Study and Review of Routing protocols for wireless sensor networks

Hiral Patel
Computer Science & Engineering Department, Parul Institute of Technology.

Prof. Neha Pandya
Assistant Professor in IT Department, Parul Institute of Technology.

Abstract

For sensing environment, wireless sensor networks consist of huge number of low-cost, low-power and small nodes which have restriction on memory, power and computation resources. These nodes are sometime deployed in unfriendly environment where they can be tempered or physically not accessible. Topology of wireless sensor network remain changing as nodes can be added and deleted from network at any time and it is biggest challenge in developing routing algorithm for wireless sensor network. In this paper we have presented some of routing protocols and algorithms available for wireless sensor network and shown comparison of them.

Keywords: Wireless sensor network (WSN), Routing Protocol.

1. Introduction

A Wireless Sensor Networking Concepts Wireless sensor networks (WSNs) have been suggested to provide a practical and economically viable approach to data gathering within locations which are difficult or prohibitively expensive to monitor via human activity [1]. The conventional wireless sensor network design consists of a set of homogeneous nodes with embedded sensors, a fixed-capacity energy source, and short-range radio transceivers. The nodes collaborate to relay information from their peers via multi-hop routing to a central sink node, at which the data can be processed and analyzed. Further extensions include the possibility of aggregating and combining this data on route. The original roots of wireless sensor network proposals lay in military research assisted by DARPA [2], and tactical deployment of a WSN offers the possibility of gaining intelligence within a region of terrain. As an example, in areas in which hostile elements operate, it is likely that the ability to survey rapidly and widely the movements of enemy troops would give a key advantage to those defending. The detection and relaying capabilities of a future wireless sensor network built upon dedicated nodes together with nodes integrated into infrastructure offer this possibility. However, in a deployment framework which implicitly assumes the presence of hostile elements, it is possible that these malicious attackers could attempt to subvert or interfere with the network itself, which implies that security of the network system and its protocols will be a fundamental requirement.

Some common applications of sensor networks are:

• Military applications such as battlefield surveillance, nuclear, biological and chemical (NBC) attack detection, and reconnaissance over enemy territory.

• Environmental applications such as wild animal tracking, air and water pollution level monitoring, forest fire detection and precision agriculture.

• Health applications such as heart rate monitoring, telemedicine and drug administration.

• Commercial applications such as highway traffic analysis, building security, structural fault detection, and power consumption measurement.

In spite of these similarities, sensor networks differ from traditional embedded wireless networks in many ways [7], some of them being:

• The scale of sensor networks is often orders of magnitude larger than that of traditional wireless networks. There may be tens of thousands of nodes in a sensor network, as compared to a few tens of nodes in a normal wireless network.

• Sensor networks are often densely and redundantly deployed, i.e. the number of nodes deployed per unit area is much greater than traditional wireless networks.

• Sensor networks are *dynamic* in the sense that nodes can get added to and deleted from the network without manual intervention, resulting in the expansion and contraction of the network after deployment.

• Sensor networks can be deployed in hostile territory, where they can be subject to communication surveillance and node capture and compromise by adversaries.

• Sensor nodes mainly use broadcast communication paradigms whereas traditional wireless networks mostly use point-to-point communication. The motivation for this paradigm shift is that in sensor networks, the focus is on the retrieval of data by attributes, and hence the individual nodes do not matter and are redundantly deployed.

Although many protocols and algorithms have been proposed for traditional wireless ad-hoc networks, they are not well suited to the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad-hoc networks are:

• The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad-hoc network Sensor nodes are densely deployed.

• Sensor nodes are prone to failures.

• The topology of a sensor network changes very frequently.

• Sensor nodes mainly use a broadcast communication paradigm, whereas most ad-hoc networks are based on point to point communication

• Sensor nodes are limited in power, computational capacities, and memory.

• As illustrated above, the communication between the sensor nodes in WSN are generally restricted due to battery size, memory size by node size, processing capacity, and communication distance between sensor nodes. Therefore, the communication between sensor nodes requires considering of maximizing energy efficiency, improving the reliability of packet transmission, reducing the complexity of algorithms besides basic function of routing [8, 9, 10].

• Routing considering energy efficiency - this can be understood from two views. One is reducing energy consumption itself through transmitting data according to a shortest path. The other is evenly distributing energy consumption. According to the application characteristics, the different approach is required.

• Routing considering reliable data transmission - the accurate and resilient data transmission is considered more importantly rather than energy efficiency. Multipath routing is often used to enhance the reliability of WSNs.

2. Routing in WSN

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 [3]. 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 I. We review some sample routing protocols in each of the categories in preceding sub-sections

Table I (Routing Protocols for WSNs)

Category	Representative Protocols
Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
Data-centric Protocols	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
Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination
Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery
Heterogeneity-based Protocols	IDSQ, CADR, CHR
QoS-based protocols	SAR, SPEED, Energy-aware routing

The lifetime of a fully active sensor node is of the order of a few days. The most energy intensive operations for a node are those of radio transmission and reception. It is found that the energy consumed is proportional to the number of packets sent or received [6]. To maximize the network lifetime, therefore, the amount of network traffic should be minimized. One way of accomplishing this is for certain network nodes to collect raw sensor readings from a number of sensor nodes and combine them into a single composite signal which is then forwarded towards the sink node. This process is called *data aggregation*. Data aggregation can greatly reduce the number of packets transmitted, which can result in large energy savings.

The routing protocols that have been proposed for sensor networks can be broadly classified as *flat* and *hierarchical* protocols. Hierarchical protocols organize the network nodes into several logical levels. This is typically implemented by a process called *cluster formation*. A cluster consists of a set of geographically proximal sensor nodes; one of the nodes serves as a *cluster head*. The cluster heads can be organized into further hierarchical levels.

The key advantage of hierarchical routing protocols is that the cluster heads can perform efficient in-network data aggregation. Routing proceeds by forwarding packets up the hierarchy until the sink node is reached. Flat routing protocols, on the other hand, attempt to find good-quality routes from source nodes to sink nodes by some form of *flooding*. Since flooding is a very costly operation in resource starved networks, smart routing algorithms restrict the flooding to localized regions. Some algorithms use probabilistic techniques based on certain heuristics to establish routing paths.

Flooding-based protocols rely primarily on flooding for route discovery. Many protocols couple query routing with data routing, i.e. source nodes transmit their observed data readings directly in response to queries from sink nodes. Such protocols can be classified as *query-driven* protocols. On the other hand, *data-driven* protocols assume that there is a separate query propagation phase by which some sensor nodes realize that their data should be sent to a sink. This phase is generally also responsible for setting up routes. Source nodes transmit their readings along these routes either periodically or whenever they observe some interesting events during the subsequent data transfer phase.

Multipath routing protocols attempt to construct several completely or partially disjoint paths from the source to the sink. This increases the resilience of the network to node failures.

Geographic routing algorithms route queries towards geographically defined regions. They are particularly suitable for sensor networks since user queries for physical phenomena such as movement are typically directed towards specific geographic regions.

Probabilistic algorithms take packet-forwarding decisions probabilistically based on several parameters such as node reputation and link reliability. The classification of the surveyed routing algorithms is presented in Table II.

Table II (Classification of sensor network routing protocols, the first seven categories are specific instances of flat routing protocols)

Routing protocol category	**Example routing protocols**
Flooding-based Query-driven	TinyOS Beaconing, PulseDirected Discussion, Rumor Routing,Braided Path Routing,GEAR
Data-driven	SPIN, GRAB, INSENS, SAR, ARRIVE
Multipath	Braided Path Routing, GRAB, INSENS, SAR
Geographic	GEAR
Probabilistic	ARRIVE
Other flat	ASCENT, Deng *et al.* [5], TBF, Data Mules
Hierarchical/ Cluster-based	SWE/MWE, LEACH, SRPSN

3. Routing Protocols

Numbers of routing protocol for sensor network have been proposed in literate in the last few years. Many of the protocols have similar functionality compare to wireless ad-hoc networks.

Challenge for sensor network protocol that become different from ad–hoc network, several interesting variations are introduced. In addition, many novel routing mechanisms have been proposed specially for sensor networks. The following subsections survey many of the sensor network routing algorithms. There are mainly two type of the routing protocols first one is flat based and second hierarchical and cluster based routing.

A. Flat routing protocol

This routing protocols are similar to the conventional multi-hop ad-hoc routing protocols. Each sensor node determines its parent node(s) for forward data packets. The nodes are not organized into hierarchical clusters in the hierarchical protocols. The advantage of this approach is that all the nodes can reach the base station without respective of their position.

Each of the flat routing protocols can be decomposed into several constituent blocks as depicted in Fig. 1. The arrows in the figure depict the *depends-on* relation between functions.

Multi-hop routing is an essential prerequisite for data aggregation; this is because there is no scope for aggregation if each node transmits directly to the base station. Similarly, reliable neighbour discovery depends on channel symmetry. If the radio links are not bidirectional(for example, as a consequence of the hidden terminal problem), then reliable communication is not possible. Link layer broadcast is a fundamental requirement for sensor network routing, since radio channels are inherently broadcast in nature.

Multi-hop routing makes it possible to achieve load balancing by restricting the power level at which sensor nodes communicate. Since the sensor nodes have severely restricted power resources, this can greatly increase the lifetime of the network. Finally failure detection and recovery is possible if each node is aware of its surrounding network topology. Most of the flat routing protocols that have been proposed for sensor networks incorporate distance vector routing algorithms. In distance vector routing [4], nodes maintain estimates of their distances from the destination nodes. Each node transmits its distance estimates to its neighbours. Each node updates its distance vector so as to minimize the distance to each destination by examining the cost to that destination reported by each of its neighbours and then adding its distance to that neighbour. The problem with the straightforward distance vector algorithm is that it takes a long time to converge after a topological change.

Several techniques are used to detect the counting to infinity problem [4] and hasten convergence in practice. For instance, some protocols use a time-to-live (TTL) field in their packets. When the TTL drops to zero, the packet is discarded. Other protocols use randomization techniques to avoid routing loops. Some other ways in which convergence is achieved are back-propagating learned costs to destinations, making route changes only at periodic intervals, eavesdropping on

the broadcast medium, running centralized shortest path algorithms and so on.

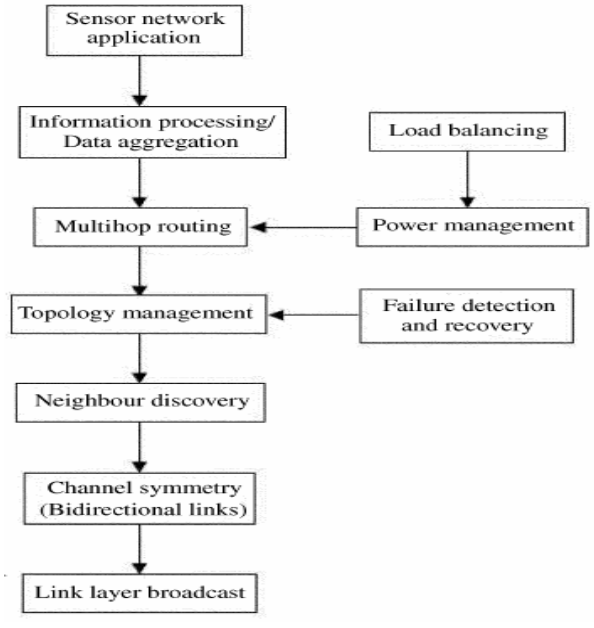

Figure 1. Depends-on hierarchy for flat sensor network routing protocols. The function at the tail of an arrow depends on the function at the head of the arrow.

B. *Hierarchical and cluster-based routing protocols*

Hierarchical routing protocols arrange the network in to different groups called cluster. Each cluster select their cluster head from network. Cluster head is responsible for collect the sensor data from the cluster member, aggregating them and transmit summary to base station .This results in removing a large number of redundant messages from the nodes and also reducing the overall power consumption in the network. It also avoids many MAC layer collisions that waste the free bandwidth. This enables the sensor network to scale to a large number of nodes.

Hierarchical routing protocols can be decomposed into several constituent blocks as depicted in Fig. 2. The dependencies are essentially similar to those for flat routing protocols with a few additions. Since hierarchical routing protocols depend on the formation of clusters, a new Cluster formation block is introduced.

Cluster formation involves not only the organization of nodes into groups, but also the election of cluster-heads. Clustering facilitates MAC layer scheduling of transmissions. The cluster-head computes and distributes the MAC schedule among its cluster nodes. Each node transmits only during its time slot; it can switch its radio off during all the other slots thereby conserving energy. Cluster maintenance depends on failure detection and recovery to determine if the cluster-head is alive or not. If the cluster-head has failed, the cluster formation process can be reinitiated. Failure detection in turn can be implemented by techniques like hierarchical heartbeat that are well suited for cluster-based topologies.

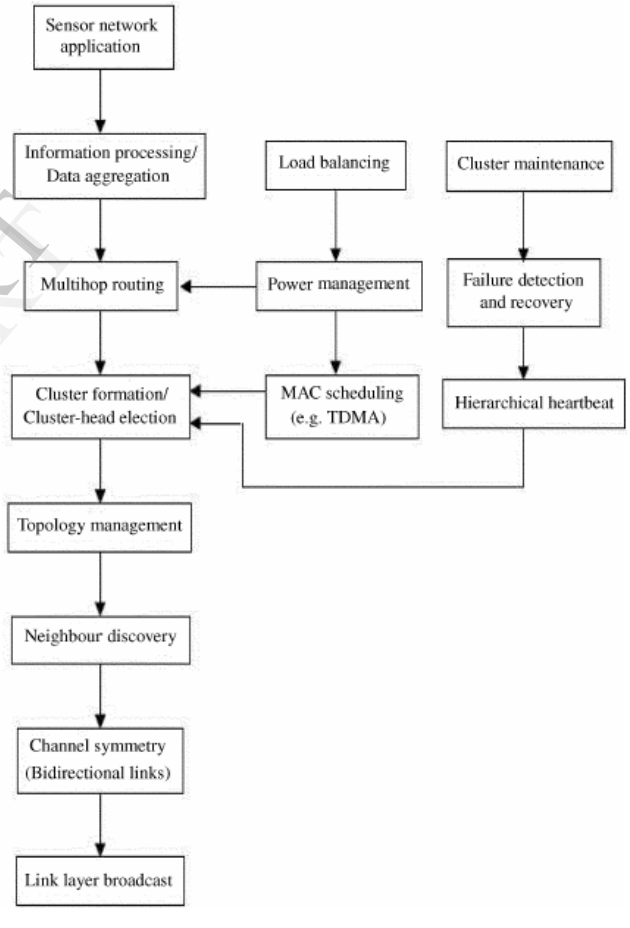

Figure 2. Depends-on hierarchy for cluster-based sensor network routing protocols. The function at the tail of an arrow depends on the function at the head of the arrow.

4. Comparisons of sensor network Routing Protocols

Table III (Comparison of WSN routing protocols)

	GPS required	Multipath routing	MAC scheduling (TDMA)	Mobility aware	Event driven	Energy distribution	Flooding involved	Intrusion tolerant	Failure recovery
TinyOS beaconing	No	No	No	No	No	Non uniform	Yes	No	No
Pulse	No	No	Yes	No	No	Non uniform	Yes	No	Yes
Directed diffusion	Yes	No	No	Yes	No	Non uniform	Yes	No	Yes
Rumor Routing	No	No	No	Yes	Yes	Non uniform	Partly	No	Yes
SPIN	No	No	Yes	No	Yes	Uniform	Partly	No	Yes
Brided multipath	No	Yes	No	Yes	No	Non uniform	No	No	Yes
GRAB	No	Yes	Yes	Yes	Yes	Non uniform	No	No	Yes
INSENS	No	Yes	Yes	No	No	Non uniform	Yes	Yes	No
SAR	No	Yes	Yes	Yes	No	Uniform	Yes	No	Yes
GEAR	Yes	No	No	No	No	Uniform	Partly	No	Yes
ARRIVE	No	Yes	Yes	No	No	Non uniform	Partly	Partly	Yes
ASCENT	No	No	Yes	No	No	Non uniform	No	No	Yes
Roubust routing	Optional	No	No	No	No	Non uniform	No	No	Yes
TBF	Yes	Yes	No	Yes	No	Non uniform	Partly in broadcasting	No	Yes
Data MULEs	No	No	No	Yes	No	Uniform	No	No	Yes
SWE/MWE	No	No	Yes	Yes	No	Uniform	Yes	No	No
LEACH	No	No	Yes	No	No	Uniform	No	No	Yes
SRPSN	Yes	No	No	No	No	Uniform	Yes	Yes	Yes

5. Conclusion And Future Work

Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. The problem of relaying data from remote sensor nodes to a central base station is of paramount importance in such applications. Severe resource constraints in the form of limited computation, memory and power make the problem of routing interesting and challenging. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks.

n this paper we have shown different routing algorithms. We have also shown the comparison of all algorithms. The routing protocols are compared in Table II and classified in Table III. For different purpose wireless sensor network protocols are used as defined above.

In future we try to modify some of energy efficient routing algorithms which used minimum consumption of energy and maximize network life time of wireless sensor network.so it will work better than before.

6. Reference

[1] K. Romer and F. Mattern, “The design space of wireless sensor networks,” Wireless Communications, IEEE, vol. 11, no. 6, pp. 54–61, Dec. 2004.

[2] Proceedings of the Distributed Sensor Nets Workshop. Department of Computer Science, Carnegie Mellon Univ., December 1978.

[3]. Jose A. Gutierrez et al, "IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area networks", IEEE Network,2001.

[4]. Radia Perlman, Interconnections: Bridges, Routers, Switches, and Internetworking protocols, Second edition, Addison-Wesley (2000).

[5]. Jing Deng, Richard Han, and Shivakant Mishra, A robust and light-weight routing mechanism for wireless sensor networks, Proc. 1st Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS 2004), 2004.

[6]. Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, and Niraj K. Jha, Analyzing the energy consumption of security protocols, Proc 2003 Int. Symp. on Low Power Electronics and Design (ISLPED), 2003, pp. 30–35.

[7]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks: a survey, Computer Networks, **38**, 393–422 (2002).

[8]. Radia Perlman, Interconnections: Bridges, Routers, Switches, and Internetworking protocols, Second edition, Addison-Wesley (2000).

[9]. Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David Culler, and Kristofer Pister, System architecture directions for networked sensors, Proc. ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS IX), 2000.

[10]. Baruch Awerbuch, David Holmer, Herbert Rubens, Kirk Chang, and I. J. Wang, The Pulse protocol: sensor network routing and power saving, Military Communications Conf. (MIL-COM 2004), 2004.