

Survey On Wireless Sensor Network

Ruby Singh

Assistant Professor
Lovely Professional University
Phagwara

Abstract

Wireless sensor network is a network in which sensors are densely deployed over an area to observe physical conditions of the environment like pressure, vibration, motion, pollutants, humidity, wind and so on. Wireless sensor network uses Micro Electro Mechanical System technology and they have gained popularity since over a decade because they can be used in diverse types of applications. In this paper there is a study of sensor network in detail.

1. Introduction

Wireless sensor network consist of sensor nodes which may range from few to millions, uses an energy source usually a battery or an embedded form of energy harvesting. Wireless sensor network are infrastructure less and self-configured network in which sensors can communicate with each other through radio signals. Sensor nodes are capable of collaborating with one another and they measures conditions of their surroundings like light, temperature, pressure and any physical phenomena that occurs around them. Sensor nodes in wireless sensor network have short range of radio transmissions and because of this constraint intermediate nodes acts as a relay nodes to transmit data towards a central location often called as sink .Wireless sensor network are typically classified into two type stationary and mobile. In stationary wireless sensor network all nodes are stationary they do not move whereas in mobile wireless sensor network all or some nodes are mobile. In wireless sensor network multiple sensors can be deployed over a large area to have a bigger coverage so if someone wants to remotely monitor that area these networks come out to be very handy. Working of wireless sensor network can be categorized into continuous or event driven. In continuous driven network sensors continuously transmit data in periodic form to base station or it can be think as continuous reporting to base station whereas in event driven wireless sensor networks whenever an event is detected then only various nodes start collecting data from their surroundings. GPS and local positioning algorithm can be used to obtain location and positioning information.

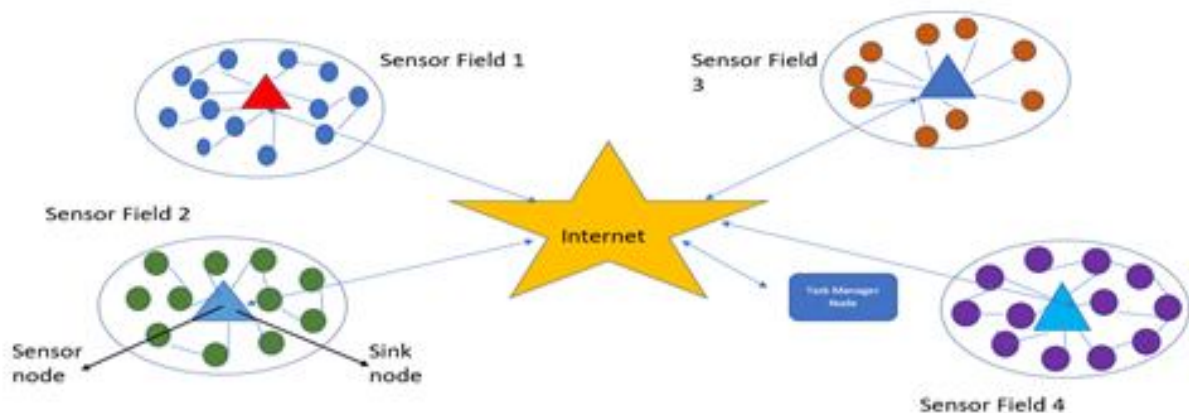


Fig1: Wireless Sensor Network

In the above diagram there are four different wireless sensor networks consist of sensor nodes which sense information and sends that information to sink where further processing and aggregation of sensed is done. Sink nodes are connected to internet. Wireless sensor networks are used for different applications like Border Surveillance applications, environmental applications, health care applications and so on.

1.1. Components of sensor node

A typical sensor node acts like a mini computing device. A sensor node has a sensing unit, processing unit, transceiver unit for communicating purposes, power for powering up the nodes for example different types of batteries are used and there are some application dependent units in addition to these working units example location finding units and mobilizer.

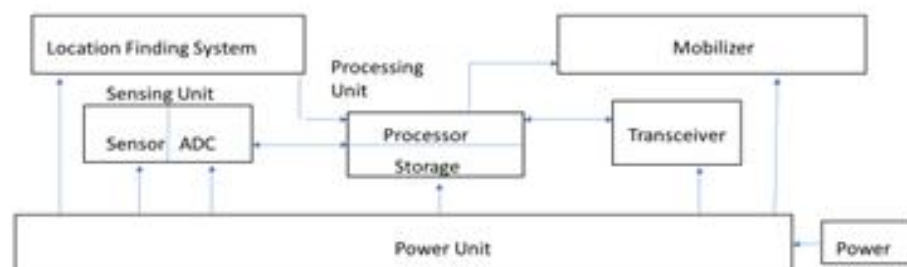


Fig 2: Subparts of sensor node

In the above diagram sensor node is comprised of four units sensing, processing, communication and power unit. Radio transceiver acts as a medium for communication and it provides connection between nodes and the network. ADC is analog to digital converter used to convert signals which are in analog form into 0's and 1's format which are called as digital signals for further processing. Longevity of the nodes is determined by power unit. Location finding system is used to determine location of nodes. Sensors in sensor network shares data with one another in ad-hoc fashion, in order to know physical co-ordinates of sensors localization is used. Localization helps to estimate the place of origin of events. One more unit mobilizer is used which basically used to move sensors to perform a task.

1.2. Areas served by Wireless Sensor Network

a. Military application

Sensors are used to detect enemy intrusion in military. Wireless sensor networks dedicated for military areas are deployed to track enemy, battlefield surveillance, target detection, tracking and surveillance of borders, nuclear detection and so on. In military field, danger of being attacked by enemies is always there. Sensors can be used to detect armored vehicles, men in foot and can be used to increase the efficiency of combat operations. Sensors used in military areas are laser sensors, radar sensors, advanced earth observation sensors and so on.

b. Health application

Wireless sensor network used for medical purposes are also called as wireless medical sensor network. These networks can be used to monitor physiological conditions of patients. Sensors in wireless medical sensor network sense heart rate, blood pressure, temperature of patients and sensor readings help doctor to know patient's conditions. Difference between wireless sensor network and wireless medical sensor network is wireless sensor network uses sensors densely deployed whereas wireless medical sensor network requires human's direct involvement. Examples of sensors used in wireless medical sensor network are pressure sensors, temperature sensors, humidity sensors, force sensors, air bubble detectors and so on.

c. Environmental Sensing

Wireless sensor networks sometimes deployed to monitor environmental conditions and report to a base station where collected data is converted into information. Environmental monitoring includes sensing of light, temperature, lake water quality monitoring, earthquake monitoring, water quality monitoring, soil moisture monitoring, volcano eruption, flooding detection, weather forecasting, chemical hazardous detection, habitat monitoring, monitoring of farms and rain forest.

d. Commercial applications

Wireless sensor network can be used in commercial application like in inventory management, detecting and controlling thefts, product quality monitoring, inventory management and so on.

2. Issues in Wireless Sensor Network

2.1. Design Issues

Wireless sensor network comprises of tiny sensor nodes covering a large area and due to size constraint battery life of these sensors are short. Sensor network consist of different types of sensors and due to this heterogenous nature several challenges arise.

Energy Issue

Size of different types of sensors is very small in wireless sensor network and this restrict size of memory, bandwidth, computation power and energy. Due to size constraint batteries are not easily replaceable especially when deployed in hostile and remote regions. Lifetime of wireless sensor network is entirely dependent on energy consumption of sensor nodes and many existing techniques are there to improve life of sensor. Energy efficient techniques like demand scheme, event scheme are used to enhance battery life of sensors in sensor network. There is one more technique clustering used for solving energy crisis issues and there is one energy efficient protocol LEACH(Low energy adaptive clustering hierarchy) which uses cluster head to reduce energy consumption in network. PEGASIS(Power Efficient gathering in sensor network) is another energy efficient protocol used for data gathering issue and sensors are deployed in the form of chain. PEGASIS distributes load among sensors so one node will not get discharged earlier than other nodes due to excessive load.

Computation

Computation of data is crucial in wireless sensor network since quantity of data which is processed by sensors is application specific and due to short battery life sensors are required to use minimum resources.

Localization

In wireless sensor network problem of finding location of nodes is called as localization of nodes. GPS(Global Positioning System), space based satellite navigation system helps to give information regarding time and location of sensor nodes in wireless sensor network. One way to solve problem of localization is to have a GPS receiver on every single sensor node but it will increase cost since GPS is expensive. One solution to this problem has been discovered that instead of using GPS device on all sensors one vehicle will be moving and carry GPS device and periodically broadcast its location. Sensors node in the network estimate their position based on the location of GPS.

Coverage

Coverage algorithms are used for sensing data in sensor network by sensor nodes. Some nodes are selected as coverage nodes and issue is to make decision who will serve as coverage nodes in the network. Coverage nodes should be chosen in a way that they can cover entire network and work efficiently as per the requirement. Minimal and maximal exposure algorithms are used for finding coverage nodes in the network.

Fault Tolerance

Graceful degradation is a term to define fault tolerance in which there is degradation but gracefully because system after degradation is still capable to perform its dedicated task.

Wireless Sensor Network is said to be fault tolerant if it is able to complete its intended task even after some of its sensor nodes stop working.

2.2. Security Issues

There are several security threats in wireless sensor network because sometimes sensor network is deployed in hostile environment. Sensitive and confidential information needs to be protected in network since medium is unreliable in wireless sensor network. Nodes in wireless sensor network may be left unattended according to the requirement of the application for which network is deployed. Nodes can also get harmed physically this is called as physical attack.

Wormhole attack

Wormhole attack comes under category of DOS which is denial of service attack. In this attack single or sometimes pair of colluding nodes are used. Replaying of packets to a local area is done by attackers. One sits at one point and listen ongoing transmission and transmits it to other end where second attacker is ready to receive. Attackers drop or transmits only selective packets and thereby disturb the network. Techniques used to avoid wormhole attack are packet leashes and TTM(Transmission Time based).

a. Packet Leashes

Packet leashes are used to prevent wormhole attack by putting restriction of location of receiver and bound packets to travel long distances. Challenge which is faced in this technique that every node must be aware of its location in sensor network.

b. TTM(Transmission Time Bases)

In route discovery and setup up phase sensors discovers routes. TTM techniques detects wormhole attack during this phase. Computation of transmission time is done and the idea is based upon the fact that time taken by a packet to travel between two intruders is higher than that between two authorized sensors. Disadvantage of this technique is performance degrades when traffic is high.

Sink Hole attack

The idea of this attack is to create false neighbors in network and attract traffic. Attacker tries to take attention of nodes by introducing high quality link. This attack prevents sink to get accurate data from sensors and it is an insider attack because attacker is present inside the network. Existing approaches are rule based, statistical method, anomaly based detection, hybrid based intrusion detection and so on.

Sybil attack

An attacker uses multiple forged identities claiming himself to be someone else. Sybil attack is categorized into three types

- a. Indirect and direct communication sybil attack
- b. Simultaneous and non simultaneous sybil attack
- c. Fabricate and stolen identities sybil attack

3. Multipath Routing

Multipath routing allows several paths in order to increase reliability of the network. There are three types of paths in this type of routing

- a. *Node Disjoint*
Common nodes are not allowed in this type means paths must be distinct.
- b. *Partially Disjoint*
Links can be shared in this type of routing.
- c. *Link Disjoint*
Nodes can be common but links cannot be shared in this type of routing.

3.1 Benefits of Multipath Routing

Load balancing is one of the advantages of multipath routing by which load can be distributed among several nodes. Network becomes fault tolerant because so many paths are used by this type of routing so if one becomes fails still we can achieve our target. Multipath routing removes the tension of energy exhaustion since we are not dependent on nodes in one single path.

3.2 Related Work

3.2.1 REAR(Reliable Energy Aware Routing Protocol)

This protocol has introduced a backup path concept in case of first path gets depleted. Energy of sensors are continuously examined and if they goes below some fixed value called as threshold value immediately other path is used for data transmission. This saves data because if one sensor gets depleted in midst of transmission it will result in data loss. REAR comes under category of reliable protocols because of the acknowledgement concept it has introduced. A packet is sent to source to giving him indication that data has not been lost during transmission by sink node. Residual energy is used by this type of protocol and selection of next hop is based on remaining energy of nodes.

3.2.2 EAR(Energy Aware Routing Protocol)

Energy aware routing protocol consist of three phases.

- a. Neighbor Discovery phase.
- b. Multipath Construction Phase.
- c. Data transmission phase.

In neighbor discovery phase neighbors gets discovered by a control packet dissemination process which contains residual energy of nodes, id of nodes and location. Second phase is multipath construction phase which is started by base station in which formation of more than one path from source to destination is done. Nodes in primary path called as primary node and nodes in secondary path are called as secondary nodes. Initially data is transmitted using first path and second is optional. Use of secondary path is dependent on energy level of primary path if it gets exhausted then only second will bring into use.

3.2.3 MMSPEED(Multipath Multi Speed Protocol)

In this protocol location of sensors are used and many redundant paths are used from source to destination. Energy consumption is ignored by this protocol.

3.2.3 REBM(Residual Energy Based Multipath Routing Protocol)

The purpose of this protocol is to enhance life of network by using residual energy of nodes in the paths. There are three phases in REBM protocol

- a. Handshaking Phase

Two types of packets are used for neighbor discovery one is hello and other is hi. Hello packet is sent by source and in return its Hi packet from sensors in direct communication range. This phase is not a one time phase since new neighbors are added into the network as per requirement. Whenever a new node comes this process is repeated. Every node in the network maintains a table containing entries of its neighbors and calculate round trip time which is time taken by data to travel from one node to another. Formula for calculating round trip time is

$$RTT_{a-b} = T_b - T_a$$

b. Preemption Algorithm

Preemption algorithm is also called as priority algorithm. Packets using REBM protocol are given priority. Lower priority packet gets preempted if higher priority packet arrives. Algorithm used for preemption is discussed below

Algorithm

While(Packet Transmission)

If (priority of newly arrived packet is equals to priority of currently executing packet)

Continue transmission

Else If (priority of newly arrived packet > priority of currently executing packet)

Preempt packet with newly arrived packet

Else

Continue transmission

}

c. Route Discovery Phase

Source receives replies from sensors with their residual energy. Formula of calculating residual energy by REBM protocol is given below

$$\text{POWER} = \text{RESIDUAL ENERGY} - \text{TOTAL POWER-RESIDUAL}$$

REBM protocol does not use any load balancing algorithm in the network.

Conclusion

In this paper basics of wireless sensor network have been studied. Study of applications of wireless sensor network, issues in network and multipath routing also have been discussed. In future work for removing all these shortcomings will be done. In sensor network inspite of these shortcomings wireless sensor network serves many applications. Application like weather forecasting, fire detection, military, wildlife detection are big contribution to us.

References

[1] G.R.Sakthidharan, Schitra," A survey on wireless sensor network- an application perspective", international conference on computer communication and informatics, (2012) .

- [2] Abdul Gani Khan, Abdur Rahman," Classification of hierarchical based routing protocols for wireless sensor network", International journal of innovations in engineering and technology,(2013),43-49.
- [3] S.Prasanna, Srinivasa Rao,"An Overview of Wireless Sensor Networks Applications and Security",International journal of soft computing and engineering(2012),2231-2307
- [4] Debnath Bhattacharyya, Tai-hoon-kim,Subhajit Pal," A comparative study of wireless sensor networks and their routing protocols", (2010),1424-8220.
- [5]Alakesh Braman, Umapathi G.R,"A comparative study on advances in LEACH routing protocol for wireless sensor networks: A survey", International journal of advanced research in computer and communication engineering(2014),volume 3,5683-5690.
- [6] Priya Maidamwar, Nekita Chavhan,"A survey on security issues to detect wormhole attack in wireless sensor network",International journal on AdHoc Networking Systems , (2012),volume 2, 37-49.