On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management

Yazeed Al-Obaisat, Robin Braun
Institute of Information and Communication Technologies
University of Technology, Sydney
Sydney, Australia
yazeedal@eng.uts.edu.au

Abstract

With the recent technological advances in wireless communications, integrated digital circuits, and micro electro mechanical systems (MEMS); development of wireless sensor networks has been enabled and become dramatically feasible. Wireless sensor networks (WSNs) are large networks made of a numerous number of sensor nodes with sensing, computation, and wireless communications capabilities. Many various routing, power management, and data dissemination protocols have been designed for wireless sensor networks (WSNs) dependent on both the network architecture and the applications that it is designed for. In this paper, we present the state of the art of wireless sensor networks' architecture and design features. Also, in this paper, we introduce recent work on routing protocols for WSNs and their design goals and challenges. Also, an overview of the application that WSNs assist in is presented. Finally, several open research questions of wireless sensor networks management and issues are suggested and put forward.

1 Introduction

With the recent technological advances in wireless communications, processor, memory, radio, low power, highly integrated digital electronics, and micro electro mechanical systems (MEMS) [1]; it becomes possible to significantly develop tiny and small size, low power, and low cost multifunctional sensor nodes. These nodes are capable of wireless communications, sensing and computation (software, hardware, algorithms). So, it is clear that wireless sensor network is the result of the combination of sensor techniques, embedded techniques, distributed information processing, and communication mechanisms. A wireless sensor network (WSN) is a network that is made of hundreds or thousands of these sensor nodes which are densely deployed in an unattended environment with the capabilities of sensing, wireless communications and computations (i.e., collecting and disseminating environmental data). Many different routing, power management and data dissemination protocols have been designed for wireless sensor networks (WSNs), dependent on both the architecture of wireless sensor network (WSN) and the applications that WSN is intended to support. These protocols support the practical existence of WSNs and efficiently make them an integral part of our lives in the real world. These protocols are different from conventional ones; in essence they need to support various unique requirements and constraints to make wireless sensor networks practically useful and operating, these requirements and constraints are introduced by factors such as: memory, small-size, low-power consumption, fault-tolerance, low-latency, scalability, adaptivity, and robustness. In this paper, we present a review of recent ongoing work on designing and developing routing protocols for wireless sensor networks, describing their advantages and deficiencies, and introduce some recommendations for enhancements.

Consequently; many different academic and industrial applications have been developed based on wireless sensor networks. These applications cover many aspects ranging from military to civilians applications. The idea beyond these applications is that; densely deploying sensor nodes with capabilities of sensing, wireless communications, and computation in an unattended environment and /or a remote large geographical area will assist in measuring ambient conditions in that specific environment, and obtaining the characteristics about phenomenon surrounding these sensors; by transforming these sensed/gathered data into electrical signals that can be processed. Moreover, other applications for wireless sensor networks can be seen in environmental monitoring and control field (e.g., robot control), high-security smart homes, tracking, and identifications and personalization [2]. Although there are some previous works on surveying the architecture, applications, and communications protocols for wireless sensor networks [3-10], this survey is distinguished from these efforts in that; it integrates the design factors and requirements of routing, power management and data dissemination protocols for WSNs with the applications that these protocols are designed to support. On the other hand, this paper introduces a thorough review of the design factors, requirements and challenges for routing, power, data dissemination protocols for wireless sensor networks, and it combines the design factors and requirements for wireless sensor networks itself with the design factors and challenges of protocols intended towards WSNs.

Our paper is structured as follows: the state of the art of wireless sensor networks architecture and design goals, challenges, and requirements are discussed in section 2. In section 3, the architecture of the protocol stack for wireless sensor networks is introduced. In section 4, we present a thorough review of the recent ongoing research on routing protocols for wireless sensor networks, describing their design goals, characteristics, challenges, classifications, assumptions, their advantages and drawbacks, and our recommendations and directions for improvement and enhancement. Section 5, presents a brief review of the applications that based on wireless sensor networks with the focus on integrating these applications with the routing, power management and data dissemination protocols that support these applications. In section 6, several open research questions of wireless sensor networks management and issues are suggested and put forward. Finally, we outline our conclusions and highlight some recommendations and directions for future work in section 7.

2 The Communication Architecture of Wireless Sensor Networks and Design Factors and Requirements.

2.1 Communications Architecture for Wireless Sensor Networks.

We mentioned above that a wireless sensor network (WSN) is a network made of a numerous number of sensor nodes with sensing, wireless communications and computation capabilities. These sensor nodes are scattered in an unattended environment (i.e., sensor field) situated far from the user as shown in Fig.1.

The upper side of the architecture above in (Fig.1) represents the communication architecture for (WSNs). The main entities that build up the architecture are [6]:

• The Sensor nodes that form the sensor network. Their main objectives are making discrete, local measurement about phenomenon surrounding these sensors, forming a wireless network by communicating over a wireless medium, and collect date and rout data back to the user via sink (Base Station).

• The sink (Base Station) communicates with the user via internet or satellite communication. It is located near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the sink by a multi-hop infrastructureless architecture through the sink.

• Phenomenon which is an entity of interest to the user to collect measurements about. This phenomenon sensed and analyzed by the sensor nodes.

• The user who is interested in obtaining information about specific phenomenon to measure/monitor its behavior.

2.2 Design Factors and Requirements

In this sub-section, we intend to describe the design factors of overall wireless sensor networks communications architecture as well as the design factors of protocols and algorithms for wireless sensor networks (WSNs). Many design factors have been addressed by many researchers in this field. These design factors are surveyed below. These factors serve as hints or guidelines to design a protocol or algorithm for WSNs.

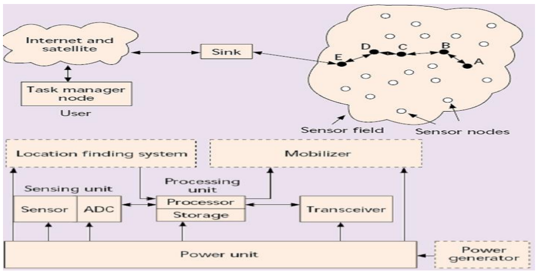

Figure 1: Sensor nodes scattered in a sensor field And The Components of a single sensor node (source [3]).

• *Reliability*: Reliability or fault tolerance or of a sensor node is the ability to maintain the sensor network functionalities without any interruption due to sensor node failure [11,12]. Sensor node may fail due to lack of energy, physical damage, communications problem, inactivity (a node becomes suspended), or environmental interference. Reliability is modeled in [12] using the Poisson distribution to capture the probability of not having a failure within the time interval (0,t):

$$R_k(t) = e^{-\lambda}k^t, \tag{1}$$

Where λ_k : is the failure rate of sensor node k and t is the time period.

• *Density and Network Size/Scalability*: hundreds, thousands or millions of sensor nodes may be deployed to study a phenomenon of interest to users. The density of these nodes affects the degree of coverage area of interest. The networks size affects reliability, accuracy, and data processing algorithms [13]. The density can range from a fewer sensor nodes to a hundred in a region that can be less than 10m in diameter. The density μ is calculated as in [12]:

$$\mu(R) = (N\pi R^2)/A, \tag{2}$$

Where N is the scattered sensor nodes in region A, and R is the radio transmission range. Basically, $\mu(R)$ gives the number of nodes within the transmission radius of each node in region A.

• *Sensor Network Topology*: the topology of a network affects many of its characteristics like; latency, capacity, and robustness. Also, the complexity of data routing and processing depends on the network topology. Densely deploying thousands of sensor nodes in sensor field (Fig.1) requires careful handling of network topology maintenance [3,13]. Paper [3] defined three phases related to topology maintenance and changes (e.g., malfunctioning of some sensor nodes); *Predeployment and deployment phase, Postdeployment phase, and Redeployment of additional nodes phase.*

• *Energy Consumption*: one of the components of sensor nodes is the power source which is limited enough. A sensor node is battery-operated. Hence; life time of a sensor node depends strongly on the battery life time, especially where no power source replenishment is possible in some applications scenarios. Since the main objectives of sensor nodes are sensing/collecting events, data processing, and data transmission through routing; then the power resource can be divided among these three operations (sensing, computation, and communications). On the other hand; life time of a sensor node plays a key role on energy efficiency and robustness of sensor node. Hence; many researches are focusing on designing power-aware protocols and algorithms for wireless sensor networks with the goal of minimization of energy expenditure [3,5,13].

• *Hardware Constraints*: sensor nose consists of four main components (the lower side of Fig.1): a sensing units, processing unit, transmission unit, and power unit. They may also have application-dependent additional components such as position/location finding systems, power generator, and mobilizer. Sensing units are usually composed of two subunits: Sensors and ADC (Analog to Digital Converter). The Analog signals produced by sensors based on the observed phenomenon are converted by ADC to digital signal and fed into the processing unit to be processed. Processing unit, generally associated with storage unit, manages the procedures that make the sensor node collaborate with other nodes to perform the assigned sensing tasks. Transmission unit that connects the sensor node to the network. Power unit may be supported by a power scavenging such as solar cells. Since most of the sensor network routing techniques and sensing tasks require knowledge of location with high accuracy, thus it is common that a sensor node has a position/location finding system. Sometimes, a mobilizer is needed to move sensor node to carry out the assigned tasks. Hence, the size of sensor node in of a great design issue [3].

• *Data Aggregation/Data Fusion*: it is the task of reducing data size by summarizing the data into a set of meaningful information via computation while data are propagating through the wireless sensor network (in this context). As sensor networks made of large number of sensor nodes; this can easily congest the network and flooding it with information [14]. Hence; a solution to data congestion in sensor networks is to use computation to aggregate or fuse data within WSN, then transmit only the aggregated data to the controller. Many approaches within the context of WSNs are proposed to facilitate data aggregation, also known as data fusion, such as; (1) diffusion algorithms which assume that homogeneous data propagate to destination throughout the network by transmitting data from one node to another, then these data may be aggregated using diffusion algorithms, (2) Streaming queries are based on SQL extension for continuous querying, And (3) Event Algebra which assists in composing simple events into composite ones with the help of event graph [13].

• *Transmission Media*: in a multi-hop sensor network, a wireless medium is used to link nodes for communications goal. These links can be formed by radio (e.g., Bluetooth compatible 2.4 GHz transceiver), Infrared which is license-free and robust to interference from electrical devices, and Optical media.

• *Security*: security aspects in WSNs have been focused on the centralized communications approaches. Some of the threats to a WSN are described in [15,16,17] and categorized as follows: Passive Information Gathering, False Node, Node Outage, Supervision of a Node, Node Malfunction, Message Corruption, Denial of Service, and Traffic Analysis (see [15,16] for more details). There is a need to develop distributed security approaches for wireless sensor network.

• *Self-Configuration*: it is essential for wireless sensor network to be self-organize; since the densely deployed sensor nodes in a sensor field may fail due to many reasons (e.g., lack of energy, physical destruction, environment interference, communications problem, inactivity, etc) and new nodes may join the network. On the other hand; sensor nodes work unattended in a dynamic environment; so they need to be self-configuration to establish a topology that supports communications under severe energy constraints. It is worthy mention that self-configuration in WSN is an essential factor to maintain a WSN functions properly and serve its purpose [18,19].

• *Network dynamics*: in many applications, the movement of sensor nodes or the base station (sink) is essential. This means that sensor nodes are moving nodes (i.e., not stationary as assumed by many of network architectures). This has arisen the routing stability issues as well as energy, bandwidth, etc. Moreover, the specific sensed phenomenon may be either dynamic (e.g., target detection/ tracking applications) or stationary (e.g., forest monitoring) depending on the applications.

• *Quality of Service*: for some applications, data delivery within a bounded latency (i.e., time constrained applications) is of great importance; otherwise, the sensed data that delivered after certain latency will be useless. In other applications (e.g., not time-constrained applications), the conservation of power is more important than the quality of the sent data. Hence; there is a trade off between the quality of service/the quality of data sent and the energy conservations or consumption depending on the applications [20,21].

• *Coverage*: the sensor node's view of the environment that it is situated in is limited both in range and in accuracy. This means the ability of sensor nodes to cover physical area of the environment is limited [13,22].

• *Connectivity*: a permanent connection between any two individual sensor nodes that are densely deployed in a sensor network defines the network connectivity. The connectivity is of great importance, since it influences communications protocols' design and data dissemination techniques. Also, it is worthy mentioning that connectivity of sensor network may not prevent the network topology from being variable and the network size from reduction as a result of the death or failure of some sensor nodes due to the reasons mentioned earlier in the paper [13,22].

3 The Architecture of the Protocol Stack for Wireless Sensor Networks

The architecture of protocol stack [3] used by the sink and sensor nodes is shown in Fig. 2. This protocol stack integrates power and routing awareness (i.e., energy-aware routing), integrates data with networking protocols (i.e., data aggregation), communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes (i.e., task management plane). This protocol stack (Fig. 2) is made up of physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane, and task management plane. The physical layer addresses the needs of a robust modulation, transmission and receiving techniques.

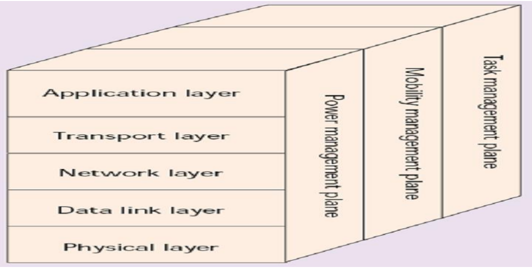

Figure 2: : The wireless sensor networks protocol stack (source [3]).

The network layer takes care of routing the data supplied by the transport layer. The transport layer helps to maintain the flow of data if the wireless sensor network application requires it. Depending on the sensing tasks, different types of application Software can be set up and used on the application layer.

The power management plane manages how a sensor node uses its power and manages its power consumption among the three operations (sensing, computation, and wireless communications). For instance, to avoid getting duplicated messages, a sensor node may turn off it receiver after receiving a message from one of its neighbors. Also, a sensor node broadcasts to its neighbors that it is low in power and can not take part in routing messages. The remaining power is reserved for sensing and detecting tasks. The mobility management plane detects and registers the movement/mobility of sensor nodes as a network control primitive. Hence; a route back to the user is always kept, and sensor nodes can keep track of who their neighbors of other sensor nodes are. Therefore, the nodes can balance their power and task usage by knowing this situation. The task management plane (i.e., cooperative efforts of sensor nodes) balances and schedules the events' sensing and detecting tasks from a specific area. Hence; not all of the sensor nodes in that specific area are required to carry out the sensing tasks at the same time. Depending on their power level, some nodes perform the sensing task more than others.

4 Sensor Networks Protocols

4.1 Design Challenges

Among the design factors and challenges for wireless sensor networks' protocol are energy depletion, robustness to dynamic environment, and scalability to numerous number of sensor nodes. Some recommended solutions to these challenges are as follows: a reduction in the active duty cycle for each sensor node, a minimization of data communications over the wireless channel (i.e., aggregation, communicate network state summaries instead of actual data), and maximization of network life time (i.e., minimum energy routing) will give hand to the energy depletion challenge. Scalability, on another hand; may be enhanced by organizing network in a hierarchical manner (e.g., clustering) and utilizing localized algorithms with localized interactions among sensor nodes, while robustness to environmental changes, may be improved through self-organizing, self-healing, self-configuring, and self-adaptive networks.

4.2 Classification of Sensor Networks Routing Protocols

There are different ways by which we can classify the sensor networks' routing protocols. According to network structure, these routing protocols can be classified as flat, hierarchical, and location-based protocols. Also, these protocols can be classified into multipath-based, query-based, negotiation-based Quality of Service (QoS)-based, or coherent-based depending on the protocol operation. Moreover, these protocols can be classified into three categories, namely, reactive, proactive, and hybrid protocols depending on route discovery. In flat-based routing, all nodes are assigned the same roles or functionalities. In hierarchical-based routing, nodes will play different roles or functionalities, aiming at routing techniques clustering the nodes with different roles so that the heads of the cluster can do some data aggregation or confusion in order to save power, while in location-based routing; sensor nodes' positions are exploited to route the data to specific regions other than the whole network. On the other hand; in reactive protocols, routes are computed on demand. In proactive protocols, routes are computed before they are needed, while hybrid protocols utilize a combination of the ideas of both reactive and proactive protocols.

4.3 WSNs vs.MANETs

A realization of sensor networks' characteristics, design, and applications require wireless ad hoc networking mechanisms. Among the existing ad hoc networks models, the mobile ad hoc networks (MANETs) are the closest to sensor networks. Although MANETs and Wireless Sensor Networks (WSNs) share some similar characteristics, such as; network topology is ad hoc (i.e., not fixed), power and bandwidth are an expensive resources, wireless communication mediums (i.e., wireless communications links) are used to connect nodes, the protocols and algorithms developed for MANETs are not suitable for the unique features and application requirements of WSNs because these two types of networks have different differences [3].

• The number of sensor nodes in WSNs can be several orders of magnitude higher than that in MANETs.

• Unlike a node in MANETs, sensor node may not have a unique global IP address because of the large amount of overhead and the numerous number of sensors.

• Sensor nodes are extremely cheaper and more tiny devices, not like ad hoc network nodes (e.g., PDAs, Laptops, etc), and usually they deployed in thousands.

• The communication paradigm used in WSNs is broadcasting, whereas MANETs are based on point-to-point communications.

• The topology of a WSN changes very frequently.

• Energy and bandwidth conservation is the main concern in WSN protocol design since power resources of sensor noses are very limited as well as computation, communication capabilities than their MANETs counterparts because of their low cost.

• Sensor nodes are prone to failure much more than nodes in MANETs. Consequently, it is so important to study new routing protocols for wireless sensor networks that will fulfill the above requirements. Many researches (academic and industrial) have been carried out on developing protocols and algorithms for WSNs with the focus on the development of energy-efficient, low-cost, secure, and fault tolerant sensor networks protocols. In this context, a thorough survey of these protocols is given with the emphasis on the design goals, characteristics, and the specific applications these protocols support.

5 Routing Protocols for WSNs

In this context, we introduce the most well-known routing protocols for wireless sensor networks. In this context, we introduce the most well-known routing protocols for wireless sensor networks.

A. Flooding

Flooding [23] is an old routing mechanism that may also be used in sensor networks. In flooding, a node sends out the received data or the management packets to its neighbors by broadcasting, unless a maximum number of hops for that packet are reached or the destination of the packets is arrived. However; there are some deficiencies for this routing technique [23]:

• Implosion: is the case where a duplicated data or packets are sent to the same node. Flooding is a function of the network topology. For instance; node A has K neighbor nodes which are neighbors of the node B, then node B will receive K copies of the data or message sent from node A .

• Overlap: if two sensor nodes cover an overlapping measuring region, both of them will sense/detect the same data. As a result, their neighbor nodes will receive duplicated data or messages. Overlapping is a function of both the network topology and the mapping of sensed data to sensor nodes.

• Resource blindness: In flooding, nodes do not take into account the amount of energy resource available to them at a given time. A WSN protocol must be energy resource-aware and adapts its sensing, communication and computation to the state of its energy.

B. GOSSIPING

Gossiping protocol is an alternative to flooding mechanism. In Gossiping [24], nodes can forward the incoming data/packets to randomly selected neighbor node. Once a gossiping node receives the messages, it can forward the data back to that neighbor or to another one randomly selected neighbor node. This technique assists in energy conservation by randomization. Although, gossiping can solve the implosion problem, it can not avoid the overlapping problem. On the other hand; gossiping distribute information slowly, this means it consumes energy at a slow rate, but the cost is long-time propagation is needed to send messages to all sensor nodes.

C. SPIN

SPIN (Sensor Protocols for Information via Negotiation) [25] is a family of adaptive protocols for WSNs. Their design goal is to avoid the drawbacks of flooding protocols mentioned above by utilizing data negotiation and resource-adaptive algorithms. SPIN is designed based on two basic ideas; (1) to operate efficiently and to conserve energy by sending meta-data (i.e., sending data about sensor data instead of sending the whole data that sensor nodes already have or need to obtain), and (2) nodes in a network must be aware of changes in their own energy resources and adapt to these changes to extend the operating lifetime of the system. SPIN has three types of messages, namely, ADV, REQ, and DATA.

• ADV: when a node has data to send, it advertises via broadcasting this message containing meta-data (i.e., descriptor) to all nodes in the network.

• REQ: an interested node sends this message when it wishes to receive some data.

• DATA: Data message contains the actual sensor data along with meta-data header. SPIN is based on data-centric routing where the sensor nodes send ADV message via broadcasting for the data they have and wait for REQ messages from interested sinks or nodes. The semantics of SPIN's meta-data format is application dependent and not supported by SPIN. In another words; SPIN uses application specific meta-data to name the sensed data. Although, SPIN has some advantages, such as (1) solving the problems associated with classic flooding protocols, and (2) topological changes are localized, it has its own drawbacks like; (1) scalability, SPIN is not scalable, (2) if the sink is interested in too many events, this could make the sensor nodes around it deplete their energy, and (3) SPIN's data advertisement technique can not guarantee the delivery of data if the interested nodes are far away from the source node and the nodes in between are not interested in that data. SPIN-1 starts when a node has new data to share. This node sends out an ADV message containing a descriptor (i.e., meta-data) about the data it has to its neighbor nodes. An interested neighbor in that data sends out a REQ message to the broadcasting node, which then in turns sends out the actual data along with the meta-data. In SPIN-2, which is simply SPIN-1 with a low-energy threshold, if a node has new data to share or received an ADV message, it will not take part in the protocol if it does not have enough energy.

D. Directed Diffusion

Directed diffusion [26] is another data dissemination and aggregation protocol. It is a data-centric and application aware routing protocol for WSNs. It aims at naming all data generated by sensor nodes by attribute-value pairs. Directed diffusion consists of several elements; first of all, naming; where task descriptors, sent out by the sink, are named by assigning attribute-value pairs. Secondly, interests and gradients; the named task description constitutes an interest that contains timestamp field and several gradient fields. Each node stores the interest in its interest cache. As the interests propagate throughout the network, the gradients from the source back to the sink are set up. Thirdly, data propagation, when the source has data for the interest, it sends out the data to the interest (i.e., sink) along the interest's gradient path. Fourthly, after the interest (sink) starts receiving low rate data events, it reinforce one particular neighbor to draw down higher quality (higher data rate) events. This feature of directed diffusion is achieved by data-driven local rules. Directed diffusion assists in saving sensors' energy by selecting good paths by caching and processing data in-network since each node has the ability for performing data aggregation and caching. On the other hand; Directed diffusion has its limitations such as; implementing data aggregation requires deployment of synchronization techniques which is not realizable in WSNs. Also, the overhead in data aggregation involves recording information. These two drawbacks may contribute to the cost of sensor node, which is not desired.

E. LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) [27] is a self-organizing, adaptive clustering-based protocol that uses randomized rotation of cluster-heads to evenly distribute the energy load among the sensor nodes in the network. LEACH based on two basic assumptions: (a) base station is fixed and located far away from the sensors, and (b) all nodes in the network are homogeneous and energy-constrained. The idea behind LEACH is to form clusters of the sensor nodes depending on the received signal strength and use local cluster heads as routers to route data to the base station. The key features of LEACH are:

- Localized coordination and control for cluster set-up and operation.
- Randomized rotation of the cluster ”base stations” or ”cluster-heads” and the corresponding clusters.
- Local compression to reduce global communication.

In LEACH, the operation is separated into fixed-length rounds, where each round starts with a setup phase followed by a steady-state phase. The duration of a round is determined priori. LEACH algorithm works as follows:

1. Advertisement phase: in this phase, nodes elect themselves to be a cluster-heads for the current round (r) through a cluster-head advertisement message. For this cluster-head advertisement, the cluster heads use CSMA MAC protocol. After the completion of this phase, and depending on the received advertisement signal strength; the non cluster-head nodes (their receivers must be kept on during this phase to hear the advertisements of all cluster-heads) determine the cluster to which they will belong to for this current round (r). At each round, a node n selects a random number k that is between 0 and 1. If k is less than a threshold T(n), then the node becomes a cluster-head for the current round (r).

$$T(n) = \begin{cases} \frac{P}{1-P(r\text{mode}(1/p))}, & \text{if } n \in G, \\ 0, & \text{otherwise.} \end{cases} \qquad (3)$$

   Where P is the desired percentage of cluster-heads, r is the current round, and G is the set of nodes that have not been cluster heads in the last $1/P$ rounds. Since k is randomly selected, then the number of cluster heads may not be fixed.

2. Cluster set-up phase: after each non-cluster-head node will has decided to which cluster it belongs, it informs the cluster-head node that it will be a member of the cluster. So, each node transmits this information back to the cluster-head using CSMA MAC protocol.

3. Schedule Creation phase: The cluster-head node receives all the messages for nodes that would like to be included in the cluster. Based on the number of nodes in the cluster, the cluster-head node creates a TDMA schedule telling each node when it can transmit. This schedule is broadcast back to the nodes in the cluster.

4. Data Transmission phase: after the creation of both the clusters and the TDMA schedule (TDMA is fixed), nodes in the cluster start transmitting the data they already have during their allocated transmission time to the cluster-head (cluster-head node keeps its receiver on all the time to receive the sent data). Once all the data (sent by nodes in the cluster) have been received by the cluster-head node, it will perform signal processing function to compress the data into a single signal (the steady-state operation of LEACH networks).

Although, LEACH has shown good features to sensor networks, such as clustering architecture, localized coordination and control, randomized rotation of cluster head, and local compression to reduce global communications (energy consumption minimization), it suffers from the following drawbacks:

- It can not be applied to time-constrained application as it results in a long latency.
- The nodes on the route a hot spot to the sink could drain their power fast. This problem known as ”hot spot” problem.
- The number of clusters may not be fixed every round due to the selection of k [28].
- It can not be applied to large sensor networks.

F. PEGASIS

PEGASIS (Power-Efficient GAthering in Sensor Information Systems) is a greedy chain-based power efficient algorithm [29]. Also, PEGASIS is based on LEACH (the scenario and the radio model in PEGASIS are the same as in LEACH). The key features of PEGASIS are

- The BS is fixed at a far distance from the sensor nodes.
- The sensor nodes are homogeneous and energy constrained with uniform energy.
- No mobility of sensor nodes.

PEGASIS is based on two ideas; Chaining, and Data Fusion. In PEGASIS, each node can take turn of being a leader of the chain, where the chain can be constructed using greedy algorithms that are deployed by the sensor nodes. PEGASIS assumes that sensor nodes have a global knowledge of the network, nodes are stationary (no movement of sensor nodes), and nodes have location information about all other nodes. PEGASIS performs data fusion except the end nodes in the chain. PEGASIS outperforms LEACH by eliminating the overhead of dynamic cluster formation, minimizing the sum of distances that non leader-nodes must transmit, limiting the number of transmissions and receives among all nodes, and using only one transmission to the BS per round. PEGASIS has the same problems that LEACH suffers from. Also, PEGASIS does not scale, can not be applied to sensor network where global knowledge of the network is not easy to get.

H. GEAR

GEAR (Geographical and Energy Aware Routing) [30] is a recursive data dissemination protocol WSNs. It uses energy aware and geographically informed neighbor selection heuristics to rout a packet to the targeted region. Within that region, it uses a recursive a geographic informed mechanism to disseminate the packet. GEAR, like other sensor networks protocols, developed according to some assumptions in mind:

- Sensor nodes are static (i.e., immobile).

- There is an existence of a localization system that enables each node to know its current position.

- Sensor nodes are energy-constrained accompanied with location information about all other nodes (i.e., each node knows its location and its energy level, and its neighbor's location and remaining energy level.

- The link that connects nodes is bi-directional, i.e., if node N can hear from a neighbor node Mi, then its transmission range can reach node Mi. GEAR has two phases: (1) forwarding the packets toward the targeted region, and (2) forwarding the packets within the targeted region. During the first phase; packets/queries are routed to the region R using energy-aware and geographically informed neighbor selection heuristics. In the second phase, and within that region R, it uses a recursive a geographic informed forwarding mechanism or restricted flooding to disseminate the packets inside R. Also, in GEAR, each node maintains state (called learned cost) $h(N, R)$ to region R. Also, each node has a learned cost, $h(N_i, R)$, of its neighbor N_i, if it does not have $h(N_i, R)$, it computes the estimated cost $c(N_i, R)$ as a default value for $h(N_i, R)$ as follows:

$$c(N_i, R) = ad(N_i, R) + (1 - \alpha)e(N_i), \tag{4}$$

where α is a tunable weight, $d(N_i, R)$ is the distance from Ni to the centroid D of R normalized by the largest such distance among all neighbors of N, and e(Ni) is the largest consumed energy at node Ni normalized by the largest consumed energy among neighbors of N. Equation (4) shows that the estimated cost is a combination of residual energy and distance to the destination. From the above analysis, we conclude that GEAR reduces the energy consumption for the route set up. On the other hand, GEAR is not scalable and does not support data diffusion.

Based on the analysis and thorough survey of the mentioned protocols, we believe that an efficient routing protocol for wireless sensor networks should have some key features, such as:

- Data Aggregation: we believe that reducing the data size quickly using computation will play a key role in supporting efficient query processing, and reducing the overall network overhead. Hence saving power.

- Dynamic clustering architecture is required. Since such architecture will preclude cluster heads from depleting their energy quickly. Hence, long network's lifetime.

- Threshold for sensor nodes on data transmission and dissemination: this will help in saving energy by reducing unnecessary transmissions (i.e., redundancy) and giving the network long lifetime.

- Randomized path selection: multi-path selection to destination could improve fault tolerance and handle the overhead of network load.

- Mobility: most of the current protocols assume that sensor nodes are static (i.e., immobile). However, for some applications or in some situations, nodes need to be mobile. Hence, new routing algorithms are needed to handle the mobility and network topology changes.

- Self-configuration: since sensor nodes are prone to failure due to some factors or new sensor nodes may join the network, an update, self-configuration, self-healing, and adaptation to changes in network topology or environmental changes should be considered.

- Security: there is a desperate need to develop distributed security approaches for wireless sensor network. Hence, achieving secure routing.

- Quality-of-Service, dependability, and localization need to be considered and given more attention. Time synchronization: time synchronization techniques are required since time plays a key role in WSNs.

6 Applications

Sensor networks are applied in a wide range of areas, such as military applications, public safety, medical, surveillances, environmental monitoring, commercial applications, habitat and tracking [31,32,33]. In general, sensor networks will be ubiquitous in the near future, since they support new opportunities for the interaction between humans and their physical world. In addition, sensor networks are expected to contribute significantly to pervasive computing and space exploration in the next decade. Deploying sensor nodes in an unattended environment will give much more possibilities for the exploration of new applications in the real world. In this context, we will look briefly at some of these applications. The idea behind these applications is that; densely deploying sensor nodes with capabilities of sensing, wireless communications, and computation in an unattended environment, will assist in measuring its ambient conditions, and obtaining the characteristics about phenomenon of interest surrounding these sensors; by transforming these sensed/gathered data into electrical signals that can be processed. Moreover, other applications for wireless sensor networks can be seen in environmental monitoring and control field (e.g., robot control), high-security smart homes, tracking, and identifications and personalization [2]. Among these applications:

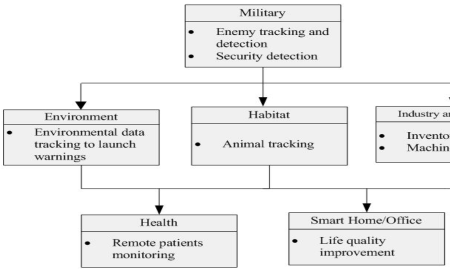

Figure 3: : Sensor Network Applications Development (source [30]).

• Military applications, such as environment monitoring, tracking and surveillance applications. Sensor nodes that from sensor network are dropped to the field of interest (e.g., behind the hostile forces, spy, etc), and remotely controlled by user who is situated far from them. User may assign new tasks to be performed by these sensor nodes.

• Environmental monitoring, such as animals tracking, forest detection and flood detection, and weather prediction and forecasting. Commercial applications: such as seismic activities monitoring and prediction, and smart environment applications.

• Health applications, such as tracking and monitoring of doctors and patients in or out the hospitals by providing them with sensors.

• Automation and control (e.g., robotics control).

7 Wireless Sensor Networks Management

In this section, our aim is to provide a discussion of the management issues for WSNs, their design impact on WSNs, and to highlight some guidelines and directions to be considered when designing a management system for WSNs. Throughout this work, we identified that wireless sensor networks are large networks made of densely deployed (hundreds, thousands or magnitude of order of ten thousands in some situations) sensor nodes in an unattended environment. In essence, nodes are of magnitude of order more than those in traditional computer networks. These nodes are characterized by constraints, namely, energy and bandwidth constraints, and nodes-as a common fact-are prone to faults. Sensor networks have different architecture than traditional wired data networks. Sensor networks are set up in a random manner. On the other hand, the WSNs are applications-dependent which implies that the management requirements also change among sensor networks, and a configuration error of a WSN in unpredictable situations may cause the fail/loss of the whole entire network even before it starts to operate [34,35,36]. Also, the behavior of WSN is highly unpredictable and dynamic [37]. All these factors have to be incorporated by various sensor network models that describe the current network's states. Some of the possible suggested models are:

• Network Topology Model: it describes the actual topology map and the connectivity and/or reachability of the network. It also may assist routing operations and obtaining information a bout future deployment of nodes [37], since the topology of a network affects many of its characteristics, such as latency, capacity, and robustness, as well as the complexity of data routing and processing. This requires careful handling of network topology maintenance [3,13]. Paper [3] defined three phases related to topology maintenance and changes (e.g., malfunctioning of some sensor nodes); Predeployment and deployment phase, Post-deployment phase, and Re-deployment of additional nodes phase.

• Residual Energy Model: describes the remaining energy level of the nodes or the network. Using this information as well as the data from network topology, coupled together; would make it possible to identify the weak areas (i.e., areas that have short lifetime) of the network [37].

Cost Model: describes the cost of equipment, energy, and human cost to maintain the desired performance levels of the network.

Usage Patterns Model: represents the activity of the network in terms of period of time for nodes' activity, quantity of data transmitted per sensor unit or the movements made by the target, and tracking of hot spots in the network to avoid hot spot problem [37].

Behavioral Model: describes the behavior of the network. Since sensor networks are highly unpredictable, dynamic, and unreliable, statistical and probabilistic models may be much more efficient in estimating the network behavior than estimating the network behavior than deterministic models.

• Coverage Area Model: a sensing coverage area map that represents the actual sensor's view of the environment and communications coverage map that describes the communication coverage area from the range of the RF transceiver [37].

The above models would build up the MIB (management Information base). Also, these models could be used for different network management functions such as: deployment of sensors, network operating parameters, coverage area supervision function, topology map discovery function, network connectivity discovery function, node localization discovery function, prediction function for future network states, monitored area definition function, design of sensor networks, energy level function, self-test function, etc [35,37]. Since sensor nodes are unattended as well as the environment these sensors are situated in; human intervention to perform some network maintenance tasks, such as configuration, protection, healing, and energy replenishment is becoming impractical. So, it is our belief that self-management solutions (self-configuration, self-healing, self-optimization, self-protection, self-service, self awareness, and self knowledge) [38,39], are a promising functional key management solution that can cope with the various unique requirements and constraints, imposed on the wireless sensor networks due to resource restrictions introduced by some factors (e.g., small-size, memory, low-power consumption, fault-tolerance, low-latency, scalability, adaptivity, and robustness). Attempts to build up management system that can combine all of these features are proposed by some interested researchers in this field. L. B. Ruiz, et al. [36,37,38], have proposed an architecture for WSN management called "MANNA". The MANNA management architecture took into account three management dimensions: (1) the management functional areas (i.e., Fault, Configuration, Accounting, Performance, and Security), (2) the management levels (i.e., Business management, Service management, Network management, Network element management, and Network element), and (3) WSN functionalities, such as Configuration, Maintenance, Sensing, Processing, and Communication. In their work [36,37,38], the authors argue that; "in WSNs, all operational, administrative and maintenance characteristics of the network elements, the network, the services, and business, as well as the adequate execution in the activities of configuration, maintenance, sensing, processing and communication are dependent on the configuration of the WSN". Also, other attempts have been carried out on the power management for WSNs [40,41,42,43]. Also, it is our belief that sensor network management could borrow from artificial intelligence approach, in general, swarm intelligence [44], in particular, to achieve scalable, robust, and adaptable management system for WSNs. Different algorithms, optimization techniques, and collective intelligence could be adapted and brought to the field of wireless sensor network.

8 Conclusion

In this paper, we presented the state of the art of wireless sensor networks; their architecture, routing protocols for WSNs, their applications. Also, in this paper, we introduced some recommendation and directions as guidelines and hints that would assist and give enhancements to the future design of protocols and algorithms for wireless sensor networks. Also, in this paper, a brief review of the application based on wireless sensor networks is given. Finally, our directions and recommendations for wireless sensor network management are suggested and put forward.

9 References

[1] B. Warneke, K.S.J. Pister, "MEMS for Distributed Wireless Sensor Networks," in Proc. of 9th International Conf. on Electronics, Circuits and Systems, Dubrovnik, Croatia, September, 2002.

[2] R. Min, et al., "Low Power Wireless Sensor Networks", in the Proceedings of International Conference on VLSI Design, Bangalore, India, January 2001.

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on Sensor Networks," IEEE Communications Magazine, vol. 40, Issue: 8, pp. 102-114, August 2002.

[4] K. Sohrabi, et al., "Protocols for Self-organization of A Wireless Sensor Network," IEEE Personal Communications, vol. 7, No. 5, pp. 16-27, October, 2000. [Available from the World Wide Web (WWW):
www.comsoc.org/pci/private/2000/oct/pdf/pottie.pdf

[5] R. C. Shah, and J. M. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Senso Networks," in proc. of IEEE Wireless Communications and Networking Conference (WCNC), Orland, FL, 2002. [available:
http://www.motelab.org/papers/wcnc.rahul.pdf]

[6] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of Wireless Micro-senor Network Models," ACM SIGMOBILE, Mobile Computing and Communications Review, vol.6, issue: 2, pp. 28-36, April, 2002. [Available from the world wide web (WWW):
http://www.cs.binghamton.edu/ nael/research/papers/
taxonomy.pdf]

[7] J. N. Al-Kamal, and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks, A survey," Wireless Communications, IEEE, vol. 11, pp. 6-28, 2004. [See also IEEE Personal Communications].

[8] K. Akkaya, and M. Younis, "A survey on Routing Protocols for Wireless Sensor Networks," Elsevier Ad Hoc network Journal, vol.3, pp.325-349, 2005

[9] K. Holger, W. Andreas, "A short Survey of Wireless Sensor Networks," Technical Report [TKN Technical Report TKN-03-018], Berlin, October, 2003. [Available:
http://www.tkn.tu-berlin.de/publications/papers/
TechReport$_{0}$3$_{0}$18.pdf]

[10] A.A. Ahmed, H. Shi, Y. Shang, "A Survey on Network Protocols for Wireless Sensor Networks," In Proc. of International Conference on Information Technology: Research and Education (ITRE'03), pp. 301 - 305, 11-13 Aug. 2003.

[11] C. Shen, C. Srisathapornphat, and C. Jaikaeo, "Sensor Information Networking Architecture and Applications", IEEE Personal Communication. pp. 52-59, Aug. 2001.

[12] K. G. Hoblos, M. Staroswiecki, and A. Aitouche, "Optimal Design of Fault Tolerant Sensor Networks," IEEE Int'l. Conf. Cont. Apps., Anchorage, AK, pp. 467-72, Sept. 2000.

[13] Eiko Yoneki, Jean Bacon, "A survey of Wireless Sensor Network technologies: research trends and middleware's role," Technical Report, no: 646, $UCAM-CL-TR-646$,
[Available from the World Wide Web
http://www.cl.cam.ac.uk/TechReports/$UCAM-CL-TR-$646.pdf]

[14] H. Cam, S. Ozdemir, P. Nair, and D. Muthuavinashippan, "ESPDA: Energy-Efficient and Secure Pattern Based Data Aggregation for Wireless Sensor Networks," in press, IEEE Sensor, Toronto, Canada, 2003.

[15] Perrig, A. et al. "Security in wireless sensor networks," Communications of the ACM (CACM), Wireless sensor networks, Special Issue: Wireless sensor networks, vol. 47, issue: 6, pp. 53-57, June, 2004.

[16] Avancha, S. et al. "Wireless Sensor Networks," Kluwer Academic/Springer Verlag Publishers, 2003.

[17] E. Shi, A. Perrig, "Designing Secure Sensor Networks," IEEE Wireless Communications, pp.38- 43, December, 2004.

[18] N. Bulusu et al., "Scalable coordination for wireless sensor networks: Self-configuring localization systems," In Proc. of the 6th International Symposium on Communication Theory and Applications (ISCTA'01), Ambleside, UK, 2001.

[19] B. Krishnamachari, "On the Complexity of Distributed Self-Configuration in Wireless Networks", Kluwer Academic Springer Publishers, Telecommunication Systems, vol. 22, issue: 1-4, pp. 33-59, 2003.

[20] Iyer, R. and L. Kleinrock, ”QoS Control for Sensor Networks,” presented at the IEEE International Communications Conference (ICC’ 03), Anchorage, AK, May 11-15. 2003.

[21] J. Kay, J. Frolik, ”Quality of Service Analysis and Control for Wireless Sensor Networks,” In Proc. of the 21st International Conf. on Mobile Ad-Hoc and Sensor Systems (MASS’04), pp. 359-368, Fort Lauderdale, Florida, USA, 25-27 October, 2004.

[22] Kay Romer and Friedemann Mattern, ”The Design Space of Wireless Sensor Networks,” IEEE Wireless Communications, pp. 54- 61, Dec. 2004. [Also, available: http://www.vs.inf.ethz.ch/publ/papers/wsn-designspace.pdf]

[23] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, ”Adaptive Protocols for Information Dissemination in Wireless Sensor Networks,” in proc. ACM MobiCom ’99, Seattle, WA, 1999.

[24] S. M. Hedetniemi, S. H. Hedetniemi, and A. Liestman, ”A Survey of Gossiping and Broadcasting in Communication Networks,” Networks, vol. 18, 1988.

[25] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, ”Negotiation-base protocols for Disseminating Information in Wireless Sensor Networks,” Wireless Networks, vol. 8, pp. 169-185, 2002.

[26] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, ”Directed Diffusion for Wireless Sensor Networking,” IEEE/ACM Transactions on Networking, vol. 11, pp. 2-16, Feb. 2003.

[27] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, ”Energy-Efficient Communication Protocol for Wireless Micro-Sensor Networks,” in Proc. of the 33rd Annual Hawaii International Conf. on System Sciences, pp. 3005-3014, 2000.

[28] S. Dai; X. Jing; L. Li, ”Research and analysis on routing protocols for wireless sensor networks,” In Proc. of International Conference on Communications, Circuits and Systems, vol. 1, pp. 407 - 411, 27-30 May, 2005.

[29] S. Lindsey, C. S. Raghavendra, ”PEGASIS: Power-Efficient Gathering in Sensor Information Systems,” presented at Proc. of IEEE Aerospace Conference, Montana, 2002.

[30] Y. Yu, R. Govindan, D. Estrin, ”Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks,” UCLA Computer Science Department UCLA-CSD TR-01-0023, May, 2001.

[31] I. Khemapech, I. Duncan and A. Miller, ”A Survey of Wireless Sensor Networks Technology”, http://www.dcs.st-and.ac.uk/ pst/resources/publications/ khemapach05survey.pdf , 2005.

[32] Ning Xu, ”A Survey of Sensor Network Applications,” available form the World Wide Web: http://enl.usc.edu/ ningxu/papers/survey.pdf

[33] V. Rajaravivarma,Y. Yang; T. Yang, ”An Overview of Wireless Sensor Network and Applications,” In Proc. of the 35th Southeastern Symposium on System Theory, pp. 432 - 436, 16-18 March, 2003.

[34] L.B. Ruiz, T.R.M. Braga,; F.A. Silva,; H.P. Assuncao, J.M.S. Nogueira, A.A.F. Loureiro, ”On the Design of a Self-Managed Wireless Sensor Network,” Communications Magazine, IEEE, vol. 43, Issue 8, pp.95 - 102, Aug. 2005.

[35] L. B. Ruiz, J. M. S. Nogueira, and A. A. F. Loureiro, ”MANNA: A Management Architecture for Wireless Sensor Networks,” IEEE Communication Magazine, vol. 41, no. 2, pp. 116-25, Feb. 2003.

[36] L.B. Ruiz, F.A. Silva, T.R.M. Braga, J.M.S. Nogueira, A.A.F. Loureiro, ”On Impact of Management in Wireless Sensors Networks” In Proc. of the 9th IEEE/IFIP Network Operations and Management Symposium (NOMS’ 04)vol. 1, pp. 657 - 670, Seoul, Korea, 19-23 April, 2004.

[37] S. B. B. Deb and B. Nath, ”A Topology Discovery Algorithm for Sensor Networks with Applications to Network Management,” Tech. rep. DCSTR-441, Dept. of Computer Science, Rutgers Univ., May 2002.

[38] IBM, ”An Architectural Blueprint For Autonomic Computing,” IBM and Autonomic Computing, April 2003. Available from the world wide web : http://www-03.ibm.com/ autonomic/pdfs/ACwpFinal.pdf

[39] IBM, IBM Redbooks, ”A Practical Guide to the IBM Autonomic Computing Toolkit,” Available from: http://www.redbooks.ibm.com/redbooks/pdfs/sg246635.pdf

[40] M.A.M. Viera, L.F.M. Viera, L.B. Ruiz, A.A.F. Loureiro, A.O. Fernandes, J.M.S. Nogueira, ”Scheduling Nodes in Wireless Sensor Networks: A Voronoi Approach,” In Proc. of the 28th Annual IEEE International Conference on Local Computer Networks (LCN ’03), pp.423 - 429, 20-24 Oct. 2003.

[41] R.M. Passos, C.J.N. Coelho, A.A.F. Loureiro, R.A.F. Mini, ”Dynamic Power Management in Wireless Sensor Networks: An Application-Driven Approach,” In Proc. of the 2nd Annu. Conference on Wireless On-demand Network Systems and Services (WONS ’05), pp. 109 - 118, 19-21 Jan. 2005.

[42] A. Sinha, A. Chandrakasan, ”Dynamic power management in wireless sensor networks,” Design and Test of Computers, IEEE, vol. 18, Issue 2, pp. 62 - 74, March-April 2001.

[43] R. Tynan, D.Marsh, D. O’Kane, G.M.P. O’Hare, ”Agents for wireless sensor network power management,” In Proc of International Conference workshops on Parallel Processing (ICPP ’05) Workshops, pp. 413 - 418, 14-17 June 2005.

[44] E. Bonabeau, M. Dorigo, and G. Theraulaz, Swarm Intelligence: From Natural to Artificial Systems, Santa Fe Institute Studies in the Sciences of Complexity, Oxford University Press, 1999.

Table 1: Comparison of some of the routing protocols in Wireless Sensor Network. Loc:Localization, Lo-A: Location Awareness.

	Class-tion	Scalability	Mobility	Data-Agg	Energy Usage	Loc	QoS	Multihop	Query	Lo-A
Flooding	Flat	Limited	No	No	High	No	No	Yes	No	No
SPIN	Data-centric	Limited	Possible	No	Limited	No	No	Yes	Yes	No
Directed	Flat	Limited	Limited	Yes	Limited	Yes	No	Yes	Yes	No
LEACH	Hierarchical	Good	Fixed BS	Yes	High	Yes	No	No	No	No
PEGASIS	Hierarchical	Good	Fixed BS	No	High	Yes	No	No	No	No
GEAR	Location	Limited	Limited	No	Limited	No	No	Yes	No	Yes