Wireless Sensor Network: An Overview

K. M. Pradhan(Dighe)
HOD, Rajarshi Shahu Mahavidyalaya Latur

M A Shinde(Bhandwalkar)
Rajarshi Shahu Mahavidyalaya Latur

Abstract

Wireless Sensor network are dense wireless networks of small, low-cost sensors, which collect disseminate environment data. Wireless sensors networks facilitate monitoring and controlling of physical environments from remote locations with better accuracy. They have applications in a variety of fields such as environmental monitoring, military purpose and gathering sensing information inhospitable locations. Sensor nodes have various energy and computational constraints because of their inexpensive nature and ad-hoc method of deployment. Considerable research has been focused at overcoming these deficiencies through more energy efficient routing, localization algorithms and system design. Our survey attempts to provide an overview of these issues as well as the solutions proposed in recent research literature.

1. Applications of sensor network

Researchers expect that the usage of wireless sensor networks will facilitate many existing applications and ultimately enable a multitude of new ones. Obviously this grand vision is depends on achieving the requirements discussed in the previous section as well as those imposed by the application. A primary constituent is the connection of the node to the physical world that is achieved by the sensing device attached.

Common sensing devices are: (1) temperature, (2) humidity, (3) light, (4) pressure, (5) acceleration, (6) acoustic, (7) vibration for seismic disorder. Some more sophisticated sensing devices include: (8) Chemical sensors for soil composition and water/air quality, (9) magnetometers, (10) mechanical sensors, and (11) ECG and other sensors for medical applications. A sensor unit might control an actuator to trigger a physical action such as turning on/off an engine or a light. The literature proposes a wide range of applications for wireless sensor networks that can be grouped in 7 main categories.

Building Automation

Sensor networks can be used to improve the monitoring of real-time temperature, air ow, humidity and other related physical parameters of a building to considerably reduce the energy consumption related to air conditioning and heating systems. Sensor nodes can be retrofitted in existing buildings or

The first version of the Philips Aquisgrain sensor node can be incorporated in buildings under construction. This is the goal of “intelligent buildings” for which wired and wireless systems like
BACnet or KNX have been already deployed. Together with a more efficient usage of the energy resources, the system would increase the comfort level of inhabitants.

Environmental monitoring

Wireless sensor networks are effectively deployed in remote areas to monitor environmental condition such as volcanic activity monitoring. Of the same typology is the monitoring of wild animals. For example WSNs have given biologists new insight into the nesting patterns of Storm Petrels on Great Duck Island. Furthermore, WSNs are applied for precision agriculture to allow targeted irrigation and fertilizing by deploying humidity/soil composition sensors such as in vineyard monitoring. WSNs are also applied to livestock breeding to monitor the health status and location of cows and other breeding animals.

Infrastructure monitoring

Infrastructure monitoring for preventive maintenance is an interesting application where WSNs are deployed to monitor vibration and mechanical stress levels of infrastructures, such as the wind response of the Golden Gate Bridge in San Francisco.

Military applications

Such applications include intruder detection and surveillance in hostile environments. WSNs can be used to report updates on the event’s source and, possibly, to estimate its direction and speed. Of the same type are military applications for detecting and counting snipers in urban warfare and for disaster relief operations. A typical example is wildfire detection where sensor nodes are equipped with thermometers and can determine their own location. The nodes can therefore collectively report to a central aggregation point that will produce a temperature map of the wildfire.

Personal healthcare

These types of applications involve the collection of data from a patient that is wearing a body area network (BAN). Such networks consist of a number of nodes attached to the body like plasters that monitor vital data of the patient. One of the nodes is usually responsible for collecting and aggregating the data before forwarding it to an ambient network that will route the data to the doctor. The usage of WSNs can avoid the usage of wires, which gives more mobility and comfort to the patient under observation.

Residential/commercial control

This type of application regards home security, where sensor nodes can be deployed to monitor domestic premises. Sensor nodes should report to the sink once they have detected an event, such as an intruder or other events such as the presence of smoke in a at. In general, a single node in isolation can detect simple events and other more complicated composite events require the collaboration of multiple nodes.
Underwater monitoring

A key aspect of such applications is the extra requirement imposed by the water communication medium that attenuates the RF signal enormously. An alternative way of communication is through acoustic signals.

Fire and Flood Detection

Large number of environmental applications makes use of WSNs. Sensor networks are deployed in forest to detect the origin of forest fires. Weather sensors are used in flood detection system to detect, predict and hence prevent floods. Sensor nodes are deployed in the environment for monitoring biodiversity. The Forest-Fires Surveillance System (FFSS) was developed to prevent forest fires in the South Korean Mountains and to have an early fire-alarm in real time. The system senses environment state such as temperature, humidity, smoke and determines forest-fires risk-level by formula. Early detection of heat is possible and this allows for the provision of an early alarm in real time when the forest-fire occurs, alerting people to extinguish forest-fires before it grows. Therefore, it saves the economical loss and environment damage. Similarly, a typical application of WSN for flood detection and prevention is the ALERT system deployed in the US. Rainfalls, water level and weather sensors are used in this system to detect, predict and hence prevent floods. These sensors supply information to a centralized database system in a pre-defined way.

2. Architecture

Architecture of node focuses to reduce cost, increase flexibility, provide fault-tolerance, improve development process and conserve energy. The sensor node consist of sensing unit, processing unit (MCU-micro controller unit), communication unit and power supply as shown in figure in which node is divided into five major blocks where each block performs some specific task. First block is power supply block composed of power battery and DC-DC which is responsible for giving energy to
the node. Battery can not replace every time so proper and efficient utilization of power must be necessary. Second block is communication block (transceiver) provide communication channel which may use radio, laser or optical and infrared. Third block is processing block which has memory (RAM), microcontroller, operating system and timer which are responsible for storing, processing and executing the events respectively. Forth block is Sensing unit composed of collection of sensor which produces the electrical signals by sensing physical environment and analog to digital converter(ADC) which transforms the signal. The type of sensor being used in a sensor node will depend on the application. Last block is software.

A. Processing unit:
 responsible for collecting data from various sources then processes it stores it. the central processing unit of sensor node determines energy consumption and computational capabilities of a node. In order to provide the flexibility for CPU implementation, large number of microcontroller, microprocessor and FPGAs (field programmable gate arrays) are available.

Microcontroller-

it is general purpose processor used for processing. It is not only consists of memory and processor but also non-volatile memory and interfaces. It helps to reduce the requirement of wiring, extra hardware, circuit board space and energy. For saving of power, microcontroller should have three states-active, sleep, idle.

FPGAs–field Programmable Gate Array is used for testing. However, it has two disadvantages i.e. it can not reduce their energy consumption. Secondly it is not feasible to make separate block for it. But it does not mean that it can not be used in sensor. In near future if ultra-low power will be developed, it will eliminate the deployment cost due to reprogrammable and reconfigurable feature.

Timer/Clock : Timer is a special type of clock. As it is asynchronous technology but for sequencing of sequence, it need timer. Timers are of different types such as electronic, electromechanical, mechanical and digital. It has also low volume and low power consumption.

Operating system: WSN uses less complex operating system as compared to general – purpose operating system in the sense that it uses few thousands of lines for coding the system whereas general-purpose consist of millions of lines of codes. Some WSN node operating system are TinyOS, Contiki, MANTIS, BTnut ans SOS etc. TinyOS is the most familiar operating system in sensor network which is event-driven and calls the appropriate event handler for execution.

Memory:

Here we use RAM as an internal memory for storing information in microcontroller. We can also use flash memory which is used for storing program code. However, Size of memory can affect consumption of power and cost. Thus, selecting the appropriate size of memory is important and can be selected according to application.
B. Power Unit:
Power block are responsible for providing energy to the sensor node for monitoring the environment at low-cost and time. It takes energy from power generator and pass to other component of node. Life of sensor node depends upon battery so battery is the important component that must be distribute properly. Power unit are required due to the following reasons—provide long life, provide stability of voltage, has capacity under load, has ability to recharge under low current, has low-self discharge.

Battery:
Batteries can be dividing into primary and secondary i.e. rechargeable or non-rechargeable and design of sensor node depends on the battery. Non-rechargeable battery is good solution since it has high density. To manage energy basically two type of technique are used-demand power management (DPM) and dynamic voltage scheduling (DVS).

C. Communication or Transceiver Unit
A transceiver is a unit in which transmitter as well as receiver is sharing same circuitry on single board. It receives command from processing unit and passes it to the other node of the network. Communication is performed through communication channels. This phase provide some network protocol in order to perform communication. Three types of communication discuss under this optical communication, Infrared and RF(Radio-frequency).

D. Sensing Unit
• **A/D converter**-
  It is used for converting the analog sign into digital signal. It takes an analog signal from sensor and converts it into digital signal and relay to microcontroller for further processing

• **Sensors**-
  WSN consists of large number of sensor nodes where each nodes contains more than one sensor at the same time depending upon the application. There are different types of sensors like acoustic sensor, resonant temperature sensor, magnetic field sensor etc. basically sensor is device that sense physical phenomenon such as pressure, motion, speed etc. and transform it into analog signal and the same signals are processed by analog to digital converter. Now-a-days sensors are used in machines, medicines, cars, manufacturing etc. sensors may be directional or omni-directional and may be passive or active. An active sensor is sensor which senses the phenomenon with active manipulation. Example of active sensor is radar. A passive sensor is sensor which senses the environment without active manipulation. Example of passive are thermometer, light, hygrometer, microphones etc.

E. Softwares
It provides four services such as i) sensor manager which provide access to sensors and manage the delivery of sensor data, ii) storage is responsible for providing the persistent storage for data
stream, iii) query manager performs query processing and manages active queries. iv) integrity services is used for access control.

4. Energy efficiency

Energy is the scarcest resource that must be utilized properly because it is impossible to recharge each node so it must be energy efficient as possible. Low-cost as it is collection of hundred and thousands sensor nodes, so cost of each node should be node minimum so that overall cost of network should also be minimum. Distributed sensing as large numbers of node are distributed in sensor network so each node can capable of collecting and storing data. Thus distributed sensing provides robustness to the system. Wireless sensor node should be wireless as many application do not require/ install infrastructure for communication. In that case sensor node will use wireless communication channel. Multihop as large number of sensor are deploying in WSN, so it is not feasible for each node in WSN, so it is not feasible for each node to reach the base station. It may require intermediate node to reach the base station. Thus the solution is multi hop. Distributed processing Each node is WSN can collect and process local data, perform aggregation on same data and then transforming it to information.

5. Localization

In WSNs, sensor nodes that are deployed into the environment in an ad hoc manner do not have prior knowledge of their location. The problem of determining the node’s location (position) is referred to as localization. Existing localization methods include global positioning system (GPS), beacon (or anchor) nodes, and proximity-based localization. Equipping the sensor nodes with a GPS receiver is a simple solution to the problem. However, such a GPS-based system may not work when the sensors are deployed in an environment with obstructions such as dense foliage areas. The beacon (anchor) method makes use of beacon (anchor) nodes, which know their own position, to help sensors determine their position. This method has its shortcoming. It does not scale well in large networks and problems may arise due to environmental conditions. Proximity-based localization makes use of neighbor nodes to determine their position and then act as beacons for other nodes. Below we review some of the key localization techniques that differ from the above methods.

Moore’s algorithm: Presents a distributed localization algorithm for location estimation without the use of GPS or fixed beacon (anchor) nodes. A key feature of this algorithm is the use of a robust quadrilateral. A robust quadrilateral is a fully-connected quadrilateral whose four sub-triangles are robust. Localization based on robust quadrilateral can be adjusted to support noisy measurements and it correctly localizes each node with a high probability.

This algorithm has three phases: cluster localization phase, cluster optimization phase, and cluster transforma- tion phase. In the first phase, each node becomes the center of a cluster and measures the distance of its one-hop neighbors. The information gathered is broadcasted. For each cluster, each node computes the complete set of robust quadrilaterals and finds the largest sub-graph of overlapping robust quadrilaterals. Position estimations for a local coordinate system are computed for as many nodes as possible using the overlap graph using a breadth-first search. The second phase is an optimization phase that can be omitted. Position estimations are refined using numerical optimization such as spring relaxation or the Newton–Raphson method. The last
phase computes the transformation between local coordinate system of connected clusters. The transformation computes the rotation, translation, and possible reflection that best aligns the nodes of two local coordinate systems. There is, however, one drawback to this system. Under conditions of low node connectivity and high measurement noise, the algorithm may not be able to localize some nodes.

RIPS: The work proposes a localization system called Radio interferometric Positioning System (RIPS) which utilizes two radio transmitters to create an interference signal. Two radio transmitters are placed at different locations and set at slightly different radio frequencies to provide ranging information for localization. At least two receivers are needed to calculate the phase offset of the observed signals. The relative phase offset is a function of the relative positions between the two transmitters and the receivers, and the carrier frequency. By measuring the relative phase offset, one can analyze and determine the relative locations of the two receivers or the location of the radio source if the receiver locations are known. Spotlight: Spotlight is a system that achieves high accuracy of localization without the use of expensive hardware like other localization systems. Spotlight uses an asymmetric architecture where computation resides on a single Spotlight device. The Spotlight device uses a steerable laser light source which illuminates the sensor nodes that are placed in a known terrain. The main idea of the Spotlight localization system is to generate controlled events in the field where the sensor nodes are deployed. An event can be defined as a lighted sensor area. Using time events perceived by a sensor node and spatiotemporal properties of the generated events, spatial information regarding the sensor node can be inferred. Results show that Spotlight is more accurate than other range-based localization schemes and much more effective for long-range localization problems. The cost of localization is low since only one single device is necessary to localize the network.

Secure localization: Secure localization focuses on securing the localization process. The goal is to prevent malicious beacon nodes from providing false location to sensors. Sensors rely on beacon information to compute their position. To prevent the localization process from being compromised, the following security requirement must be satisfied. Sensors must only accept information from authenticated beacon nodes. Sensors should only use information that has not been tampered. Sensors should be able to request location information at anytime. Upon a location request, information exchange must take place immediately and not at a later time. Neither a source’s nor sensor’s location should be disclosed at any time to prevent malicious nodes from taking over a location in the network. If any one of these requirements is breached, the localization process is compromised.

6. Routing

Since a distributed network has multiple nodes and services many messages, and each node is a shared resource, many decisions must be made. There may be multiple paths from the source to the destination. Therefore, message routing is an important topic. The main performance measures affected by the routing scheme are throughput (quantity of service) and average packet delay (quality of service). Routing schemes should also avoid both deadlock and livelock (see below). Routing methods can be fixed (i.e. pre-planned), adaptive, centralized, distributed, broadcast, etc. Perhaps the simplest routing scheme is the token ring. Here, a simple topology and a straightforward fixed protocol result in very good reliability and precomputable QoS.
token passes continuously around a ring topology. When a node desires to transmit, it captures the token and attaches the message. As the token passes, the destination reads the header, and captures the message. In some schemes, it attaches a ‘message received’ signal to the token, which is then received by the original source node. Then, the token is released and can accept further messages. The token ring is a completely decentralized scheme that effectively uses TDMA. Though this scheme is very reliable, one can see that it results in a waste of network capacity. The token must pass once around the ring for each message. Therefore, there are various modifications of this scheme, including using several tokens, etc.

**Fixed routing schemes**

often use Routing Tables that dictate the next node to be routed to, given the current message location and the destination node. Routing tables can be very large for large networks, and cannot take into account real-time effects such as failed links, nodes with backed up queues, or congested links.

**Adaptive routing schemes**

depend on the current network status and can take into account various performance measures, including cost of transmission over a given link, congestion of a given link, reliability of a path, and time of transmission. They can also account for link or node failures. Routing algorithms can be based on various network analysis and graph theoretic concepts in Computer Science (e.g. A-star tree search), or in Operations Research- including shortest-route, maximal flow, and minimum-span problems. Routing is closely associated with dynamic programming and the optimal control problem in feedback control theory. Shortest Path routing schemes find the shortest path from a given node to the destination node. If the cost, instead of the link length, is associated with each link, these algorithms can also compute minimum cost routes. These algorithms can be centralized (find the shortest path from a given node to all other nodes) or decentralized (find the shortest path from all nodes to a given node). There are certain well-defined algorithms for shortest path routing, including the efficient Dijkstra algorithm [Kumar 2001], which has polynomial complexity. The Bellman-Ford algorithm finds the path with the least number of hops. Routing schemes based on competitive game theoretic notions have also been developed.

**Deadlock and Liveloack.**

Large-scale communication networks contain cycles (circular paths) of nodes. Moreover, each node is a shared resource that can handle multiple messages flowing along different paths. Therefore, communication nets are susceptible to *deadlock*, wherein all nodes in a specific cycle have full buffers and are waiting for each other. Then, no node can transmit because no node can get free buffer space, so all transmission in that cycle comes to a halt. *Liveloack*, on the other hand, is the condition wherein a message is continually transmitted around the network and never reaches its destination. Liveloack is a deficiency of some routing schemes that route the message to alternate links when the desired links are congested, without taking into account that the message should be routed closer to its final destination. Many routing schemes are available for routing with deadlock and liveloack avoidance.
Flow Control.

In queuing networks, each node has an associated queue or buffer that can stack messages. In such networks, flow control and resource assignment are important. The objectives of flow control are to protect the network from problems related to overload and speed mismatches, and to maintain QoS, efficiency, fairness, and freedom from deadlock. If a given node A has high priority, its messages might be preferentially routed in every case, so that competing nodes are choked off as the traffic of A increases. Fair routing schemes avoid this. There are several techniques for flow control: In buffer management, certain portions of the buffer space are assigned for certain purposes. In choke packet schemes, any node sensing congestion sends choke packets to other nodes telling them to reduce their transmissions. Arithmetic schemes have a fixed number of ‘permits’ for the network. A message can be sent only if a permit is available. In window or kanban schemes, the receiver grants ‘credits’ to the sender only if it has free buffer space. Upon receiving a credit, the sender can transmit a message. In Transmission Control Protocol (TCP) schemes (Tahoe and Reno) a source linearly increases its transmission rate as long as all its sent messages are acknowledged for. When it detects a lost packet, it exponentially decreases its transmission rate. Since lost packets depend on congestion, TCP automatically decreases transmissions when congestion is detected.

9. Conclusion

Wireless sensor networks become more popular these days because of its low cost, less power requirement, performance and high references potential application areas. This paper elaborates the deploy node characteristics and functioning of each module of WSN architecture. Security issues and design challenges are analyzed and enlisted. Although a great work has been done in relation with wireless sensor networks, till date and still many efforts are needed in the direction of design and security of WSN.

References
[8] Patrick Bultynck and Chantal Reliquet
[9] Ma Yajie, Mark Richards, Moustafa Ghanem, Yike Guo, and John
Hassard. Air pollution monitoring and mining based on sensor grid in London.
