Chapter 1

Overview of Wireless Sensor Network

M.A. Matin and M.M. Islam

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/49376

1. Introduction

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the onboard sensors start collecting information of interest. Wireless sensor devices also respond to queries sent from a "control site" to perform specific instructions or provide sensing samples. The working mode of the sensor nodes may be either continuous or event driven. Global Positioning System (GPS) and local positioning algorithms can be used to obtain location and positioning information. Wireless sensor devices can be equipped with actuators to "act" upon certain conditions. These networks are sometimes more specifically referred as Wireless Sensor and Actuator Networks as described in (Akkaya et al., 2005).

Wireless sensor networks (WSNs) enable new applications and require non-conventional paradigms for protocol design due to several constraints. Owing to the requirement for low device complexity together with low energy consumption (i.e. long network lifetime), a proper balance between communication and signal/data processing capabilities must be found. This motivates a huge effort in research activities, standardization process, and

industrial investments on this field since the last decade (Chiara et. al. 2009). At present time, most of the research on WSNs has concentrated on the design of energy- and computationally efficient algorithms and protocols, and the application domain has been restricted to simple data-oriented monitoring and reporting applications (Labrador et. al. 2009). The authors in (Chen et al., 2011) propose a Cable Mode Transition (CMT) algorithm, which determines the minimal number of active sensors to maintain K-coverage of a terrain as well as K-connectivity of the network. Specifically, it allocates periods of inactivity for cable sensors without affecting the coverage and connectivity requirements of the network based only on local information. In (Cheng et al., 2011), a delay-aware data collection network structure for wireless sensor networks is proposed. The objective of the proposed network structure is to minimize delays in the data collection processes of wireless sensor networks which extends the lifetime of the network. In (Matin et al., 2011), the authors have considered relay nodes to mitigate the network geometric deficiencies and used Particle Swarm Optimization (PSO) based algorithms to locate the optimal sink location with respect to those relay nodes to overcome the lifetime challenge. Energy efficient communication has also been addressed in (Paul et al., 2011; Fabbri et al. 2009). In (Paul et al., 2011), the authors proposed a geometrical solution for locating the optimum sink placement for maximizing the network lifetime. Most of the time, the research on wireless sensor networks have considered homogeneous sensor nodes. But nowadays researchers have focused on heterogeneous sensor networks where the sensor nodes are unlike to each other in terms of their energy. In (Han et al., 2010), the authors addresses the problem of deploying relay nodes to provide fault tolerance with higher network connectivity in heterogeneous wireless sensor networks, where sensor nodes possess different transmission radii. New network architectures with heterogeneous devices and the recent advancement in this technology eliminate the current limitations and expand the spectrum of possible applications for WSNs considerably and all these are changing very rapidly.

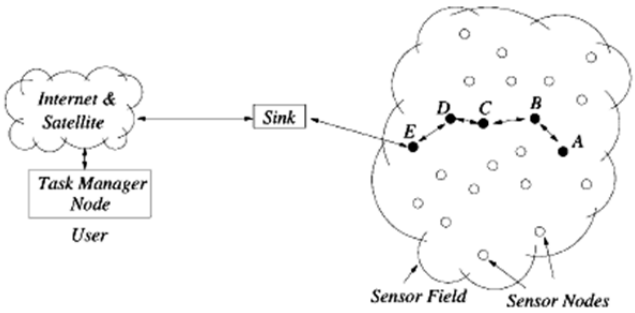

Figure 1. A typical Wireless Sensor Network

2. Applications of wireless sensor network

Wireless sensor networks have gained considerable popularity due to their flexibility in solving problems in different application domains and have the potential to change our lives

in many different ways. WSNs have been successfully applied in various application domains (Akyildiz et al. 2002; Bharathidasan et al., 2001), (Yick et al., 2008; Boukerche, 2009), (Sohraby et al., 2007), and (Chiara et al., 2009;Verdone et al., 2008), such as:

Military applications: Wireless sensor networks be likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems.

Area monitoring: In area monitoring, the sensor nodes are deployed over a region where some phenomenon is to be monitored. When the sensors detect the event being monitored (heat, pressure etc), the event is reported to one of the base stations, which then takes appropriate action.

Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.

Health applications: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.

Environmental sensing: The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc. Some other major areas are listed below:

- Air pollution monitoring
- Forest fires detection
- Greenhouse monitoring
- Landslide detection

Structural monitoring: Wireless sensors can be utilized to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc enabling Engineering practices to monitor assets remotely with out the need for costly site visits.

Industrial monitoring: Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.

Agricultural sector: using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Irrigation automation enables more efficient water use and reduces waste.

3. Design issues of a wireless sensor network

There are a lot of challenges placed by the deployment of sensor networks which are a superset of those found in wireless ad hoc networks. Sensor nodes communicate over wireless, lossy lines with no infrastructure. An additional challenge is related to the limited,

usually non-renewable energy supply of the sensor nodes. In order to maximize the lifetime of the network, the protocols need to be designed from the beginning with the objective of efficient management of the energy resources (Akyildiz et al., 2002). Wireless Sensor Network Design issues are mentioned in (Akkaya et al., 2005), (Akyildizet al., 2002), (SensorSim; Tossim, Younis et al., 2004), (Pan et al., 2003) and different possible platforms for simulation and testing of routing protocols for WSNs are discussed in (NS-2, Zeng et al., 1998, SensorSim, Tossiim). Let us now discuss the individual design issues in greater detail.

Fault Tolerance: Sensor nodes are vulnerable and frequently deployed in dangerous environment. Nodes can fail due to hardware problems or physical damage or by exhausting their energy supply. We expect the node failures to be much higher than the one normally considered in wired or infrastructure-based wireless networks. The protocols deployed in a sensor network should be able to detect these failures as soon as possible and be robust enough to handle a relatively large number of failures while maintaining the overall functionality of the network. This is especially relevant to the routing protocol design, which has to ensure that alternate paths are available for rerouting of the packets. Different deployment environments pose different fault tolerance requirements.

Scalability: Sensor networks vary in scale from several nodes to potentially several hundred thousand. In addition, the deployment density is also variable. For collecting high-resolution data, the node density might reach the level where a node has several thousand neighbours in their transmission range. The protocols deployed in sensor networks need to be scalable to these levels and be able to maintain adequate performance.

Production Costs: Because many deployment models consider the sensor nodes to be disposable devices, sensor networks can compete with traditional information gathering approaches only if the individual sensor nodes can be produced very cheaply. The target price envisioned for a sensor node should ideally be less than $1.

Hardware Constraints: At minimum, every sensor node needs to have a sensing unit, a processing unit, a transmission unit, and a power supply. Optionally, the nodes may have several built-in sensors or additional devices such as a localization system to enable location-aware routing. However, every additional functionality comes with additional cost and increases the power consumption and physical size of the node. Thus, additional functionality needs to be always balanced against cost and low-power requirements.

Sensor Network Topology: Although WSNs have evolved in many aspects, they continue to be networks with constrained resources in terms of energy, computing power, memory, and communications capabilities. Of these constraints, energy consumption is of paramount importance, which is demonstrated by the large number of algorithms, techniques, and protocols that have been developed to save energy, and thereby extend the lifetime of the network. Topology Maintenance is one of the most important issues researched to reduce energy consumption in wireless sensor networks.

Transmission Media: The communication between the nodes is normally implemented using radio communication over the popular ISM bands. However, some sensor networks

use optical or infrared communication, with the latter having the advantage of being robust and virtually interference free.

Power Consumption: As we have already seen, many of the challenges of sensor networks revolve around the limited power resources. The size of the nodes limits the size of the battery. The software and hardware design needs to carefully consider the issues of efficient energy use. For instance, data compression might reduce the amount of energy used for radio transmission, but uses additional energy for computation and/or filtering. The energy policy also depends on the application; in some applications, it might be acceptable to turn off a subset of nodes in order to conserve energy while other applications require all nodes operating simultaneously.

4. Structure of a wireless sensor network

Structure of a Wireless Sensor Network includes different topologies for radio communications networks. A short discussion of the network topologies that apply to wireless sensor networks are outlined below:

4.1. Star network (single point-to-multipoint) (Wilson, 2005)

A star network is a communications topology where a single base station can send and/or receive a message to a number of remote nodes. The remote nodes are not permitted to send messages to each other. The advantage of this type of network for wireless sensor networks includes simplicity, ability to keep the remote node's power consumption to a minimum. It also allows low latency communications between the remote node and the base station. The disadvantage of such a network is that the base station must be within radio transmission range of all the individual nodes and is not as robust as other networks due to its dependency on a single node to manage the network.

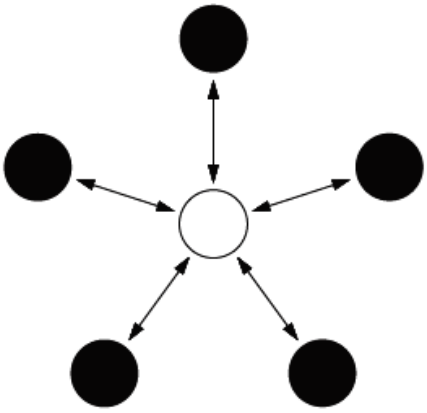

Figure 2. A Star network topology

4.2. Mesh network (Wilson, 2005)

A mesh network allows transmitting data to one node to other node in the network that is within its radio transmission range. This allows for what is known as multi-hop communications, that is, if a node wants to send a message to another node that is out of radio communications range, it can use an intermediate node to forward the message to the desired node. This network topology has the advantage of redundancy and scalability. If an individual node fails, a remote node still can communicate to any other node in its range, which in turn, can forward the message to the desired location. In addition, the range of the network is not necessarily limited by the range in between single nodes; it can simply be extended by adding more nodes to the system. The disadvantage of this type of network is in power consumption for the nodes that implement the multi-hop communications are generally higher than for the nodes that don't have this capability, often limiting the battery life. Additionally, as the number of communication hops to a destination increases, the time to deliver the message also increases, especially if low power operation of the nodes is a requirement.

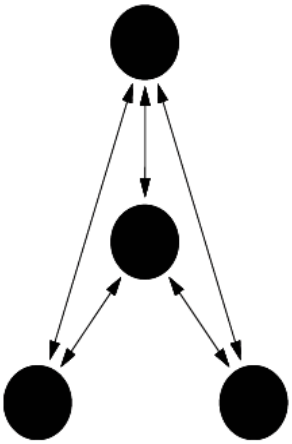

Figure 3. A Mesh network topology

4.3. Hybrid star – Mesh network (Wilson, 2005)

A hybrid between the star and mesh network provides a robust and versatile communications network, while maintaining the ability to keep the wireless sensor nodes power consumption to a minimum. In this network topology, the sensor nodes with lowest power are not enabled with the ability to forward messages. This allows for minimal power consumption to be maintained. However, other nodes on the network are enabled with multi-hop capability, allowing them to forward messages from the low power nodes to other nodes on the network. Generally, the nodes with the multi-hop capability are higher power, and if possible, are often plugged into the electrical mains line. This is the topology implemented by the up and coming mesh networking standard known as ZigBee.

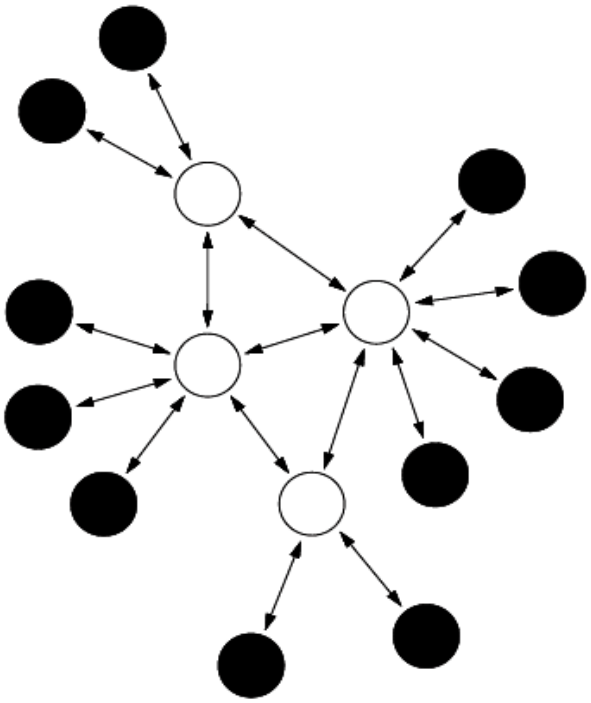

Figure 4. A Hybrid Star – Mesh network topology

5. Structure of a wireless sensor node

A sensor node is made up of four basic components such as sensing unit, processing unit, transceiver unit and a power unit which is shown in Fig. 5. It also has application dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analogue to digital converters (ADCs) (Akyildiz et al., 2002). The analogue signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit is generally associated with a small storage unit and it can manage the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units can be supported by a power scavenging unit such as solar cells. The other subunits, of the node are application dependent.

A functional block diagram of a versatile wireless sensing node is provided in Fig. 6. Modular design approach provides a flexible and versatile platform to address the needs of a wide variety of applications. For example, depending on the sensors to be deployed, the signal conditioning block can be re-programmed or replaced. This allows for a wide variety

of different sensors to be used with the wireless sensing node. Similarly, the radio link may be swapped out as required for a given applications' wireless range requirement and the need for bidirectional communications.

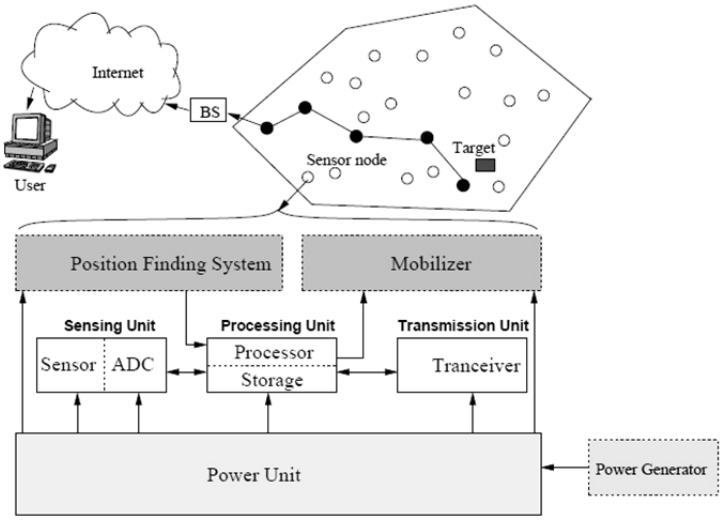

Figure 5. The components of a sensor node

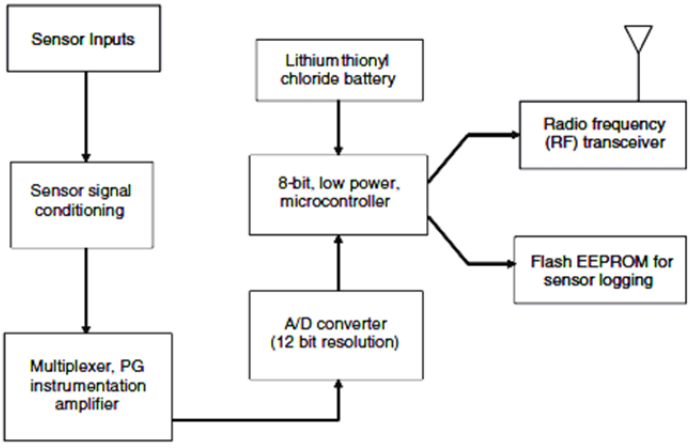

Figure 6. Functional block diagram of a sensor node

Using flash memory, the remote nodes acquire data on command from a base station, or by an event sensed by one or more inputs to the node. Moreover, the embedded firmware can be upgraded through the wireless network in the field.

The microprocessor has a number of functions including:

- Managing data collection from the sensors
- performing power management functions
- interfacing the sensor data to the physical radio layer
- managing the radio network protocol

A key aspect of any wireless sensing node is to minimize the power consumed by the system. Usually, the radio subsystem requires the largest amount of power. Therefore, data is sent over the radio network only when it is required. An algorithm is to be loaded into the node to determine when to send data based on the sensed event. Furthermore, it is important to minimize the power consumed by the sensor itself. Therefore, the hardware should be designed to allow the microprocessor to judiciously control power to the radio, sensor, and sensor signal conditioner (Akyildiz et al., 2002).

6. Communication structure of a wireless sensor network

The sensor nodes are usually scattered in a sensor field as shown in Fig. 1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink and the end users. Data are routed back to the end user by a multi-hop infrastructure-less architecture through the sink as shown in Fig. 1. The sink may communicate with the task manager node via Internet or Satellite.

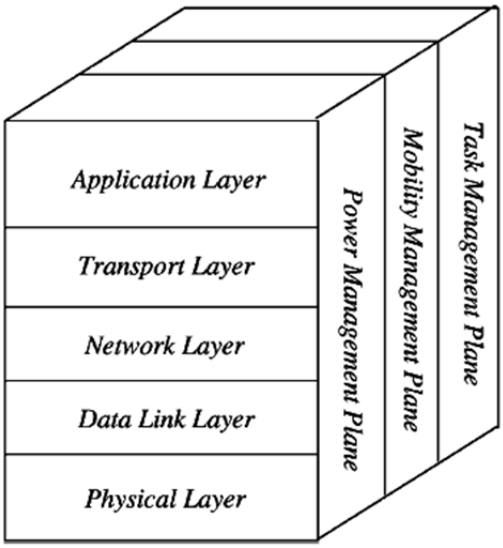

Figure 7. Wireless Sensor Network protocol stack

The protocol stack used by the sink and the sensor nodes is given in Fig. 7. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium and promotes cooperative efforts of sensor nodes. The protocol stack consists of the application layer, transport layer,

network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane (Akyildiz et al., 2002). Different types of application software can be built and used on the application layer depending on the sensing tasks. This layer makes hardware and software of the lowest layer transparent to the end-user. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer, specific multi-hop wireless routing protocols between sensor nodes and sink. The data link layer is responsible for multiplexing of data streams, frame detection, Media Access Control (MAC) and error control. Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbours' broadcast. The physical layer addresses the needs of a simple but robust modulation, frequency selection, data encryption, transmission and receiving techniques.

In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall energy consumption.

7. Energy consumption issues in wireless sensor network

Energy consumption is the most important factor to determine the life of a sensor network because usually sensor nodes are driven by battery. Sometimes energy optimization is more complicated in sensor networks because it involved not only reduction of energy consumption but also prolonging the life of the network as much as possible. The optimization can be done by having energy awareness in every aspect of design and operation. This ensures that energy awareness is also incorporated into groups of communicating sensor nodes and the entire network and not only in the individual nodes (Bharathidasan et al. 2001).

A sensor node usually consists of four sub-systems (Bharathidasan et al. 2001):

- a computing subsystem : It consists of a microprocessor(microcontroller unit, MCU) which is responsible for the control of the sensors and implementation of communication protocols. MCUs usually operate under various modes for power management purposes. As these operating modes involves consumption of power, the energy consumption levels of the various modes should be considered while looking at the battery lifetime of each node.
- a communication subsystem: It consists of a short range radio which communicate with neighboring nodes and the outside world. Radios can operate under the different modes. It is important to completely shut down the radio rather than putting it in the Idle mode when it is not transmitting or receiving for saving power.
- a sensing subsystem : It consists of a group of sensors and actuators and link the node to the outside world. Energy consumption can be reduced by using low power components and saving power at the cost of performance which is not required.

- a power supply subsystem : It consists of a battery which supplies power to the node. It should be seen that the amount of power drawn from a battery is checked because if high current is drawn from a battery for a long time, the battery will die faster even though it could have gone on for a longer time. Usually the rated current capacity of a battery being used for a sensor node is less than the minimum energy consumption. The lifetime of a battery can be increased by reducing the current drastically or even turning it off often.

To minimize the overall energy consumption of the sensor network, different types of protocols and algorithms have been studied so far all over the world. The lifetime of a sensor network can be increased significantly if the operating system, the application layer and the network protocols are designed to be energy aware. These protocols and algorithms have to be aware of the hardware and able to use special features of the micro-processors and transceivers to minimize the sensor node's energy consumption. This may push toward a custom solution for different types of sensor node design. Different types of sensor nodes deployed also lead to different types of sensor networks. This may also lead to the different types of collaborative algorithms in wireless sensor networks arena.

8. Protocols & algorithms of wireless sensor network

In WSN, the main task of a sensor node is to sense data and sends it to the base station in multi hop environment for which routing path is essential. For computing the routing path from the source node to the base station there is huge numbers of proposed routing protocols exist (Sharma et al., 2011). The design of routing protocols for WSNs must consider the power and resource limitations of the network nodes, the time-varying quality of the wireless channel, and the possibility for packet loss and delay. To address these design requirements, several routing strategies for WSNs have been proposed in (Labrador et al., 2009), (Akkaya et al., 2005), (Akyildiz et al. 2002), (Boukerche, 2009, Al-karaki et al., 2004, Pan et al., 2003) and (Waharte et al., 2006).

The first class of routing protocols adopts a flat network architecture in which all nodes are considered peers. Flat network architecture has several advantages, including minimal overhead to maintain the infrastructure and the potential for the discovery of multiple routes between communicating nodes for fault tolerance.

A second class of routing protocols imposes a structure on the network to achieve energy efficiency, stability, and scalability. In this class of protocols, network nodes are organized in clusters in which a node with higher residual energy, for example, assumes the role of a cluster head. The cluster head is responsible for coordinating activities within the cluster and forwarding information between clusters. Clustering has potential to reduce energy consumption and extend the lifetime of the network.

A third class of routing protocols uses a data-centric approach to disseminate interest within the network. The approach uses attribute-based naming, whereby a source node queries an attribute for the phenomenon rather than an individual sensor node. The interest

dissemination is achieved by assigning tasks to sensor nodes and expressing queries to relative to specific attributes. Different strategies can be used to communicate interests to the sensor nodes, including broadcasting, attribute-based multicasting, geo-casting, and any casting.

A fourth class of routing protocols uses location to address a sensor node. Location-based routing is useful in applications where the position of the node within the geographical coverage of the network is relevant to the query issued by the source node. Such a query may specify a specific area where a phenomenon of interest may occur or the vicinity to a specific point in the network environment.

In the rest of this section we discuss some of the major routing protocols and algorithms to deal with the energy conservation issue in the literatures.

1. Flooding: Flooding is a common technique frequently used for path discovery and information dissemination in wired and wireless ad hoc networks which has been discussed in (Akyildiz et al., 2002). The routing strategy of flooding is simple and does not rely on costly network topology maintenance and complex route discovery algorithms. Flooding uses a reactive approach whereby each node receiving a data or control packet sends the packet to all its neighbors. After transmission, a packet follows all possible paths. Unless the network is disconnected, the packet will eventually reach its destination. Furthermore, as the network topology changes, the packet transmitted follows the new routes. Fig. 8 illustrates the concept of flooding in data communications network. As shown in the figure, flooding in its simplest form may cause packets to be replicated indefinitely by network nodes.

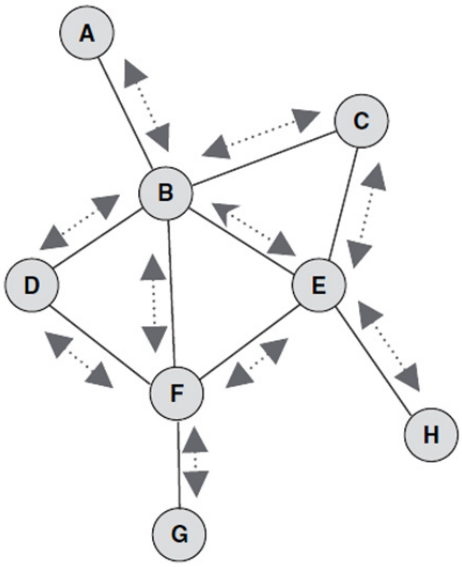

Figure 8. Flooding in data communication networks

1. Gossiping:

To address the shortcomings of flooding, a derivative approach, referred to as gossiping, has been proposed in (Braginsky et al., 2002). Similar to flooding, gossiping uses a simple forwarding rule and does not require costly topology maintenance or complex route discovery algorithms. Contrary to flooding, where a data packet is broadcast to all neighbors, gossiping requires that each node sends the incoming packet to a randomly selected neighbor. Upon receiving the packet, the neighbor selected randomly chooses one of its own neighbors and forwards the packet to the neighbor chosen. This process continues iteratively until the packet reaches its intended destination or the maximum hop count is exceeded.

2. Protocols for Information via Negotiation (SPIN):

Sensor protocols for information via negotiation (SPIN), is a data-centric negotiation-based family of information dissemination protocols for WSNs (Kulik et al., 2002). The main objective of these protocols is to efficiently disseminate observations gathered by individual sensor nodes to all the sensor nodes in the network. Simple protocols such as flooding and gossiping are commonly proposed to achieve information dissemination in WSNs. Flooding requires that each node sends a copy of the data packet to all its neighbors until the information reaches all nodes in the network. Gossiping, on the other hand, uses randomization to reduce the number of duplicate packets and requires only that a node receiving a data packet forward it to a randomly selected neighbor.

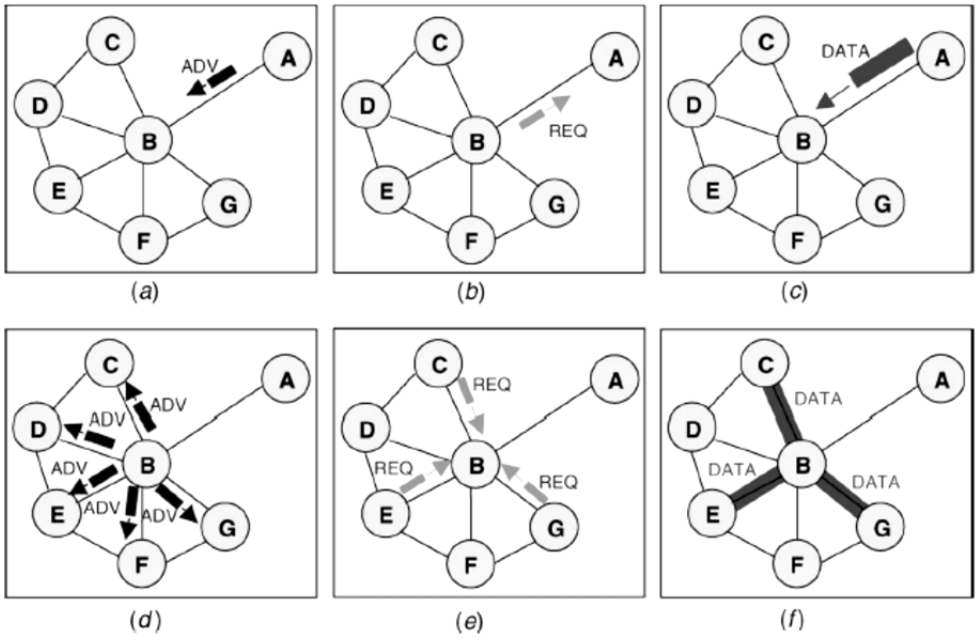

Figure 9. SPIN basic protocol operation

3. Low-Energy Adaptive Clustering Hierarchy (LEACH)

Low-energy adaptive clustering hierarchy (LEACH) is a routing algorithm designed to collect and deliver data to the data sink, typically a base station (Heinzelman et. al. 2000). The main objectives of LEACH are:

- Extension of the network lifetime
- Reduced energy consumption by each network sensor node
- Use of data aggregation to reduce the number of communication messages

To achieve these objectives, LEACH adopts a hierarchical approach to organize the network into a set of clusters. Each cluster is managed by a selected cluster head. The cluster head assumes the responsibility to carry out multiple tasks. The first task consists of periodic collection of data from the members of the cluster. Upon gathering the data, the cluster head aggregates it in an effort to remove redundancy among correlated values. The second main task of a cluster head is to transmit the aggregated data directly to the base station over single hop. The third main task of the cluster head is to create a TDMA-based schedule whereby each node of the cluster is assigned a time slot that it can use for transmission. The cluster head announces the schedule to its cluster members through broadcasting. To reduce the likelihood of collisions among sensors within and outside the cluster, LEACH nodes use a code-division multiple access–based scheme for communication.

The basic operations of LEACH are organized in two distinct phases. The first phase, the setup phase, consists of two steps, cluster-head selection and cluster formation. The second phase, the steady-state phase, focuses on data collection, aggregation, and delivery to the base station. The duration of the setup is assumed to be relatively shorter than the steady-state phase to minimize the protocol overhead.

At the beginning of the setup phase, a round of cluster-head selection starts. To decide whether a node to become cluster head or not a threshold T(s) is addressed in (Heinzelman et. al. 2000) which is as follows:

$$T(s) = \begin{cases} \dfrac{p_{opt}}{1 - p_{opt}.(r.\mathrm{mod}.\dfrac{1}{p_{opt}})}, if s \in G' \\ 0, otherwise \end{cases} \quad (1)$$

Where r is the current round number and G is the set of nodes that have not become cluster head within the last $1/p_{opt}$ rounds. At the beginning of each round, each node which belongs to the set G selects a random number 0 or 1. If the random number is less than the threshold T(s) then the node becomes a cluster head in the current round.

4. Threshold-sensitive Energy Efficient Protocols (TEEN and APTEEN):

Two hierarchical routing protocols called TEEN (Threshold-sensitive Energy Efficient sensor Network protocol), and APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) are proposed in (Manjeshwar et al., 2001) and (Manjeshwar et al.,

2002) , respectively. These protocols were proposed for time-critical applications. In TEEN, sensor nodes sense the medium continuously, but the data transmission is done less frequently. A cluster head sensor sends its members a hard threshold, which is the threshold value of the sensed attribute and a soft threshold, which is a small change in the value of the sensed attribute that triggers the node to switch on its transmitter and transmit. Thus the hard threshold tries to reduce the number of transmissions by allowing the nodes to transmit only when the sensed attribute is in the range of interest. The soft threshold further reduces the number of transmissions that might have otherwise occurred when there is little or no change in the sensed attribute. A smaller value of the soft threshold gives a more accurate picture of the network, at the expense of increased energy consumption. Thus, the user can control the trade-off between energy efficiency and data accuracy. When cluster-heads are to change, new values for the above parameters are broadcast. The main drawback of this scheme is that, if the thresholds are not received, the nodes will never communicate, and the user will not get any data from the network at all.

5. Power-Efficient Gathering in Sensor Information Systems (PEGASIS):

Power-efficient gathering in sensor information systems (PEGASIS) (Lindsey et al., 2002) and its extension, hierarchical PEGASIS, are a family of routing and information-gathering protocols for WSNs. The main objectives of PEGASIS are twofold. First, the protocol aims at extending the lifetime of a network by achieving a high level of energy efficiency and uniform energy consumption across all network nodes. Second, the protocol strives to reduce the delay that data incur on their way to the sink.

The network model considered by PEGASIS assumes a homogeneous set of nodes deployed across a geographical area. Nodes are assumed to have global knowledge about other sensors' positions. Furthermore, they have the ability to control their power to cover arbitrary ranges. The nodes may also be equipped with CDMA-capable radio transceivers. The nodes' responsibility is to gather and deliver data to a sink, typically a wireless base station. The goal is to develop a routing structure and an aggregation scheme to reduce energy consumption and deliver the aggregated data to the base station with minimal delay while balancing energy consumption among the sensor nodes. Contrary to other protocols, which rely on a tree structure or a cluster-based hierarchical organization of the network for data gathering and dissemination, PEGASIS uses a chain structure.

6. Directed Diffusion:

Directed diffusion (Intanagonwiwat et al., 2000) is a data-centric routing protocol for information gathering and dissemination in WSNs. The main objective of the protocol is to achieve substantial energy savings in order to extend the lifetime of the network. To achieve this objective, directed diffusion keeps interactions between nodes, in terms of message exchanges, localized within limited network vicinity. Using localized interaction, direct diffusion can still realize robust multi-path delivery and adapt to a minimal subset of network paths. This unique feature of the protocol, combined with the ability of the nodes to aggregate response to queries, results into significant energy savings.

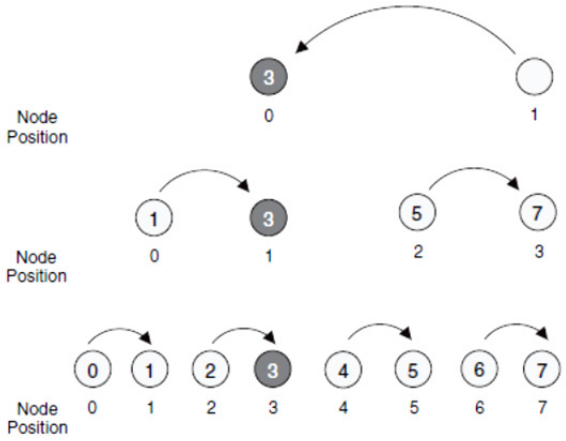

Figure 10. Chain-based data gathering and aggregation scheme

The main elements of direct diffusion include interests, data messages, gradients, and reinforcements. Directed diffusion uses a publish-and-subscribe information model in which an inquirer expresses an interest using attribute–value pairs. An interest can be viewed as a query or an interrogation that specifies what the inquirer wants.

7. Geographic Adaptive Fidelity (GAF):

GAF (Xu et al., 2001) is an energy-aware location-based routing algorithm designed mainly for mobile ad hoc networks, but may be applicable to sensor networks as well. The network area is first divided into fixed zones and forms a virtual grid. Inside each zone, nodes collaborate with each other to play different roles. For example, nodes will elect one sensor node to stay awake for a certain period of time and then they go to sleep. This node is responsible for monitoring and reporting data to the BS on behalf of the nodes in the zone. Hence, GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity.

9. Security issues in wireless sensor network

Security issues in sensor networks depend on the need to know what we are going to protect. In (Zia et al., 2006), the authors defined four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability. Another security goal in sensor network is introduced in (Sharma et al., 2011).Confidentiality is the ability to conceal message from a passive attacker, where the message communicated on sensor networks remain confidential. Integrity refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network. Authentication Need to know if the messages are from the node it claims to be from, determining the reliability of message's origin. Availability is to determine if a node has the ability to use the resources and the network is available for the messages to move on. Freshness implies that receiver receives the recent and fresh data and ensures that no adversary can replay the old data. This requirement is

especially important when the WSN nodes use shared-keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN (Sen, 2009). To achieve the freshness the mechanism like nonce or time stamp should add to each data packet.

Having built a foundation of security goals in sensor network, the major possible security attacks in sensor networks are identified in (Undercoffer et al., 2002) . Routing loops attacks target the information exchanged between nodes. False error messages are generated when an attacker alters and replays the routing information. Routing loops attract or repel the network traffic and increases node to node latency. Selective forwarding attack influences the network traffic by believing that all the participating nodes in network are reliable to forward the message. In selective forwarding attack malicious nodes simply drop certain messages instead of forwarding every message. Once a malicious node cherry picks on the messages, it reduces the latency and deceives the neighboring nodes that they are on a shorter route. Effectiveness of this attack depends on two factors. First the location of the malicious node, the closer it is to the base stations the more traffic it will attract. Second is the percentage of messages it drops. When selective forwarder drops more messages and forwards less, it retains its energy level thus remaining powerful to trick the neighboring nodes. In sinkhole attacks, adversary attracts the traffic to a compromised node. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible. Sybil attacks are a type of attacks where a node creates multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can be used against routing algorithms and topology maintenance; it reduces the effectiveness of fault tolerant schemes such as distributed storage and disparity. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously. In wormhole attacks an adversary positioned closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link. Here an adversary convinces the nodes which are multi hop away that they are closer to the base station. This creates a sinkhole because adversary on the other side of the sinkhole provides a better route to the base station. In Hello flood attacks a Broadcasted message with stronger transmission power is pretending that the HELLO message is coming from the base station. Message receiving nodes assume that the HELLO message sending node is the closest one and they try to send all their messages through this node. In this type of attacks all nodes will be responding to HELLO floods and wasting the energies. The real base station will also be broadcasting the similar messages but will have only few nodes responding to it. Denial of service (DoS) attacks occur at physical level causing radio jamming, interfering with the network protocol, battery exhaustion etc. An specific type of DoS attack, Denial-of-service attack has been explored in (Raymond et al., 2009), in which a sensor node's power supply is targeted. Attacks of this type can reduce the sensor lifetime from years to days and have a devastating impact on a sensor network.

1. Layering based security approach:

- Application layer

Data is collected and managed at application layer therefore it is important to ensure the reliability of data. Wagner (Wanger, 2004) has presented a resilient aggregation scheme which is applicable to a cluster based network where a cluster leader acts as an aggregator in sensor networks. However this technique is applicable if the aggregating node is in the range with all the source nodes and there is no intervening aggregator between the aggregator and source nodes. To prove the validity of the aggregation, cluster leaders use the cryptographic techniques to ensure the data reliability.

- Network layer

Network layer is responsible for routing of messages from node to node, node to cluster leader, cluster leaders to cluster leaders, cluster leaders to the base station and vice versa.

- Data link layer

Data link layer does the error detection and correction, and encoding of data. Link layer is vulnerable to jamming and DoS attacks. TinySec (Karlof et al., 2004) has introduced link layer encryption which depends on a key management scheme. However, an attacker having better energy efficiency can still rage an attack. Protocols like LMAC (Hoesel et al., 2004) have better anti-jamming properties which are viable countermeasure at this layer.

- Physical Layer

The physical layer emphasizes on the transmission media between sending and receiving nodes, the data rate, signal strength, frequency types are also addressed in this layer. Ideally FHSS frequency hopping spread spectrum is used in sensor networks.

10. Conclusion & future work

The aim of this chapter is to discuss few important issues of WSNs, from the application, design and technology points of view. For designing a WSN, we need to consider different factors such as the flexibility, energy efficiency, fault tolerance, high sensing fidelity, low-cost and rapid deployment, above all the application requirements. We hope the wide range of application areas will make sensor networks an integral part of our lives in the future. However, realization of sensor networks needs to satisfy several constraints such as scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly tight and specific for sensor networks, new wireless ad hoc networking protocols are required. To meet the requirements, many researchers are engaged in developing the technologies needed for different layers of the sensor networks protocol stack.

Future research on WSN will be directed towards maximizing area throughput in clustered Wireless Sensor Networks designed for temporal or spatial random process estimation, accounting for radio channel, PHY, MAC and NET protocol layers and data aggregation

techniques, simulation and experimental verification of lifetime-aware routing, sensing spatial coverage and the enhancement of the desired sensing spatial coverage evaluation methods with practical sensor model.

The advances of wireless networking and sensor technology open up an interesting opportunity to manage human activities in a smart home environment. Real-life activities are often more complex than the case studies for both single and multi-user. Investigating such complex cases can be very challenging while we consider both single- and multi-user activities at the same time. Future work will focus on the fundamental problem of recognizing activities of multiple users using a wireless body sensor network.
Wireless Sensor Networks hold the promise of delivering a smart communication paradigm which enables setting up an intelligent network capable of handling applications that evolve from user requirements. We believe that in near future, WSN research will put a great impact on our daily life. For example, it will create a system for continual observation of physiological signals while the patients are at their homes. It will lower the cost involved with monitoring patients and increase the efficient exploitation of physiological data and the patients will have access to the highest quality medical care in their own homes. Thus, it will avoid the distress and disruption caused by a lengthy inpatient stay.

Author details

M.A. Matin
Institut Teknologi Brunei, Brunei Darussalam

M.M. Islam
North South University, Dhaka, Bangladesh

11. References

A. Boukerche. Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks, John Wiley & Sons, Inc., 2009.

A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002, pp. 195-202.

A. Manjeshwar and D. P. Agarwal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.

B. Paul, M. A. Matin," Optimal Geometrical Sink Location Estimation for Two Tiered Wireless Sensor Networks" IET Wireless Sensor Systems, vol.1, no.2, pp.74-84, June 2011,doi: 10.1049/iet-wss.2010.0073, IET UK.

Bharathidasan, A., Anand, V., Ponduru, S. (2001), Sensor Networks: An Overview, Department of Computer Science, University of California, Davis 2001. Technical Report

C. Intanagonwiwat, R. Govindan, D. Estrin, ''Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,'' Proceedings of the 6th ACM 226 ROUTING PROTOCOLS FOR WIRELESS SENSOR NETWORKS International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, Aug. 2000, pp. 56–67.

C. karlof, N. Shastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, SenSys'04, November 3-5 2004, Baltimore, Maryland, USA

Chiara, B.; Andrea, C.; Davide, D.; Roberto, V. An Overview on Wireless Sensor Networks Technology and Evolution. Sensors 2009, 9, 6869-6896.

Chi-Tsun Cheng, Chi K. Tse, and Francis C. M. Lau, "A Delay-Aware Data Collection Network Structure for Wireless Sensor Networks", IEEE Sensors Journal, Vol. 11, No. 3, pp. 699-710, March 2011.

D. Braginsky, D. Estrin, ''Rumor Routing Algorithm for Sensor Networks,'' Proceedings of the 1st Workshop on Sensor Networks and Applications (WSNA'02), Atlanta, GA, Oct. 2002.

D. Wagner, Resilient aggregation in sensor networks, In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM Press, 2004, pp. 78-87.

D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff. Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols. IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 367-380, 2009.

Fabbri, F.; Buratti, C.; Verdone, R.; Riihij¨arvi, J.; M¨ah¨onen, P. Area Throughput and Energy Consumption for Clustered Wireless Sensor Networks. In Proceedings of IEEE WCNC 2009, Budapest, Hungary, 2009

Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless micro-sensor networks. In: Proceedings of the 33rd International Conference on System Sciences (HICSS), pp. 1–10 (2000)

I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. Computer Networks, 38(4):393–422, 2002.

I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. A survey on sensor networks. IEEE Communications Magazine. 40 (8) (2002) 102–114.

J. Kulik, W. R. Heinzelman, H. Balakrishnan, ''Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks,'' Wireless Networks, Vol. 8, 2002, pp. 169–185.

J. Pan, Y. Hou, L. Cai, Y. Shi and S. X. Shen, 'Topology Control for Wireless Sensor Networks' Proc. 9th ACM Int. Conf. on Mobile Computing and Networking, San Diego, USA, September, 2003, pp. 286-29.

J. Sen. A survey on wireless sensor network security. International Journal of Communication Networks and Information Security (IJCNIS), 1(2):59–82, August 2009.

J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, Security for sensor networks, 2002 CADIP Research Symposium.

J. Yick, B. Mukherjee, D. Ghosal. Wireless sensor network survey, Computer Networks 52 (12) (2008) 2292–2330.

J.N. Al-Karaki, A.E. Kamal, Routing techniques in wireless sensor networks: a survey, IEEE Wireless Communications (2004).

K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Elsevier Journal of Ad Hoc Networks 3 (3) (2005) 325–349.

L.V. Hoesel and P. Havinga, A Lightweight Medium Access Protocol (LMAC) for wireless sensor networks: reducing preamble transmissions and transceiver state switches, in the proceedings of INSS, June 2004.

M A Matin, and Md. Nafees Rahman, "Lifetime improvement of Wireless Sensor Networks" 3rd IEEE International conference on Communication Software and Networks (ICCSN) 2011, Xi'an, China, May 27-29, 2011, pp.475-479.

M. A. Labrador, P. M. Wightman. Topology Control in Wireless Sensor Networks. Springer Science + Business Media B.V. 2009.

Ns-2 [Online]. Available: http://www.isi.edu/nsnam/ns/

S Sharma and S K Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks", ICCCS'11 February 2011.

S. Lindsey, C. Raghavendra, ''PEGASIS: Power-Efficient Gathering in Sensor Information Systems,'' IEEE Aerospace Conference Proceedings, 2002, Vol. 3, No. 9–16 pp. 1125–1130.

S. Waharte, R. Boutaba, Y. Iraqi, and B. Ishibashi, "Routing protocols in wireless mesh networks: challenges and design considerations," Multimedia Tools Appl., vol. 29, no. 3, pp. 285–303, 2006.

SensorSim [Online]: Available: http://nesl.ee.ucla.edu/projects/sensorsim/

Sohraby, K.; Minoli, D.; Znati, T. Wireless Sensor Networks: Technology, Protocols and Applications; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2007.

TOSSIM [Online]. Available: http://docs.tinyos.net/index.php/TOSSIM

Verdone, R.; Dardari, D.; Mazzini, G.; Conti, A. Wireless Sensor and Actuator Networks; Elsevier: London, UK, 2008.

Wilson, J. Sensor Technology Handbook; Elsevier/Newnes: Burlington, MA, USA, 2005.

X. Chen and N. Rowe, "An Energy-Efficient Communication Scheme in Wireless Cable Sensor Networks", Proc. of IEEE International Conference on Communications (IEEE ICC), June 2011

X. Han, X. Cao, E. L. Lloyd and C. Shen, "Fault-Tolerant Relay Node Placement in Heterogeneous Wireless Sensor Networks", IEEE Transaction on Mobile Computing, Vol. 9, No. 5, May 2010

X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," SIGSIM Simulation Digest, vol. 28, no. 1, pp. 154-161, 1998.

Y. Xu, J. Heidemann, D. Estrin, ''Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking 2001, pp. 70-84.

Younis, O., Fahmy, S. HEED: a hybryd, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mobile Comput. 3(4), 366–379 (2004)

Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006.