International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 4, ISSN (Online) 2249 –071X, ISSN (Print): 2278 – 4209

Study of Routing Algorithms in Wireless Sensor Networks

P. Asha
M.Tech.,
Pydah college of Engineering and Technology, Kakinada, A.P., India

A. Kamala Priya Assistant Professor, Dept. of CSE, Pydah College of Engineering and Technology, Kakinada, A.P., India

P. Suresh Babu
Assistant Professor, Kaushik College of Engineering, Visakhapatnam, A.P., India

***Abstract* — Wireless sensor networking is an emerging technology that promises a wide range of potential applications in both civilian and military areas. A wireless sensor network (WSN) typically consists of a large number of low - cost, low - power, and multifunctional sensor nodes that are deployed in a region of interest. These sensor nodes are small in size but are equipped with sensors, embedded microprocessors, and radio transceivers. Therefore, they have not only sensing, but also data processing and communicating capabilities. The main task of wireless sensor nodes is to sense and collect data from a target domain, process the data, and transmit the information back to specific sites where the underlying application resides. Achieving this task efficiently requires the development of an energy-efficient routing protocol to set up paths between sensor nodes and the data sink. The path selection must be such that the lifetime of the network is maximized. The characteristics of the environment within which sensor nodes typically operate, coupled with severe resource and energy limitation, make the routing problem very challenging. This paper presents an overview of routing algorithms in wireless sensor networks.**

***Index Terms* — LEACH, Routing, Sensor network, SPIN.**

I. Introduction

The need to monitor and measure various physical phenomena (e.g. temperature, fluid levels, vibration, strain, humidity, acidity, pumps, generators to manufacturing lines, aviation, building maintenance and so forth) is common to many areas including structural engineering, agriculture and forestry, healthcare, logistics and transportation, and military applications. Wired sensor networks have long been used to support such environments and, until recently, wireless sensors have been used only when a wired infrastructure is infeasible, such as in remote and hostile locations. But the cost of installing, terminating, testing, maintaining, trouble-shooting, and upgrading a wired network makes wireless systems potentially attractive alternatives for general scenarios. A wireless sensor network (WSN) [1][2] consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration , pressure , humidity, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Figure 1 shows an example of a wireless sensor network.

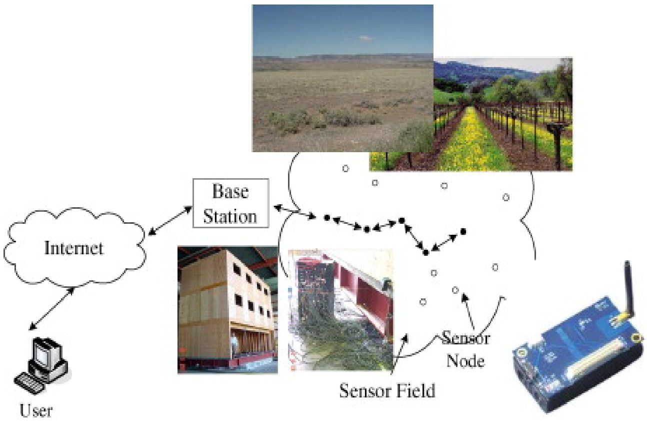

Fig.1 : Wireless sensor network example

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

The main task of wireless sensor nodes is to sense and collect data from a target domain, process the data, and transmit the information back to specific sites where the underlying application resides. Achieving this task efficiently requires the development of an energy-efficient routing protocol to set up paths between sensor nodes and the data sink. The path selection must be such that the lifetime of the network is maximized. The characteristics of the environment within which sensor nodes typically operate, coupled with severe resource and energy limitation, make the routing problem very challenging. This paper presents an overview of routing algorithms in wireless sensor networks. This paper is organized as follows: Section 2 presents data- centric algorithms. Section 3 presents

Copyright © 2012 IJECCE, All right reserved

cluster- based algorithms. Section 4 presents location-based algorithms. Section 5 presents random routing algorithms. And finally section 6 presents the conclusion.

II. Data Centric Algorithms

Data-centric algorithms[3][4] are based on the specifics of data. Schemes like directed diffusion, sensor protocols for information via negotiation (SPIN) and power aware many-to-many routing fall into this category.

A. Directed Diffusion

In directed diffusion the data-collecting node, called the sink, sends out interest, which is a task description, to all sensors, as shown in Figure 2(a). The task descriptors are named by assigning attribute-value pairs that describe the task. Each sensor node stores the interest entry in its cache. The interest entry contains a timestamp field and several gradient fields. As the interest is propagated throughout the sensor network, the gradients from the source back to the sink are set up. When the source has data for the interest, the source sends the data along the interest's gradient path, as shown in Figure 2(b).

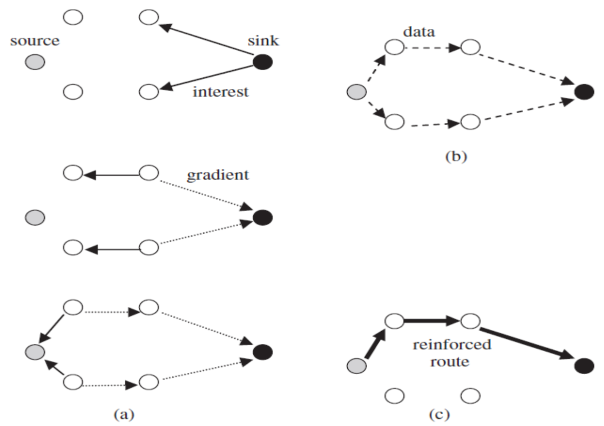

Fig.2: Directed diffusion (a) interest dissemination; (b) data dissemination; (c) route reinforcement

The interest and data propagation and aggregation are determined locally. Also, the sink must refresh the interest and reinforce one of the paths when it starts receiving data from the source. When one of the paths is reinforced(Figure 2(c)) by the sink, the source node starts sending the packets only through the reinforced path but not all the available gradients. Note that directed diffusion is based on data-centric routing where the sink broadcasts the interest.

B. Sensor Protocols for Information via Negotiation (SPIN)

SPIN is a family of adaptive protocols based on the idea that sensor nodes operate more efficiently and conserve energy by sending data that describe the sensor data instead of sending the whole data, unless the whole data are explicitly requested. SPIN has three types of message: ADV, REQ and DATA. Before sending a DATA message, a sensor broadcasts an ADV message containing a descriptor, i.e. meta-data, of the DATA. If a neighbor is interested in the data, it sends a REQ message for the DATA and DATA is sent to this neighbor sensor node. The neighbor sensor node then repeats this process, as illustrated in Figure 3. As a result, the nodes that are interested in the data will get a copy.

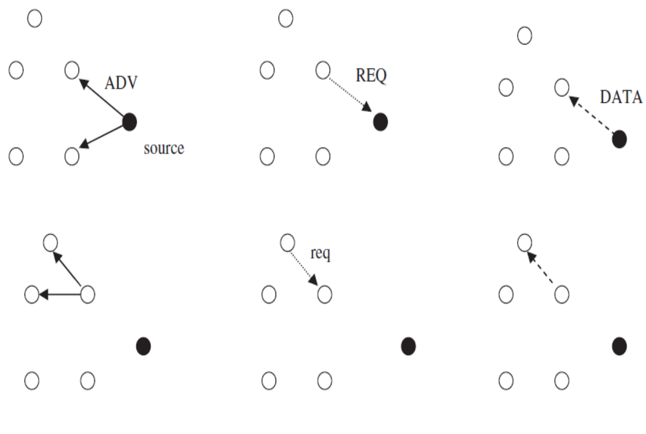

Fig.3: SPIN

C. Power-Aware Many-to-Many Routing (PAMR)

PAMR is designed for sensor and actuator networks where sensors send their data directly to the interested actuators, and both power and delay are considered in the routing decisions. In PAMR, actuators register their interest in data with the nodes in the sensor network by broadcasting a registration message. A registration message includes fields such as node identification (node_id), actuator identification (actuator_id), echelon, minimum power available (minPA), total power available (totalPA) and task(s). Node_id is the identification of the sending node. When an actuator broadcasts a registration message, it initializes the node_id field with its own id, and the nodes that repeat the message update this field. Every node that repeats a registration message replaces the node_id field with its own id. Echelon means the minimum number of hops required to reach a node from an actuator. The totalPA is found by summing up the power available in every node along the route. The minPA is the power available in the node that has minimum power along the route. A node that relays a registration message adds its power available (ownPA) to the totalPA. It also replaces the minPA field with its ownPA if the ownPA is lower than the minPA value. Before transmitting the registration message, the actuator initializes the echelon and totalPA as 0 and the minPA as the maximum possible PA value.

Sensor nodes do not repeat all the received registration messages. They first check if the registration message is for a new route. A route that meets one of the following criteria is a new route:

- The registration table does not have any entry for the actuator in the registration message.
- The registration table has at least one entry for the actuator, but none of these entries for the actuator is from the uplink node in the registration message.
- The registration table has an entry for the actuator and uplink node in the registration message;

Copyright © 2012 IJECCE, All right reserved

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 4, ISSN (Online) 2249 –071X, ISSN (Print): 2278 – 4209

however, at least one of the tasks in the message is not indicated in the related registration table entry.

III. CLUSTER BASED ALGORITHMS

Low-energy adaptive clustering hierarchy (LEACH) is an example of a cluster-based sensor network routing algorithm[3][4].

A. Low-energy adaptive clustering hierarchy

LEACH is a clustering-based protocol that minimizes energy dissipation in sensor networks. The purpose of LEACH is to select sensor nodes randomly as cluster heads, so the high energy dissipation in communicating with the base station is spread to all sensor nodes in the sensor network. The operation of LEACH is separated into two phases: the set-up phase and the steady phase. The duration of the steady phase is longer than the duration of the set-up phase in order to minimize the overhead.

During the set-up phase, a sensor node *n* chooses a random number between 0 and 1. If this random number is less than a predetermined threshold, *t*, the sensor node becomes a cluster head. The threshold *t* is calculated as:

$$t = \begin{cases} \dfrac{P}{1 - P \times [r \bmod 1/P]} & \text{if } n \in G \\ 0 & \text{otherwise} \end{cases}$$

In this equation *P* is the desired percentage to become a cluster head, *r* is the current round and *G* is the set of nodes that have not been selected as a cluster head in the last 1/*P* rounds. After a node is self-selected as a cluster head, it advertises this to all its neighbors. The sensor nodes receive advertisements and they determine the cluster that they want to belong to, based on the signal strength of the advertisements from the cluster heads. The sensor nodes inform their cluster head that they will be a member of the cluster, and then the cluster head assigns a time slot for every sensor node in which they can send data to the cluster head.

During the steady phase, the sensor nodes can begin sensing and transmitting data to the cluster heads. The cluster heads also aggregate data from the nodes in their cluster before sending them to the base station. After a certain period of time spent in the steady phase, the network goes into the set-up phase again.

IV. LOCATION BASED ROUTING ALGORITHMS

Geographic Adaptive Fidelity (GAF) is an example of location – based routing algorithm[3][4].

A. Geographic Adaptive Fidelity (GAF)

Geographic Adaptive Fidelity or GAF[5] is an energy-aware location-based routing algorithm designed primarily for mobile ad hoc networks, but is used in sensor networks as well. This protocol aims at optimizing the performance of wireless sensor networks by identifying equivalent nodes with respect to forwarding packets. In GAF protocol, each node uses location information based on GPS to associate itself with a "virtual grid" so that the entire area is divided into several square grids, and the node with the highest residual energy within each grid becomes the master of the grid. Two nodes are considered to be equivalent when they maintain the same set of neighbor nodes and so they can belong to the same communication routes. Source and destination in the application are excluded from this characterization.

Nodes use their GPS-indicated location to associate itself with a point in the virtual grid. Inside each zone, nodes collaborate with each other to play different roles. For example, nodes will elect one sensor node to stay awake for a certain period of time and then they go to sleep. This node is responsible for monitoring and reporting data to the sink on behalf of the nodes in the zone and is known as the master node. Other nodes in the same grid can be regarded as redundant with respect to forwarding packets, and thus they can be safely put to sleep without sacrificing the "routing fidelity" (or routing efficiency). The slave nodes switch between off and listening with the guarantee that one master node in each grid will stay awake to route packets. For example, nodes 2, 3 and 4 in the virtual grid B in Fig 4 are equivalent in the sense that one of them can forward packets between nodes 1 and 5 while the other two can sleep to conserve energy. Hence, GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity. Each node uses its GPS-indicated location to associate itself with a point in the virtual grid.

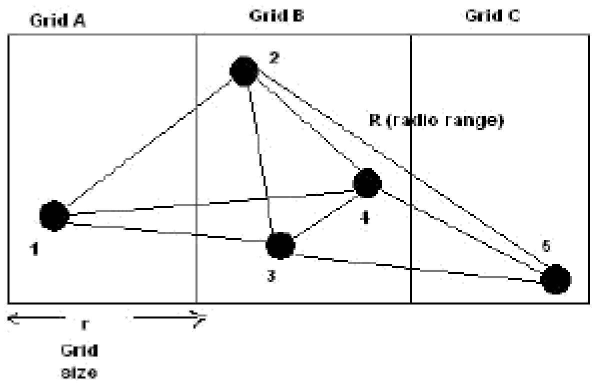

Fig.4: Virtual grid structure in the GAF protocol

V. RANDOM ROUTING ALGORITHMS

A. Purely Random Propagation (PRP)

In PRP[6], information shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all the nodes that are within its receiving range. When a source node wants to send information shares to the sink, it includes a TTL of initial value *N* in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its

Copyright © 2012 IJECCE, All right reserved

neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing this share towards the sink using normal min-hop routing.

B. Non-repetitive Random Propagation(NRRP)

NRRP[6] is based on PRP, but it improves the propagation efficiency by recording all the nodes that the propagation has traversed so far. More specifically, NRRP adds a "node-in-route" (NIR) field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the up-stream node is appended to the share's NIR field. Nodes included in NIR are excluded from the random pick of the next hop of propagation. This nonrepetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

C. Directed Random Propagation(DRP)

DRP[6] improves the propagation efficiency by using two-hop neighborhood information. More specifically, DRP adds a "last-hop neighbor list" (LHNL) field to the header of each share. Before a share is propagated to the next node, the relaying node first replaces the old content in the LHNL field of the share by its neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list, and randomly picks one node from its neighbors that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, and so on. Whenever the LHNL fully overlaps with or contains the relaying node's neighbor list, a random neighbor is drawn, just as in the case of the PRP scheme. According to this propagation method, DRP reduces the chance of propagating a share back and forth by eliminating this type of propagation within any two immediate consecutive steps. Compared with PRP, DRP attempts to push a share outward away from the source, and thus leads to better propagation efficiency for a given TTL value.

VI. CONCLUSION

A wireless sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or an information technology (IT) framework. The main task of wireless sensor nodes is to sense and collect data from a target domain, process the data, and transmit the information back to specific sites where the underlying application resides. Achieving this task efficiently requires the development of an energy-efficient routing protocol to set up paths between sensor nodes and the data sink. Several routing algorithms exist. Some of them are data- centric, cluster- based, location- based and random routing algorithms.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks" International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, vol. 1, issue no. 2, pp. 85-95.

[3] S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[4] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith. Parametric probabilistic sensor network routing. In *Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA)*, pages 122–131, 2003.

[5] Y. Xu, J. Heidemann, D. Estrin,\Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking 2001, pp. 70-84.

[6] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking*, 15(6):1490–1501, Dec. 2007.

AUTHORS PROFILE

P. Asha
Pursuing her M.Tech from Pydah College of Engineering & Technology, Kakinada, A.P., India. Her research interest includes Computer Networks, Wireless Sensor Networks and Network Security.

A. Kamala Priya
Working as Asst. Professor in Pydah College of Engineering & Technology, Kakinada, A.P., India. Her research interest includes Computer Networks, Wireless Sensor Networks and Network Security.

P. Suresh Babu
Working as Asst. Professor in Kaushik College of Engineering, Visakhapatnam, A.P., India. His research interest includes Data Mining, Database Management System and Computer Networks.