A Research Review on Wireless Sensor Techniques

Shefali Thakur¹, Saurabh Sharma²
¹,² Sri Sai University Palampur

Abstract: With the more quickly developing in hardware industry, little economical battery fuelled remote sensors have had an effect on the correspondences with the physical world. The Wireless Sensor Networks (WSN) comprises of many sensor hubs which are asset obliged. WSN hubs screen different physical and ecological conditions agreeably. WSN utilizes different hubs for the correspondence. WSN has turned into one of the intrigued territories in the field of exploration from most recent couple of years. To upgrade the lifetime of the entire systems vitality decrease is the essential thought for outline and investigate of the bunching and directing conventions. This paper portrays the investigation of different vitality proficient steering conventions in WSNs which are essential for their outlining reason in order to meet the different asset imperatives.

Keywords: Wireless sensor network, clustering, Network lifetime, Energy efficient, Routing Protocols, Cluster Head.

I. INTRODUCTION

Wireless sensor network (WSN) is broadly considered as a standout amongst the most critical advances for the twenty-first century [1]. In the previous decades, it has gotten colossal consideration from both the academia and industry everywhere throughout the world. A WSN regularly comprises of a substantial number of minimal effort, low-control, and multifunctional wireless sensor nodes, with sensing, wireless communications and reckoning abilities [2,3]. A wireless sensor network is an ad-hoc infrastructure of sensing, communicating elements that gives the ability of observing, reacting in specific environment. The environment can be an information technology framework, the physical world or a biological system. This paper describes the study of various energy efficient routing protocols in WSNs which are important for their designing purpose so as to meet the various resource constraints. Routing in WSNs is extremely difficult task due to the inherent qualities that recognize these systems from different other wireless networks like mobile ad hoc networks or cellular systems. Networking unattended sensor nodes may have profound effect on the efficiency of many military and civil applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management.

II. NETWORK DESIGN OBJECTIVES

Most sensor networks are application particular and have diverse application prerequisites. In this manner, all or part of the accompanying principle plan targets is considered in the configuration of sensor systems:

A. Small node size
   Since sensor nodes are generally conveyed in a brutal or unfriendly environment in extensive numbers, reducing node size can encourage node arrangement. It will likewise decrease the power utilization and expense of sensor nodes.

B. Low node cost
   Since sensor nodes are generally conveyed in a cruel or threatening environment in huge numbers and can't be reused, decreasing expense of sensor nodes is imperative and will come about into the expensediminishment of entire syste

C. Low power utilization
   Since sensor nodes are powered by battery and it is regularly extremely troublesome or even difficult to charge or energize their batteries, it is significant to decrease the power utilization of sensor nodes such that the lifetime of the sensor nodes, additionally The entire system is delayed.

D. Reliability
   Network protocols intended for sensor networks must give error control and remedy mechanisms to guarantee reliable information conveyance over noisy, error-prone, and time-varying wireless channels.
E. Fault tolerance

Sensor nodes are inclined to disappointments because of harsh organization situations and unattended operations. In this manner, sensor nodes ought to be fault tolerant and have the capacity of self-testing, adjusting toward oneself, repairing toward oneself, and recovering toward oneself.

F. Security

A sensor network ought to acquaint effective security mechanisms to prevent the data information in the network or a sensor node from unapproved access or malicious attacks.

G. QoS support

In sensor networks, different applications may have different quality-of-service (QoS) requirements in terms of delivery latency and packet loss. Thus, network protocol design should consider the QoS requirements of specific applications.

III. ROUTING CHALLENGES AND DESIGN ISSUES IN WSNS

In spite of the incalculable utilizations of WSNs, these systems have a few confinements, e.g., constrained energy supply, restricted processing power, and restricted bandwidth of the wireless connections joining sensor nodes. One of the principle outline objectives of WSNs is to complete information correspondence while attempting to delay the lifetime of the system and prevent connectivity degradation by utilizing aggressive energy management techniques. The outline of routing protocols in WSNs is affected by numerous testing variables. These elements must be overcome before productive correspondence can be attained to in WSNs. We condense a portion of the steering difficulties and outline issues that influence routing process in WSNs.

A. Node deployment

Node deployment in WSNs is application dependent and influences the execution of the routing protocol. The deployment can be either deterministic or randomized. In deterministic organization, the sensors are manually placed and information is directed through pre-determined ways. On the other hand, in arbitrary node deployment, the sensor nodes are scattered haphazardly making a base in a specially appointed way.

B. Energy consumption without losing accuracy

Sensor nodes can go through their constrained supply of energy performing calculations and transmitting information in a wireless environment. As such, energy-conserving forms of communication and processing are fundamental. Sensor node lifetime demonstrates an in number reliance on the battery lifetime [4]. In a multihop WSN, each node assumes a double part as information sender and information switch. The breaking down of some sensor nodes because of power failure can result in huge topological changes and may oblige rerouting of packets and rearrangement of the system.

C. Sensor locations

Another test that confronts the configuration of routing protocols is to deal with the areas of the sensors. The vast majority of the proposed conventions expect that the sensors either are outfitted with worldwide situating framework (GPS) beneficiaries or utilize some restriction strategy [5] to find out about their areas.

D. Coverage

In WSNs, every sensor node acquires a certain perspective of nature. A given sensor's perspective of nature is constrained both in extent and in exactness; it can just cover a restricted physical range of the earth. Thus, region scope is additionally an essential configuration parameter in WSNs.

IV. ROUTING PROTOCOLS IN WSNS

In this section, we survey the state-of-the-art routing protocols for WSNs. In general, routing in WSNs can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes positions are exploited to route data in the network.
These protocols can be further classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation. In addition to the above, routing protocols can be classified into three categories, namely, proactive, reactive, and hybrid protocols depending on how the source finds a route to the destination. In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas. When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols.

Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements [6]. Many routing algorithms were developed for wireless networks in general. All major routing protocols proposed for WSNs may be divided into seven categories as shown in Table 1. Some of the protocols are reviewed as follows.

<table>
<thead>
<tr>
<th>CATAGORY</th>
<th>REPRESENTATIVE PROTOCOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location-based Protocols</td>
<td>MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF</td>
</tr>
<tr>
<td>Data-centric Protocols</td>
<td>SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQUIRE, EAD, Information-Directed Routing, Gradient-Based Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination</td>
</tr>
<tr>
<td>Hierarchical Protocols</td>
<td>LEACH, PEGASIS, HEED, TEEN, APTEEN</td>
</tr>
<tr>
<td>Mobility-based Protocols</td>
<td>SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination</td>
</tr>
<tr>
<td>Multipath-based Protocols</td>
<td>Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery</td>
</tr>
<tr>
<td>Heterogeneity-based Protocols</td>
<td>IDSQ, CADR, CHR</td>
</tr>
<tr>
<td>QoS-based protocols</td>
<td>SAR, SPEED, Energy-aware routing</td>
</tr>
</tbody>
</table>

A. Geographic Adaptive Fidelity (GAF)

GAF [15] is primarily proposed for MANETs and is an energy-aware routing protocol, but can also be used for WSNs because it favors energy conservation. The design of GAF is motivated based on an energy model that considers energy consumption due to the reception and transmission of packets as well as idle (or listening) time when the radio of a sensor is on to detect the presence of incoming packets. GAF basically depends on the principle of turning off unwanted sensors while maintaining a fixed level of routing fidelity (or uninterrupted connectivity between communicating sensors).

As shown in Figure 1, the GAF state transition diagram has mainly three states, namely, discovery, active, and sleeping. In the sleeping state of a sensor, then, for energy savings, it turns off its radio. When it enters the discovery state of a sensor, it exchanges discovery messages in the same grid to learn about othersensors. And Even in the active state, a sensor continuously broadcasts its discovery messages about its state to inform equivalent sensors. The total time spent in each one of these following states can be tuned depending on several factors, such as its needs and sensor mobility by the application. GAF’s main motive to maximize the
system lifetime by reaching a state where each grid has only one active sensor based on sensor ranking rules. For example, a sensor in the active state has a higher rank than a sensor in the discovery state. A sensor with longer expected lifetime has a higher rank.

B. Sensor Protocols for Information via Negotiation (SPIN)
SPIN [7] protocol was designed to improve classic flooding protocols and overcome the problems they may cause, for example, implosion and overlap. The SPIN protocols are resource aware and resource adaptive. The sensors running the SPIN protocols are able to compute the energy consumption required to compute, send, and receive data over the network. Thus, they can make informed decisions for efficient use of their own resources. The SPIN protocols have mainly two key mechanisms namely negotiation and resource adaptation. SPIN enables the sensors to negotiate with each other before any data dissemination can occur in order to avoid injecting non-useful and redundant information in the network. SPIN uses meta-data as the descriptors of the data that the sensors want to disseminate. The notion of meta-data avoids the occurrence of overlap given sensors can name the interesting portion of the data they want to get. It may be noted here that the size of the meta-data should definitely be less than that of the corresponding sensor data.

There are two protocols in the SPIN family: SPIN-1 (or SPIN-PP) and SPIN-2 (or SPIN-EC) [7]. While SPIN-1 uses a negotiation mechanism to reduce the consumption of the sensors, SPIN-2 uses a resource-aware mechanism for energy savings. Both protocols allow the sensors to exchange information about their sensed data, thus helping them to obtain the data they are interested in.

C. Directed Diffusion
Directed diffusion [8] is a data-centric routing protocol for sensor query dissemination and processing. It meets the main requirements of WSNs such as energy efficiency, scalability, and robustness. Directed diffusion has various key elements namely data naming, interests and gradients, data propagation, and reinforcement. A sensing capability can be demonstrated by a number of attribute-value pairs. In the directed diffusion process, in the beginning, the sink specifies a low information rate for upcoming events. After that, the sink can reinforce one particular sensor to send events with a higher data rate by resending the original interest message with a smaller interval. Likewise, if a neighboring sensor receives this interest message and finds that the sender's interest has a higher data rate than before, and this data rate is higher than that of any existing gradient, it will reinforce one or more of its neighbours.

D. Rumor Routing
Rumor routing is a logical compromise between query flooding and event flooding app schemes. Rumor routing is an efficient protocol if the number of queries is between the two intersection points of the curve of rumor routing with those of query flooding and event flooding. Rumor routing is based on the concept of agent, which is a long-lived packet that traverses a network and informs each sensor it encounters about the events that it has learned during its network traverse. An agent will travel the network for a certain number of hops and then die.

E. Low-energy adaptive clustering hierarchy (LEACH)
LEACH [9] is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption. In LEACH, the clustering task is rotated among the nodes, based on duration. Direct communication is used by each cluster head (CH) to forward the data to the base station (BS). It uses clusters to prolong the life of the wireless sensor network. LEACH is based on an aggregation (or fusion) technique that combines or aggregates the original data into a smaller size of data that carry only meaningful information to all individual sensors. LEACH divides the network into several cluster of sensors, which are constructed by using localized coordination and control not only to reduce the amount of data that are transmitted to the sink, but also to make routing and data dissemination more scalable and robust. LEACH uses a randomize rotation of high-energy CH position rather than selecting in static manner, to give a chance to all sensors to act as CHs and avoid the battery depletion of an individual sensor and dieing quickly. The operation of LEACH is divided into rounds having two phases each namely (i) a setup phase to organize the network into clusters, CH advertisement, and transmission schedule creation and (ii) a steady-state phase for data aggregation, compression, and transmission to the sink.

F. Disjoint Paths
Sensor-disjoint multipath routing [10] is a multipath protocol that helps find a small number of alternate paths that have no sensor in common with each other and with the primary path. In sensor-disjoint path routing, the primary path is best available whereas the
alternate paths are less desirable as they have longer latency. The disjoint makes those alternate paths independent of the primary path. Thus, if a failure occurs on the primary path, it remains local and does not affect any of those alternate paths. The sink can determine which of its neighbors can provide it with the highest quality data characterized by the lowest loss or lowest delay after the network has been flooded with some low-rate samples. Although disjoint paths are more resilient to sensor failures, they can be potentially longer than the primary path and thus less energy efficient.

G. Braided Paths

Braided multipath [10] is a partially disjoint path from primary one after relaxing the disjointedness constraint. To construct the braided multipath, first primary path is computed. Then, for each node (or sensor) on the primary path, the best path from a source sensor to the sink that does not include that node is computed. Those best alternate paths are not necessarily disjoint from the primary path and are called idealized braided multipaths. Moreover, the links of each of the alternate paths lie either on or geographically close to the primary path. Therefore, the energy consumption on the primary and alternate paths seems to be comparable as opposed to the scenario of mutually tereate and primary paths. The braided multipath can also be constructed in a localized manner in which case the sink sends out a primary-path reinforcement to its first preferred neighbor and alternate-path reinforcement to its second preferred neighbor.

V. CONCLUSION

One of the main challenges in the design of routing protocols for WSNs is energy efficiency due to the scarce energy resources of sensors. The ultimate objective behind the routing protocol design is to keep the sensors operating for as long as possible, thus extending the network lifetime. The energy consumption of the sensors is dominated by data transmission and reception. Therefore, routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors, and hence the network lifetime. In this paper, we have surveyed a sample of routing protocols by taking into account several classification criteria, including location information, network layering and in-network processing, data centricity, path redundancy, network dynamics, QoS requirements, and network heterogeneity. For each of these categories, we have discussed a few example protocols.

REFERENCES