

A Survey On Routing Protocols In Wireless Sensor Network

Shakeel Ahmed

CVR College of Engineering, Department of ECE., Ibrahimpatan, R.R.District, A.P., India

Email: shakeel_be@yahoo.com

Abstract—The recent advances and the convergence of micro electro-mechanical systems technology, integrated circuit technologies, microprocessor hardware and nano technology, wireless communications, Ad-hoc networking routing protocols, distributed signal processing, and embedded systems have made the concept of Wireless Sensor Networks (WSNs). Sensor network nodes are limited with respect to energy supply, restricted computational capacity and communication bandwidth. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture. To prolong the lifetime of the sensor nodes, designing efficient routing protocols is critical. Even though sensor networks are primarily designed for monitoring and reporting events, since they are application dependent, a single routing protocol cannot be efficient for sensor networks across all applications. In this paper, the design issues of sensor networks and a classification and comparison of routing protocols is presented. This paper reveals the important features that need to be taken into consideration while designing and evaluating new routing protocols for sensor networks.

Index Terms—Sensor Network, Routing Protocols.

I. INTRODUCTION

Sensor networks have emerged as a promising tool for monitoring (and possibly actuating) the physical world, utilizing self-organizing networks of battery-powered wireless sensors that can sense, process and communicate. In sensor networks, energy is a critical resource, while applications exhibit a limited set of characteristics. Thus, there is both a need and an opportunity to optimize the network architecture for the applications in order to minimize resource consumed. The requirements and limitations of sensor networks make their architecture and protocols both challenging and divergent from the needs of traditional Internet architecture.

A sensor network is a network of many tiny disposable low power devices, called nodes, which are spatially distributed in order to perform an application-oriented global task. These nodes form a network by communicating with each other either directly or through other nodes. One or more nodes among them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired networks. The primary component of the network is the sensor, essential for monitoring real world physical conditions such as sound, temperature, humidity, intensity, vibration,

pressure, motion, pollutants etc. at different locations. The tiny sensor nodes, which consist of sensing, on board processor for data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Figure 1 shows the structural view of a sensor network in which sensor nodes are shown as small circles. Each node typically consists of the four components: sensor unit, central processing unit (CPU), power unit, and communication unit. They are assigned with different tasks. The sensor unit consists of sensor and ADC (Analog to Digital Converter). The sensor unit is responsible for collecting information as the ADC requests, and returning the analog data it sensed. ADC is a translator that tells the CPU what the sensor unit has sensed, and also informs the sensor unit what to do. Communication unit is tasked to receive command or query from and transmit the data from CPU to the outside world. CPU is the most complex unit. It interprets the command or query to ADC, monitors and controls power if necessary, processes received data, computes the next hop to the sink, etc.

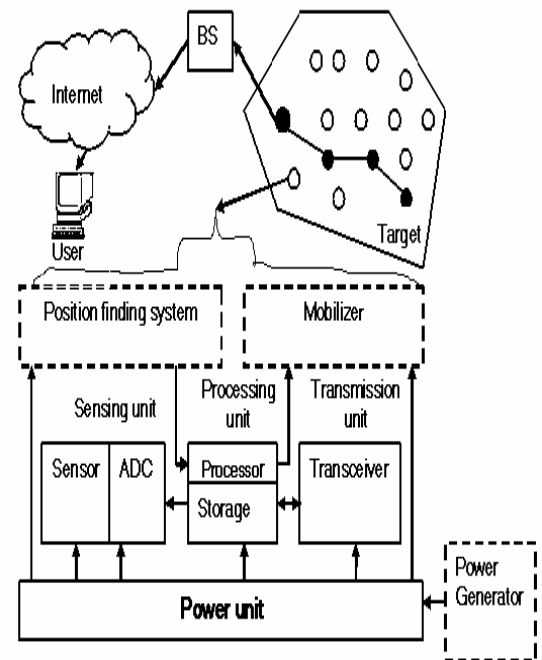


Figure 1: Structural view of sensor network

Power unit supplies power to sensor unit, processing unit and communication unit. Each node may also consist of the two optional components namely Location finding system and Mobilizer. If the user requires the knowledge of location with high accuracy then the node should push Location finding system and Mobilizer may be needed to move sensor nodes when it is required to carry out the assigned tasks.

II. COMPARISON OF MANETS AND SENSOR NETWORKS

MANETS (Mobile Ad-hoc NETWORKS) and sensor networks are two classes of the wireless Adhoc networks with resource constraints. MANETS typically consist of devices that have high capabilities, mobile and operate in coalitions. Sensor networks are typically deployed in specific geographical regions for tracking, monitoring and sensing. Both these wireless networks are characterized by their ad hoc nature that lack pre deployed infrastructure for computing and communication. Both share some characteristics like network topology is not fixed, power is an expensive resource and nodes in the network are connected to each other by wireless communication links. WSNs differ in many fundamental ways from MANETS as mentioned below.

- Sensor networks are mainly used to collect information while MANETS are designed for distributed computing rather than information gathering.
- Sensor nodes mainly use broadcast communication paradigm whereas most MANETS are based on point-to-point communications.
- The number of nodes in sensor networks can be several orders of magnitude higher than that in MANETS.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.
- Sensor nodes are much cheaper than nodes in a MANET and are usually deployed in thousands.
- Sensor nodes are limited in power, computational capacities, and memory where as nodes in a MANET can be recharged somehow.
- Usually, sensors are deployed once in their lifetime, while nodes in MANET move really in an Ad-hoc manner.
- Sensor nodes are much more limited in their computation and communication capabilities than their MANET counterparts due to their low cost.

III. APPLICATIONS OF SENSOR NETWORKS

In the recent past, wireless sensor networks have found their way into a wide variety of applications and systems with vastly varying requirements and characteristics. The

sensor networks can be used in Disaster Relief, Emergency Rescue operation, Military, Habitat Monitoring, Health Care, Environmental monitoring, Home networks, detecting chemical, biological, radiological, nuclear, and explosive material etc.

IV. CLASSIFICATION OF ROUTING PROTOCOLS

The design space for routing algorithms for WSNs is quite large and we can classify the routing algorithms for WSNs in many different ways. Routing protocols are classified as

1. Node centric,
2. Data-centric, or location-aware (geo-centric) and
3. QoS based routing protocols.

Most Ad-hoc network routing protocols are node-centric protocols where destinations are specified based on the numerical addresses (or identifiers) of nodes. In WSNs, node centric communication is not a commonly expected communication type. Therefore, routing protocols designed for WSNs are more data-centric or geocentric. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. Here data is usually transmitted from every sensor node within the deployment region with significant redundancy. In location aware routing nodes know where they are in a geographical region. Location information can be used to improve the performance of routing and to provide new types of services. In QoS based routing protocols data delivery ratio, latency and energy consumption are mainly considered. To get a good QoS (Quality of Service), the routing protocols must possess more data delivery ratio, less latency and less energy consumption.

Routing protocols can also be classified based on whether they are reactive or proactive. A proactive protocol sets up routing paths and states before there is a demand for routing traffic. Paths are maintained even there is no traffic flow at that time. In reactive routing protocol, routing actions are triggered when there is data to be sent and disseminated to other nodes. Here paths are setup on demand when queries are initiated.

Routing protocols are also classified based on whether they are destination-initiated (Dst-initiated) or source-initiated (Src-initiated). A source-initiated protocol sets up the routing paths upon the demand of the source node, and starting from the source node. Here source advertises the data when available and initiates the data delivery. A destination initiated protocol, on the other hand, initiates path setup from a destination node.

Routing protocols are also classified based sensor network architecture. Some WSNs consist of homogenous nodes, whereas some consist of heterogeneous nodes. Based on this concept we can classify the protocols whether they

are operating on a flat topology or on a hierarchical topology. In Flat routing protocols all nodes in the network are treated equally. When node needs to send data, it may find a route consisting of several hops to the sink. A hierarchical routing protocol is a natural approach to take for heterogeneous networks where some of the nodes are more powerful than the other ones. The hierarchy does not always depend on the power of nodes. In Hierarchical (Clustering) protocols different nodes are grouped to form clusters and data from nodes belonging to a single cluster can be combined (aggregated). The clustering protocols have several advantages like scalable, energy efficient in finding routes and easy to manage.

V. DESIGN ISSUES OF ROUTING PROTOCOLS

Initially WSNs was mainly motivated by military applications. Later on the civilian application domain of wireless sensor networks have been considered, such as environmental and species monitoring, production and healthcare, smart home etc. These WSNs may consist of heterogeneous and mobile sensor nodes, the network topology may be as simple as a star topology; the scale and density of a network varies depending on the application. To meet this general trend towards diversification, the following important design issues of the sensor network have to be considered.

A. Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures.

B. Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds, thousands or more and routing schemes must be scalable enough to respond to events.

C. Production Costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks and hence the cost of each sensor node has to be kept low.

D. Operating Environment

We can set up sensor network in the interior of large machinery, at the bottom of an ocean, in a biologically or chemically contaminated field, in a battle field beyond the enemy lines, in a home or a large building, in a large warehouse, attached to animals, attached to fast moving vehicles, in forest area for habitat monitoring etc.

E. Power Consumption

Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi-hop routing will consume less energy than direct communication. However, multi-hop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink. Sensor nodes are equipped with limited power source (<0.5 Ah 1.2V). Node lifetime is strongly dependent on its battery lifetime.

F. Data Delivery Models

Data delivery models determine when the data collected by the node has to be delivered. Depending on the application of the sensor network, the data delivery model to the sink can be Continuous, Event driven, Query-driven and Hybrid. In the continuous delivery model, each sensor sends data periodically. In event-driven models, the transmission of data is triggered when an event occurs. In query driven models, the transmission of data is triggered when query is generated by the sink. Some networks apply a hybrid model using a combination of continuous, event-driven and query driven data delivery.

G. Data Aggregation/Fusion

Since sensor nodes might generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the combination of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average. As computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation. This technique has been used to achieve energy efficiency and traffic optimization in a number of routing protocols

H. Quality of Service (QoS)

The quality of service means the quality service required by the application, it could be the length of life time, the data reliable, energy efficiency, and location-awareness, collaborative-processing. These factors will affect the selection of routing protocols for a particular application. In some applications (e.g. some military applications) the data should be delivered within a certain period of time from the moment it is sensed.

I. Data Latency and Overhead

These are considered as the important factors that influence routing protocol design. Data aggregation and multi-hop relays cause data latency. In addition, some routing protocols create excessive overheads to implement their algorithms, which are not suitable for serious energy constrained networks.

J. Node Deployment

Node deployment is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths. However in self organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an Ad-hoc manner. In that infrastructure, the position of the sink or the cluster head is also crucial in terms of energy efficiency and performance. When the distribution of nodes is not uniform, optimal positioning of cluster head becomes a pressing issue to enable energy efficient network operation.

VI. COMPARISON OF ROUTING PROTOCOLS

In this paper following routing protocols are compared according their design characteristics.

- SPIN: Sensor Protocols for Information via Negotiation.
- DD: Directed Diffusion
- RR: Rumor Routing
- GBR: Gradient Based Routing.
- CADR: Constrained Anisotropic Diffusion Routing.
- COUGAR
- ACQUIRE: ACTIVE QUery forwarding In sensoR nEtworks
- LEACH: Low Energy Adaptive Clustering Hierarchy.
- TEEN & APTEEN: [Adaptive] Threshold sensitive Energy Efficient sensor Network.
- PEGASIS: The Power-Efficient GATHERing in Sensor Information Systems.
- VGA: Virtual Grid Architecture Routing.
- SOP: Self Organizing Protocol.
- GAF: Geographic Adaptive Fidelity.
- SPAN
- GEAR: Geographical and Energy Aware Routing
- SAR: Sequential Assignment Routing.
- SPEED: A real time routing protocol.

Table I. represents Classification and Comparison of routing protocols in WSNs. This table is based on the survey of [1] & [2] and modified according to application requirements.

Routing Protocols	Classification	Power Usage	Data Aggregation	Scalability	Query Based	Over head	Data delivery model	QoS
SPIN	Flat / Src-initiated / Data-centric	Ltd	Yes	Ltd	Yes	Low	Event driven	No
DD	Flat/ Data-centric/ Dst-initiated	Ltd	Yes	Ltd	Yes	Low	Demand driven	No
RR	Flat	Low	Yes	Good	Yes	Low	Demand driven	No
GBR	Flat	Low	Yes	Ltd	Yes	Low	Hybrid	No
CADR	Flat	Ltd		Ltd	Yes	Low	Continuously	No
COUGAR	Flat	Ltd	Yes	Ltd	Yes	High	Query driven	No
ACQUIRE	Flat/ Data-centric	Low	Yes	Ltd	Yes	Low	Complex query	No
LEACH	Hierarchical/ Dst-initiated /Node-centric	High	Yes	Good	No	High	Cluster-head	No
TEEN & APTEEN	Hierarchical	High	Yes	Good	No	High	Active threshold	No
PEGASIS	Hierarchical	Max	No	Good	No	Low	Chains based	No
VGA	Hierarchical	Low	Yes	Good	No	High	Good	No
SOP	Hierarchical	Low	No	Good	No	High	Continuously	No
GAF	Hierarchical / Location	Ltd	No	Good	No	Mod	Virtual grid	No
SPAN	Hierarchical / Location	Ltd	Yes	Ltd	No	High	Continuously	No
GEAR	Location	Ltd	No	Ltd	No	Mod	Demand driven	No
SAR	Data centric	High	Yes	Ltd	Yes	High	Continuously	Yes
SPEED	Location/Data centric	Low	No	Ltd	Yes	Less	Geographic	Yes

Table I. Classification and Comparison of routing protocols in WSNs.

CONCLUSION

WSNs have opened the doors to many applications. WSNs are limited with respect to energy supply, restricted computational capacity and communication bandwidth. One of the factor which effects the performance of the WSN is the routing protocol. Thus, designing efficient routing protocol is critical. Its time that designers pay attention to several parameters, one of them being QOS.

REFERENCES

- [1] J. C. Castillo, T. Olivares and L. Orozco, "Routing Protocols for WSNs," in *Proc. Research Institute of Informatics, SPAIN, 2008*.
- [2] S. Misra et al. (eds.), *Guide to Wireless Sensor Networks*, Computer Communications and Networks,
- [3] DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.
- [4] Jamal N. Al-daraki, Ahmed E. Kamal, "Routing Techniques in WSNs," Iowa State University, Ames, 2000.