Int. J. Communications, Network and System Sciences, 2015, 8, 312-328
Published Online August 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.88031

An Appraisal of Wireless Sensor Networks: Profiles and Characters

Adedoyin Olayinka Ajayi, Boniface Kayode Alese, Adebayo Olusola Adetunmbi

Department of Computer Science, Federal University of Technology, Akure, Nigeria
Email: dedoyyin@gmail.com, kaalfad@yahoo.com, bayoadetunmbi@gmail.com

Received 19 October 2014; accepted 15 August 2015; published 18 August 2015

Abstract

This paper presents an in-depth evaluation of Wireless Sensor Networks. Wireless Sensor Networks have been highlighted as the major component that enables the development of modern infrastructures, such as the Smart Grid. As part of an on-going edification process on the subject matter, this paper brings to fore the many important functions and components of Wireless Sensor Networks, including application areas, functional architectures, physical topological design, communication protocols, routing schemes and Wireless Sensor Network hardware capabilities.

Keywords

Wireless Sensor Networks, Topology, Protocols, Routing Schemes, Smart Grid

1. Introduction

Wireless Sensor Networks (WSNs) are a very interesting and challenging area of the ever-evolving field of communications networks. The field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities [1]. A wireless sensor network consists of a large number of sensor nodes that may be randomly and densely deployed. Sensors are devices that respond to a physical stimulus heat, light, sound, pressure, magnetism, motion, etc., and convert that into an electrical signal. They perform an input function. Devices which perform an output function are generally called Actuators and are used to control some external device, for example movement. Both sensors and actuators are collectively known as Transducers. Transducers are devices used to convert energy of one kind into energy of another kind [2].

In other descriptions, [3] expressed WSN as consisting of small devices—called sensor nodes—with RF radio, processor, memory, battery and sensor hardware. In their research, they described sensor nodes as small electronic components capable of sensing many types of information from the environment, including temperature;

How to cite this paper: Ajayi, A.O., Alese, B.K. and Adetunmbi, A.O. (2015) An Appraisal of Wireless Sensor Networks: Profiles and Characters. *Int. J. Communications*, *Network and System Sciences*, **8**, 312-328.
http://dx.doi.org/10.4236/ijcns.2015.88031

light; humidity; radiation; the presence or nature of biological organisms; geological features; seismic vibrations; specific types of computer data; and more. These sensor nodes are capable of gathering, processing, and communicating information to other nodes and to the outside world. A simple architectural description of a sensor node is presented in **Figure 1** below.

In generalized terms therefore, a wireless sensor network consists of spatially distributed autonomous sensors meant to cooperatively monitor physical or environmental conditions.

2. Applications of WSNs

We categorize the applications of WSNs into three phases:

1) Applications based on areas of usage.

2) Application classes based on areas of deployment in scenarios identified in (1) above.

3) Application classes based on features of operations.

In the first categorization, sensor networks have numerous application areas, including health; agriculture; geology; retail; military; home; and emergency management; factory automation and maintenance, supply chain and asset management or physical security and control [4]. **Figure 2** shows, more specifically, various application areas of wireless sensor networks.

In the second categorization, [1] selected three application classes for Sensor Networks namely; environmental data collection, security monitoring, and sensor node tracking. A brief description is presented.

1) A canonical environmental data collection application is one where a research scientist wants to collect several sensor readings from a set of points in an environment over a period of time in order to detect trends and interdependencies. The scientist would want to collect data from hundreds of points spread throughout the area and then analyze the data offline [1].

At the network level, the environmental data collection application is characterized by having a large number of nodes continually sensing and transmitting data back to a set of base stations that store the data using traditional methods. These networks generally require very low data rates and extremely long lifetimes.

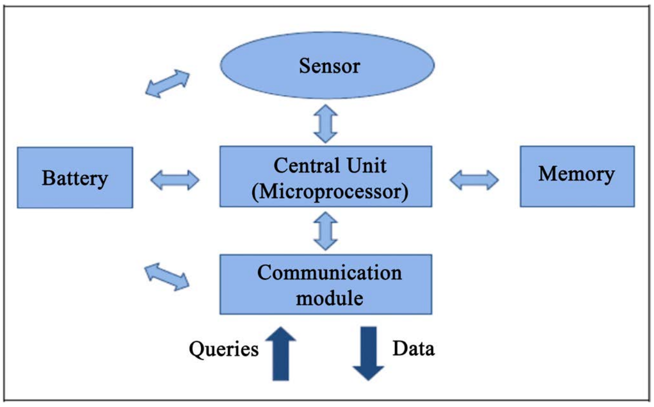


Figure 1. Basic architecture of a sensor node. Source: [2].

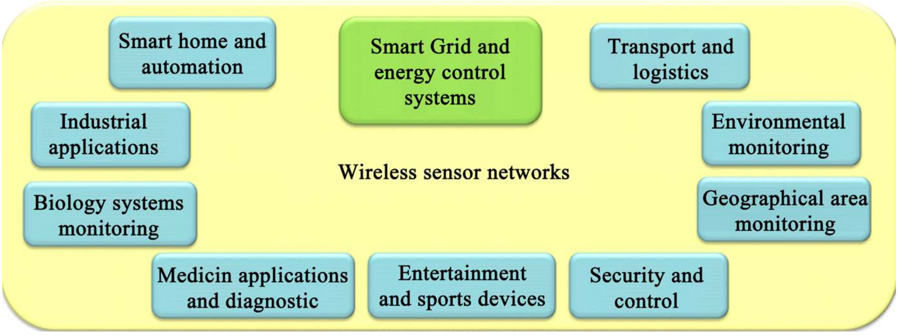

Smart home and automation
Smart Grid and energy control systems
Transport and logistics
Industrial applications
Environmental monitoring
Wireless sensor networks
Biology systems monitoring
Geographical area monitoring
Medicin applications and diagnostic
Entertainment and sports devices
Security and control

Figure 2. Application areas of WSN. Source: [5].

2) Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. These are "report by exception" networks.

3) The third usage scenario of WSNs discussed by [1] is the tracking of a tagged object through a region of space monitored by a sensor network. There are many situations where one would like to track the location of valuable assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. However, with these systems it is impossible to determine the current location of an object. For example, UPS tracks every shipment by scanning it with a barcode whenever it passes through a routing center. The system breaks down when objects do not flow from checkpoint to checkpoint. In typical work environments it is impractical to expect objects to be continually passed through checkpoints. With wireless sensor networks, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. Instead of sensing environmental data, these nodes will be deployed to sense the RF messages of the nodes attached to various objects.

In the third category, sensor networks are broken down into two classes namely Querying and Tasking Applications, as shown in **Figure 3** below, based on the features of their operations [6].

Querying Applications concern how information collected by a sensor network can be retrieved based on specified criteria. An instance of this and a major application of sensor networks is environment sensing to extract information from the physical environments. A sensor node can be encoded to collect temperature, humidity, light, pressure, chemical substances, or vibration information subject to its hardware capability [6] [7], and report it to the application. Applications may make use of simple queries to obtain raw sensor data conveyed directly from each sensor node.

Tasking applications involve encoding sensor nodes to perform specific actions upon certain events. Events can be physical environment changes, messages from nearby sensor nodes, or triggers from hardware/software modules inside a sensor node [6]. A task can be as simple as asking single sensor nodes to report information autonomously when they sense something unusual about their environments. More composite tasks require distributed synchronization among sensor nodes to realize higher accuracy or efficiency. For example, tracking a moving object in an area by simply having every single sensor node intermittently monitor its environment can be energy inefficient. But in a case where the sensor nodes surrounding the tracked object synchronize and work together, more comprehensive and correct information can be gathered with higher efficiency capability [6] [8].

3. The Functional Architecture, Physical Topology, Routing Schemes and Communication Protocols for WSNs

The main entities that build up the architecture of the WSN as presented in [9] and [10] are described as follows.

1) 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).

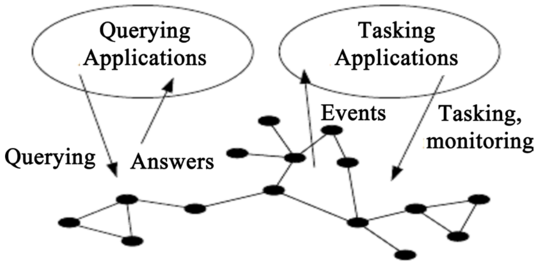


Figure 3. Querying and tasking applications in sensor networks. (Source: [6]).

2) The sink 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 infrastructure-less architecture through the sink.

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

4) The user who is interested in obtaining information about specific phenomenon to measure/monitor its behaviour.

Since the sensor network is more application specific when compared to conventional networks (designed to accommodate various applications), there is particular emphasis that the architecture of the sensor network be designed and adapted to suit a special task so as to optimize the system performance, maximize the operation lifetime, and minimize the cost [11]. **Figure 4** below shows the various layers of functions of the sensor network, as illustrated by [11].

The functions of each layer are briefly described below:

1) The sensing layer performs the work of data acquisition from the detected objects.

2) The communication layer performs the tasks of data correlation, data compression, data dissemination, and routing. The function of this layer is to deliver the statistical observation results to the collecting center (the sink). Due to energy constraints of the wireless sensor networks and terrain characteristics, the MAC (media access control) protocols and network protocols adopted should be energy aware. The data dissemination mechanism determines which part or which kind of the information should be transmitted, while the routing mechanism makes the decision how to transmit the data and which routes should be followed. The routing and data dissemination mechanisms may affect each other to achieve maximum energy efficiency. A security layer may also be inside the communication layer that deals with security and authentication problems for some applications.

3) The data fusion layer processes data received from the communication layer and combines them using various signal processing, data fusion, artificial intelligence, and other decision-making techniques as well as the prior knowledge of sensor performance and object characteristics. After the appropriate calculation and analysis, the data fusion layer produces the final detection results of a sensor network.

4) The uppermost layer is the user layer, which provides a man-machine interface with displaying and interaction functions and presents the final results to human and/or computer systems in the different required forms.

3.1. Topology Definitions

In discussing the different *topologies* in WSN, we start by defining two types of nodes—Source and Sink. The Sink was defined earlier as a base station. The Source is any component in the network that can provide information, *i.e.*, generally a sensor or an actuator node. The Sink is a Component where information is required. The Sink(s) sends queries or commands to the source nodes in the sensing region while the sensor nodes collaborate to accomplish the sensing task and send the sensed data to the Sink(s). Also, generally, the term "hop" refers to the link between any two nodes.

Developers have a number of choices of topology for configuring WSNs. [12] and [13] discussed different types of topology used in WSNs.

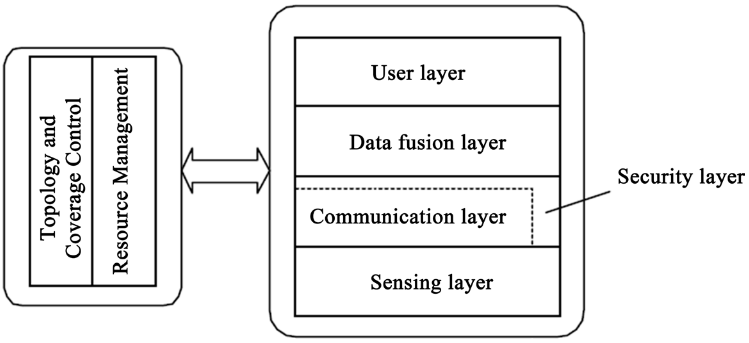


Figure 4. The functional layers of wireless sensor networks. (Source: [11]).

1) Single-Sink and Multi-Sink Network

a) Single-sink network: In this type of WSN, there is only one sink located near or in the sensing region, as illustrated in **Figure 5**. All sensor nodes send their collected data to this sink.

b) Multi-sink network: Here, there may be many sinks located in different positions close to or inside the sensing region, as shown in **Figure 6**. Sensor nodes can send their data to the nearest sink, which can balance the traffic load of sensor nodes.

2) Simple Single-Hop and Multi-Hop Network

a) Simple Single-hop topology: In this topology, every node communicates directly with the gateway or the data collector. Due to minimum networking concerns, this topology simplifies the network wherever it is realizable, and therefore network control is easy to implement since all sensor nodes transmit their data directly to the sink. **Figure 7(a)** and **Figure 7(b)** shows the Single-hop network structure and the Single-hop Star topology respectively.

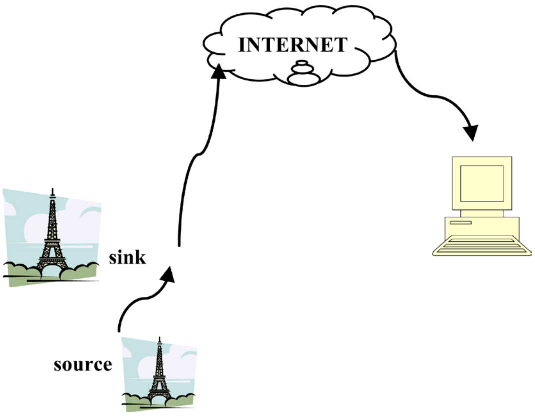


Figure 5. Single-sink WSN topology. (Source: [13]).

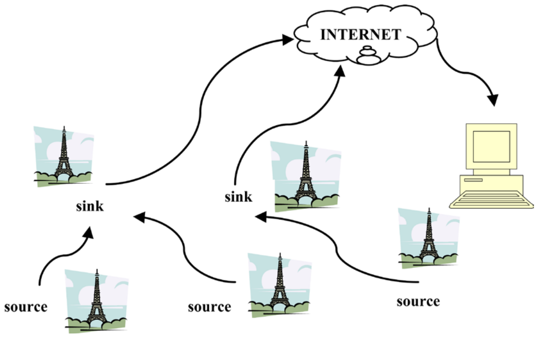


Figure 6. Multi-sink WSN topology. (Source: [13]).

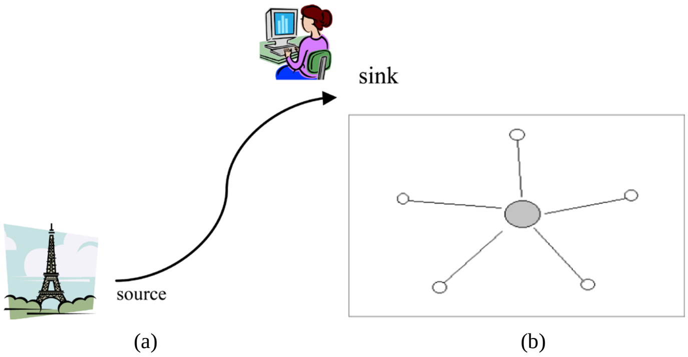


Figure 7. (a) Single-hop WSN topology. (Source: [13]); (b) Single-hop star topology. (Source: [12]).

However, due to its design only, the biggest limitation it possesses is the problem of scalability. It requires long-range wireless communication, which is costly in terms of energy consumption and hardware implementation. The nodes that are at a large distance from the gateway will have poor quality connections with the gateway. Thus, this topology is good to be used only when the number of nodes in the network is very small and the coverage area does not extend beyond the radio transmission range of around 30 meters, like the kind of range achievable in a building, and is suitable for applications in small sensing areas with sparsely deployed sensor nodes.

b) Simple Multi-hop Topology: This topology is more useful and necessary in covering large areas. In this topology, the signal goes from one sensor to the other until it reaches the gateway. Sensor nodes transmit their sensed data to the sink using short-range wireless communication via one or more intermediate nodes. Each intermediate node must perform routing and forward the data along a multi-hop path. Hence, the route of the signal is determined by a particular routing protocol.

Depending upon whether the network is random or organized, it can look like structures shown in **Figure 8(a)** or **Figure 8(b)**, respectively:

Multi-hop networks have a wider range of applications at the cost of higher control complexity.

3) Flat Multi-hop Architecture: Here, each node plays the same role in performing a sensing task and all sensor nodes are peers.

As shown in **Figure 9**, each sensor node communicates with the sink via a multihop path and uses its peer nodes as relays.

4) Hierarchical Multi-hop Architecture: Also called a two-tier cluster topology, the hierarchical multi-hop structure, is the most common architecture for larger WSNs. In this topology, nodes within a specific region send their data to a local clusterhead. In turn all such cluster heads from different regions send their collected data to the gateway [12]. In simple terms, sensor nodes in a hierarchical network are arranged in groups called clusters. The cluster members send their data to the cluster heads. The cluster heads forwards the data to the sink.

3.1.1. Designing Topologies for WSNs

The performance issues associated with different network topologies were discussed by [14]. Since mobility is not an issue, the question concerns what the best topology for a wireless network of sensors is, assuming placement of these sensors can be controlled and the sensor locations fixed relative to each other. One major factor in the selection of a topology is the extent of contention for the wireless media. The degree of contention will differ depending on the application because the message pattern and overall message generation rate are functions of

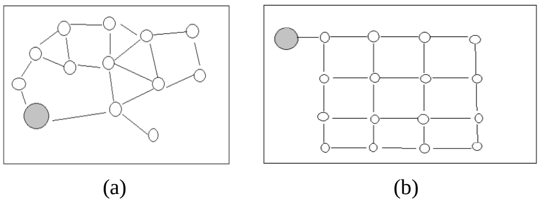


Figure 8. (a) Multi-hop star topology (random); (b) Multi-hop star topology (organized). (Source: [12]).

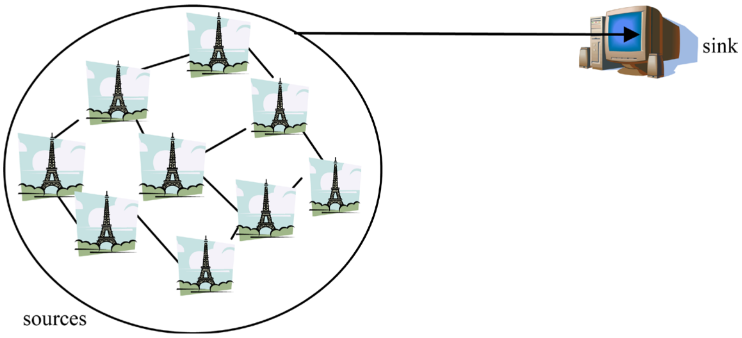


Figure 9. Flat multi-hop architecture. (Source: [13]).

the application [14]. [14] generalized each of the different topologies that can be used in WSNs as a grid on nodes in two or three dimensions. The vertices of this grid are the nodes that will transmit the packets, and the edges are the neighbors of each node that will receive the transmission. The optimal path was found between a source (*S*) and a destination (*D*) or the shortest path between them. Therefore:

The WSN, WSN (*m*, *n*), is an *m* × *n* grid, where *m* × *n* represents the number of nodes in the network. Each node is represented as (*y*, *x*) for $0 \le y \le m-1$ and $0 \le x \le n-1$. For each of the topologies, the following was assumed:

$$S = (y_s, x_s) \tag{1}$$

$$D = (y_d, x_d) \tag{2}$$

$$\Delta y = \| y_s - y_d \| \tag{3}$$

$$\Delta x = \| x_s - x_d \| \tag{4}$$

Each network was defined by identifying the neighbors of each node according to the different number of neighbors (as shown in **Figure 10**) and presenting the optimal number of hops (links) from a source to a destination.

The next task would be identifying whether two nodes are neighbors and the optimal number of hops between a source and a destination. For the purpose of this research, we will only describe the two-dimensional topology with up to five neighbours, as presented by [14]:

a) Three-Neighbors WSN: according to **Figure 11(a)**

1) two nodes are neighbors if:

$$\{(y,x),(y,x+1)\} \text{ for } x < n-1 \tag{5}$$

$$\{(y,x),(y+1,x)\} \text{ for } (y,x) \text{ and } y < m-1 \tag{6}$$

2) two nodes are not neighbors if:

$$\{(y,x),(y+1,x)\} \text{ for odd } (y,x) \text{ and } y < m-1 \tag{7}$$

3) Optimal number of hops (*s*, *d*)

$$\begin{cases} \Delta x + \Delta y & \text{if } \Delta x \ge \Delta y \\ 2\Delta y \pm 1 & \text{if } \Delta x < \Delta y \end{cases} \tag{8}$$

b) Five-Neighbor WSN: According to **Figure 11(b)**,

1) Two nodes are neighbors if:

$$\{(y,x),(y,x+1)\} \text{ for } x < n-1 \tag{9}$$

$$\{(y,x),(y+1,x)\} \text{ for } x < m-1 \tag{10}$$

$$\{(y,x),(y+1,x+1)\} \text{ for even } x \tag{11}$$

$$\{(y,x),(y-1,x-1)\} \text{ for odd } x \tag{12}$$

2) Optimal number of hops (*s*, *d*)

$$= \begin{cases} \Delta x + 2 & \text{if } x_s \ge x_d \text{ and } y_s > y_d \text{ or } x_s \le x_d \text{ and } y_s < y_d \\ \Delta x \pm \Delta y & \text{Otherwise} \end{cases} \tag{13}$$

The description of the two-dimensional topology with up to three neighbors will serve as part of our future research work.

3.1.2. Parameters for Measuring the Effectiveness of a Topology

[1] and [12] described parameters for determining the effectiveness of a topology. Some of these factors include:

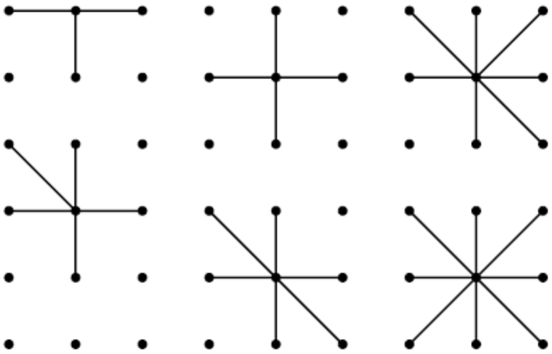


Figure 10. Possible number of neighbors, as illustrated in [14].

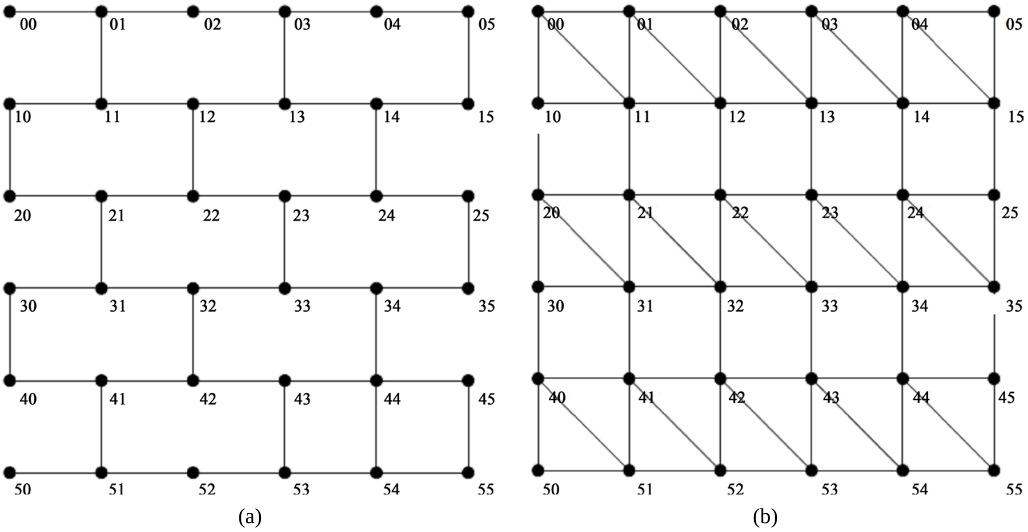


Figure 11. (a) Two-dimensional topology with up to three neighbors; (b) Two-dimensional topology with up to five neighbors.

1) Range and coverage

Range and coverage are undoubtedly the most important necessity in a WSN starting from node to node range at a given transmission power and data rate. The main factors affecting range of a wireless network are the quality of physical layer and the efficiency of data transmission through the network. The coverage requirements are elimination of dead spots in the network and the extent of coverage area in range, both of which are closely related to range [12].

2) Scalability

Scalability in WSN means being able to cope up with network cells as small as a few nodes to cells of thousands or even tens of thousands of nodes as well as increasing the size of existing network by order of magnitude without employing expensive cellular communication or other long range solutions. This is also an important feature as assessments can only be performed on a small test network before the solution is generalized.

3) Expected Transmission Count (ETX)

ETX accounts for data loss due to medium access contention and environmental hazards and considers the number of transmissions needed to successfully transmit a packet over a link.

4) Hop Count

Hop count is the most commonly used metric in wireless multi-hop networks. The path having the minimum number of links between a given source and the destination node is the optimal path and is selected.

5) Power consumption/Network Longevity

In most of the published communication protocols for WSNs, network lifetime extension has been mentioned as an important optimization objective. The position of nodes can affect the network lifetime significantly, as we would see in the next sub-section. For example, a non-uniform or random node distribution in a given area may lead to bottlenecks and unbalanced traffic. On the other hand, uniform distribution of nodes in a network may result in depletion of energy of nodes that are close to the base station at a rate higher than the other nodes, which in turn will reduce the network lifetime [12].

3.2. Routing Protocols for WSNs

Different routing, power management and data dissemination protocols have been designed for WSNs, dependent on both the architecture of 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 human lives in the real world. These protocols are different from conventional ones in that 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 [9]. [9] and [15] discussed a number of protocols in their various researches. Three of these protocols are described below:

1) Low-Energy Adaptive Clustering Hierarchy (LEACH): LEACH is a self-organizing, adaptive clustering-based protocol using randomized rotation of cluster-heads to evenly distribute the energy load among the sensor nodes in the network [9] [15]. The data will be collected by cluster heads from the nodes in the cluster and after processing and data aggregation forwards it to base station. LEACH based on two basic assumptions:

- Base station is fixed and located far away from the sensors, and
- All nodes in the network are homogeneous and energy-constrained.

The three important features of LEACH are:

- Localized co-ordination and control for cluster setup.
- Randomized cluster head (or cluster base-station) rotation.
- Local compression to reduce global data communication.

By forming cluster, the energy usage is low within the cluster but drains the energy resource for the cluster head. The cluster heads need to be more powerful than other common nodes of the networks of fixed cluster heads in order to perform maximum long distance communication. LEACH is a fully cluster-base protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as cluster-heads (CHs) among the different sensor nodes and periodically changes the role of cluster-heads so that the energy load is totally distributed among the different nodes.

In LEACH, the role of the cluster-head (CH) nodes is to compress the data arriving from the different nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. However, data collection is centralized and is performed periodically. This protocol proves to be the most appropriate and suitable when constant monitoring is needed by the sensor network. In this situation it may be possible that a user may not need all the data immediately. Hence, periodic data transmissions are unnecessary which may cause the wastage of the limited energy of the sensor nodes. After a given interval of time, the role of the CH is randomly rotated so that uniform energy dissipation in the sensor network is obtained.

The operation of LEACH protocol has been divided into two phases, the setup phase and the steady state phase [15]. In the setup phase (described as a join of advertisement phase and cluster set-up phase by [9], the clusters are organized and CHs are selected. For this cluster-head advertisement, the cluster heads use CSMA (carrier sense multiple access) MAC (medium access control) protocol. In the steady state phase (described as schedule creation phase and data transmission phase by [9]), the actual data transfer to the base station takes place. 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 (time-division multiple-access) schedule telling each node when it can transmit. This schedule is broadcast back to the nodes in the cluster. 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 duration of the steady state phase is longer than the duration of the setup phase in order to minimize the overhead. During the setup phase, a predetermined fraction of nodes, *p*, elect themselves as CHs as follows. A sensor node chooses a random number, *v*, between 0 and 1. If this random number is less than a threshold value, *T*(*n*), the node becomes a cluster-head for the current round. The threshold value is calculated based on an equation that incorporates the desired percentage to become a cluster-head in the current round from the set of nodes that have not been selected as a cluster-head in the last (1/*P*) rounds. The threshold value is given by:

$$T(n) = \begin{cases} P\big/\left(1 - P\left(r \bmod (1/p)\right)\right) & \text{if } n \in G \\ 0 & \text{Otherwise} \end{cases} \tag{14}$$

where *P* is the desired percentage of cluster-heads (a predetermined fraction of nodes), *r* is the current round, and *G* is the set of nodes that have not been cluster heads in the last 1/*P* rounds (that is, the set of nodes that are involved in the CH election). Since *p* is randomly selected, then the number of cluster heads may not be fixed [9] [15].

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:

- Cluster head nodes spend the more energy in comparison to others.
- It cannot 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 *p*.

2) Advanced-Low-Energy Adaptive Clustering Hierarchy (A-LEACH): Due to the setbacks identified in the LEACH protocol, researchers worked on an upgrade on the protocol. A-LEACH is a clustering-based protocol architecture where nodes make autonomous decision without any central intervention. ALEACH proposes a new cluster head selection algorithms that enables selecting best suited node for cluster head, algorithms for adaptive clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes. ALEACH improves the threshold equation of LEACH by introducing two terms: General probability (G_p) and Current State probability (CS_p).

$$T(n) = G_p + CS_p = k\big/\left(N - k\left(r \bmod (N/k)\right)\right) + E_{\text{current}}\big/E_{n\text{-max}} \times k/N \tag{15}$$

where, *k* = Expected number of cluster heads in a round, *N* = Total number of nodes in the networks, *r* = Current round, E_{current} = Current energy, $E_{n\text{-max}}$ = Initial energy.

A major advantage of A-LEACH is that it improves system life time and energy efficiency in terms of different simulation performance metrics [15].

3) Geographical and Energy Aware Routing (GEAR): GEAR is a recursive data dissemination protocol WSNs described by [9]. GEAR 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 M_i, then its transmission range can reach node M_i.

GEAR has two phases:

- Forwarding the packets toward the targeted region, and
- 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 neighbour 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 neighbour 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:

$$c(N_i, R) = ad(N_i, R) + (1-\alpha)e(N_i) \tag{16}$$

where α is a tunable weight, $d(N_i, R)$ is the distance from N_i to the centroid *D* of *R* normalized by the largest such distance among all neighbors of *N*, and $e(N_i)$ is the largest consumed energy at node N_i normalized by the largest consumed energy among neighbors of *N*.

Equation (16) shows that the estimated cost is a combination of residual energy and distance to the destination. From the above analysis, it is concluded 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, Dynamic clustering architecture requirements, Randomized path selection, Mobility, Quality-of-Service, Dependability, Localization, Security and Self-configuration (Al-Obaisat and Braun, 2006).

Other routing protocols described in [9] and [15] include:

- PEGASIS (Power-Efficient GAthering in Sensor Information Systems),
- HEED (Hybrid Energy-Efficient Distributed Clustering),
- Directed Diffusion,
- GOSSIPING,
- SPIN (Sensor Protocols for Information via Negotiation),
- Flooding,
- SPEED(Stateless Protocol for End-to-End Delay),
- ACQUIRE (Active Query Forwarding in Sensor Networks),
- COUGAR,
- E-LEACH (Energy LEACH),
- LEACH-B (Balanced-Low Energy Adaptive Clustering Hierarchy),
- LEACH-F (Fixed number of Cluster-Low Energy Adaptive Clustering Hierarchy),
- Re-Cluster-LEACH,
- MR-LEACH (Multi-hop hop routing-Low Energy Adaptive Clustering Hierarchy),
- TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol),
- APTEEN (Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol), and
- SPEED (Stateless Protocol for End-to-End Delay).

3.3. Communication Protocols for WSN

Even though sensor nodes communicate through the wireless medium, protocols and algorithms proposed for traditional wireless ad hoc networks may not be well suited for sensor networks. Ad hoc wireless networks usually do not rely on pre-existing infrastructure such as access points as in managed wireless networks and all devices connected therein have equal status on the network [16]. Sensor networks are application specific (in that they influence the capability to provide users with specialized applications), and the sensor nodes work collaboratively together. In addition, the sensor nodes have massive energy constraints in comparison to conventional wireless adhoc devices. [17] summarized the major differences between sensor networks and ad hoc networks. These differences are summarized below:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use a broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensor nodes.
- Sensor networks are deployed with a specific sensing application in mind; ad hoc networks are mostly con-

structed for communication purposes [17].

These differences forced developers to give some special attention to the design of communication protocols for WSNs.

Communication protocols in sensor networks are the fundamental cornerstone that glues distributed applications together. The deeply embedded nature of sensor networks presents some of the most interesting challenges in the design of their communication protocols [18]. New research topics span all protocol stack layers, primarily motivated by a tighter interaction between the network and its physical environment as will be discussed by studying the architecture of the Protocol Stack for Wireless Sensor Networks by [9]. 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). At the Mandatory Access Control (MAC) layer, new protocols are needed that enforce message priorities consistently with time and distance constraints that arise from environmental interactions. According to [18], awareness of the physical environment must also be incorporated into the network layer; for example, location should bean essential attribute of addressable networked objects [18] [19]. Location-assisted routing protocols such as LAR [20] and DREAM [21], as well as location services for adhoc wireless networks were described by [18].

The conventional wireless ad hoc network protocol design is mainly based on a layered stack in which each layer is designed and operated in isolation [22]. The interfaces between layers are static and independent of the individual network constraints and applications. By using the approach used in traditional network protocols, the network design is streamlined. Nevertheless, there is a constraint of timely delivery in the low resource scenario presented in WSNs and the traditional approach of network protocol design may result in rather low performance because of its lack of flexibility, scalability and optimality [23]. The protocol stack discussed by [9] is shown in **Figure 12**. This protocol stack 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. 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. 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). In an example illustration, to avoid getting replicated or doubled messages, a sensor node may turn off its receiver on receipt of a message from one of its neighbors. Also, a node transmits to its neighbors that it is low in power and be part of a transmission. The remaining power may be 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 [9].

The protocol stack discussed above is in close proximity to the cross-layer design described by [22], shown in **Figure 13**. The protocol model supports optimization and adaptability across multiple layers.

The concept of the cross-layer design is that, each layer is not developed in isolation, but in an integrated and hierarchical framework. Therefore, the strict border between different layers is loosened. Some control messages as well as information concerning a layer's status will be exchanged among different layers so that the system can take advantage of the interdependencies between them.

For example, the link layer can adjust rate, power, and coding to satisfy application requirements based on current channel and network conditions; MAC layer can be adaptive to underlying link and interference conditions, delay constraints, and bit priorities; Routing protocols can be developed according to up-to-date link, network, and traffic conditions. In practice, cross-layer design may be exercised in some, rather than all, layers in the protocol stack [22].

[24] described communication protocols in WSNs based on classification into six classes, with most of the classes bearing resemblance to the protocol stack in [9] and [22], and to some of the layers of the ISO/OSI Reference Model. The six classes described by [24] include the following:

- Application Layer Protocols.
- Transport Layer Protocols.

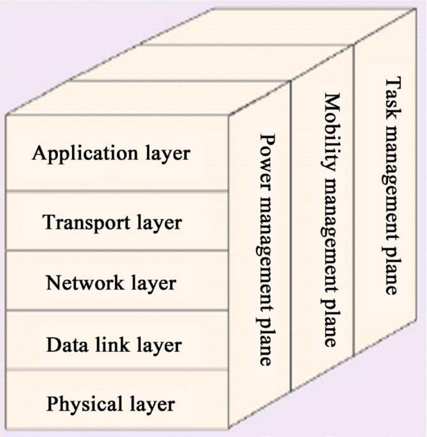


Figure 12. The wireless sensor networks protocol stack. (Source: [9]).

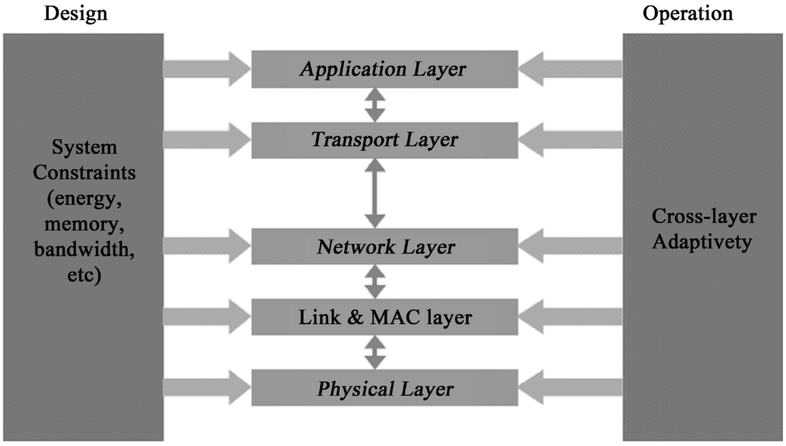


Figure 13. Cross-layer protocol stack in WSNs. (Source: [22]).

- Network Layer Protocols.
- Data Link Layer Protocols.
- Time Synchronization Protocols.
- Localization Protocols.

The localization technique is as imperative, as many WSN communication protocols require knowledge of location. Time Synchronization Protocols are those needed to allow the sensor nodes in the sensor field maintain a similar time within a certain tolerance throughout the lifetime of the network [24]. In order to support time correlated sensor readings and low-duty cycle operation of our data collection application scenario, nodes must be able to maintain precise time synchronization with other members of the network. Nodes need to sleep and awake together so that they can periodically communicate. Errors in the timing mechanism will create inefficiencies that result in increased duty cycles. In distributed systems, clocks drift apart over time due to inaccuracies in timekeeping mechanisms. Depending on temperature, voltage, humidity, time keeping oscillators operate at slightly different frequencies. High-precision synchronization mechanisms must be provided to continually compensate for these inaccuracies [1]. Some of the factors influencing time synchronization in large systems also apply to sensor networks [24]. These factors may include: Temperature, Phase Noise, Frequency noise, Asymmetric delay and Clock glitches. Enabling protocols include: network time protocol (NTP), the reference-broadcast synchronization (RBS), and the time-diffusion synchronization protocol (TDP) [24]. Also, Precision time protocol (PTP) defined by the standard IEEE 1588 provides time synchronization with up to nanosecond precision over ethernet networks [25]. Global positioning system (GPS) and simple time network protocol (STNP) are other ways of achieving time synchronization.

[24] proposed three possible application layer protocols: sensor management protocol; task assignment and

data advertisement protocol; and sensor query and data dissemination protocol. While many application areas for sensor networks have been defined and proposed, potential application layer protocols for sensor networks remain largely unexplored.

The essence of Transport Layer Protocols is seen from the collaborative nature of the sensor network paradigm, a collaboration that brings with it several advantages over traditional sensing, including greater accuracy, larger coverage area, and extraction of localized features. The realization of these potential gains, however, directly depends on efficient, reliable communication between the sensor network entities, *i.e.*, the sensor nodes and the sink. To accomplish this, a reliable transport mechanism is imperative.

In general, the main objectives of the transport layer are:

- to bridge application and network layers by application multiplexing and demultiplexing;
- to provide data delivery service between the source and the sink with an error control mechanism tailored according to the specific reliability requirement of the application layer; and
- to regulate the amount of traffic injected into the network via flow and congestion control mechanisms.

Transport layer mechanisms are essential to achieving higher level error and congestion control, it is still imperative to have data-link layer functionalities in the sensor networks. In general, the data link layer is primarily responsible for multiplexing data streams, data frame detection, medium access, and error control; it ensures reliable point-to-point and point-to-multipoint connections in a communication network [24]. Nevertheless, the collaborative and application-oriented nature of the sensor networks and the physical constraints of the sensor nodes, such as energy and processing limitations, determine the way in which these responsibilities are fulfilled.

4. WSNs Hardware Capabilities

[1] studied the capabilities of modern WSN hardware. Hill's study allows interested parties to understand what bit rate, power consumption, memory and cost they can expect to achieve. A balance must be maintained between capability, power consumption and size in order to best address application needs. This section gives a quick overview of modern technology and the trade-offs between different technologies, as presented by [1]. The section starts with a background of energy storage technology and continues through the radio, CPU, and sensors.

4.1. Energy

Just as power consumption of system components are often expressed in milliamps, batteries are generally rated in milliamp-hours (mAh). In theory, a 1000 mAh battery could support a processor consuming 10 mA for 100 hours. In practice this in not always true. Due to battery chemistry, voltage and current levels vary depending on how the energy is extracted from a battery. Additionally, as batteries discharge their voltage drops. If the system is not tolerant to a decrease in voltage it may not be possible to use the full rated capacity of a battery. For example, a 1.5 V alkaline battery is not considered empty by the manufacturer until it is outputting only 0.8 V [1].

There are three common battery technologies that are applicable for wireless sensor networks—Alkaline, Lithium, and Nickel Metal Hydride. A common AA Alkaline battery is rated at 1.5 V, but during operation it ranges from 1.65 to 0.8 V as shown in **Figure 14** and is rated at 2850 mAh. With a volume of just 8.5 cm^3, it has an energy density of approximately 1500 Joules/cm^3. While providing a cheap, high capacity, energy source, the major drawbacks of alkaline batteries are the wide voltage range that must be tolerated and their large physical size. Additionally, lifetimes beyond 5 years cannot be achieved because of battery self-discharge. The shelf-life of an alkaline battery is approximately 5 years. Lithium batteries provide an incredibly compact power source. The smallest versions are just a few millimetres across. Additionally, they provide a constant voltage supply that decays little as the battery is drained. Devices that operate off of lithium batteries do not have to be as tolerant to voltage changes as devices that operate off of alkaline batteries.

Additionally, unlike alkaline batteries, lithium batteries are able to operate at temperatures down to −40˚C [1].

One of the drawbacks of lithium batteries is that they often have very low nominal discharge currents. Nickel Metal Hydride batteries have the benefit of being easily rechargeable. The downside to rechargeable batteries is a significant decrease in energy density. According to [1], an AA size NiMH battery has approximately half the energy density of an alkaline battery at approximately 5 times the cost.

4.2. Radio

As earlier depicted, the design of power and bandwidth efficient radios is one of the main research and

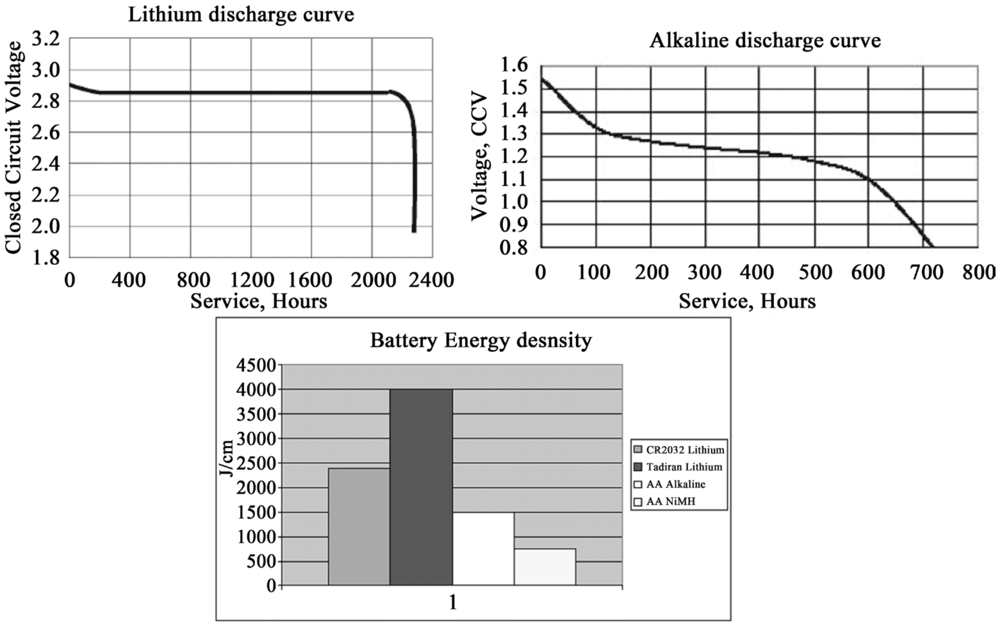


Figure 14. Battery characteristics for lithium, alkaline and NiMH batteries. The discharge characteristics of alkaline batteries make it essential to design a system to tolerate a wide range of input voltages. (Source: [1]).

development tasks in the study of Wireless Sensor Nets. Radios are almost the highest energy consumers in practical application scenarios. Modern low-power, short range transceivers consume between 15 and 300 milliwatts of power when sending and receiving. A key hardware observation is that low power radios consume approximately the same amount of energy when in receive or transmit mode. This energy is consumed if the radio is on; the actual power emitted out of the antenna only accounts for a small fraction of the transceiver's energy consumption. A significant fraction goes to internal operation. Because of this, the overall cost of radio communication can easily be dominated by the receiver power consumption—a metric that is often ignored in wireless studies [1].

4.3. Processor

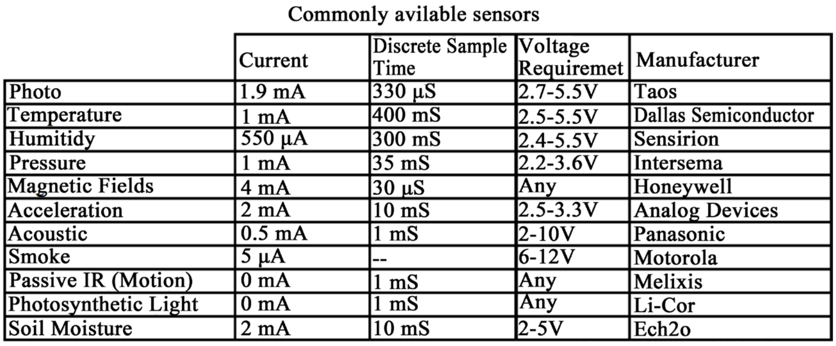
Modern microcontrollers integrate flash storage, RAM, analog-to-digital converters and digital I/O onto a single integrated circuit that costs between $1 and $5 [1]. Their tight integration makes them ideal for use in deeply embedded systems like wireless sensor networks. When selecting a microcontroller family, some of the key requirements are energy consumption, voltage requirements, cost, support for peripherals and the number of external components required.

4.4. Sensors

The last decade has seen an explosion in sensor technology. There are currently thousands of potential sensors ready to be attached to a wireless sensing platform. Additionally, advances in MEMS and carbon nano-tubes technology are promising to create a wide array of new sensors. They range from simple light and temperature monitoring sensors to complex digital noses. **Figure 15** outlines a collection of common micro-sensors and their key characteristics, as illustrated by [1].

5. Concluding Remarks and Future Research Directions

This research work has carried out an in-depth analysis and evaluation of Wireless Sensor Networks. This research work, and the research described in [26], are part of a first phase of fully defining the problem space. We have prior indicated in [26] that the increasingly widespread deployment of sensor networks has almost simultaneously heightened security issues. Since transmitted data in sensors are via wireless communication, mechanisms to prevent unauthorized users from prying on transmitted information or introducing malicious data



Commonly avilable sensors

	Current	Discrete Sample Time	Voltage Requiremet	Manufacturer
Photo	1.9 mA	330 µS	2.7-5.5V	Taos
Temperature	1 mA	400 mS	2.5-5.5V	Dallas Semiconductor
Humitidy	550 µA	300 mS	2.4-5.5V	Sensirion
Pressure	1 mA	35 mS	2.2-3.6V	Intersema
Magnetic Fields	4 mA	30 µS	Any	Honeywell
Acceleration	2 mA	10 mS	2.5-3.3V	Analog Devices
Acoustic	0.5 mA	1 mS	2-10V	Panasonic
Smoke	5 µA	--	6-12V	Motorola
Passive IR (Motion)	0 mA	1 mS	Any	Melixis
Photosynthetic Light	0 mA	1 mS	Any	Li-Cor
Soil Moisture	2 mA	10 mS	2-5V	Ech2o

Figure 15. Power consumption and capabilities of commonly available. (Source: [1]).

into the network have to be put in place, to prevent, for example, leakage of user private information. Further, WSNs make use of one-to-many and many-to-many communication architectures; this wireless broadcast communication is exposed to security risks; to put it more concretely, an adversary can eavesdrop and alter communication messages, and insert malicious messages. In alternative situations, nodes in a sensor network may be lost due to power exhaustion or malicious attacks. To extend the lifetime of the sensor network, new node deployment is necessary. During new node deployment, in military scenarios for example, adversaries may directly deploy malicious nodes or manipulate existing nodes to introduce malicious "new" nodes through many kinds of attacks. All of these facts make it very necessary to absolutely guarantee the safety and security of information communicated in the WSN. Research has, most times, focused on making sensor networks feasible and useful; and not much emphasis has been placed on security. Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation. The major obstacles realized from the need to provide security in WSNs are the restrictions in the setup of wireless sensors. To prevent attacks, encryptions of the communication data and mutual authentication between sensor nodes are needed. While there have been numerous security schemes in that research area, concerns still remain about how such schemes impact the extreme energy limitations of wireless sensors. Sensor nodes are restricted in power consumption (sensors are battery-powered), bandwidth, memory, and calculation capability. These constraints hinder the deployment of most modern cryptographic solutions known to be secure. Complex algorithms in the cryptographic world usually take longer to run and also consume more energy than can be provided by battery-powered sensors. Also, crypto methods, such as encryption and authentication using public-key cryptosystems, are not reasonable, because sensor nodes have very low calculation capability and small memory and they are not able to operate such crypto algorithms within sufficient time.

In our future researches, we will attempt to find solutions to some of these issues including those of computational and energy efficiency.

References

[1] Hill, J.L. (2003) System Architecture for Wireless Sensor Networks. Doctor of Philosophy dissertation, University of California, Berkeley.

[2] Kao, W. (2012) Sensor Devices and Sensor Network: Applications for the Smart Grid/Smart Cities. Sensors Con.

[3] Ilyas, M. and Mahgoub, I. (2005) Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. CRC PRESS LLC, Boca Raton.

[4] Coale (2013) Wireless Sensor Network Technology. http://coalesenses.com/index.php?page=technology

[5] Kolenc, M. and Zajc, M. (2011) Wireless Sensor Networks and Data Analysis in Smart Grids. 7*th IEEE International Symposium on Information and Communication Technologies—INTSIKT* 2011—"*Smart City*", Tuzla, 6-7 June 2011. Http://www.ldos.si/slo/01_Members/23_Mitja_Kolenc/Wireless%20sensor%20networks%20and%20data%20analysis%20in%20Smart%20grids%20(1).pdf

[6] Shen, C.-C., Jaikaeo, C. and Srisathapornphat, C. (2005) Sensor Network Architecture and Applications. In: Ilyas, M. and Mahgoub, I., Eds., *Handbook of Sensor Networks*: *Compact Wireless and Wired Sensing Systems*, CRC Press LLC, Boca Raton.

[7] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) Wireless Sensor Networks: A Survey. *Computer Networks*, **38**, 393-422. http://dx.doi.org/10.1016/S1389-1286(01)00302-4

[8] Huang, Q., Lu, C. and Roman, G.-C. (2003) Reliable Mobicast via Face-Aware Routing. Tech. Rep. WUCSE-2003-49, Washington University, St. Louis.

[9] Al-Obaisat, Y. and Braun, R. (2006) On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management. Institute of Information and Communication Technologies, University of Technology, Sydney.

[10] Tilak, S., Abu-Ghazaleh, N. and Heinzelman, W. (2002) A Taxonomy of Wireless Micro-Senor Network Models. *ACM SIGMOBILE*, *Mobile Computing and Communications Review*, **6**, 28-36.
http://www.cs.binghamton.edu/nael/research/papers/taxonomy.pdf
http://dx.doi.org/10.1145/565702.565708

[11] Papavassiliou, S. and Zhu, J. (2005) Architecture and Modeling of Dynamic Wireless Sensor Networks. In: Ilyas, M. and Mahgoub, I., Eds., *Handbook of Sensor Networks*: *Compact Wireless and Wired Sensing Systems*, CRC Press LLC, Boca Raton.

[12] Kaur, G. and Garg, R.M. (2012) Energy Efficient Topologies for Wireless Sensor Networks. *International Journal of Distributed and Parallel Systems* (*IJDPS*), **3**, 179-192. http://dx.doi.org/10.5121/ijdps.2012.3516

[13] Lucas, I. (2011) Wireless Sensor Network Protocols. ITIC, Universidad de Mendoza, Provincia de Mendoza.

[14] Salhieh, A. and Schwiebert, L. (2005) Power-Efficient Topologies for Wireless Sensor Networks. In: Ilyas, M. and Mahgoub, I., Eds., *Handbook of Sensor Networks*: *Compact Wireless and Wired Sensing Systems*, CRC Press LLC, Boca Raton.

[15] Kumar, P., Singh, M.P. and Triar, U.S. (2012) A Review of Routing Protocols in Wireless Sensor Network. *International Journal of Engineering Research & Technology* (*IJERT*), **1**.

[16] Wiki (2014) Wikipedia: Wireless Ad hoc Networks. http://en.wikipedia.org/wiki/Wireless_ad_hoc_network

[17] Su, W., Cayirci, E. and Akan, O.B. (2005) Overview of Communication Protocols for Sensor Networks. In: Ilyas, M. and Mahgoub, I., Eds., *Handbook of Sensor Networks*: *Compact Wireless and Wired Sensing Systems*, CRC Press LLC, Boca Raton.

[18] Abdelzaher, T., Stankovic, J., Son, S., Blum, B., He, T., Wood, A. and Lu, C. (2005) Communication Architecture and Programming Abstractions for Real-Time Embedded Sensor Networks. In: Ilyas, M. and Mahgoub, I., Eds., *Handbook of Sensor Networks*: *Compact Wireless and Wired Sensing Systems*, CRC Press LLC, Boca Raton.

[19] Hightower, J. and Borriello, G. (2001) Location Systems for Ubiquitous Computing. *IEEE Computer*, **34**, 57-66.
http://dx.doi.org/10.1109/2.940014

[20] Ko, Y.-B. and Nitin, V. (1998) Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. *Proceedings of the* 4th *Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, 25-30 October 1998, 66-75. http://dx.doi.org/10.1145/288235.288252

[21] Basagni, S., Chlamtac, I., Syrotiuk, V.R. and Woodward, B.A. (1998) A Distance Routing Effect Algorithm for Mobility (DREAM). *Proceedings of the* 4th *Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, 25-30 October 1998, 76-84. http://dx.doi.org/10.1145/288235.288254

[22] Wang, Q. and Hassanein, H. (2005) A Comparative Study of Energy-Efficient (E^2) Protocols for Wireless Sensor Networks. In: Ilyas, M. and Mahgoub, I., Eds., *Handbook of Sensor Networks*: *Compact Wireless and Wired Sensing Systems*, CRC Press LLC, Boca Raton.

[23] Goldsmith, A.J. and Wicker, S.B. (2002) Design Challenges for Energy-Constrained Ad Hoc Wireless Networks. *IEEE Wireless Communications*, **9**, 8-27. http://dx.doi.org/10.1109/MWC.2002.1028874

[24] Su, W. and Akyildiz, I.F. (2003) Perceptive Localization Framework for Sensor Networks. Georgia Tech Technical Report.

[25] Wang, W., Xu, Y. and Khanna, M. (2011) A Survey on the Communication Architectures in Smart Grid. *Computer Networks*, **55**, 3604-3629. http://dx.doi.org/10.1016/j.comnet.2011.07.010

[26] Ajayi, A.O., Alese, B.K., Fadugba, S.E. and Owoeye, K. (2014) Sensing the Nation: Smart Grid's Risks and Vulnerabilities. *International Journal of Communications*, *Network*, *System Sciences*, **7**, 151-163.
http://www.scirp.org/journal/paperinformation.aspx?paperID=46061#.U33BU3-9KSM
http://dx.doi.org/10.4236/ijcns.2014.75017