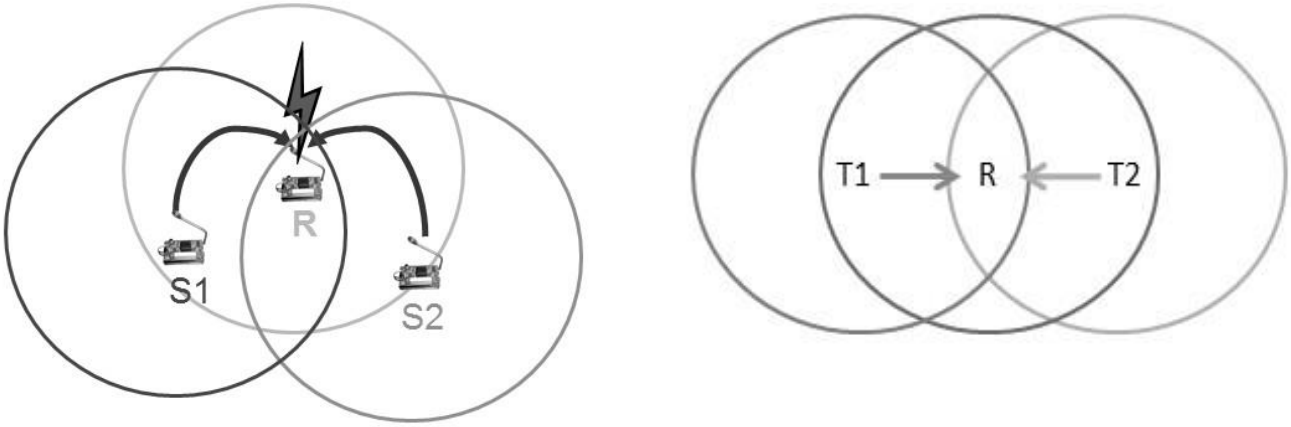
1. Request toSend(RTS)
2. Clear toSend(CTS)

RTS/CTS is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem. The RTS/CTS frames can cause a new problem called the exposed terminal problem. These control frames duty includes

1. If sender sees CTS, transmitsdata.
2. If other node sees CTS, will idle for specifiedperiod.
3. If other node sees RTS but not CTS, free tosend

2.3.1 Hidden terminalproblem:

Other senders' information are hidden from the current sender, so that transmissions at the same receiver cause collisions. That is for example if two persons are trying to communicate third person at the same time, then third person will be in dilemma to which person he has to communicate. At that time for proper communication one of the sender' will hide another sender by dominating. In the similar fashion other senders' information are hidden from the current sender. This problem is called "**Hidden terminal/Node problem**"



(a) **(b)**

Figure 2.1 (a) & (b) Hidden node problem

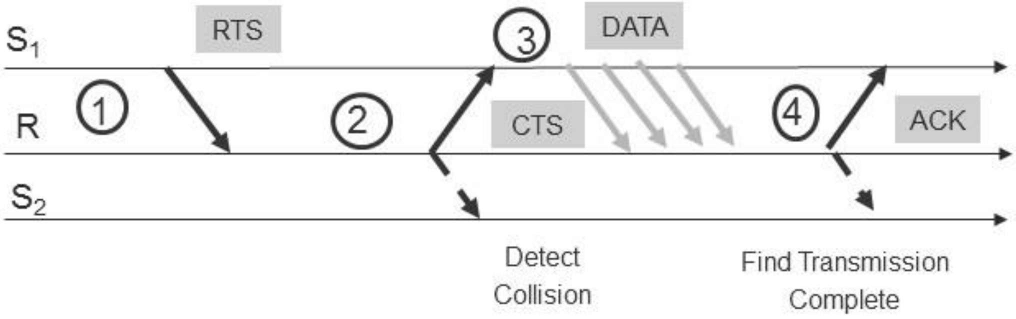


Figure 2.2 Data transmission in Hidden node problem

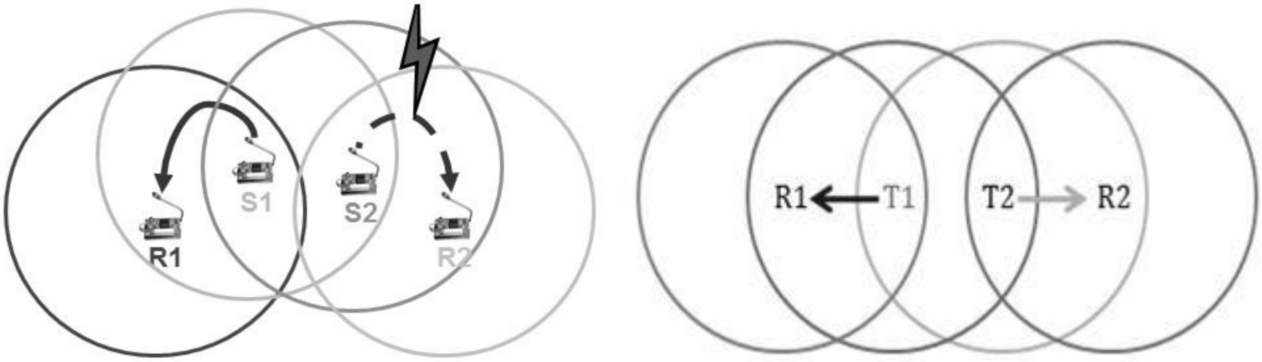
From figure 2.1(b) we can observe that transmitters T1 and T2 can't see each other, both send to receiver R. Then RTS/CTS can help

- Both T1 and T2 would send RTS that R would seefirst.
- R only responds with one CTS (say, echoing T1'sRTS).
- T2 detects that CTS doesn't match and won'tsend.

2.3.2 Exposed terminalproblem:

- ✓ The sender mistakenly thinks that the medium is in use, so that it unnecessarily defers the transmission. That is for example if in a communication network there aretwo transmitters and two receivers, then one sender/transmitter exchanges RTS-CTS with one receiver, then second sender mistakenly thinks that the medium is in use, so it needlessly submits the transmission. From figure 2.3(b) we can observe that T1 sending to R1, T2 wants to send to R2. As T2 receives packets, carrier sense would prevent it from sending to R2, even though wouldn’t interfere. Then RTS/CTS canhelp
    - ▪ T2 hears RTS from T1, but not CTS fromR1

- T2 knows its transmission will not interfere at T1'sreceiver
- T2 is safe to transmit toR2.



(a) **(b)**

Figure 2.3 (a) & (b) Exposed Node/terminal problem

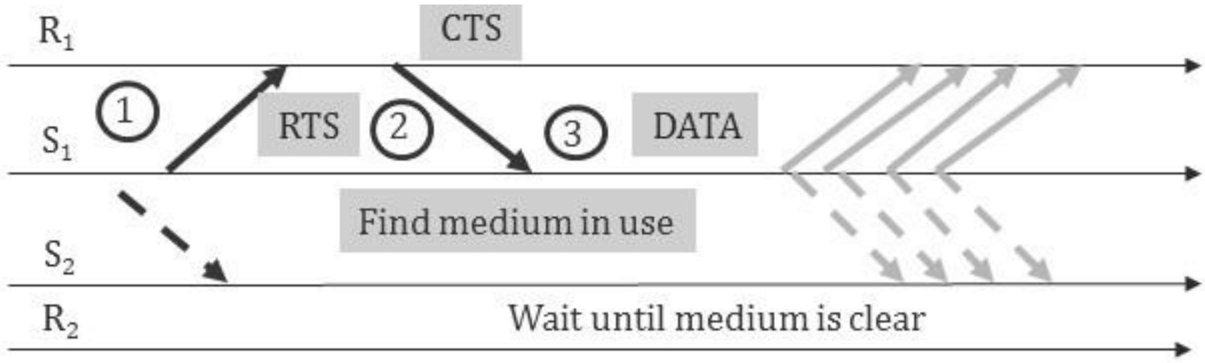


Figure 2.4 Data transmission in Exposed node problem

2.4 Wireless Ad-hoc Networks (WANETs):

Wireless ad hoc network (WANET) is a decentralized technology designed for the establishment of a network anywhere and anytime without any fixed infrastructure to support the mobility of the users in the network. The network is ad-hoc because each node is willing to forward data for other nodes. Wireless ad-hoc networks can be further classified by their application:

1. **Mobile ad hoc networks (MANETs):** MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected withoutwires.
2. **Vehicular ad hoc networks (VANETs):** VANETs are used for communication between vehicles and roadsideequipment.
3. **Intelligent vehicular ad hoc networks**: In VANETs are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents. Vehicles are using radio waves to communicate with eachother.

4. **Smart-Phone Ad-hoc networks (SPANs):** SPANs influence the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smartphones to create peer-to- peer networks without depends on cellular carrier networks, wireless access points, or traditional networkinfrastructure.
5. **Internet-based Mobile Ad-hoc networks (iMANETs):** iMANETs are ad hoc networks that link mobile nodes and fixed Internet-gatewaynodes.

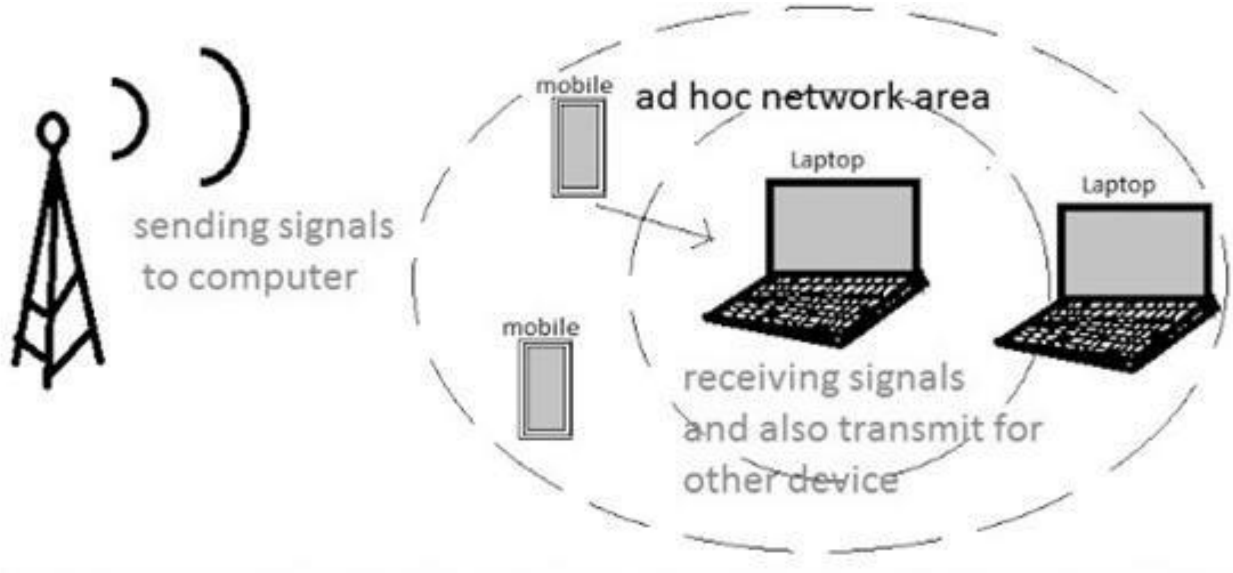


Figure 2.5 Example of Wireless Ad-hoc Network (WANET)

2.5 Mobile Ad-HOC Networks(MANETs):

A Mobile Ad-hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. A mobile ad-hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other.

Example of MANETs: Node 1 and node 3 are not within range of each other, however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc Network.

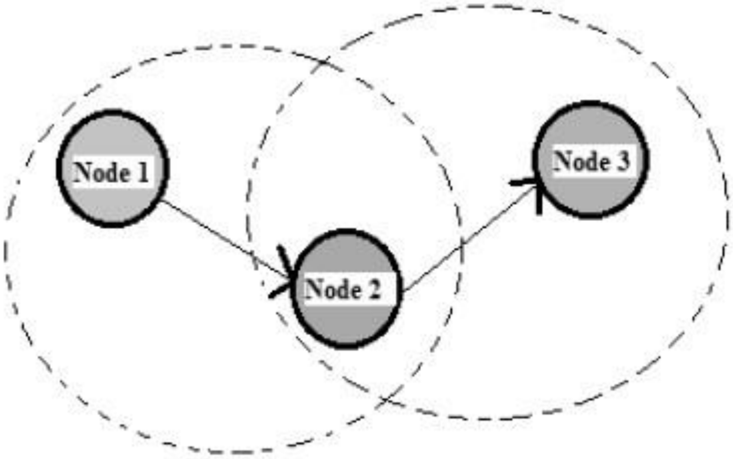


Figure 2.6: Example of MANETs

2.5.1 MANETsCharacteristics:

1. *Distributed operation*: There is no central control of the network operations, the control of the network is distributed among thenodes.
2. *Multi hop routing*: When a node tries to send information to other nodes which is out of its range, the packet should be forwarded via one or more intermediatenodes.

3. *Autonomous terminal*: In MANET, each mobile node is an independent node (could function ashost/router).
4. *Dynamic topology*: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictabletime.
5. *Light-weight terminals*: The nodes at MANET are mobile with less CPU capability, low power storage and small memorysize.
6. *Shared Physical Medium*: The wireless communication medium is accessible to any entity with the appropriate equipment and adequateresources.

2.5.2 MANETsChallenges:

1. *Limited bandwidth:* Wireless link continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio’s maximum transmissionrate.
2. *Dynamic topology:* Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected ascompromised.
3. *Routing Overhead:* In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routingoverhead.
4. *Hidden terminal problem:* The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
5. *Packet losses due to transmission errors:* Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility ofnodes.
6. *Mobility-induced route changes:* The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent routechanges.
7. *Battery constraints:* Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of thedevice.
8. *Security threats:* The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous securityattacks.

2.5.3 MANETVULNERABILIES:

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:

1. *Lack of centralized management:* MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hocnetwork.
2. *No predefined Boundary:* In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are

allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

1. *Cooperativeness:* Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt networkoperation.
2. *Limited power supply:* The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited powersupply.
3. *Adversary inside the Network:* The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the externalattack.

2.5.2 ROUTING PROTOCOLS:

Ad-Hoc network routing protocols are commonly divided into three main classes as Proactive, Reactive and Hybrid protocols.

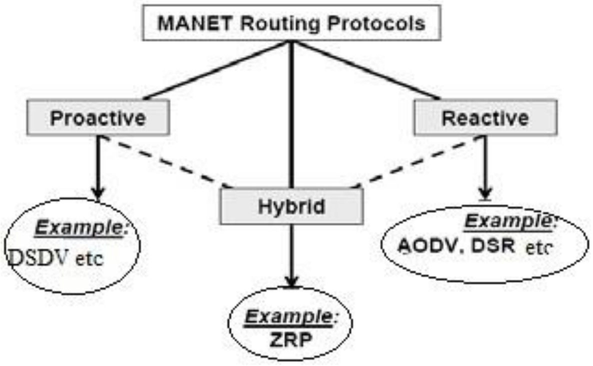


Figure 2.7 Routing protocols in MANETs

1) Proactive Protocols: Proactive, or table-driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Examples of such schemes are the conventional routing schemes: Destination sequenced distance vector (DSDV). They attempt to maintain consistent, up- to-date routing information of the whole network. It minimizes the delay in communication and allows nodes to quickly determine which nodes are present or reachable in thenetwork.

2) Reactive Protocols: Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing(DSR).

3) Hybrid Protocols: They introduces a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extramemory.

2.5.3 Security Attacks inMANETs:

he attacks can be categorized into two types based on behavior as Passive or Active attack.

1. *Passive attacks:* It does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic or accumulates/collects data fromit.
2. *Active attacks:* Active attacks are very severe attacks on the network that prevent message flow between thenodes.

They can be internal or external. Active attacks are classified into three groups:

a) *Dropping Attacks:* Compromised nodes or selfish nodes can drop all packets that are not destined forthem.

b) *Modification Attacks:*. These attacks modify packets and disturb the overall communication between networknodes.

c) *Fabrication Attacks:* In this attacker send fake message to the neighbouring nodes without receiving any relatedmessage.

2.5.4 MANETsApplications:

Some of the typical applications include:

1. *Military battlefield:* Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarter.
2. *Collaborative work:* For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a givenproject.
3. *Local level:* Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchangeinformation.
4. *Personal Area Network and Bluetooth*: A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobilephone.
5. *Commercial Sector*: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network isneeded.

2.6 Vehicular ad hoc networks(VANETs):

VANETs are used for communication between vehicles and roadside equipment. A Vehicular Ad- Hoc Network or VANET is a sub form of Mobile Ad-Hoc Network or MANET that provides communication between vehicles and between vehicles and road-side base stations with an aim of providing efficient and safe transportation. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET introduces more challenges aspects as compare to MANET because of high mobility of nodes and fast topology changes in VANET. Various routing protocols have been designed and presented by researchers after considering the major challenges involved in VANETs. VANET can achieve affective communication between moving node by using different ad-hoc networking tools such as Wi-fi IEEE 802.11 b/g, WiMAX IEEE 802.10, Bluetooth,IRA.

2.6.1 Characteristics ofVANETs

There are various appealing and attractive features that make a difference from other types of networks.

1) *High Mobility:* The nodes present in VANETs move at a very high speed. These moving nodes can be protected saved from attacks and other security threats only if their location is predicable. High mobility leads to various other issues inVANET
2) *Rapidly Changing Network Topology:* Vehicles moving at high speed in VANET lead to quick changes in networktopology.
3) *No Power constraints:* Power constraint always exists in various networks but in VANETs vehicles are able to provide power to on board unit (OBU) via the long life battery. So energy constraint is not always an essential challenge as inMANETs.
4) *Unbounded Network Size:* The network size in VANET is geographically unbounded because it can be generated for one city or onecountry.
5) *Time Critical:* Timely delivery of information is very essential. Actions can be performed accordingly only when information is available when it isrequired.
6) *Frequent changing information:* Ad-Hoc nature of VANET motivates the nodes to gather information from other vehicles and roadside units. As vehicles move and change their path, information related to traffic and environment also changes veryrapidly.
7) *Wireless Communication:* Nodes are connected and exchange their information through wireless.
8) *Variable network density:* The network density is changed according to traffic density; it is very high in traffic jam and low in suburbantraffic.
9) *High computability ability:* Due to computational resources and sensors, the computational capacity of the node isincreased.

2.6.2 Components ofVANETs:

VANET is an autonomous self-organizing wireless network. VANETs contains following entities:

1) *Vehicles:* Vehicles are the nodes of vehicular network. VANET address the wireless communication between vehicles (V2V) and between vehicles and infrastructure access point (V2I).
2) *Infrastructure:* Infrastructure related to outside environment include road side base station. Base stations are the roadside unit and they are located at dedicated location like junctions or near parking spaces. Their main functions are to increase the communication area of the ad hoc network by re-allocating the information to others and to run safety application like low bridge warning, accident warningetc.
3) *Communication channels:* Radio waves are a type of electromagnetic radiation with wavelengths

in the electromagnetic spectrum longer than infrared light. Radio waves have frequencies from 190 GHz to 3Khz. Radio propagation model plays a strong role in the performance of a protocol to determine the number of nodes within one collisiondomain.

2.6.3 Communication inVANET:

Various types of communication technique are used in VANET. Some of them are given below:

1) *Vehicle to Vehicle Communication:* It refers to inter vehicle communication. Vehicles or a group of vehicles connect with one another and communicate like point to point architecture. It proves to be very helpful for cooperativedriving.
2) *Vehicle to Infrastructure Communication*: Number of base stations positioned in close proximitywithafixedinfrastructuretothehighwaysisnecessarytoprovidethefacilityof

uploading/downloading of data from/to the vehicles. Each infrastructure access point covers a cluster.

3) *Cluster to Cluster Communication*: In VANETs network is split into clusters that are self-managed group of vehicles. Base Station Manager Agent (BSMA) enables communications between the clusters. BSMA of one cluster communicates with that of othercluster.

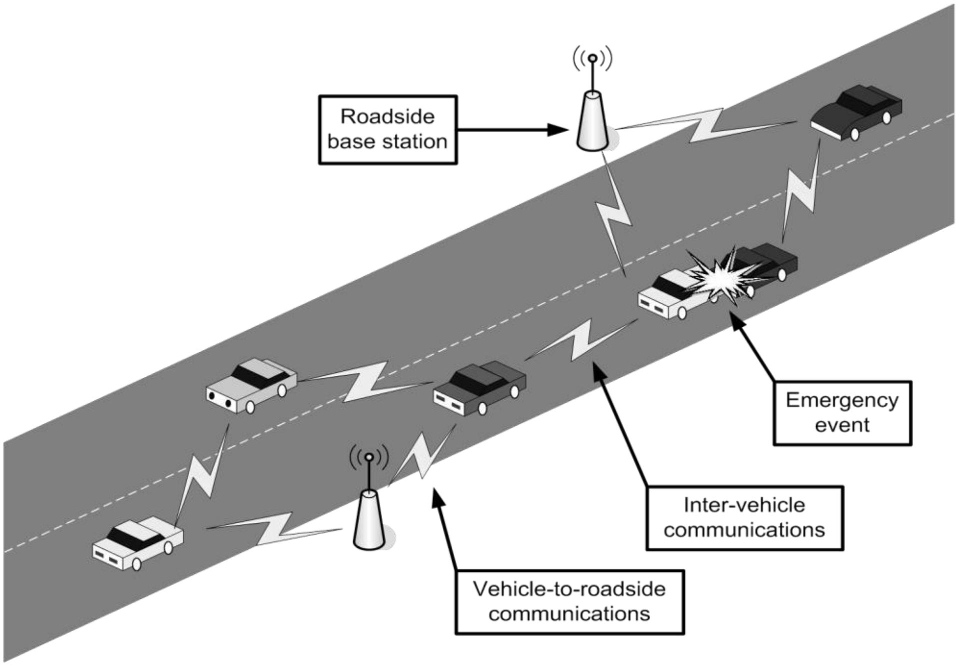


Figure 2.8 Example of VANET

2.6.4 Security Requirements forVANETs:

1) *Authentication:* In VANET greedy drivers or the other adversaries can be condensed to a greater extent by authentication mechanism that ensures that the messages are sent by the actual nodes. Authentication, however, increases privacy concerns, as a basic authentication scheme of connecting the identity of the sender with the message. It, therefore, is absolutely essential to validate that a sender has a certain property which gives certification as per the application. For example, in location based services this property could be that a vehicle is in a particular location from where it claims tobe.
2) *Message Integrity:* Integrity of message ensures that the message is not changes in transit that the messages the driver receives are notfalse.
3) *Message Non-Repudiation:* In this security based system a sender can be identified easily. But only specific authority is approved for sender identification. Vehicle could be identified from the authenticated messages itsends.
4) *Access control:* Vehicles must function according to rules and they should only perform those

tasks that they are authorized to do. Access control is ensured if nodes act according to specified authorization and generate messagesaccordingly.

5) *Message confidentiality:* Confidentiality is required to maintain privacy in a system. Law enforcement authority can only enforce this privacy between communicatingnodes.

6) *Privacy:* This system is used to ensure that the information is not leaked to the unauthorized people. Third parties should not be able to track vehicle movements as it is a violation of personal privacy. Location privacy is also important so that no one should be able to learn the past or future locations ofvehicles.

7) *Real time guarantees:* It is essential in VANET, as many safety related applications depend on strict time guarantees. This feature is necessarily required in time sensitive road safety applications to avoidcollisions

2.6.5 Challenges inVANET:

There are many issues in VANET. Some of them are given below:

1) *Technical Issue:* Due to high portability, the network topology and channel condition changes rapidly. It is difficult to manage network and control congestion collision in network. In VANET the electromagnetic waves of communication are used and these are affected by environment. Environmental impact need to be considered in VANET. Other technical issues are related to design and architecture of Maclayer.
2) *Security Issue:* VANET is time critical where safety related message should be delivered with 100ms transmission delay. Even authenticate node can perform malicious activities than can disturb the network. The major challenge is to distribute privacy keys among vehicles.
3) *Security Requirement issue:* Authentication ensures that the message is created by the authorized user. Non repudiation means a node can’t deny that she/he doesn’t transmit message. It may be crucial to determine correct sequence. A regular verification of data is required to eliminate the falsemessaging.
4) *Attackers onVANET:*
    a. Insider and outsider: Insiders are the authenticated members of network whereas Outsiders are the intruders and hence limited capacity toattack.
    b. Malicious and Rational: Malicious attackers have not any personal benefit after attack; they just harm the functionality of the network. Rational attacks can be predicable as they have the personal profit.
    c. Active and Passive: Active attackers generate signals or packet whereas passive attackers only sense thenetwork.
5) *Attacks in VANET:* Hijackers hijacks the session easily after connection establishment. Generally, a driver is itself owner of the vehicles so getting owner’s identity can put the privacy at risk. Eavesdropping is a most common attack on confidentiality. Routing attacks are the attacks which destroy the vulnerability of network layer routingprotocols.

2.6.6 VANET: Smartvehicle

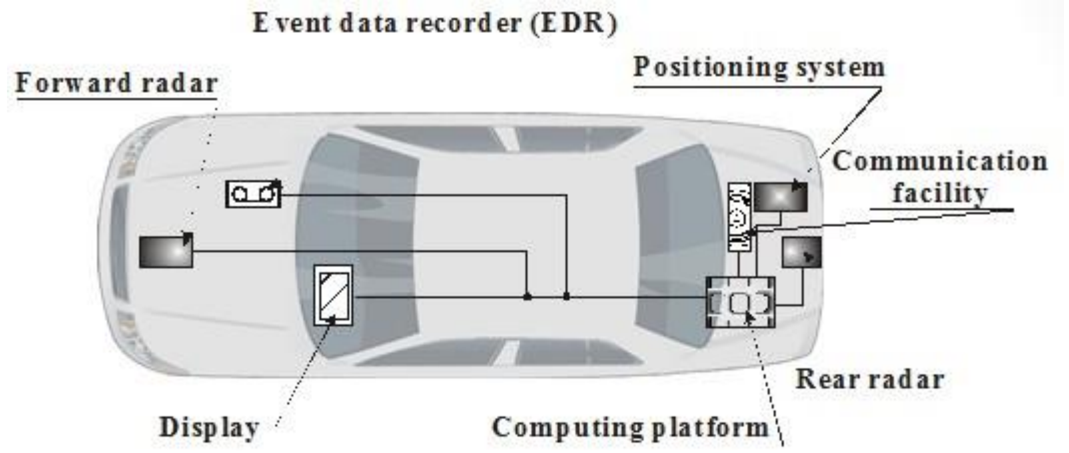


Figure 2.9 Smart vehicle used in VANETs

- ✓ **EDR:** Used in vehicles to register all important parameters, such as velocity, acceleration, etc. especially during abnormal situations(accidents).
- ✓ **Forward radar:** Used to detect any forward obstacles as far as 200meters
- ✓ **Positioning System:** Used to locatevehicles
- ✓ **Computing platform:** Inputs from various components are used to generate useful information

2.6.7 Intelligent vehicular ad hoc networks: InVANETs are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents. Vehicles are using radio waves to communicate with eachother.

UNIT-IV

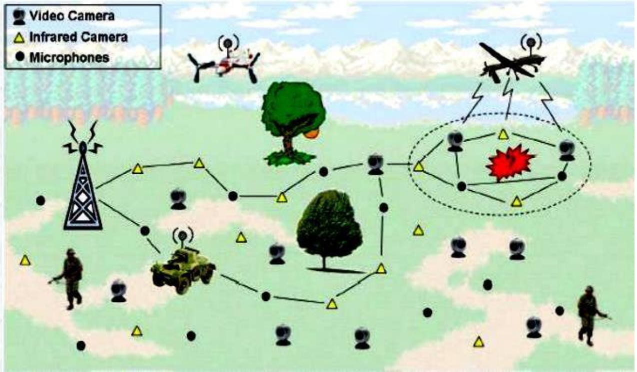
1. Infrastructure Establishment forWSN

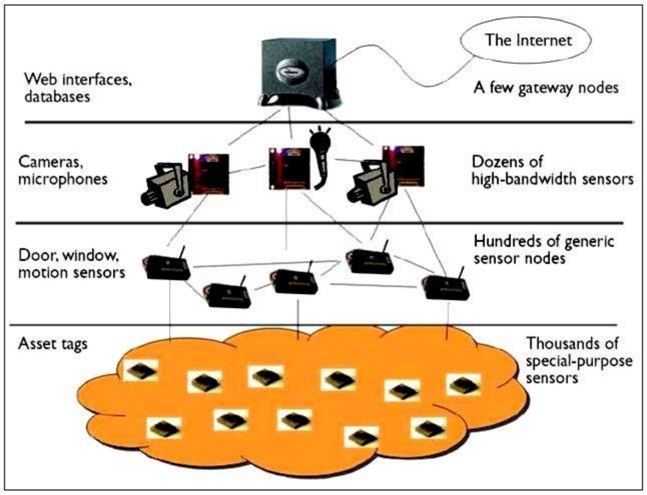
- ***Localization and Positioning,tracking:***

  Properties of positioning, Possible approaches, Task driven Sensing, Rolls of Sensor nodesand utilities, Information based sensor tracking, joint routing and information aggregation, SensorNetworkDatabases-BIGDATA,Sensornetworkplatformsand tools,Single-hop localization, Positioning in multi-hop environments, Impact of anchorplacement,

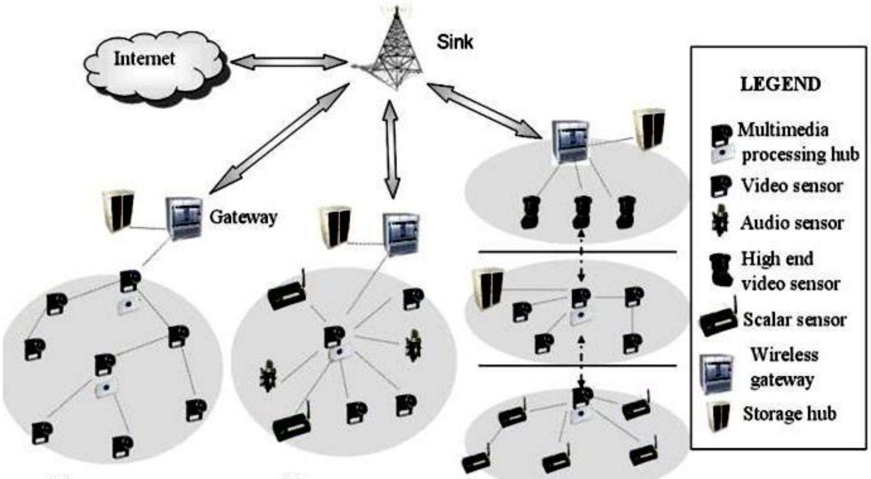
- ***Operating Systems forWSN:***

  OS Design Issues, Examples of OS(Architecture, Design Issues, Functions): Tiny OS, Mate, Magnet OS, MANTIS, Nano-RK OS Architecture Block Diagram, LiteOS Architectural BlockDiagram, LiteFSArchitectural Block Diagram, Content delivery networks.Introduction to Internet of Things(IoT).




The Internet
Web interfaces, databases
A few gateway nodes
Cameras, microphones
Dozens of high-bandwidth sensors
Door, window, motion sensors
Hundreds of generic sensor nodes
Asset tags
Thousands of special-purpose sensors

Architecture:



(a) Single-tier flat, homogeneous sensors, distributed processing, centralized storage

(b) Single-tier clustered, heterogeneous sensors, centralized processing, centralized storage

(c) Multi-tier, heterogeneous sensors, distributed processing, distributed storage

Definition:

Thetaskofinitiatingcollaborativeenvironmentforsensornetworkwhenthatnetworkisactivatedis called infrastructureestablishment.

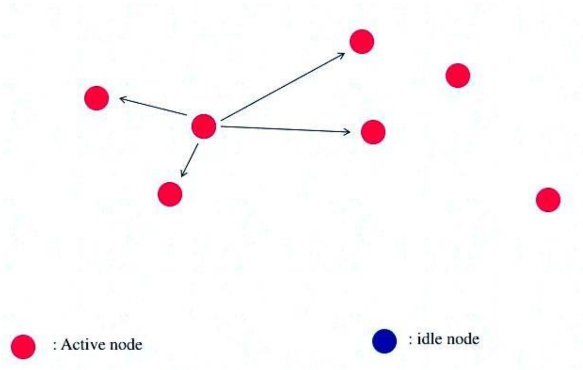
When sensor network is activated various task must be performed to establish necessary infrastructure that will allow useful collaborative work to be performed:

1) Discovering othernodes
2) Radio power adjustment to ensure adequateconnectivity.
3) Clusterformation.
4) Node placement in a common temporal and specialframework.

Some common techniques used to establish the network are:

1) Topologycontrol
2) Clustering
3) Timesynchronization
4) Localization

2. TopologyControl



- A sensor node that wakes up execute a protocol to discover which other nodes it can communicate with.(bidirectional).
- Atinitialstateeachnodetrytoconnectwithneighborsaccordingtotheradiolink capacity of its own.
- The neighbor is determined by the radio power of the node as well as local topology and other conditions that may degrade performance of the radio link.
- Sensornodearecapableofbroadcastinglessthattheirmaximumpossibleradiopower.(energy saving and network life time)
- Example : Homogeneous topology : all nodes with same transmission range.

Critical Transmission Range Problem

Computing minimum common transmitting range "r” such that the network is connected.

Solution :

1) Depends on physical placement of thenode.
2) If node location is known CTR problem has a simplesolution.

CTR is defined as longest edge of minimum spanning tree

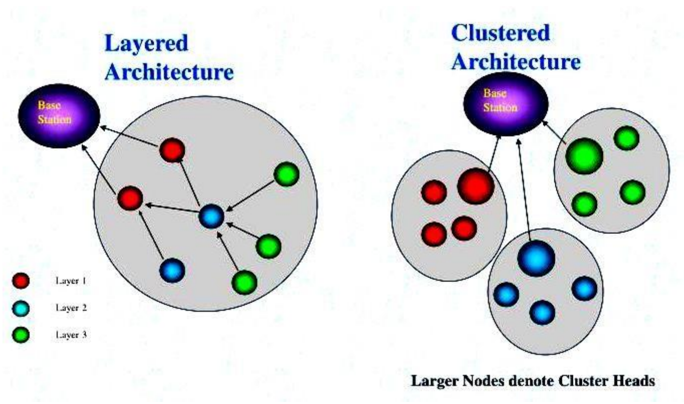
Solution to CTR problem

Example :

GRG (Geometric Random Graph):

N points are distributed into a region according to some distribution and then some aspect of the node placement is investigated with high probability

3. Clustering,



Hierarchical architecture enables more efficient use of sensor resources such as:

- Frequencyspectrum
- Bandwidth
- Power

Advantages:

1) Health monitoring of network iseasy.

2) Identifying misbehaving node iseasy.

3) Somenodescanactaswatchdogsforothernodes.

4) Maintenance of network iseasy.

Cluster formation:

1) Initially unique ids (UIDs) are assigned to eachnode

2) NodewithhigherIDthanitsuncoveredneighborsdeclaresitselfasclusterhead.

3) Clusterheadnominatednodesthencommunicatewitheachother.

4) Nodethatcancommunicatewithtwoormoreclusterheadsmaybecomegateway.

Gateway: node that aid in passing traffic from one cluster to other.

Uncovered neighbors: node that have not been already claimed by another cluster head.

4. Timesynchronization,

- ➢ Everynodeisoperatingindependentlysotheirclocksmaynotbesynchronizedwith eachother.
- ➢ Itisimportanttorunnetworkefficiently

    - To detectevents
    - Forlocalization
    - Estimatinginternodesdistances.
    - To arrange TDMAschedule

- InwirednetworkNTPisusedtoachievecoordinateduniversaltime(UTC).
- InNTPhighlyaccurateclockismountedononeofthemachineofthenetwork. This is not applicable forWSN :
    - Nomasterclocksareavailable.
    - Inconsistent commondelay.
    - Connections are variable/dynamic andunpredictable.
- Timedifferencecausedbythelackofcommontime originiscalledasclockphasedifference or clockbias.
- Methods for clock synchronization in WSN:

1) Clock phase diff estimation using three messageexchanges.
2) Intervalmethod.
3) Referencebroadcast.

5. Localization andPositioning,

- What?
    - To determine the physical coordinates of a group of sensor nodes in a wireless sensor network(WSN)
    - Duetoapplicationcontext,useofGPSisunrealistic,therefore,sensorsneedtoself-organize a coordinatesystem

- Why?
    - To report data that is geographicallymeaningful
    - Servicessuchasroutingrelyonlocationinformation;geographicroutingprotocols; context-based routingprotocols,
      location-aware services

Localization in Wireless Sensor Networks

In general, almost all the sensor network localization algorithms share three main phases

- DISTANCEESTIMATION
- POSITIONCOMPUTATION
- LOCALIZATIONALGHORITHM

- ❖ The distance estimation phase involves measurement techniques to estimate the relative distance between thenodes.
- ❖ The Position computation consists of algorithms to calculate the coordinates of the unknown node with respect to the known anchor nodes or other neighboringnodes.
- ❖ The localization algorithm, in general, determines how the information concerning distances and positions, is manipulated in order to allow most or all of the nodes of a WSN to estimate their position. Optimally the localization algorithm may involve algorithms to reduce the errors and refine the nodepositions.

Distance Estimation

There are four common methods for measuring in distance estimation technique:

- ANGLE OF ARRIVAL(AOA)
- TIME OF ARRIVAL(TOA)
- TIME DIFFERENT OF ARRIVAL(TDOA)
- THE RECEIVED SIGNAL STRENGH INDICATOR(RSSI)

- ANGLE OF ARRIVAL method allows each sensor to evaluate the relative angle between received radio signals
- TIMEOFARRIVALmethodtriestoestimatedistancesbetweentwonodesusing time basedmeasures
- TIMEDIFFERENTOFARRIVALisamethodfordeterminingthedistancebetween a mobile station and nearby synchronized basestation
- THERECEIVEDSIGNALSTRENGTHINDICATORtechniquesareusedtotranslate signal strength intodistance

Position Computation

The common methods for position computation techniques are:

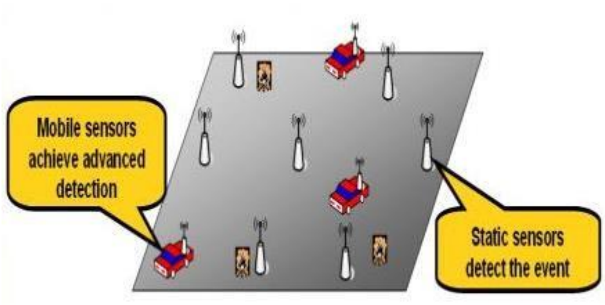
- LATERATION
- ANGULATION

□ LATERATION techniques based on the precise measurements to three non collinear anchors. Lateration with more than three anchors called multilateration.

□ ANGULATIONortriangulationisbasedoninformationaboutanglesinsteadofdistance

<u>Classifications of Localization Methods</u>

According to the ways of Sensors implementation, we classify the current wireless sensor network localization algorithms into several categories such as:


Mobile sensors achieve advanced detection
Static sensors detect the event

- Centralized vsDistributed
- Anchor-free vsAnchor-based
- Range-free vsRange-based
- Mobile vsStationary

6. Sensor Tasking andControl.

- Because of Limited battery power and Limited bandwidth careful tasking and the control idneeded.
- Information collected from thesensors.
  - — All information aggregation is needed.
  - — Selective information aggregation isneeded.
- Which sensor nodes to activate and what information to transmit is a criticalissue.
- Classical algorithms are not suitable for WSN :
  - — Sense values are notknown.
  - — Cost of sensing may vary with the data.

Designing strategy for Sensor Tasking and Ctrl:

1) What are the important object in the environment to be sensed?
2) What parameters of these object arerelevant?
3) What relations among these objects are critical to whatever high level information we need toknow?
4) Which is the best sensor to acquire a particularparameter?
5) How many sensing and the communication operations will be needed to accomplish the task?
6) How coordinated do the world models of the different sensor need tobe?
7) At what level do we communicate information in a spectrum from a signal tosymbol?

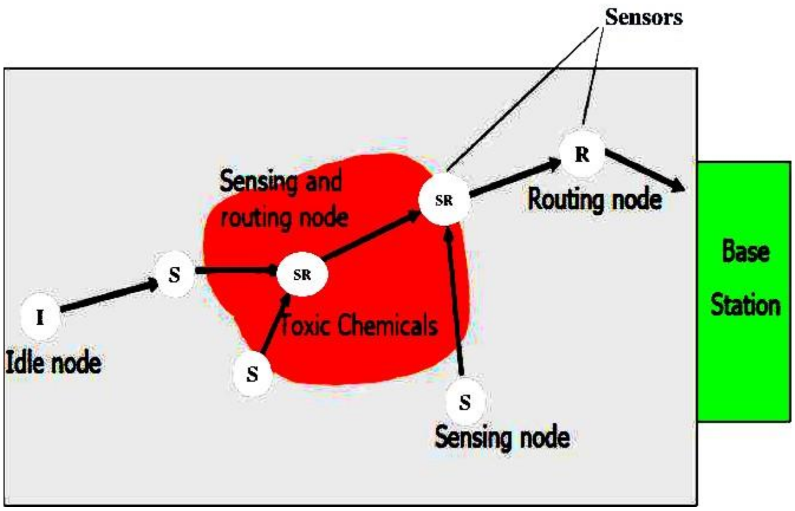
Roles of Sensor nodes and utilities

- A sensor may take on a particular role depending on the application task requirement and resource availability such as node power levels.

Example:

- Nodes, denoted by SR, may participate in both sensing androuting.
- Nodes, denoted by S, may perform sensing only and transmit their data to othernodes.
- Nodes, denoted by R, may decide to act only as routing nodes, especially if their energy reserved is limited. Nodes, denoted by I, may be in idle or sleep mode, to preserve energy.

Roles of Sensor nodes


Sensors
Sensing and routing node
SR
SR
R
Routing node
S
I
Idle node
S
Toxic Chemicals
S
Sensing node
Base Station

UNIT-V

1. Sensor Network Platforms and Tools

Commercially available sensor nodes:

1. Specialized sensing platform such as Spec node designed at University of California-Berkeley.
2. Generic Sensor platform – BerkeleyMote.
3. High bandwidth sensing platform such asiMote.
4. Gateway platform such as Stargate (Sinknode).

- Areal-worldsensornetworkapplicationmostlikelyhas toincorporateallthese elements, subject to energy, bandwidth, computation, storage, and real-time constraints
- Therearetwotypesofprogrammingforsensornetworks,thosecarriedoutbyend users and those performed by applicationdevelopers.

End users

- An end user may view a sensor network as a pool of data and *interact with the network via queries*.
- JustaswithquerylanguagesfordatabasesystemslikeSQL
- goodsensornetworkprogramminglanguageshouldbeexpressiveenoughto encode application logic at a high level ofabstraction
- Atthesame timebestructured enoughtoallowefficientexecutiononthe distributedplatform.

Application developer

- Anapplicationdevelopermustprovideendusersofasensornetwork with the capabilities of data acquisition, processing, andstorage.
- Unlikegeneraldistributedordatabase
- Systems, collaborative signalandinformation processing (CSIP) softwarecomprisesreactive,concurrent,distributedprogramsrunningon

adhoc,resource-constrained,unreliablecomputationandcommunication platforms.

2. Sensor Node Hardware – BerkeleyMotes

- ➢ Sensor node hardware can be grouped into threecategories.
    - ❖ Augmentedgeneral-purposecomputers
    - ❖ Dedicatedembeddedsensornodes
    - ❖ System-on-chip
- ➢ Berkeleymotesdue to their smallform factor, open source software development,andcommercialavailability,havegainedwidepopularityin thesensornetworkresearchcommunity.

❖ **<u>Augmentedgeneral-purposecomputers</u>**

□ + Off-the-shelf operating systems such as WinCE, Linuxand

- ▪ Off-the-shelf operating systems such as WinCE, Linuxand
- ▪ With standard wireless communication protocols such as 802..11 or Bluetooth. Relatively higher processingcapability
- ▪ More powerhungry
- ▪ Fullysupported
- ▪ Popular programminglanguages
- ▪ Ex:PDAs

❖ **<u>Dedicatedembeddedsensornodes</u>**

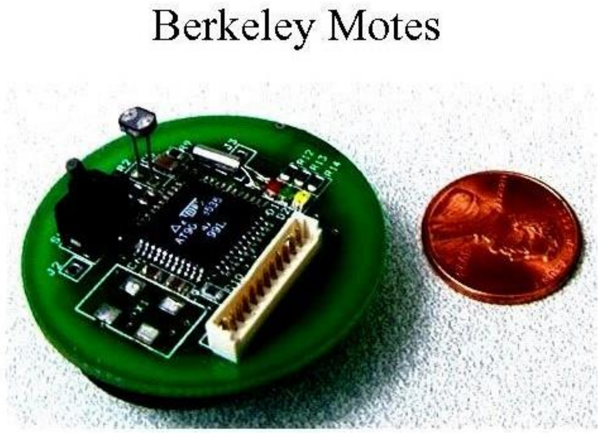
- ▪ Inordertokeeptheprogramfootprintsmalltoaccommodatetheirsmallmemory size,programmersoftheseplatformsaregivenfullaccesstohardwarebutbarely any operating system support.
- ▪ Typicallysupportatleastoneprogramminglanguage,suchasC.
- ▪ Ex: mica, liny0S,nesC

❖ **<u>System-on-chip(SOC)</u>**

- ▪ Build extremely low power and small footprint sensor nodes that still provide certainsensing,computation,andcommunicationcapabilities.

- Currentlyintheresearchpipelinewithnopredefinedinstructionset,thereis no software platform supportavailable.

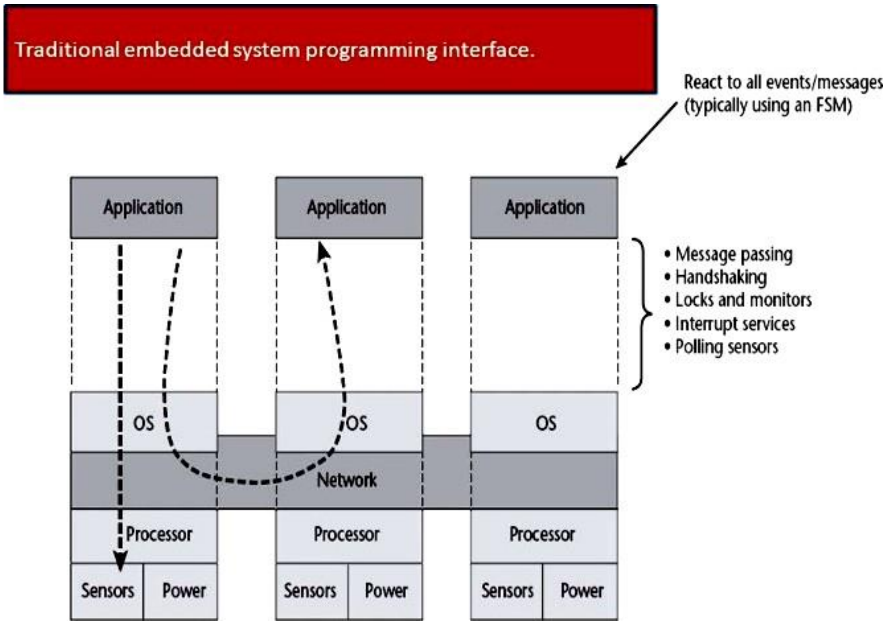
Berkeley Motes



- Berkeley Mote with processing board, sensing board and AA battery pack.
- The mote was essentially a small form factor computer with self-contained processing, sensing and powerresources.
- TinyOS provides a set of software components that allows applications to interact with the processor, network transceiver and thesensors.

3. ProgrammingChallenges

- Event-driven execution allows the system to fall into low-power sleep mode when no interesting events need to be processed.
- At the extreme, embedded operating systems tend to expose more hardware controls to the programmers, who now have to directly face device drivers and scheduling algorithms, and optimize code at the assemblylevel.


Traditional embedded system programming interface.

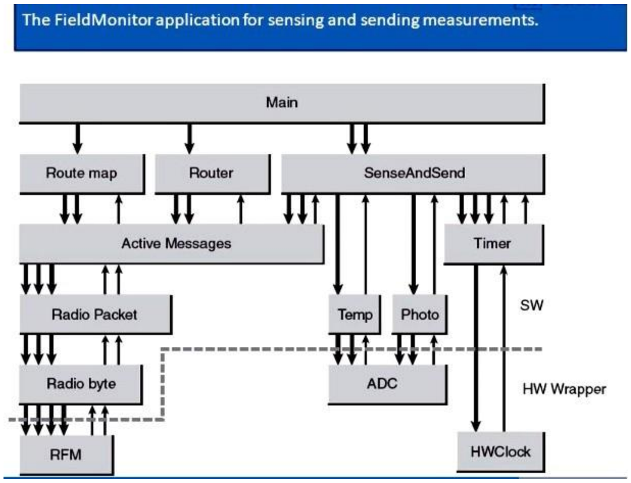
- Traditional programming technologies rely on operating systems to provide abstractionforprocessing,I/O,networking,anduserinteraction hardware.
- Whenapplyingsuchamodeltoprogrammingnetworkedembeddedsystems,suchas sensor networks, the application programmers need to explicitly deal with message passing,eventsynchronization,interrupthanding,andsensorreading.

4. Node level softwareplatforms

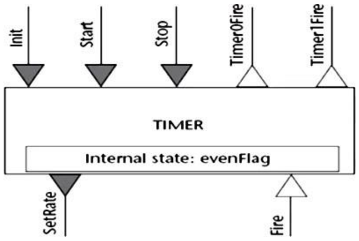
- Node-centricdesignmethodologies:Programmersthinkintermsofhowa nodeshouldbehaveintheenvironment.
- Anode-levelplatformcanbeanodecentricoperating system, which provides hardwareandnetworkingabstractionsofasensornodetoprogrammers.
- Atypicaloperatingsystemabstractsthehardwareplatformbyprovidingasetof services for applications, including filemanagement.
- Memoryallocation,taskscheduling,peripheraldevicedrivers,andnetworking.

Operating System: TinyOS

- LetusconsideraTinyOSapplicationexampleFieldMonitor
- Whereallnodesinasensorfieldperiodicallysendtheirtemperatureandphoto sensor readings to a base station via an ad hoc routingMechanism

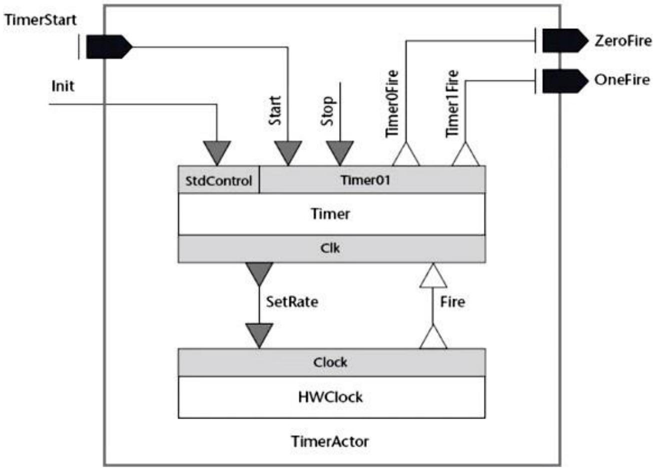

The FieldMonitor application for sensing and sending measurements.

The Timer component and its interfaces



- InnesC,codecanbeclassifiedintotwotypes:
- *Asynchronouscode(AC):Codethatisreachablefromatleastone*interrupt handler.
- *Synchronous code (SC): Code that is only reachable fromtasks.*

TinyGALS


TimerStart
Init
Start
Stop
Timer0Fire
Timer1Fire
ZeroFire
OneFire
StdControl
Timer01
Timer
Clk
SetRate
Fire
Clock
HWClock
TimerActor

Node-levelSimulators

- Node-leveldesignmethodologiesareusuallyassociatedwithsimulatorsthatsimulate the behavior of a sensor network on a per -nodebasis.
- Using simulation, designers can quickly study the performance in terms oftiming, power, bandwidth, andscalability.

5. State-centricprogramming.

- Applications more than simple distributedprograms
    - Applications depend on state of physicalenvironment
- CollaborationGroups
    - Set of entities that contribute to stateupdates
    - Abstracts network topology and communication protocols
- Multi-target trackingproblem
    - Global state decoupled into separatepieces
        - Each piece managed by different principle
        - State updated by looking at inputs from otherprinciples
        - Collaboration groups define communication and roles of eachprinciple

<u>Definition:</u>

X: State of a system U:

Inputs

Y: Outputs

K: Update index

F: State update function

G: Output observation function