Global Journal of Enterprise Information System
http://www.ejournal.co.in/gjeis
April - June 2011
Volume-3 Issue-II

# Wireless Sensor Networks: *Applications and Issues*

**V.K.Saraswat**
Dr. B.R. Ambedkar University
Institute of Computer and Information Science
Agra, India
vk.saraswat@gmail.com

**Arun Bakshi**
Gitarattan International Business School
Rohini, New Delhi, India
lakshayabakshi@gmail.com

## ABSTRACT

In today's scenario, wireless sensor network is one of the most important technologies used. Wireless communications and electronics are now available in low cost, consume less power and provide multifunctional miniature devices which are beneficial for use in remote sensing applications. These factors have improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of sensing, data processing and communication capabilities.

Sensor network protocols and algorithms must possess self-organizing capabilities. One important characteristic of sensor networks is that protocols and algorithms used in it are self-organizing which means that each sensor node is independent and creates it own infrastructure according to different situations. Another unique feature of sensor networks is the cooperative effort of sensor nodes which means instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. Sensor networks are predominantly data-centric rather than address-centric. So, sensed data are directed to an area containing a cluster of sensors rather than particular sensor addresses. This cluster may contain redundant data. To reduce redundancy and increase the level of accuracy, aggregation is performed. This can be done using the aggregator node within the cluster which further reduces communication bandwidth requirements.

A network hierarchy and clustering of sensor nodes allows for network scalability, robustness, efficient resource utilization and lower power consumption. The fundamental objectives for sensor networks are reliability, accuracy, flexibility, cost effectiveness and ease of deployment.

## KEYWORDS

Wireless Communication | Sensor Networks | Reliability | Data-Centric

## PREAMBLE

Sensor network is an interdisciplinary research area that draws on contributions from signal processing, networking and protocols, databases and information management, distributed algorithms, and embedded systems and architecture. A sensor is a transducer that converts a physical phenomenon such as heat, light, sound or motion into electrical or other signals that may be further manipulated by other apparatus. A basic unit in a sensor network is a sensor node. Sensor node is equipped with an on-board sensors, processor, memory, wireless modem, and power supply. Sensor node is also abbreviated as a node. Sometimes a node with a single sensor on board is also called a senor, this creates some confusion.

## SENSOR NETWORK CHALLENGES

The challenges we face in designing sensor network systems and applications include:

- **Limited hardware**

Limited amount of hardware resources is used to optimize the maximum output is one of the biggest challenges of sensor networks. Each node in sensor network has limited processing, storage, and communication capabilities, and limited energy supply and bandwidth.

- **Limited Support for networking**

Peer-to-peer network is used with mesh topology. Network is dynamic, mobile and equipped with unreliable connectivity. No routing protocols or register has been used. Therefore, node itself acts both as a router and as an application host.

- **Limited support for software development**

The tasks are typically real-time and massively distributed, involve dynamic collaboration among nodes, and must handle multiple competing events. Global properties can be specified only via local instructions. Because of the coupling between applications and system layers, the software architecture must be co-designed with the information processing architecture.

Further wireless sensor network uses a wide variety of applications and to impact these applications in real world environments, we need more efficient protocols and algorithms. Designing a new protocol or algorithm address some challenges which are need to be clearly understood. These challenges are summarized below:

- **Physical Resource Constraints**

One of the most important physical constraints is power supply. Effective lifetime of sensor network can be determined by its power supply. Hence, energy consumption is the main design issue protocol. Other constraints are limited computational power and memory size which determines the size of data stored in each sensor node. Therefore, protocols designed should be simple and light-weighted. Communication channels are also limited which are shared by all nodes within each other's transmission range as a result communication delay increases.

- **Ad-hoc Deployment**

In some applications, ad-hoc deployments of sensor nodes are required with respect to some specific area. The sensor nodes are randomly installed without prior knowledge of infrastructure and topology. In such situation, it is the responsibility of sensor nodes to identify its connectivity and distribution among nodes.

- **Fault-Tolerance**

A sensor node may fail due to some physical damage or lack of energy. It is up to the communication protocols to lodge these changes in the network.

- **Scalability**

Generally Hundreds or thousands of sensor nodes are to be deployed in most of the applications. This is the responsibility of the protocols to scale enough to communicate with such large number of sensor nodes.

- **Quality of Service**

In some real time sensor applications as soon as the data is sensed, it must be delivered in certain period of time, before it becomes obsolete. QOS is the major parameter for such applications.

- **Unattended operation**

Many sensor applications require human intervention only during the time of deployment. If further changes or reconfiguration is needed, this all be done by the nodes themselves.

- **Untethered**

Nodes are having finite source or energy and not connected to any external energy source. Thus energy must be optimally used for processing and communication. For better optimization, communication should be minimized as much as possible.

- **Security**

Security is very critical parameter in sensor networks, given some of the proposed applications. An effective compromise must be obtained, between the low bandwidth requirements of sensor network applications and security demands for secure data communication in the sensor networks (which traditionally place considerable strain on resources)Thus, unlike traditional networks, where the focus is on maximizing channel throughput with secure transmission.

## SYSTEM ARCHITECTURE AND DESIGN ISSUES

The performance of a secure routing protocol is closely depended on the architectural model and design of the sensor networks, base on the application

| CPU | 8 bit, 4 MHz |
|---|---|
| Storage | 8K Instruction Flash<br>512 bytes RAM<br>512 bytes EEPROM |
| Communication | 916 MHz radio |
| Bandwidth | 10 Kilobits per second |
| Operating System | Tiny OS |
| OS code space | 3500 bytes |
| Available code space | 4500 bytes |

Basic configuration of a simple sensor node requirements different architectures and design goals/constraints has been considered for sensor networks. The basic configuration of a simple sensor node is described by above table; configuration depends on the requirements of the applications.

- **Security Implementation**

In the designing phase of wireless networks, secure data communication is the main concern of sensor networks, especially if to be deployed in the battle fields, a hostile area. Therefore, the protocols design must be in accordance to the data communication security protocols. Any conflict among these protocols might create challenge for the network security.

- **Energy Considerations**

One of the important parameters to be taken care of during the creation of infrastructure and designing the routes for transmission is energy. As the transmission power of a wireless radio is proportional to distance squared or may be higher order in case of obstacles, multi-hop routing consumes less power than direct communication but it will increase overhead for topology management and medium access control. Direct communication performs well if the nodes are very close to sink.

- **Data Aggregation/Fusion**

Similar or redundant data might be generated from multiple nodes. To reduce redundancy and increase the level of accuracy, data aggregation is performed by the help of functions like suppression, min, max and average. Redundant data is suppressed or eliminated using aggregator node. Data aggregation can also help to save energy as computation would be less energy consuming than communication.

- **Network Dynamics**

There are three basic components, sensor nodes, sink and user which monitor the events in a sensor network. Most of the network architectures assume that sensor nodes are stationary. Some applications require the mobility of sinks or cluster-heads (gateways). It is more challenging to route messages from or to moving nodes, because route stability becomes an important factor for optimization, in addition to energy, bandwidth etc.

Depending upon the application the sensed event can be static or dynamic.

- **Node Deployment**

The deployment of sensor nodes in topological manner depends on the application area. It can affect the performance of routing protocol.

Deployment can be deterministic or self-organized. In deterministic approach, nodes are manually placed and data is transmitted through pre-determined paths whereas in self-organizing approach, nodes are randomly placed to identify connectivity and distribution of node according to the situations, thus creating an infrastructure in ad-hoc manner.

- **Data Delivery Models**

Data is delivered using different models based on the requirement of applications. Data delivery model can be continuous, query-driven, event-driven or hybrid. In continuous data delivery model, data is delivered on periodic basis. In event-driven model, data is transmitted as the event is triggered. In query driven model, data is transmitted with respect to the query being generated. Some applications require the combination of these models for appropriate delivery of data.

- **Node Capabilities**

Depending on the sort of work a node can be dedicated to a particular special function such as relaying, sensing and aggregation since engaging the three functionalities at the same time on a node might quickly drain the energy of that node. Inclusion of heterogeneous set of sensors raises multiple technical issues making data routing more challenging.

Security Implementation Security is data communication is a main concerning parameter for providing secure communication in sensor networks, while designing wireless networks, as wireless sensor networks may be deployed in hostile areas such as battle fields .therefore, design of protocol should work with the data communication security protocols, as any conflict between these protocols might create challenge in network security.

## WIRELESS SENSOR NETWORKS Vs. TRADITIONAL WIRELESS NET WORK

A Sensor network is designed to perform a set of high level information processing tasks such as detection, tracking, or classification. Measures of performance for these tasks are well defined, including detection of false alarms or misses, classification errors, and track quality. Applications of sensor networks are wide ranging and can vary significantly in application requirements, modes of deployment (e.g., ad hoc versus instrumented environment), sensing modality, or means of power Supply (e.g., battery versus wall-socket). Sample commercial and military applications include:

There are many existing protocol, techniques and concepts from traditional wireless network, such as cellular network, mobile ad-hoc network, wireless local area network and Bluetooth, are applicable and still used in wireless sensor network, but there are also many fundamental differences which lead to the need of new protocols and techniques.

**Some of the most important characteristic differences are summarized below:**

Protocols, techniques and concepts from traditional wireless networks (e.g. Bluetooth, Wireless local area network, cellular network, mobile ad-hoc network) are still being used in wireless sensor network. But some fundamental differences lead to the need of new protocols and techniques. Some of these differences are summarized as:

- Hundreds or thousands of nodes are used in wireless sensor network. Sensor network may need to extend the monitored area and has to increase the number of nodes. For this, sensor network needs to be highly scalable.
- As the number of nodes is too large, addresses are not assigned to the sensor nodes. Sensor nodes are data centric rather than address centric. This requires collaborative effort between nodes.
- Sensor nodes uses broadcast communication paradigm, whereas ad hoc networks uses point-to-point communications.
- Sensor nodes are much cheaper than nodes in ad hoc networks.
- Wireless sensor networks are environment-driven. In traditional wireless networks, data is generated by human whereas in sensor networks, data is generated when changes occurs in the environment. Sensor networks are used to gather information whereas mobile ad-hoc networks are used for distributed computing

.

In wireless sensor network, data collected by neighboring nodes are often quite similar. This makes it possible to develop routing and aggregation techniques that can help to reduce redundancy and to improve energy efficiency. Thus, unlike traditional networks, where the focus is on maximizing channel throughput or minimizing node deployment, the major consideration in a sensor network is to extend the system lifetime as well as the system security

## APPLICATIONS OF SENSORS

- Environmental monitoring (e.g., traffic, habitat, security)
- Industrial sensing and diagnostics (e.g. appliances, factory, supply chains)
- Infrastructure protection (e.g. power grids, water distribution)
- Battlefield awareness (e.g. multi-target tracking)
- Context-aware computing (e.g. intelligent home, responsive environment)

- **Military Applications:** Sensor networks are widely used in military sensing. Wireless sensor networks can be used for military command, control, computing, communications, surveillance, intelligence, reconnaissance and targeting systems. The Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) from the Defense Advanced Research Project Agency (DARPA) are applied very successfully in the military sensing.

- **Environmental Monitoring:** Another application for sensor networks is to monitor the environment. It is widely applied in habitat monitoring, agriculture research, fire detection. For example, Smoke alarms are placed in many companies.

- **Medical Application:** Sensor networks are also used in medical sciences. It can be used to monitor patient's physiological data, to control the drug administration track and monitor patients and doctors inside a hospital.

- **Home Application:** Concepts like "Smart Environment: Residential Laboratory" and "Smart Kindergarten" are applied in home applications.

- **Traffic Monitoring:** The sensor node has a built-in magneto-resistive sensor that measures changes in the Earth's magnetic field caused by the presence or passage of a vehicle in the proximity of the node. A low-power radio relays the detection data to the AP at user-selectable periodic reporting intervals or on an event driven basis. By placing two nodes a few feet apart in the direction of traffic, accurate individual vehicle speeds can be measured and reported.

- **Robotics Control:** Robotics has matured as a system integration engineering field defined as "the intelligent connection of the perception to action". Programmable robot manipulators provide the "action" component. A variety of sensors and sensing techniques are available to provide the "perception".
- **Habitat Monitoring**: The intimate connection with its immediate physical environment allows each sensor to provide localized measurements and detailed information that is hard to obtain through traditional instrumentation.

## SECURITY REQUIREMETNS

**Data Confidentiality:** Highly sensitive data is communicated in some applications of sensor network. Therefore, secure communication must be needed. A malicious node may change the data by adding some irrelevant information within the packet. This should also be taken into consideration.

**Data Freshness:** This constraint is required in the environments where shared-key-strategies are employed in the design. Data freshness tells that the data is up to date. It also ensures that no old messages have been repeated.

**Self-Organization:** In general a wireless sensor network is a ad hoc network that necessitates every sensor node to be self-governing and flexible enough to be self-systematized and self-curing according to different circumstances.

**Time Synchronization:** When a data packet travels between a pair of sensors, sensors may require to

compute the end to end delay of packet delivery. Group synchronization for tracking applications may also be required in case of a collaborative sensor network.

**Secure Localization:** the reliability of a sensor network if proportional to its ability to accurately and automatically locate each sensor in the network. Information about accurate position is a must to pinpoint the location of a fault. In this regard, three phase Secure Positioning for Sensor Networks (SPINE) algorithm is used.

**Authentication:** It allows a receiver to verify that the data is received from the authorized sender. For this purpose, both sender and receiver share a secret key to compute message authentication code (MAC) of all communicated data.

## CONCLUSION

As the computing power is emerged everywhere, role of sensor networks becoming more important. It requires high level of security and energy efficiency which are the major parameters to enhance the quality of life. Its scope is tremendously increasing and is likely to be widely used in future. But issues like privacy of data generated may have some negative impacts also. This can cause the limited use of a significant technology for the betterment of the futuristic information era. To make best use of this powerful technology, privacy issues should be given due consideration at the product design stage itself. Combination of legal requirements and industry best practices can also be of great help

## FUTURE SCOPE

Sensor networks will grow in size because of lower cost, better protocols and advantages of dense networks.

There is an increasing emphasis for future processing and communication requirements to be met by embedded devices. As devices become ever smaller, cheaper and better provisioned, the visions of smart dust, intelligent environments and ambient computing become more realistic. Wireless Sensor Networks (WSN) also bring specific research challenges – especially in terms of automated discovery, configuration and cooperation to optimize services and message routing over the network.

Proponents of this new technology see a world with deployments to improve a wide range of operations. Engineers could wirelessly monitor miles of gas and oil pipelines stretching across arid land for ruptures, damage, and tampering. Rescue workers might detect signs of life under the rubble of a collapsed building after an earthquake, thanks to a network of sensors inside the structure. Armed forces could keep an eye on a combat zone or a vast international border via a sensor network that could promptly provide alerts of any intrusion or illicit trafficking.

## REFERENCES

i. Ismail H. Kasimoglui Ian .F. Akyildiz, "Wireless sensor and actor :research challenges.", *(Elsevier) Journal*, 2(38):351-367, 2004.
ii. Sungha Pete Kim Bo-Cheng Charles Lai, David D. Hwang,
iii. "Reducing radio energy consumption of key management protocols for wireless sensor networks," *ACM 1-58113-929-2/04/0008*, 9-11, August 2004.
iv. P.Nair, H.Cam, S.Ozdemir and D. Muthuavinashiappan, "Espda: Energy-efficient and secure pattern based data aggregation for wireless sensor networks," *Computer Communications IEEE Sensors*, 29:446-455, 2006.
v. Jonathan Jen-Rong Chen, Prasan Kumar Sahoo and Ping-Tai Sun, "Efficient security mechanisms for the distributed wireless sensor networks," *Proceedings of the IEEE Third International Conference on Information Technology and Applications (ICITA'05)*, pages 0-7695-2316-1, 2005.
vi. Vijay Garg, M.S. Meitei, S. Raman, A. Kumar, N. Tewari and R.K. Ghosh. *"Ad hoc networks"*, pages 168-185, 2006.
vii. Debao Xiao Meijuan Wei Ying Zhou, "Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks,", *"Industrial Electronics and Applications, 2006 1ST IEEE Conference,"*, pages 1-4, May 2006.
viii. Feng Zhao, Leonidas J. Guibas, *"Wireless sensor networks, An information processing approach"*, ELSEVIER (Morgan Kaufmann Publications), 2003.