

A Review on Hierarchical Routing Protocols for Wireless Sensor Networks

Zahariah Manap · Borhanuddin Mohd Ali ·
Chee Kyun Ng · Nor Kamariah Noordin · Aduwati Sali

Published online: 21 February 2013
© Springer Science+Business Media New York 2013

Abstract The routing protocol for Wireless Sensor Networks (WSNs) is defined as the manner of data dissemination from the network field (source) to the base station (destination). Based on the network topology, there are two types of routing protocols in WSNs, they are namely flat routing protocols and hierarchical routing protocols. Hierarchical routing protocols (HRPs) are more energy efficient and scalable compared to flat routing protocols. This paper discusses how topology management and network application influence the performance of cluster-based and chain-based hierarchical networks. It reviews the basic features of sensor connectivity issues such as power control in topology set-up, sleep/idle pairing and data transmission control that are used in five common HRPs, and it also examines their impact on the protocol performance. A good picture of their respective performances give an indication how network applications, i.e whether reactive or proactive, and topology management i.e. whether centralized or distributed would determine the network performance. Finally, from the ensuring discussion, it is shown that the chain-based HRPs guarantee a longer network lifetime compared to cluster-based HRPs by three to five times.

Keywords Routing protocols · Hierarchical · Clustering · Sensor networks

Z. Manap (✉)

Department of Telecommunication Engineering, Faculty of Electronics and Computer Engineering,
Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
e-mail: mz502@yahoo.com; zahariah@utem.edu.my

B. M. Ali · C. K. Ng · N. K. Noordin · A. Sali

Department of Computer and Communication Systems Engineering, Faculty of Engineering,
Universiti Putra Malaysia, Selangor, Malaysia
e-mail: borhan@eng.upm.edu.my

C. K. Ng

v e-mail: mpnck@eng.upm.edu.my

N. K. Noordin

e-mail: nknordin@eng.upm.edu.my

A. Sali

e-mail: aduwati@eng.upm.edu.my

1 Introduction

Over the last two decades, a new class of short-range wireless communication networks has appeared to facilitate the needs of monitoring and control of physical environment especially in remote and unreachable areas. These networks are called wireless sensor networks (WSNs). The nature of WSNs is some kind of a personal area network (PAN) which interconnects a number of devices wirelessly. The physical and MAC layers of WSNs comply with the IEEE 802.15.4 standard that is uniquely designed for low-rate wireless personal area networks (LR-WPAN) [1,2].

Wireless Sensor Network becomes a new technology trend when human, machines and the environment are being integrated autonomously. This is made possible by advances in processor, memory and microelectronics devices which allow the sensing and computing elements to be integrated together in small devices to perform the programmed tasks [3–5]. These networks are generally used in disaster relief applications, battlefield surveillance, environmental control, habitat monitoring, intelligent buildings, facility management, machine surveillance, preventive maintenance, precision agriculture, medicines and healthcare, and transport and logistics.

The IEEE 802.15.4 standard allows WSNs to operate at low data rates, low complexity and low cost, suitable for applications which require random deployment, long operational duration and mass of sensor motes quantity. This standard supports star and peer-to-peer network topologies which are two of the most favorite topologies in WSNs. In terms of energy conservation, the beacon-enabled super frame of IEEE 802.15.4 enables WSNs to be working in energy save mode which is either *sleep* or *idle* mode [1]. IEEE 802.15.4 guarantees a very low hop delay [2], allowing the data transmission to be executed in a multi-hop architecture and avoiding fast energy drainage due to long range data propagation.

The routing protocol for WSNs is defined as the manner of data dissemination from the network field (source) to the base station (BS). This protocol takes place in the network layer of the protocol stack. Many routing protocols have been proposed starting with the two simplest methods called flooding and gossiping [6,7]. Flooding applies simple multicast data dissemination whereby the data is forwarded in a broadcast manner until it reaches the BS. The routing approach in flooding is simple with no routing table needed and has low transmission delay. However, this protocol drains the energy of the nodes drastically when all nodes take part in handling a single data packet, thus shortening the network lifetime. The most critical problem introduced by flooding is data implosion, where a node receives multiple copies of the same data. Meanwhile the gossiping tries to eliminate data implosion problem by randomly selecting a neighbor to pass the data with the hope that the data will eventually arrive at the BS. However, this approach might increase the transmission delay especially in a large network. These two protocols have shown that energy efficiency and transmission delay are two important factors to be considered in designing routing protocols for WSNs.

A more sophisticated approach known as data-centric routing protocol [5] has been introduced to avoid data implosion problem and reduce transmission delay. In these protocols, the route for data transmission is determined prior to the real data transmission from source to destination. The BS explores the network by broadcasting small size query packets to the nodes. The query packets specify the attributes of the required data. The node that owns the required data will send a feedback to the BS. Then, the most suitable route is chosen to disseminate the real data to the BS. The weakness of data-centric routing protocols is that they are only suitable for on-demand data applications such as event detection or intrusion detection. If this type of routing protocols is applied in monitoring applications, the accuracy

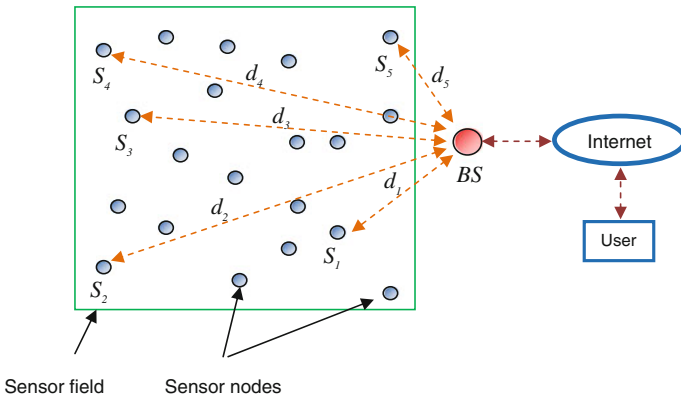


Fig. 1 The basic network architecture of a WSN with direct transmission routing protocol

of the data is somewhat doubtful since the data from a single node does not represent the real condition of the environment. For a small scale network, data-centric routing protocols offer an acceptable transmission delay. However, in large scale networks, propagation delay caused by the negotiation process and a very long multi-hop path increases the transmission delay, thus limiting the scalability of the WSNs.

To overcome the latency problem and promote scalability, some HRP have been proposed. They are namely Low-energy Adaptive Clustering Hierarchy (LEACH) [8], Threshold Sensitive Energy Efficient Sensor Network (TEEN) [9], Adaptive Periodic TEEN (APTEEN) [10], Power-efficient Gathering in Sensor Information Systems (PEGASIS) [11] and Power-efficient Data Gathering and Aggregation Protocol-power Aware (PEDAP-PA) [12]. This paper reviews the mechanism and design strategies that influence the performance of these five HRP.

The subsequent sections are arranged as follows; the next section gives an overview of WSNs, followed by an introduction of routing protocols for WSNs in Sect. 3. Section 4 gives related survey works while Sect. 5 briefly describes general features of HRP. Section 6 describes the mechanism of each of the five HRP. The performance of the five HRP is evaluated in Sect. 7. Finally, this paper is concluded in Sect. 8.

2 Overview of WSNs

WSN is a type of short range wireless communications network that is ideal for monitoring and detection applications. Two main categories of WSN applications are space monitoring such as for the environment, and for event detection such as against intrusion or for wildlife monitoring. All these generally operate in hostile or unreachable fields. This network provides the information about the activities in the field to the remote user via the internet. Figure 1 shows the basic architecture of a WSN. It consists of a large number of sensor nodes that are located randomly to cover a network field, a gateway (or BS), the internet and the user. Basically, the function of the sensor nodes is to sense the changes or activities around their vicinity and route the data to a BS, whilst the BS integrates the WSN and the internet.

Every sensor node in a WSN is able to interact among themselves as well as with their environment by sensing and transmitting physical parameters [6]. Each of the nodes consists of a memory, communication device, controller, sensor and power supply as shown in Fig. 2.

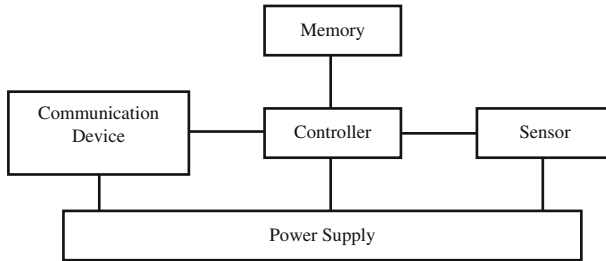


Fig. 2 Basic components of a sensor node [6]

The function of the controller is to perform data computations before sending it to the next node. The memory temporarily stores the sensed/aggregated data and other parameters that are defined in the protocol. The communication device is the radio part which enables communication between nodes and the BS. This device consists of a transmitter and a receiver or a combined transceiver. The RF-based transceivers with a typical communication frequencies between 433 MHz and 2.4 GHz [6] are normally used as the transceiver for the sensor nodes. Most sensor nodes in the market are powered by a very limited voltage source such as an AA battery or coin cell.

The energy from the power supply on the sensor node board is consumed by three main components; communication device, controller and sensor. Each of the sensor node’s components must consume the energy wisely to optimize the energy conservation. For example, the communication device is used in data communication regarding how the data should be routed to the destination. Hence, it is important to ensure that the routing protocol in sensor networks is energy efficient. The next part, the controller is basically used for data computation. This part deals with the complexity of algorithm and data overhead. Low computational complexity and data overhead respectively help to minimize energy consumptions. However, computation consumes less energy than communications. Therefore, complex computation is acceptable as long as it can save more energy in data routing.

Since the major portion of the energy is consumed for data communications, the main issue in WSNs is an efficient way to route the data from sensor nodes to the BS while maintaining acceptable latency. The network shown in Fig. 1 uses the simplest data routing protocol known as direct transmission (DT). In DT, data is directly transmitted from each and every node to the BS. To explain the weakness of DT routing protocol, five nodes are designated in Fig. 1 as S_1, S_2, S_3, S_4 and S_5 and the distance from each corresponding node to the BS as d_1, d_2, d_3, d_4 and d_5 respectively. The energy consumed by each node to transmit k bits of data within distance d is [8]:

$$E_{Tx}(k, d) = E_{elec} * k + \epsilon_{amp} * k * d^2 \tag{1}$$

where E_{elec} is the energy used to run the transmitter circuitry in nJ/bit and ϵ_{amp} is the energy used by transmit amplifier to achieve acceptable signal to noise ratio (SNR) in pJ/bit/m². The energy consumed by each node to receive k bits of data is [8]:

$$E_{Rx}(k) = E_{elec} * k \tag{2}$$

From (1) and (2), energy is needed not only to transmit but also to receive the data. However, higher energy is expended for data transmission than that of data reception. The energy consumption for data transmission relies mainly on the distance squared whereby the farther the node from the BS, the higher the energy is consumed to transmit the data. In Fig. 1, S_2, S_3

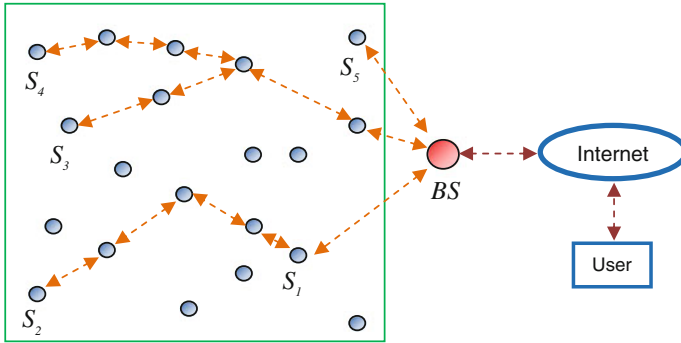


Fig. 3 The multi-hop architecture of a WSN

and S_4 consume much higher energy compared to S_1 and S_5 since the data transmission from these nodes involves long distances. These nodes will die out much quicker than S_1 and S_5 , leaving the area that are covered by the nodes unattended. Therefore, in WSNs environment where the sensor nodes are scattered all over the field, DT is only suitable for nodes which are close to the BS. As an alternative in order to reduce energy consumption in data transmission, the data is made to travel in short distances as shown in Fig. 3. In this multi-hop architecture, neighboring nodes perform cooperative tasks by passing the data from one node to another until the data reaches the BS.

The simplest multi-hop routing protocol is minimum transmission energy (MTE) [13]. In this protocol, data is routed to the BS through intermediate nodes which act as routers. An example of protocol that proposes MTE approach is found in [13]. In that paper, the routers are chosen so that data is routed to the BS with the minimum energy cost. The relationship between energy cost of MTE and DT for transmitting data packet from a sensor node to the BS is given by:

$$E_{i \rightarrow r \rightarrow BS} < E_{i \rightarrow BS} \tag{3}$$

where the left side expression denotes the energy cost from node i to the BS through a router r and the right side expression denotes the energy cost for DT. To analyze this expression, we put a weight to represent the distances between nodes as in Fig. 4. Considering the d^2 in (1), if S_3 sends the data directly to the BS, d^2 equals 81. However, if S_1 and S_2 are chosen as the routers, d^2 is only equal to 42.

In a multi-hop architecture, the total path seems to be longer than that in DT. However, when the propagation model of the environment is taken into account, several short-distance transmissions are better than a single high energy transmission. Hence, it can be said that by reducing the transmission distances it can improve the energy efficiency. Because of this, many multi-hop data routing protocols have been proposed such as flooding, gossiping and data-centric routing protocols as described earlier. However, due to some weaknesses associated with these protocols, hierarchical architecture is appended on top of multi-hop architecture to maintain the network performance over a larger field area.

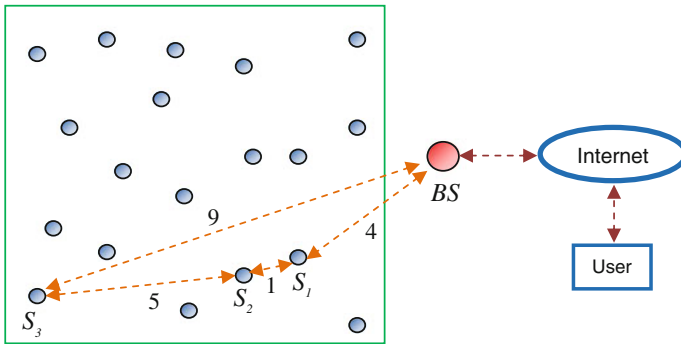


Fig. 4 Example of MTE routing path

Table 1 Comparison between proactive and reactive networks

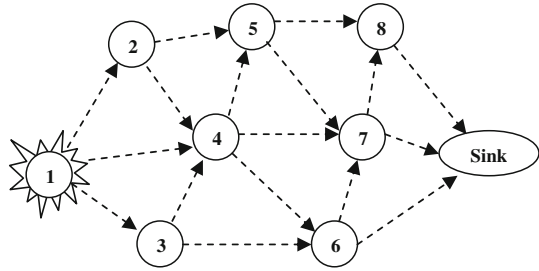
Description	Proactive networks	Reactive networks
Type of applications	Periodic monitoring	Critical monitoring/event detection
Mode of sensing circuitry	Periodically switch on	Always on
Mode of communication device	Periodically switch on	Always on
Data delivery	Periodic/continuous	Event driven / On demand

3 Routing Protocols in WSNs

The routing protocol depends on the user’s interest or network applications. Based on the network applications, routing in WSNs are of two types; proactive and reactive. There is also a possibility to combine both applications in one network called hybrid network. In a proactive network, the data is collected from the whole network or several regions of the network field. The idea is to update the BS with the current information of the network field’s condition, for example on the current temperature or humidity in the monitored area. The process of data gathering in proactive network involves all or almost all sensor nodes, where the data sensed by individual node is accounted to determine the current condition. The report will be sent to the BS periodically regardless of whether there are any changes occurring in the field. This network is normally used for monitoring applications. Conversely, in a reactive network, the data is sent to the BS based on user’s request or if there is any critical change in the network field. Critical change is defined as an event which gives a signal that exceeds the predetermined threshold value. Only dedicated nodes or the nodes which are close to the event will take part in data gathering and dissemination. This kind of network is suitable for critical event detection and monitoring. The differences of the two networks are summarized in Table 1.

In WSNs, the sensor nodes can be deployed either in a deterministic manner, where they are placed manually in the network area or by using random deployment [7]. Deterministic deployment is easier and straight forward since the nodes can be deliberately arranged to distribute evenly in network area. The nodes can be located so that they are not interfering with each other or the interference and overlapped coverage between neighboring nodes is minimized. This eases the protocol stacks implementation. Nonetheless, deterministic deployment is only applicable for reachable areas such as for local surveillance monitoring,

Fig. 5 The implosion problem in flooding



parking lot monitoring and patients monitoring applications. For hostile and unreachable areas such as in the forest or volcanic field, the only option is to randomly deploy the sensor nodes in the field of interest. Random deployment yields the location of the nodes to be pervasive all over the field. The nodes can be sparse in one region whilst dense in another or there might be some regions which are not covered by the nodes. Hence, a large quantity of the sensor nodes need to be deployed to ensure that every inch of the field of interest falls under sensing coverage. Yet random and densely located, the most challenging task of the implemented protocols is to ensure that the sensor nodes are capable of self-organizing.

In dense and random nodes topology, the probabilities for two or more nodes to sense the activity in the same area is very high. The closer nodes will surely sense the same activity and send the same data to the BS. To reduce data redundancy, some routing protocols such as the ones proposed in [14–16] make use of the capability of nodes to adjust the transmitted power adaptively depending on the algorithm needs. In a proactive network, the data sensed by one node may represent a certain region, thus, sending the same data from the same region is a waste of energy. To conserve energy, closer nodes which are sensing the same area are paired [10] so that they take turn in doing the sensing task. Likewise, in a reactive network, all nodes which are in the event's vicinity must work together [17] to ensure the correct and accurate data is reported to the BS. Implementing idle/sleep pairing may ignore some important data, thus reducing the accuracy. Hence, the routing protocol must be designed by considering the type of applications and the user's requirements to ensure that the performance of the network can be optimized.

Since the transmission mode of a sensor node is in broadcast manner [18], simple multi-hop routing protocol such as flooding may cause implosion [19] problem as depicted in Fig. 5. Implosion is a phenomenon where a node receives several copies of the same data from two or more neighbors during the data dissemination process. As depicted in Fig. 5, suppose node 1 has the data to be transmitted to the sink. Node 1 transmits the sensed data to node 2, node 3 and node 4 since it considers those three nodes as its neighbors. Node 2 transmits the same data to node 4 and node 5 whilst node 3 also transmits the same data to node 4 and node 6. Thus, node 4 receives three copies of the same data from node 1, node 2 and node 3. This situation continues until the sensed data successfully reaches the destination with so many nodes receiving several copies of the same data. Hence, along the way, there are so many unnecessary transmissions that occur.

Although flooding does not require routing algorithm and topology maintenance, the implosion problem precludes this protocol as energy efficient [6, 20]. For power constraint systems like WSNs, this type of data routing is not acceptable since a lot of energy is wasted for unnecessary data transmissions.

To overcome implosion, data fusion or data aggregation approach is introduced in data-centric routing protocols. Some examples of data-centric routing protocols are sensor protocol

for information via negotiation (SPIN) [19], directed diffusion [3], energy-aware routing [21], rumor routing [22] and active query forwarding in sensor networks (ACQUIRE) [23]. Generally, data-centric routing protocols imply the establishment of two-way communications between neighboring nodes by sending requests and responds to ensure only the data are sent to the nodes which require it. This method may overcome duplication in data transmission thus conserve overall network energy. Interestingly, the use of neighbor's information in these methods helps to reduce the need for global information such as the nodes' address or IP. All nodes need to know certain information of their neighbors such as the current energy level, energy requirement and the distance between them in order for them to pass the data.

However, data-centric routing protocols only work well in small scale sensor networks. In large scale networks, they may cause transmission delay. This is because as the number of nodes increases, the data is propagated through long multi-hop paths. In addition, the data-centric approaches need to deal with request and advertisement packet transmissions which are considered as the communication overheads. As a solution, HRP is introduced with the objective of reducing the transmissions distances between nodes and BS.

4 Related Survey Works

Routing protocol issues have received more attentions in WSNs with the emerging of various algorithms to fulfill the requirement of high energy efficiency. This has inspired researchers to survey the routing protocol algorithms, and highlight their features, mechanisms, techniques and performance to give the overall picture of the issue. In this section we distinguish our paper from the previous surveys and state our scope of review. To the best of authors' knowledge, there are six other surveys reviewing the routing protocols in WSN [7, 24–28]. The authors in [7, 24–26] reviewed the routing protocols in WSNs in general while the other two surveys in [27, 28] focused on the cluster-based routing protocols.

Akkaya and Younis in [7] gave a broad perspective on three main categories of routing protocols for WSNs including hierarchical protocols. The authors presented the classification for various approaches pursued in each category of protocols. That survey is very comprehensive and gives a good introduction to routing protocols in WSNs. Al-Karaki and Kamal [24] addressed the routing challenges and design issues in WSNs. The authors also described and categorised the different approaches for data routing in WSNs. However, both surveys of [7] and [24] did not show the simulation based performance results of the routing protocols. Villalba et al. [25] and Singh et al. [26] highlighted almost the same issues as in [7] and [24], except that the authors in [25] propose an optimization technique in routing protocol called Simple Hierarchical Routing Protocol (SHRP).

Abbasi and Younis in [27] gave a broad perspective on clustering algorithms by presenting a taxonomy and general classification of several published clustering schemes. The comparison of clustering algorithms was presented based on certain features of clustering such as convergence rate, cluster stability, cluster overlapping, location awareness and mobility. Singh et al. in [28] reviewed the mechanisms and features of a few published cluster-based routing protocols such as energy-efficient hierarchical clustering (EEHC), LEACH, enhanced-LEACH (E-LEACH), LEACH-centralized (LEACH-C), multi-hop LEACH (M-LEACH), LEACH with fixed cluster (LEACH-F), PEGASIS, hierarchical PEGASIS (H-PEGASIS), Hybrid, Energy-Efficient Distributed Clustering (HEED), TEEN and APTEEN. However, there are no comparisons in the aspect of performance evaluations presented in both surveys [27, 28]. In [28], the authors did not discuss the strengths and weaknesses of each protocol over another.

The significance of this paper compared with the above six surveys is that it focuses on the basic features of sensor connectivity issues such as power control in topology set-up, sleep/idle pairing and data transmission control used in the earliest cluster-based and chain-based HRP. Another element that distinguishes this paper is that it compares the performance of the said HRPs in terms of network lifetime. The significant impact, strengths and weaknesses of the strategies and approaches used in each of the HRPs are also described in this paper. Furthermore, in analyzing the network lifetime, the performance of HRPs are compared based on two realistic metrics, which are the First Node Dies (FND) and Half of the Nodes Alive (HNA) which are introduced in [38] in addition to the last node dies (LND).

5 Hierarchical Routing Protocols (HRPs)

HRPs are found to be very energy efficient when this type of routing protocol was first introduced in [8]. The special feature of this approach is that it provides self-organization capabilities to allow large scale network deployment. Basically, in a hierarchical architecture, some nodes take responsibility to perform high energy transmission while the rest perform normal task. Power-aware algorithm is used to select eligible high energy nodes to relay the data from normal nodes to the BS. HRPs can be categorized into two types based on the topology management, they are cluster-based HRPs [8–10] and chain-based HRPs [11, 12]. In cluster-based HRPs, sensor nodes are grouped into clusters and each of these clusters are led by one of the nodes, called the cluster head (CH). A CH acts as an intermediate node between cluster members and the BS. In chain-based HRPs, all nodes in the field are connected in a chain structure. Then, the most energy healthy node is chosen as the chain leader to mediate the data transmission from normal nodes and the BS. In both types of HRPs, there are other design features applied to further enhance the performance such as data fusion, threshold values set up, and sleep/idle pairing.

In terms of operation, a HRP consists of two phases. The first phase is the set-up phase, when the sensor nodes are organized to form hierarchical architecture either in a cluster-based or chain-based manner. The second phase is the steady state phase, when data are routed from sensor nodes to the BS. The hierarchical architecture of a cluster-based or chain-based HRP can be set up by using distributed algorithm or centralized algorithm. In [8–11], a stochastic approach is used to form clusters and chains. This is a fully self-organized approach where no global knowledge is needed local interactions are needed between nodes. However, random approach is deemed not capable of producing optimal architecture. Thus, many newer protocols use centralized approach where the hierarchical architecture is determined by the BS. For example, LEACH-C [20] and APTEEN [10] use simulated annealing technique to form optimal clusters. The simulation results from both works show that optimal clusters can reduce data packet loss, thus increasing the throughput and data accuracy [18]. The drawback of applying centralized algorithm is it limits the self-organization feature of the WSNs. However, the great performance of centralized algorithm proves that optimal hierarchical architecture is essential to guarantee good performance of a WSN. To maintain both self-organization capability and energy efficiency, HRPs must be accomplished with a distributed topology control algorithm that is capable of providing optimal architecture.

There are a large number of hierarchical routing protocols (HRPs) for WSNs that has been proposed in the literature. Most of the HRPs reference to LEACH [8] which is the pioneer work on HRP, as the benchmark to evaluate the performance of their respective protocols. Although LEACH was proposed more than 10 years ago, its tremendous performance in terms of energy conservation has made it a significant reference in almost all later HRPs such

Table 2 The parameters used in the simulations [18]

Parameter	Value
Network dimension	100 m × 100 m
BS location	75 m from the field
No. of nodes	100
Initial energy	2 J
E_{elec}	50 nJ/bit
ϵ_{amp}	10 pJ/bit/m ²
$\epsilon_{two-ray-ground}$	0.0013 pJ/bit/m ⁴
d_o	87 m
E_{DA}	5 nJ/bit/signal
Data size	500 bytes

as in [29, 30, 15, 31–36]. Therefore, in this paper, we choose LEACH as the first protocol to be reviewed. The objective is to compare two types of topology management in HRP, namely cluster-based and chain-based on the fixed WSNs. TEEN [9] and APTEEN [10] are among the earliest cluster-based HRP that implement different strategies to overcome unnecessary transmissions in LEACH while maintaining some basic features of LEACH. While PEGASIS [11] and PEDAP-PA [12] are among the earliest HRP that implement chained topology. The five basic HRP are reviewed in order to show the advantages and tradeoffs of the techniques and strategies proposed in each of the HRP as described in the conclusion. A good picture of their respective performances give an indication how network applications, i.e whether reactive or proactive, and topology management, i.e. whether centralized or distributed affect the network performance.

6 Mechanism and Design Features of HRP

Generally, HRP are designed to provide scalability to WSNs while maintaining high energy efficiency. This section discusses and evaluates the mechanism and strategies used in five HRP which are LEACH [8], TEEN [9], APTEEN [10], PEGASIS [11] and PEDAP-PA [12].

6.1 Simulation Set-up

The simulations for all five HRP were done in the network simulator 2 (NS-2). All HRP use the energy model as described by (1) and (2) and the parameters used in the simulation are listed in Table 2. The parameters are based on the simulations done in [18]. We simulate all five HRP on a 100 m × 100 m network field with 100 sensor nodes that are randomly deployed. The BS is located 75 m from the sensor field. All nodes are heterogeneous with initial energy supply of 2 J. The energy for the radio electronics, E_{elec} is set to 50 nJ/bit. The energy for radio transmitter, ϵ_{amp} is set to 10 pJ/bit/m² for transmission distances less than 87 m (d_o). For the transmission distances greater than 87 m, the energy for radio transmitter, $\epsilon_{two-ray-ground}$ is set to 0.0013 pJ/bit/m⁴. The energy consumed for data aggregation, E_{DA} is set to 5 nJ/bit/signal and the size of each data message is 500 bytes.

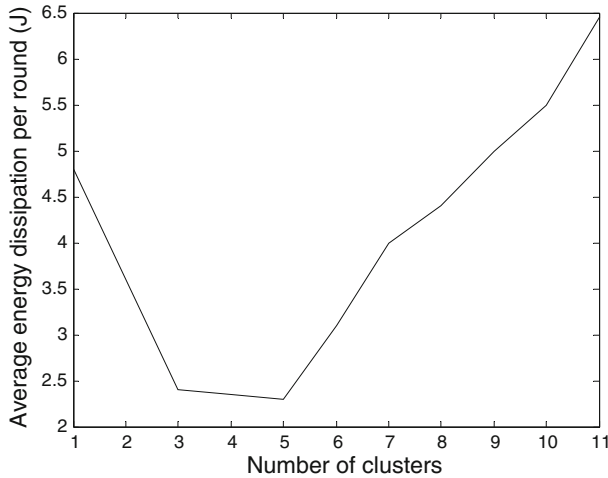


Fig. 6 Average energy dissipated per number of clusters formed [8]

6.2 Low-Energy Adaptive Clustering Hierarchy (LEACH)

Heinzelman et al. [8] proposed LEACH routing protocol that considers fair load distribution among all nodes in the network based on a probability function. The operation of LEACH is broken into rounds. There are two phases involved in each round; the set-up phase, when the clusters are formed, and the steady-state phase, when the data from all nodes are forwarded to the BS. At the beginning of the set-up phase, several nodes will independently elect themselves as a CH based on their current energy level and the threshold value, $T(n)$ which is determined by:

$$T(n) = \begin{cases} \frac{P}{1 - P * (r \bmod \frac{1}{P})}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where P is the desired percentage of CH and G is the set of nodes that have not become CHs in the last $1/P$ rounds. The author reported that, for a 100-node WSN, the optimum number of CHs is about 5% of the total number of nodes. The result of the simulation from [8] is redrawn in Fig. 6. The graph shows that the cost is the lowest in terms of average energy when the 100 nodes are clustered into three to five clusters.

The mechanism of LEACH is described in Fig. 7. For brevity, one BS and only three nodes are shown in the figure. The BS will broadcast the query to the entire network. Assuming that in that particular round, S_1 elects itself as a CH based on the probability function in (4), S_1 will advertise its status to the non-CH nodes (S_2 and S_3) by broadcasting an advertisement (ADV) message. The ADV message contains the information of the CH, required attribute (A) and report time (T_R). S_2 and S_3 will choose to join the closest CH in order to minimize the transmission distance. Since the ADV message from all CHs are sent at the same transmit energy, the nodes will regard the CH from which it receives the strongest ADV message as the closest one. If the ADV message received from S_1 is the strongest one, then S_2 and S_3 join S_1 by sending an acknowledgement (ACK) message of its membership to S_1 .

After completing the set-up phase, the steady-state phase begins. S_1 creates and broadcasts a time division multiple access (TDMA) schedule which allocates a transmit time slot to each

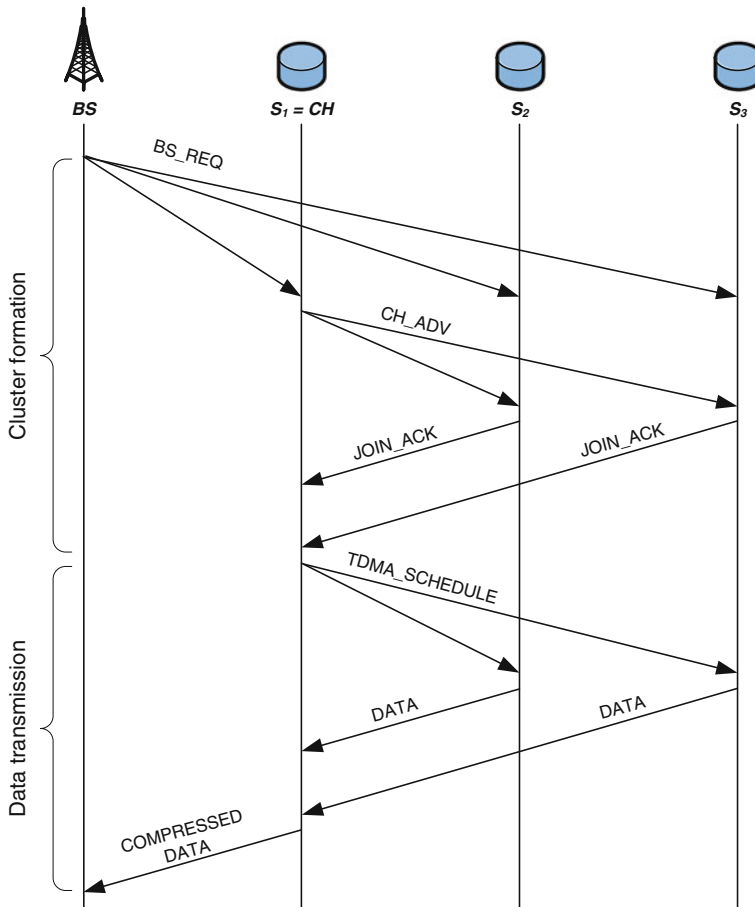


Fig. 7 Flow of mechanism in LEACH

of the cluster members. This schedule allows the cluster members to turn into sleep mode and activate their transceiver circuit just before the allocated transmit slot. All non-CH nodes are assumed to have data to transmit during their allocated slot. A CH has to wait until it receives the data from all cluster members before compressing the data into one single packet and sending it to the BS.

The packet transmission from CH to BS may involve a long range of distance which consumes high energy. The CH-BS transmissions will rapidly reduce the energy of the CHs. To avoid the CHs to die out quicker than other nodes, the role of CH is rotated among nodes in every round. Once a node has become a CH, it will not be eligible to become a CH again within the next $1/P$ rounds. This approach effectively avoids one node to experience frequent long range transmissions within a short period. This approach balances the load among the nodes, prolongs network lifetime and guarantees the quality of the network to be maintained for a longer period.

Heinzelman et al. [8] compare the performance of LEACH with DT and MTE. From the graphs in Fig. 8, it is obvious that LEACH protocol postpones the first node dies (FND) after

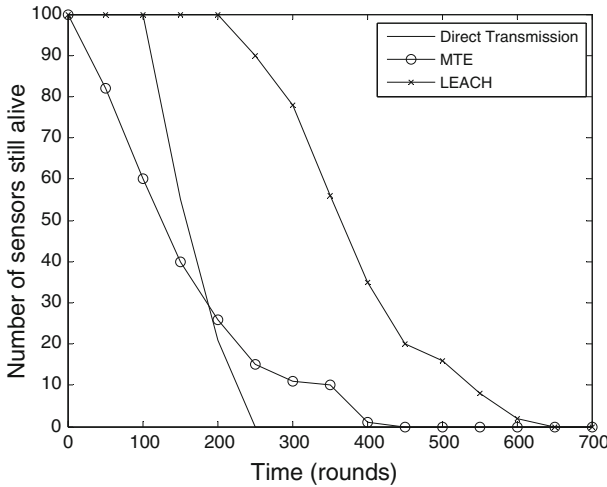


Fig. 8 Comparison of the network lifetime for LEACH, DT and MTE

200 rounds whereas all other nodes die out after 600 rounds. This is two times better than that of DT and four times better than MTE.

LEACH proves that reducing intra-cluster transmission distance may result in higher energy efficiency. Despite its great performance over those conventional methods, LEACH does not guarantee that the energy supplied is efficiently used to successfully send the data to the BS. The random approach of cluster formation in LEACH does not guarantee optimal clusters that are equal in size and well distributed in the network field. The clusters in LEACH are formed based on the distance between normal nodes and the CH. Every node will choose to join the closest CH. An example of clusters formed in LEACH is shown in Fig. 9. The result was obtained by using Matlab. The network of 100 sensor nodes is grouped into six clusters. The problem with this cluster formation is that the clusters formed are not uniform in size. The unbalanced number of cluster members within all clusters can be seen where there is one cluster consisting of only four nodes including the CH, while other clusters are cramped with up to 25 nodes. This will lead to unequal length of TDMA frame generated in each cluster.

The time-line for LEACH operation is shown in Fig. 10. Figure 10a shows the time-line for a cluster showing the label number of cluster members of up to four nodes; in this scenario more frames can be sent to the CH. Figure 10b shows the time-line for a cluster of 16 nodes, where due to longer TDMA frames, only one or two frames can be sent to the CH.

To describe the drawback of non-uniform cluster size, a simple analysis has been done towards the time-line of LEACH operation. For brevity, let's assume that all nodes can generate data at a uniform rate of 5packets/s. If the steady state duration for one round of operation is set by the network to be 5s, the CH of a smaller cluster as shown in Fig. 10a can allocate five guarantee time slot (GTS) to each of its cluster members. After the CH send the first beacon, every node will send one packet during its GTS and go to sleep mode until the next beacon is sent by the CH. After five beacons have been broadcasted by the CH, all buffered data packets will be sent to the CH. In this simple analysis, all data packets generated by the cluster members of smaller cluster are successfully sent to the CH. Therefore, no data loss occurs in the smaller cluster. In contrast, in the larger cluster as shown in Fig. 10b, only 20 data packets generated by the cluster members can be successfully delivered to the

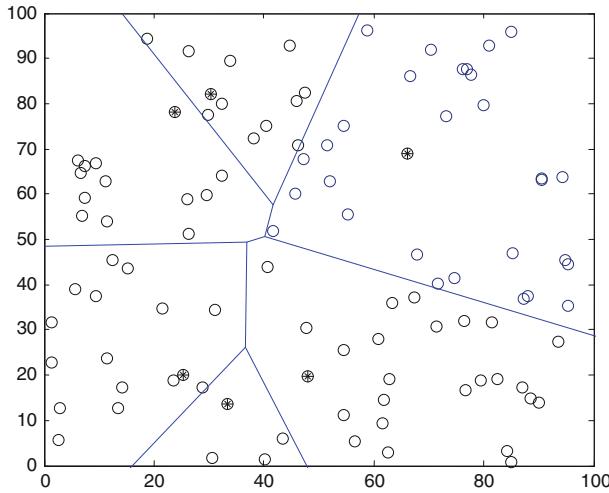


Fig. 9 The clusters formed in LEACH

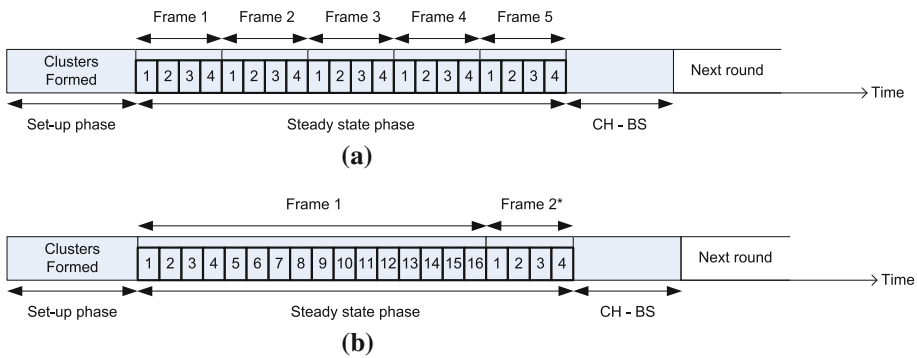


Fig. 10 The time-line of LEACH operation for (a) a small cluster, and (b) a larger cluster

CH within the steady state time, yielding 75% data loss. This shows that LEACH is only suitable for low data traffic applications. For critical environmental monitoring applications such as fire detection or volcanic field monitoring where the field area needs to be closely monitored, high data traffic will be generated. Therefore, LEACH is not the best option. It can be concluded that LEACH conserve more energy compared to conventional routing protocols but it does not guarantee high data throughput at the BS [18].

Another weakness of LEACH is that it may introduce high data latency. The duration of one operation round is set by the network based on the longest TDMA schedule in order to assure that all nodes are able to send at least one packet. Non-uniform cluster size will lead to long steady state duration that may defer the data transmission from CHs to the BS. The latency will be very high and thus decreases the network efficiency. Therefore, it can be said that although TDMA may absolutely prevent data collisions within clusters, it may also introduce delay. Other than low data throughput and latency, LEACH also suffers from high energy consumption due to unnecessary data transmissions. LEACH assumes all nodes to have data to send in every round. If there are no significant changes in one node's vicinity throughout several consecutive rounds, the node might be transmitting the same

data repeatedly. In this case, not only a lot of energy is wasted for the transmission, this will also burden the CHs in accomplishing data processing. Another factor that may lead to energy wastage due to unnecessary transmissions is overhearing. This happens when the CHs broadcast their ADV message to recruit the cluster members. While the messages are meant for closest nodes, the distant nodes might also receive the messages. Although these messages are small in size, the accumulated effect of energy consumption for this purpose reduces the energy efficiency, thus shortening the average network lifetime.

6.3 Threshold Sensitive Energy Efficient Sensor Network (TEEN)

Manjeshwar and Agrawal [9] proposed TEEN which is meant for reactive network such as in critical events monitoring applications where the network responds immediately to drastic changes in the environment. TEEN adopts the cluster formation as in LEACH with some modifications to the radio model. During cluster change time in TEEN, there are two other parameters broadcasted by the CHs to the cluster members in addition to A_{and} and T_R ; the hard threshold (H_T) and the soft threshold (S_T). After clusters are successfully formed, the operation of TEEN starts. All non-CH nodes are put in the idle mode. Whenever a node senses any changes in its vicinity that reaches the value of H_T , the transceiver of the node is switched on and the sensed data is sent to the CH. At the same time, the node itself stores the sensed data for future reference. The stored data is called as sensed value (SV). In the subsequent rounds, the node will transmit its current sensed data if it differs from SV by the amount of S_T or greater. The value of SV is refreshed every time transmission occurs. By using this approach, the BS will only get the data when there are drastic changes in the network field, thus the data transmission in TEEN is not a continuous process. This cuts a great number of unnecessary data transmissions, which therefore conserves more energy.

The introduction of H_T and S_T positively impacts the network lifetime as shown in Fig. 11. After 1,000 rounds, there are 50 nodes still alive in TEEN while in LEACH, the network has died long before. This gives TEEN 163% longer network monitoring time than LEACH. The FND occurs after 550 rounds, which is longer than in LEACH by a factor of 2.75. As these protocols are implemented in monitoring applications where the network quality must be maintained as long as possible, obviously TEEN can guarantee a better network quality than LEACH does. TEEN proves that the introduction of H_T and S_T may eliminate unnecessary nodes-CH and CH-BS transmissions by suppressing the below-threshold data. The complexity of the computation due to the introduction of the thresholds is tolerable since it consumes less energy compared to the amount of energy that can be saved. Hence, the implementation of the threshold parameters is the core feature that promotes the good performance of TEEN. The introduction of these parameters eliminates data redundancy, giving a better network quality and prolonging the network lifetime.

The implementation of the threshold parameters in TEEN is intended to reduce unnecessary transmissions. However, the weakness of this technique is that it can leave the network unattended. Since the network will only send a report to the BS whenever the nodes sense a signal greater than H_T , during the time in which the BS does not receive any data from the network, it will consider that the environment has no significant changes or no critical events in the network at the moment. However, if this condition continues for such a long period, the network acts like a dead field where the BS has no idea about the network's current condition. The BS is not reported about the current energy level of the nodes whereas the nodes are still sensing the environment which eventually will drain their energy and cause the nodes to die out. Therefore, a mechanism that alerts the BS about the current condition must be introduced to avoid the 'silent network' phenomenon.

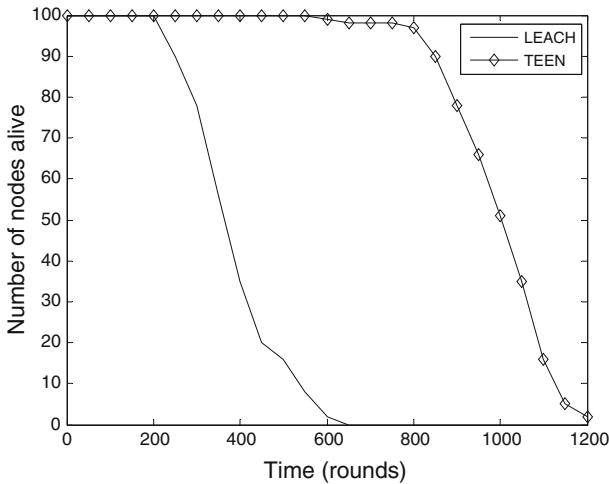


Fig. 11 Comparison of the network lifetime between TEEN and LEACH

The energy efficiency of TEEN depends on the number of transmissions. This means that, if there is a lot of data transmission in the network, the amount of energy consumed by the whole network is high and vice versa. In the environment where the attribute of interest changes rapidly, the nodes may frequently sense the critical changes and thus activate their transmitter. The worst case might happen where all nodes sense a signal value that is greater than H_T . In this case, the operation of TEEN will be very similar to the operation of LEACH. Since TEEN does not apply TDMA scheduling for node to CH transmissions, the possibility of collisions is very high. On the other hand, in a low traffic environment such that the critical changes occur in certain regions of the network field, the involvement of all nodes in cluster formation is not necessary since not all nodes transmit the data to the CH. As TEEN is targeted for reactive network applications, it is understood that only the nodes around the event's vicinity will detect any critical changes. The non-participating nodes will drain their energy for handshaking process and have to pay for overhead cost, but do not contribute to the network's throughput. Therefore, cluster-based topology management is not suitable for reactive network applications unless the clusters are formed only by several nodes which have significant observation value over the changes. Several nodes should work cooperatively in data gathering because the data sent by one single node is not that accurate due to the limited capability of the sensor circuitry [5]. Thus, the network should set the appropriate size of the cluster depending on the level of criticalness of the applications.

6.4 Adaptive Periodic TEEN (APTEEN)

Manjeshwar and Agrawal [10] proposed a protocol for hybrid networks to improve the performance of TEEN, which they called APTEEN. This protocol facilitates both proactive and reactive network applications. To avoid 'silent network' scenario, a new parameter called count time (T_C) is introduced to trigger periodic reports to the BS. By using this approach, although there are no critical changes in the field, the network is forced to send a report describing the current condition of the network in every T_C . The value of H_T , S_T and T_C can be adjusted by the user to balance between data accuracy and energy efficiency.

The mechanism of APTEEN is divided into two phases as in LEACH and TEEN. However, to form optimal clusters, APTEEN uses a different approach of topology architecture algorithm in the set-up phase. APTEEN takes advantage of the unlimited power supply that the BS has. This protocol uses BS-centralized clustering algorithm for cluster formation state as described in [37]. The optimum selection of CHs and cluster formation are executed by the BS based on the information of current energy level provided by the network in the previous round. By using this technique, a well managed hierarchical architecture is established whereby the location of CHs is evenly distributed over the network field and the number of cluster members is uniform in all clusters.

At the steady state phase, APTEEN applies a sleep/idle pairing technique to reduce the highly correlated data being sent by the nodes to the CH. This technique pairs every two close nodes by using simulated annealing approach. Each of the nodes in pairs will alternately take the role to handle queries and send messages from/to the CH. APTEEN uses a modified version of TDMA frame whereby every sleeping node is allocated a shorter time slot and every idle node is allocated a longer time slot. This allows sleeping nodes to be able to send critical data at any time within the cluster time to back up the function of idle nodes. Each sleep/idle pair may change their status at anytime within the cluster time. With this, the BS will receive the critical data without delay.

Figure 12 shows the comparison of the network lifetime for APTEEN, TEEN and LEACH. Generally, the performance of APTEEN lies between LEACH and TEEN. After 800 rounds, there are 87 nodes still alive in APTEEN, 95 nodes still alive in TEEN while no node are alive in LEACH. Based on half of nodes alive (HNA) metric described in [38], APTEEN achieves 78 % of the network lifetime compared to TEEN. However, this is much better than LEACH as such it extends the network lifetime by more than 100 %. Sleep/idle pairing does not seem to help much in enhancing the performance since sleep nodes are still allocated with GTS and able to send data. Although modified TDMA schedule used in this protocol is simple (in terms of data computation) and collision-free MAC protocol [39], it causes high latency due to sleep delay [40] introduced by sleeping nodes. In addition, sleeping nodes may also introduce idle listening at the CH side if no drastic changes occur during their allocated slots. Apart from that, the option for every node to change their operation mode at any time within the cluster time, obviates the sleep/idle pairing process. Sleep/idle pairing can significantly affect the network if a sleep node remains in that mode until it receives a wake up signal from its partner while certain conditions hold. Nevertheless, APTEEN deserves appreciation for the ability to accommodate both on demand and periodic queries. Therefore, APTEEN shows a high versatility while maintaining acceptable performance in terms of energy consumption.

The BS-centralized cluster formation approach used in APTEEN is able to form optimal clusters where the location of the clusters is well distributed in the network field and the number of cluster members is uniform for all clusters. The optimal clusters can produce high throughput, decrease delay and improve energy efficiency. However, it ignores the most important feature that a WSN should possess, that is the capability of self-organization. Applying centralized algorithm in routing protocol can nullify the self-organizing capability in WSNs. However, it is not easy to implement self-organized topology control that can provide optimal clusters, therefore, the results obtained by APTEEN at least may provide some ideas of the design of a distributive topology control.

6.5 Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

Lindsey and Raghavendra [11] proposed PEGASIS, a chain-based HRP for proactive networks. PEGASIS is a fully distributed HRP where it applies distributed algorithm during

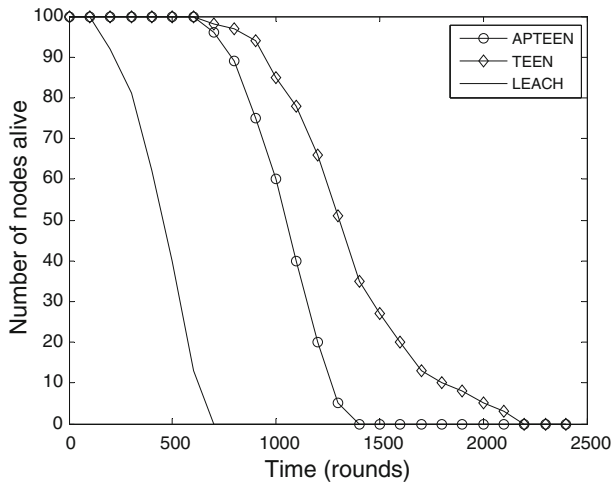


Fig. 12 Comparison of the network lifetime for APTEEN, TEEN and LEACH

topology set-up phase and steady state phase. The main difference between PEGASIS and previously discussed HRP is the way it manages the sensor nodes topology. Instead of grouping sensor nodes into clusters, PEGASIS applies chain forming at the beginning of each round. Upon deployment, each node is assumed to know its neighbors. The greedy algorithm is used to select a start node which will initiate the chain forming process. This node is normally the farthest node from the BS. The start node will then select the closest neighbor to which it will set a connection path. The second node that joins the chain then will select its closest neighbor and set a new connection path. The process goes on until all nodes have joined the chain.

An example of the PEGASIS chain is shown in Fig. 13. For brevity, let us assume that there are only nine sensor nodes in the field. The nodes are denoted as $S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$ and S_9 . To check the closest neighbor of each node, a weighted number is considered to represent the distance between nodes. Assuming S_8 as the start node, a connection path is set between S_8 and S_6 , indicated by a solid line. The connection path setup continues until all nine nodes have joined the chain, with the condition that a node that has already joined the chain cannot be revisited. After the chain is constructed, the most energy healthy node is selected randomly as the chain leader. Let's assume that S_7 is selected as the chain leader for that particular round. S_7 will pass a token frame to the end node, S_8 . Upon receiving the token frame, S_8 transmits its data and forward the token frame to S_6 which will fuse the received data with its own data. Then S_6 transmits the fused data and forwards the token frame to S_2 . The process of data fusion continues until all nodes transmit their data and the token frame reaches S_7 . The direction of data flow is indicated by the arrows. After receiving the token, S_7 will fuse the received data packet with its own data before sending a single data packet to the BS.

The simulation result in Fig. 14 depicts the performance of PEGASIS in comparison to LEACH and DT. Considering HNA metric, PEGASIS prolongs the network lifetime by up to four times over that of LEACH and by up to 30 times better than DT. The first node dies FND of PEGASIS occurs after 1,200 rounds, which is 1,000 rounds later than the FND in LEACH. After the FND in PEGASIS, the number of nodes that are still alive decreases gradually till 2,500 rounds of operation. Then the nodes rapidly die out until the last node

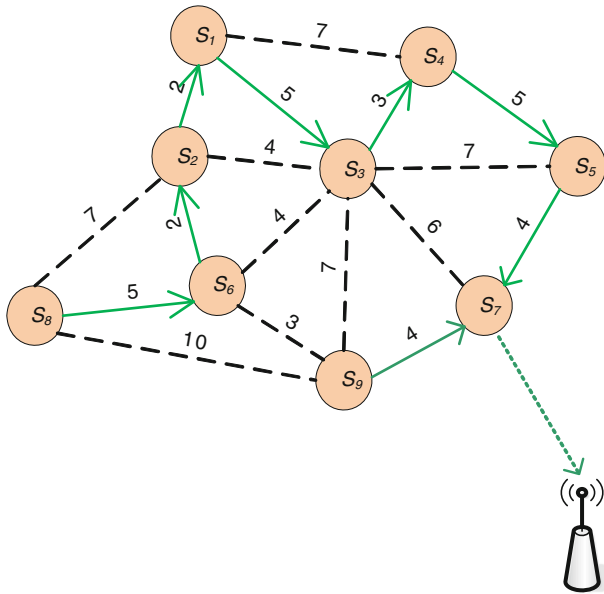


Fig. 13 Chain construction and data aggregation in PEGASIS

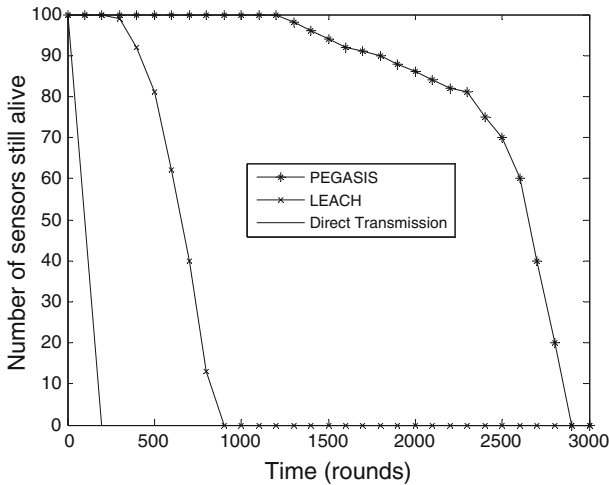


Fig. 14 Comparison of network lifetime for PEGASIS, LEACH and DT

dies at 2,900 rounds. On the other hand, in LEACH the number of nodes that are still alive decreases rapidly just after the FND. This shows that PEGASIS can maintain quality network for a longer period of time.

The superior performance of PEGASIS is a result of the energy saving and load balancing strategies. Chain topology reduces transmission distances and data receptions per sensor node. In PEGASIS, a node only has to transmit and receive from its neighbor nodes in the chain. In addition, PEGASIS performs distributed data fusion and chain leader role's rotation that balance the load distribution among the nodes. These

strategies postpone the FND, thus guaranteeing a good quality for the network over a longer time. Apart from eliminating overhead cost for cluster formation, chain forming and other complementary strategies implemented in PEGASIS prolong the network lifetime.

The drawback of PEGASIS is that it uses relative neighborhood graph (RNG) [6] to determine the closest neighbor at each node. This algorithm is performed in a distributive manner where the interaction occurs between neighboring nodes within one-hop distance. However, since a node that has joined the chain cannot be revisited, the nodes that join the chain at a later time may become very distant from each other as the chain grows. Therefore, in large scale networks, the energy consumption are stretched exponentially since the energy to transmit data is proportional to distance squared. The RNG algorithm may also result in suboptimal paths where data from some nodes have to travel through several hops whereas alternatively, there is a shorter path is available; Fig. 13 explains this problem. For example, data from node S_8 has to travel through S_6 , S_2 , S_1 , S_3 , S_4 before finally reaching S_7 , giving the distance weight of 26. If the algorithm is able to optimize the path by searching two hops ahead, the data from S_8 can be routed to S_6 and S_9 before reaching S_7 , giving a distance weight of 12. This reduces the distance by about 54 % which may exponentially reduce the energy consumption.

Another weakness of PEGASIS is caused by the MAC protocol employed. The token passing MAC protocol that is implemented during steady state phase requires the nodes to be awake at all time in order not to miss the token frame. Thus, the transceiver circuit must be put in either transmit state or receive state. The transmitting node which temporarily possesses the token frame must be in the transmit state while the other nodes are in the receive state. With this requirement, PEGASIS cannot implement energy saving strategy through power management. It is even worse if PEGASIS is employed in large scale networks where the chain will be very long. If only one token frame circulates in the logical ring, high amount of energy will be wasted for idle listening. Moreover, if a large scale network is considered, PEGASIS also results in high latency, and as the sensors are prone to failure due to energy drainage or loss of connectivity, it is very difficult to maintain the logical token ring or bus. If a node fails during the token passing process, the token frame will be lost and the logical ring needs to be reconfigured.

6.6 Power Efficient Data gathering and Aggregation Protocol-Power Aware (PEDAP-PA)

Tan and Körpeoglu [12] propose PEDAP and PEDAP-PA. Both protocols are centralized chain-based HRP. Like the abovementioned four HRPs, the main objective of PEDAP is also to prolong the network lifetime. The mechanism of PEDAP and PEDAP-PA is similar to PEGASIS except for the algorithm used in the chain forming process. Instead of forming the chain by using local interaction between nodes, PEDAP and PEDAP-PA apply the computation of the link costs all over network before constructing the minimum spanning trees (MST). The MST is the best tree that gives the shortest paths in interconnecting all nodes in the field. The approach used in PEDAP and PEDAP-PA can reduce the overall link cost of data communications. Taking the same scenario as in Fig. 13, an optimized chain is formed by PEDAP and PEDAP-PA as shown in Fig. 15. The MST approach eliminates long distance data transmissions by optimizing the link paths, this is done by changing the direction of data propagation.

This paper focuses on PEDAP-PA since this version is more significant compared to its original version, as far as energy conservation is concerned. As the quality of the network decreases rapidly after the FND, PEDAP-PA implements a load balancing strategy to post-

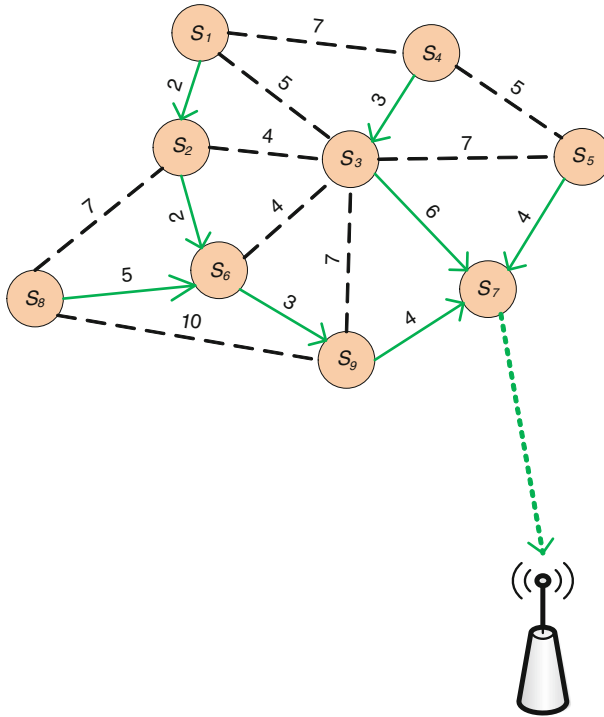


Fig. 15 Possible chain construction and data aggregation in PEDAP and PEDAP-PA

pone the occurrence of FND. The computation of the link costs is done with reference to the remaining energy of each node as follows:

$$C_{ij}(K) = \frac{2 * E_{elec} + k + \epsilon_{amp} * k * d_{ij}^2}{e_i} \tag{5}$$

$$C_{vi}(K) = \frac{E_{elec} * k + \epsilon_{amp} * k * d_{ib}^2}{e_i} \tag{6}$$

Equation (5) computes the link cost between two neighboring nodes i and j where E_{elec} and ϵ_{amp} are mentioned in Table 2, k is the data size and d_{ij}^2 is the distance between node i and node j . Equation (6) computes the link cost between node i and the BS where d_{ib}^2 is the distance between node i and the BS. The term e_i represents the normalized value of the remaining energy of node i with respect to the maximum possible energy in the battery. By using (5), nodes with lesser residual energy will be included later in the chain so that they receive less number of messages. Figure 16 shows the comparison of the network lifetime for PEDAP-PA, PEGASIS and LEACH. Considering HNA metric, it is clear that the PEDAP-PA outperforms PEGASIS by 4% and about 3 times better than LEACH. The FND in LEACH occurs after 200 rounds and in PEGASIS after 1200 rounds. With the load balancing strategy implemented in PEDAP-PA, the FND happens after 2,100 rounds. This means that PEDAP-PA guarantees full network coverage for 75% longer period compared to PEGASIS and about 10 times longer compared to LEACH. Thus it is clear that PEDAP-PA guarantees a good quality of the network for longer period than LEACH and PEGASIS.

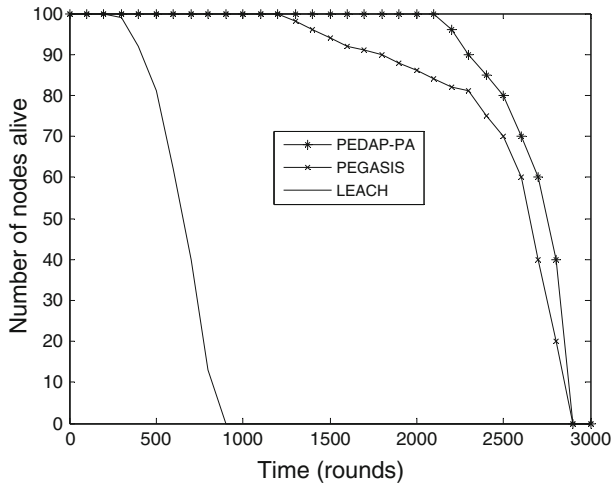


Fig. 16 Comparison of the network lifetime for PEDAP-PA, PEGASIS and LEACH

A very clear drawback of PEDAP-PA is that the topology management is done at the BS level. As discussed before, centralized algorithm limits the self-organization capability of the WSNs, thus it limits the scalability of the network.

7 Performance Evaluation of Various HRP

Generally, all HRP described in Sect. 6 aims to prolong the network lifetime by enhancing the efficiency of energy consumption. However, depending on the applications, there is a need to tolerate between data throughput and longevity. For example, in critical applications such as in disaster relief or volcanic monitoring, data accuracy is more important. This needs some energy to be sacrificed for performing frequent data transmissions. The approach of giving the authority to the user in adjusting the threshold values in TEEN [9] and APTEEN [10], makes these protocols more versatile. With this, the protocols can be implemented in various applications ranging from non-critical monitoring to critical event detection applications.

Every protocol described in Sect. 6 has different strategy in achieving their respective objectives. Heinzelman et al. [8] apply nodes grouping strategy to reduce the transmission distances between nodes and CH role rotation strategy to balance the energy consumption among the nodes. These two strategies have been proven to successfully increase the energy conservation by two times compared to DT. Manjeshwar and Agrawal [9] introduce H_T and S_T on the same cluster-based topology as in LEACH to eliminate unnecessary transmissions. This strategy saves significant amount of energy and prolongs network lifetime by up to 163% compared to LEACH. APTEEN [10] extends the performance of TEEN by forming optimal clusters to improve data throughput and applying sleep/idle pairing to eliminate redundant data. The performance of APTEEN lies between LEACH and TEEN. Lindsey and Raghavendra [11] dwell on the topology setup algorithm and local computation to evenly distribute the load among sensor nodes. This protocol shows a much better performance compared to cluster-based protocols. The fifth protocol, PEDAP-PA [12] applies centralized path determination algorithm to reduce transmission distances. This delays the occurrence of FND and provides the longest network lifetime compared to the other four protocols.

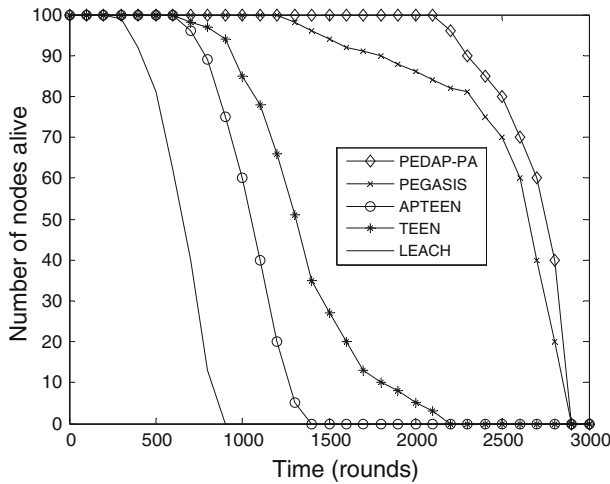


Fig. 17 System lifetime using LEACH, TEEN, APTEEN, PEGASIS, PEDAP-PA

Table 3 Performance evaluation of HRP

Performance parameters	LEACH [8]	TEEN [9]	APTEEN [10]	PEGASIS [11]	PEDAP-PA [12]
Energy Efficiency	Poor	Moderate	Moderate	Good	Best
Network Lifetime	Shortest	Long	Long	Longer	Longest
Self-organization capability	High	High	Low	High	Low
Network Quality Maintenance	Poor	Moderate	Moderate	Good	Best
Throughput	Low	Low	High	Low	High
Latency	High	Low	Moderate	High	Moderate

The graphs in Fig. 17 show the network lifetime for each of all five HRP described in Sect. 6. Generally, the graphs have the same trend where at the early stage of operation, all nodes remain alive up to certain rounds before the FND. The FND point is different for each protocol. After the FND, the number of living nodes degrades until all of them die out due to energy drainage. The FND describes the ability of a protocol to maintain a good quality of the network’s function. The later the occurrence of FND, the longer the quality of network’s function. However, depending on the applications, the FND sometimes is not the main interest of the protocols. For example, in monitoring applications, a more interesting metric to look at is the HNA. Considering both FND and HNA metrics, the graphs shows that PEDAP-PA has the best performance, followed by PEGASIS, TEEN, APTEEN and LEACH. It is also clear that chain-based protocols perform much better than cluster-based protocols, and the BS-centralized protocols give better performance compared to distributed protocols. The performance evaluation of HRP is summarized in Table 3, while Table 4 lists the design strategies and features of the HRP.

In summary, the five HRP can be categorized into two types of protocol depending on the hierarchical topology; namely cluster-based and chain-based. The HRP that fall under cluster-based are LEACH, TEEN and APTEEN while the HRP that fall under chain-based are PEGASIS and PEDAP-PA. Obviously, the great performance of the two chain-based HRP is caused by two factors. Firstly, chain-based architecture provides the protocol with

Table 4 Design strategies of HRP's

Description	LEACH [8]	TEEN [9]	APTEEN [10]	PEGASIS [11]	PEDAP-PA [12]
Hierarchical topology	Cluster-based	Cluster-based	Cluster-based	Chain-based	Chain-based
Hierarchical level	Single level	Single level	Single level	Multi-level	Multi-level
Intra-cluster transmissions	Direct transmission	Direct transmission	Direct transmission	Multi-hop	Multi-hop
Data fusion/aggregation	CH-centralized	CH-centralized	CH-centralized	Distributed	Distributed
Topology set up algorithm	Distributed	Distributed	BS-centralized	Distributed	BS-centralized
Periodic monitoring	✓	X	✓	✓	✓
Critical event detection	X	✓	✓	X	X
Rotation of coordinator's role	✓	✓	✓	✓	✓
Power aware algorithm	✓	✓	✓	✓	✓
Type of network	Fixed	Fixed	Fixed	Fixed	Fixed

a multi-level hierarchy which allows multi-hop data transmission from ordinary nodes to the coordinator. Conversely, cluster-based HRP's apply direct transmission within the clusters which may involve long range distances. This result depicts the radio model as discussed in Sect. 2. Secondly, distributed data fusion that is applied in chain-based HRP's balances the load among the nodes, thus optimizing their current energy level. On the other hand, in cluster-based HRP's, data fusion is burdened to the CH alone which quickly drains its energy. Another positive effect of the load balancing strategy applied in the chain-based HRP's is that the occurrence of the FND can be postponed for a significant number of rounds compared to cluster-based HRP's. With more living nodes around, the quality of the network can be guaranteed for a longer period.

The algorithm used in topology setup may also affect the HRP's performance. For chain-based HRP's, the best performance shown by PEDAP-PA proves that BS-centralized algorithm produce optimal topology compared to distributed algorithm. Likewise in cluster-based HRP's, BS-centralized cluster formation algorithm used in APTEEN enhances its performance over LEACH. The effect of forming optimal topology is that the network can produce higher throughput. The tradeoff of applying centralized algorithm is that the protocols will lose their self-organization capability which limits the network scalability.

8 Conclusion

This paper reviews the design strategies used in five HRP's and examines their contribution to the protocol performance. These HRP's are namely Low-energy Adaptive Clustering Hierarchy (LEACH), Threshold Sensitive Energy Efficient sensor Network (TEEN), Adaptive Periodic TEEN (APTEEN), Power-efficient Gathering in Sensor Information Systems (PEGASIS) and Power Efficient Data Gathering and Aggregation Protocol-power Aware (PEDAP-PA). These HRP's can be categorized into two types which are cluster-based and chain-based depending on the hierarchical topology formed to facilitate the routing protocol. Two main factors that can drain a sensor node's energy quickly are the transmission distance and number of received data packets that the node has to handle. It is found that the chain-based HRP's guarantee a longer network lifetime by three to five times when compared to cluster-based HRP's. Centralized topology management algorithms can produce optimal hierarchical topology to enhance the network performance. Load balancing strategies such as rotation of coordinator's role and distributed data fusion can postpone the occurrence of FND which guarantees a good quality of the network for a longer period.

References

1. Lu, G., Krishnamachari, B., & Raghavendra, C. (2004). Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks. In *Efficient wireless communications and networks (EWCN)* (Vol. 4, pp. 701–706).
2. Zheng, J., & Lee, M. (2006). A comprehensive performance study of IEEE 802.15.4. *Sensor Network Operations, Chapter, 4*, 218–237.
3. Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000). Directed diffusion: A scalable and robust communication paradigm for sensor networks. In *ACM/IEEE international conference on mobile computing and networking* (pp. 56–67). New York, NY, USA: ACM.
4. Dressler, F. (2008). A study of self-organisation mechanisms in ad hoc and sensor networks. *Computer Communications*, 31(13), 3018–3029.
5. Akyildiz, I., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, 40(8), 102–114.

6. Holger, K., & Willig, A. (2006). *Protocols and architectures for wireless sensor networks* (1st ed.). New York: Wiley.
7. Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3), 325–349.
8. Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In *International conference on systems sciences* (Vol. 2, pp. 10). Hawaii: Citeseer.
9. Manjeshwar, A., & Agrawal, D. (2001). TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. In *International workshop on parallel and distributed computing issues in wireless networks and mobile computing* (pp. 2009–2015).
10. Manjeshwar, A., & Agrawal, D. (2002). APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In *International parallel and distributed processing symposium* (pp. 195–202).
11. Lindsey, S. & Raghavendra, C. (2002). PEGASIS: Power-efficient gathering in sensor information systems. In *IEEE aerospace conference* (Vol. 3, pp. 1125–1130).
12. Tan, H., & Körpeo lu, I. (2003). Power efficient data gathering and aggregation in wireless sensor networks. *ACM SIGMOD Record*, 32(4), 66–71.
13. Meng, T., & Rodoplu, V. (2002). Distributed network protocols for wireless communication. In (Vol. 4, pp. 600–603). IEEE.
14. Latiff, N., Tsimenidis, C., & Sharif, B. (2007). Energy-aware clustering for wireless sensor networks using particle swarm optimization. In *IEEE international symposium on personal, indoor and mobile radio communications* (pp. 1–5). IEEE.
15. Kumar, D., Aseri, T., & Patel, R. (2009). EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks. *Computer Communications*, 32(4), 662–667.
16. Madiraju, S., Mallanda, C., Kannan, R., Durresi, A., & Iyengar, S. (2005). EBRP: Energy band based routing protocol for wireless sensor networks. In (pp. 67–71). IEEE.
17. Charambolous, C., & Cui, S. (2008). A bio-inspired distributed clustering algorithm for wireless sensor networks. In *International conference on wireless internet (WICON)*. Maui, Hawaii, USA: ACM.
18. Heinzelman, W. (2000). *Application-specific protocol architectures for wireless networks*. Cambridge: Massachusetts Institute Of Technology.
19. Heinzelman, W., Kulik, J., & Balakrishnan, H. (1999). Adaptive protocols for information dissemination in wireless sensor networks. In *ACM/IEEE international conference on mobile computing and networking* (pp. 174–185). New York, NY, USA: ACM.
20. Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on wireless communications*, 1(4), 660–670.
21. Shah, R., & Rabaey, J. (2002). Energy aware routing for low energy ad hoc sensor networks. In *Wireless communications and networking conference* (Vol. 1, pp. 350–355). Citeseer.
22. Braginsky, D., & Estrin, D. (2002). Rumor routing algorithm for sensor networks. In *ACM international workshop on wireless sensor networks and applications* (pp. 22–31). New York, NY, USA: ACM.
23. Sadagopan, N., Krishnamachari, B., & Helmy, A. (2003). The ACQUIRE mechanism for efficient querying in sensor networks. In *IEEE international workshop on sensor network protocols and applications* (pp. 149–155). Citeseer.
24. Al-Karaki, J., & Kamal, A. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, 11(6), 6–28.
25. Garcia Villalba, L. J., Sandoval Orozco, A. L., Trivino Cabrera, A., & Barenco Abbas, C. J. (2009). Routing protocols in wireless sensor networks. *Sensors*, 9(11), 8399–8421.
26. Singh, S. K., Singh, M., & Singh, D. (2010). Routing protocols in wireless sensor networks: A survey. *International Journal of Computer science and engineering Survey (IJCSSES)*, 1(2), 63–83.
27. Abbasi, A., & Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, 30(14–15), 2826–2841.
28. Singh, S. K., Singh, M., & Singh, D. (2010). A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks. *International Journal of Advanced Networking and Application (IJANA)*, 2(02), 570–580.
29. Muruganathan, S., Ma, D., Bhasin, R., & Fapojuwo, A. (2005). A centralized energy-efficient routing protocol for wireless sensor networks. *Communications Magazine, IEEE*, 43(3), S8–S13.
30. Sha, C., Wang, R., Huang, H., & Sun, L. (2010). Energy efficient clustering algorithm for data aggregation in wireless sensor networks. *The Journal of China Universities of Posts and Telecommunications*, 17, 104–122.
31. Soro, S., & Heinzelman, W. B. (2009). Cluster head election techniques for coverage preservation in wireless sensor networks. *Ad Hoc Networks*, 7(5), 955–972.

32. Kim, J. M., Park, S. H., Han, Y. J., & Chung, T. M. (2008). CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks. In *Advanced communication technology, 2008. ICACT 2008. 10th international conference on, 2008* (Vol. 1, pp. 654–659). IEEE.
33. Nam, C. S., Jeong, H. J., & Shin, D. R. (2008). The adaptive cluster head selection in wireless sensor networks. In *Semantic computing and applications, 2008. IWSCA'08. IEEE international workshop on, 2008* (pp. 147–149). IEEE.
34. Zhang, R., Wang, L., Geng, S., & Jia, Z. (2008). A balanced cluster routing protocol of wireless sensor network. In *Embedded software and systems symposia, 2008. ICSS symposia'08. International conference on, 2008* (pp. 221–225). IEEE.
35. Thein, M. C. M., & Thein, T. (2010). An energy efficient cluster-head selection for wireless sensor networks. In *Intelligent systems, modelling and simulation (ISMS), 2010 international conference on, 2010* (pp. 287–291). IEEE.
36. Chamam, A., & Pierre, S. (2010). A distributed energy-efficient clustering protocol for wireless sensor networks. *Computers Electrical Engineering*, 36(2), 303–312.
37. Chandrakasan, A., Smith, A., & Heinzelman, W. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4), 660–670.
38. Handy, M., Haase, M., & Timmermann, D. (2002). Low energy adaptive clustering hierarchy with deterministic cluster-head selection. In *International workshop on mobile and wireless communications network, 2002* (pp. 368–372). Citeseer.
39. Kulkarni, S. & Arumugam, M. (2004). TDMA service for sensor networks. In *International conference on distributed computing systems workshop* (pp. 604–609).
40. Demirkol, I., Ersoy, C., & Alagoz, F. (2006). MAC protocols for wireless sensor networks: A survey. *IEEE Communications Magazine*, 44(4), 115–121.

Author Biographies



Zahariah Manap received her B.E and M.E. in Communication and Computer Engineering from Universiti Kebangsaan Malaysia, Selangor, Malaysia in 2000 and 2003 respectively. She has been working as a lecturer at UTeM, Melaka, Malaysia since 2003, teaching many subjects in the field of electronics and telecommunications engineering. She is currently a Ph.D. student at Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia. Her research interests include clustering algorithms and routing protocols in Wireless Sensor Networks.



Borhanuddin Mohd Ali obtained his B.Sc. (Hons) Electrical and Electronics Engineering from Loughborough University in 1979; M.Sc. and Ph.D. from University of Wales, UK, in 1981 and 1985, respectively. He became a lecturer at the Faculty of Engineering UPM in 1985, made a Professor in 2002, and Director of Institute of Multimedia and Software, 2001–2006. He has been with MIMOS as a Principal Researcher, heading the Wireless Networks and Protocol Research Lab in 2007–2010 before came back to UPM. He was then heading the Institute of Advanced Technology (ITMA), UPM as director in 2010–2012. In 1997 he co founded the national networking testbed project code named Teman, and became Chairman of the MYREN Research Community in 2002, the successor to Teman. His research interest is in Wireless Communications and Networks where he publishes over 80 journal and 200 conference papers. He is a Senior Member of IEEE, a member of IET and a Chartered Engineer.



Chee Kyun Ng received his Bachelor of Engineering and Master of Science degrees majoring in Computer & Communication Systems from Universiti Putra Malaysia, Serdang, Selangor, Malaysia, in 1999 and 2002 respectively. He has also completed his PhD programme in 2007 majoring in Communications and Network Engineering at the same university. He is currently undertaking his research on wireless multiple access schemes, wireless sensor networks and smart antenna system. His research interests include mobile cellular and satellite communications, digital signal processing, and network security. Along the period of his study programmes, he has published over 100 papers in journals and in conferences.



Nor Kamariah Noordin received her B.Sc. in Electrical Engineering majoring in Telecommunications from University of Alabama, USA, in 1987. She became a tutor at the Department of Computer and Electronics Engineering, Universiti Putra Malaysia, and pursued her Masters Degree at Universiti Teknologi Malaysia and Ph.D. at UPM. She then became a lecturer in 1991 at the same department where she was later appointed as the Head from year 2000 to 2002. She is currently the Director of Corporate Planning Division at the Office of the Vice Chancellor. During her more than 20 years at the department she has been actively involved in teaching, research and administrative activities. She has supervised a number of undergraduate students as well as postgraduate students in the area of wireless communications, which led to receiving some national and UPM research awards. Her research work also led her to publish more than 100 papers in journals and in conferences.



Aduwati Sali is currently a Lecturer at Department of Computer and Communication Systems, Faculty of Engineering, Universiti Putra Malaysia (UPM) since July 2003. She obtained her PhD in Mobile Satellite Communications from University of Surrey, UK, in July 2009, her MSc in Communications and Network Engineering from UPM in April 2002 and her BEng in Electrical Electronics Engineering (Communications) from University of Edinburgh in 1999. She worked as an Assistant Manager with Telekom Malaysia Bhd from 1999 until 2000. She involved with EU-IST Satellite Network of Excellence (SatNEx) I & II from 2004 until 2009. She is the principle investigator for projects under the funding bodies Malaysian Ministry of Science, Technology and Innovation (MOSTI), Research University Grant Scheme (RUGS) UPM and The Academy of Sciences for the Developing World (TWAS-COMSTECH) Joint Grants. Her research interests are radio resource management, MAC layer protocols, satellite communications, wireless sensor networks, disaster management applications, 3D video transmissions.