CHAPTER 2

OVERVIEW OF WIRELESS SENSOR NETWORKS

This chapter provides an overview of WSN routing techniques, localisation schemes, mobile elements, and currently available actor coordination strategies in wireless sensor and actor networks (WSANs). The literature review reflects the most important themes applicable to this research thesis, and briefly describes the most important characteristics of each one of them.

2.1 INTRODUCTION

In wired networks two main algorithms are used for routing messages, namely link-state and distance vector algorithms (Abolhasan et al., 2004). In link-state routing, each node periodically broadcasts the link-state costs of its neighbouring nodes to all other nodes using a flooding strategy. Upon receipt of one of these update packets; a node uses the information in a shortest path to calculate the next hop node for each destination. In distance-vector routing, each node keeps the distance for every destination. This allows each node to select the shortest path to each destination. The distance-vector information is updated at each node by a periodical dissemination of the current estimate of the shortest distance to every node. The traditional link-state and distance-vector algorithm are not suitable for WSN applications because the periodic route updates deplete the power supply of the nodes rapidly.

2.2 ROUTING IN WSNS

Routing in WSNs is concerned with finding the shortest path between the source node and the destination sink while sending the minimum number of messages. Two classical mechanisms for relaying data within a network without requiring continual knowledge of network topology and routing algorithms are flooding and gossiping (Kazem Sohraby, 2007).

2.2.1 Classical routing techniques

2.2.1.1 Flooding

Flooding uses a reactive approach whereby each node receiving a data or control packet re-broadcasts the message received to all its neighbours. After transmission, a packet follows all possible paths. This process continues recursively, until the message reaches its intended destination. To prevent a packet from circulating indefinitely in the network, either a hop count field or a time-to-live field is included in the packet. As the packet travels across the network, the hop count is decremented by one for each hop that it traverses. When the hop count reaches zero, the packet is simply discarded. Similarly, the time-to-live field, records the number of time units that a packet is allowed to live within the network. At the expiration of this time, the packet is no longer forwarded.

Despite the simplicity of its forwarding rule and the relatively low-cost maintenance that it requires, flooding suffers several deficiencies when used in WSNs including:

1. ***traffic implosion***, whereby two or more nodes sensing the same area send similar messages to the same neighbour node. This duplication of messages consumes a large amount of energy as sensor nodes use almost the same amount of energy to receive messages as the nodes use to transmit, because of the short transmission distances used in WSNs;
2. ***overlap problem***, which occurs when two nodes covering the same region send packets containing similar information to the same node; and
3. ***resource blindness*** caused by not taking into consideration the energy constraints of the sensor nodes when forwarding messages. As such, the node's energy may deplete rapidly, reducing considerably the lifetime of the network.

2.2.1.2 Gossiping

Gossiping also uses a simple forwarding rule and does not require costly topology maintenance or complex route discovery algorithms. Instead of sending the packet to all neighbours, in gossiping a receiving node randomly chooses one of its neighbours to forward the received message to. This process continues iteratively until the message reaches its destination or the maximum number of hops for the message is exceeded.

Gossiping avoids the implosion problem by limiting the number of packets that each node sends to its neighbour to one copy.

The random selection of the node to route a message can cause propagation delays (Akkaya & Younis, 2003) or result in the message becoming stuck in a circular route without ever reaching its intended destination.

2.2.2 Current routing techniques

Current routing techniques for WSNs are dependent on the underlying network topology. There are various categories of WSN routing protocols, including cluster-based, data-centric, hierarchical, location-based, quality of service, network flow or data-aggregation protocols (Akkaya & Younis, 2003). In the following sections, routing protocols in WSNs have been broadly classified into four categories, namely flat, hierarchical, geographic (location), or network-structure based protocols. Figure 2.1 briefly summarises the key routing categories and provides examples of their various implementations (Al-Karaki & Kamal, 2004; Akkaya & Younis, 2003; Umar et al., 2007).

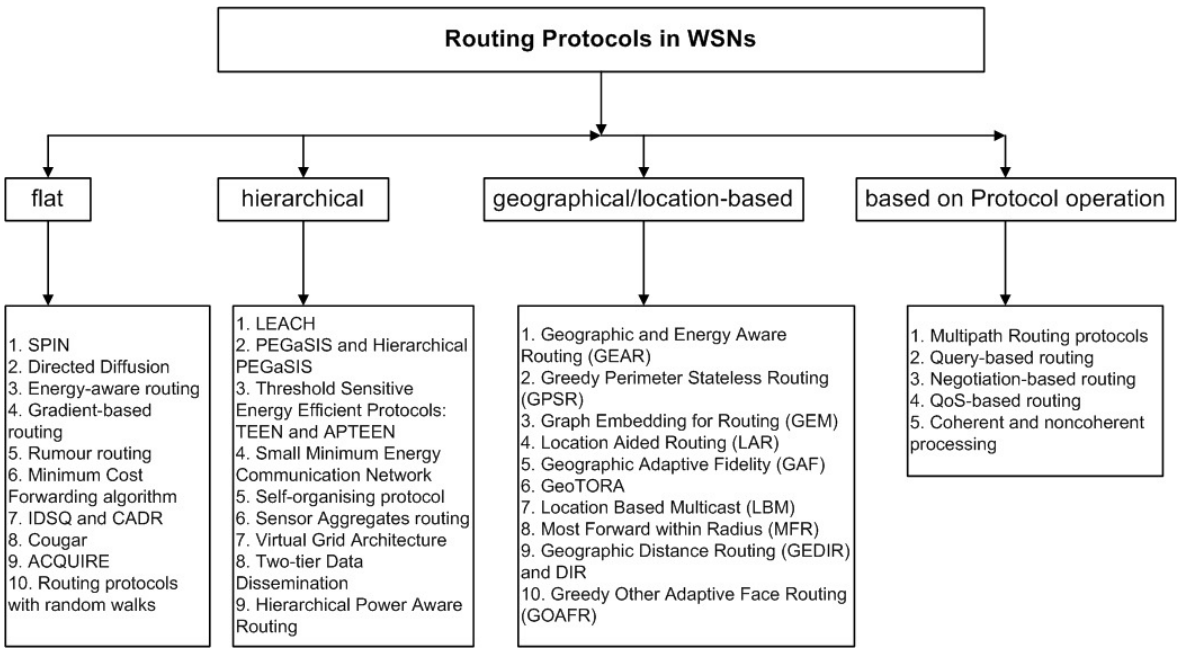

Figure 2.1: Current routing categories

Niezen et. al compare flooding, multi-hop routing, *L*ow *E*nergy *A*daptive *C*lustering *H*ierarchy (LEACH) and ad hoc on-demand distance vector (AODV) (Niezen et al., 2007). In their results, flooding proves to be worse than multi-hop routing and the LEACH protocol in terms of time for node(s) to fail, while AODV sends even more messages in the network than the flooding protocol; it was not initially designed for a WSN low-power environment.

2.2.2.1 Flat or data-centric routing protocols

All nodes are equal and collaborate with one another to perform a sensing task. The application area is densely populated with nodes and it is not practically viable to assign a unique global identifier to each node (such as an IP-type address). The lack of an identifier makes it difficult to distinguish which node or sets of nodes in a specific locality to query, or which nodes can route a message to a specific destination node. This lack of knowledge of the correct position of a set of nodes results in many unnecessary messages being transmitted, which reduces node lifetime within the WSN. To reduce the number of redundant messages, data-centric routing has been proposed. Attributes are assigned to specify the properties of data. A query is sent based on specific data attributes and only nodes with information that complies with the requested data attributes respond. Nodes can also follow an event-driven model and only send data when an event occurs.

2.2.2.2 Hierarchical (clustered) routing protocols

As the application area, network size and node density increase, the possibility of the sink (base station) becoming overloaded increases. As the number of messages within the network increases, a single sink may be unable to handle all communication effectively in a reasonable time-frame. To enable more effective communication, it has been proposed that the WSN be divided into clusters, with each cluster assuming similar roles to the single sink, to increase the efficiency and scalability of the network. Nodes send event data and respond to queries from a designated cluster, creating a hierarchical model for data routing. There can be a single layer of clusters or the clusters can be multi-tiered. Some of the advantages of clustering include (Abbasi and Younis, 2007):

1. Localises a route within a cluster and reduces the size of the route table.

2. Conserves communication bandwidth by preventing sensor nodes from exchanging messages with nodes outside their cluster and limiting the scope of inter-cluster interactions between cluster heads.
3. Reduces maintenance of network topology as sensors are only concerned with changes within their cluster and their cluster head.
4. Effects aggregation of data collected by sensors in cluster.
5. Ensures increased node longevity by allowing nodes to switch to low-power sleep mode most of the time.

2.2.2.3 Location or geographical routing protocols

Sensors can be randomly deployed within an application area (e.g. dropped from an aircraft in hostile military situations or due to natural disasters restricting access to an area), or manually placed at specific points within an application area (e.g. in an indoor factory or an outdoor field for agricultural monitoring). Many network functions such as geographic routing, coverage and tracking and location-dependent computing require prior knowledge of the position of nodes in a WSN. In geographic routing, a data message is routed to a geographic region instead of a destination node specified by an address (as in IP networks) (Umar et al., 2007). Routing protocols can use the location of a node to determine which nodes should forward a message.

2.3 ROUTING DESIGN CHALLENGES

In the Chapter 1 section 1.2.1, the main factors to consider when designing a WSN for a specific application are discussed. The focus is now placed on the specific design aspects of energy-efficient routing protocols in WSNs. There are many overlaps between design features for WSN applications and design issues for routing protocols in WSNs, because in both, efficient utilisation of the limited energy supply is a primary requirement. One of the main design goals of a WSN routing protocol is to carry out data communication while trying to prevent connectivity degradation by employing aggressive energy management techniques (Al-Karaki & Kamal, 2004). The following are the main factors to consider when designing a routing protocol for a WSN (Al-Karaki & Kamal, 2004; Akkaya & Younis, 2003; Umar et al., 2007; Korpeoglu, 2007).

1. ***Node deployment***: Sensors can be manually placed and data routed through pre-determined paths, or randomly scattered in a self-organising system, resulting in an ad hoc routing infrastructure. In randomly deployed, self-organising systems, the distribution of nodes is not uniform and the position of the sink or cluster head is crucial in terms of energy efficiency and performance.
2. ***Energy consumption without losing accuracy (node lifetime)***: Most WSNs are multi-hop networks because it uses more energy to transmit data over larger distances (approximately proportional to the distance squared) than using a single hop to the sink. The death of a node due to power failure can cause significant topological changes and may require re-routing of packets and reorganisation of the network. Therefore, as most wireless sensors are dependent on batteries, energy-saving forms of computation and communication are necessary. The use of multi-hop networks increases the complexity of topology management and medium access control protocols.
3. ***Data-reporting method***: The routing protocol is highly influenced by the data-reporting method in terms of energy consumption and route calculations. The three types of data-reporting methods are:
    a. **time-driven**: data about the surrounding environment sent to the sink at periodic time intervals;
    b. **query-driven**: when a node receives a message requesting information about the immediate environment it responds with a message to the sink containing the relevant data; and
    c. **event-driven**: changes in the surrounding environment exceed pre-defined limits, resulting in the actuator triggering an event. The sensor transmits a message to the sink to notify the sink of the triggered alarm.

    If the WSN application requires continuous monitoring and reporting, then a larger amount of traffic will be generated. Data-aggregation techniques would have to be taken into consideration in the design of the routing protocol. If the application only requires messages to be sent once a specific critical value has been breached, then very little data will be transmitted within the network.
4. **Node/link heterogeneity**: If the nodes in a WSN are not homogeneous, then some nodes may have more energy resources than others and some nodes may monitor

different aspects of the surrounding environment, thus using more or less energy than other nodes in a WSN. Generally the sink node or cluster heads (in a hierarchical topology) may have more energy, memory and processing resources than other nodes, as they will receive more messages and may be required to transmit these messages to the external human user. Designing a routing protocol has to take cognisance of the different resources available to nodes in a WSN and the different types of data-reporting methods that will be used.

5. **Destination specification**: the intended destination of a message can be based on the numerical addresses (or identifiers) of nodes, the geographic location of nodes or the type of data being transmitted. The routing path can be a destination-initiated or source-initiated protocol. Generally destination-initiated routing protocols, where the sink initiates path setup, are proactive in that the routing path is set up before there is a demand for routing traffic, whereas a source-initiated routing path is reactive and the routing protocol is activated when a data message needs to be sent and distributed to other nodes.
6. **Fault tolerance**: failure of a few nodes (due to energy depletion, physical damage or environmental interference), should not affect the overall functionality of the WSN. However, if many nodes fail, medium access control (MAC) and routing protocols must accommodate the formation of new links and routes to the sink and should provide multiple levels of redundancy.
7. **Scalability, connectivity, coverage**: a WSN may contain tens, hundreds or thousands of sensor nodes. This initial high density of sensor nodes should ensure that all nodes are highly connected and there is sufficient coverage of the application area. Any routing scheme must be able to work with small as well as large numbers of nodes, and should be able to respond to events within the application area. As battery life ends and nodes fail, the routing protocols must adapt to changing network topology and reduced network size.
8. **Network dynamics**: Routing requirements are different for fixed sensor and sink nodes compared to mobile sinks and/or sensor nodes. Routing messages from or to moving nodes is more challenging, since the network topology changes and routes to the destination change. Keeping track of dynamic events is also more difficult. The network can operate in a reactive mode when monitoring static events. For dynamic

events, more traffic is generated to be routed to the sink, as the sink has to be periodically notified of the current location of the event.

9. **Transmission media**: As the communication medium is wireless, new approaches to MAC design and routing protocols have to be considered to conserve energy.
10. **Data aggregation**: Nodes located relatively close to one another will have similar types of data to report to the sink. The analogous data from various closely located nodes can be aggregated before a single message is transmitted to the sink, in order to reduce the number of messages transmitted within the WSN application area. The data from multiple sources is combined according to a specific aggregation function to achieve energy efficiency and data transfer optimisation in a number of routing protocols. Data aggregation increases the overall complexity of the WSN application and negates the use of many security techniques for WSN applications.
11. **Quality of service**: Some WSN applications may have a bounded time limit on when a message must reach its destination. Most WSN applications consider conservation of energy more important than message latency or the quality of data sent and energy-aware routing protocols are required to capture this requirement.

2.4 LOCALISATION

The usefulness of information received from sensor nodes is directly related to being able to predict the sensor's location accurately in relation to observed phenomena or triggered events. Therefore, all wireless sensor nodes in a network need to provide some form of data (in addition to the sensing information), that indicates the node's position. The process of determining the position of nodes in a WSN is called localisation (Aspnes, Goldenberg and Yang, 2004).The ability to determine the location of nodes in a WSN accurately is important for both network operation and data interpretation (Lederer et al., May 2008). Many network functions, such as geographic routing, coverage and tracking and location-dependent computing, require prior knowledge of the position of nodes in a WSN. Some examples of WSNs that require data about a node's (or triggered events') location include applications such as surveillance and tracking moving targets or hazardous material, as well as fire monitoring and certain military applications.

Power, cost and density constraints limit the number of nodes that can be equipped with a location-finding system. Therefore, it is not feasible for all sensor nodes to be equipped with a GPS (Savvides et al., 2001) or similar types of location-determining equipment. Also, network localisation is dependent on the application (indoor or outdoor, mobile or static), the range of nodes, the deployment environment (for example, wooded or rocky areas may limit the node range), signal interference and the density of sensors over the application area.

Savvides et al. describe six categories of localisation systems, which can be divided into active and passive localisation (Savvides et al., 2004). In active localisation, sensor nodes actively emit signals into the environment in order to measure the target range. In passive localisation, range measurements are calculated from monitoring of received signals. Techniques such as radio received signal strength (energy), time difference of arrival and angle of arrival are measured for each received packet and used to estimate a single node's location with respect to a known node (Farahani, 2008). Many WSN localisation algorithms are based on measurements between neighbouring sensors for location estimation. Figure 2.2 briefly summarises the main categories.

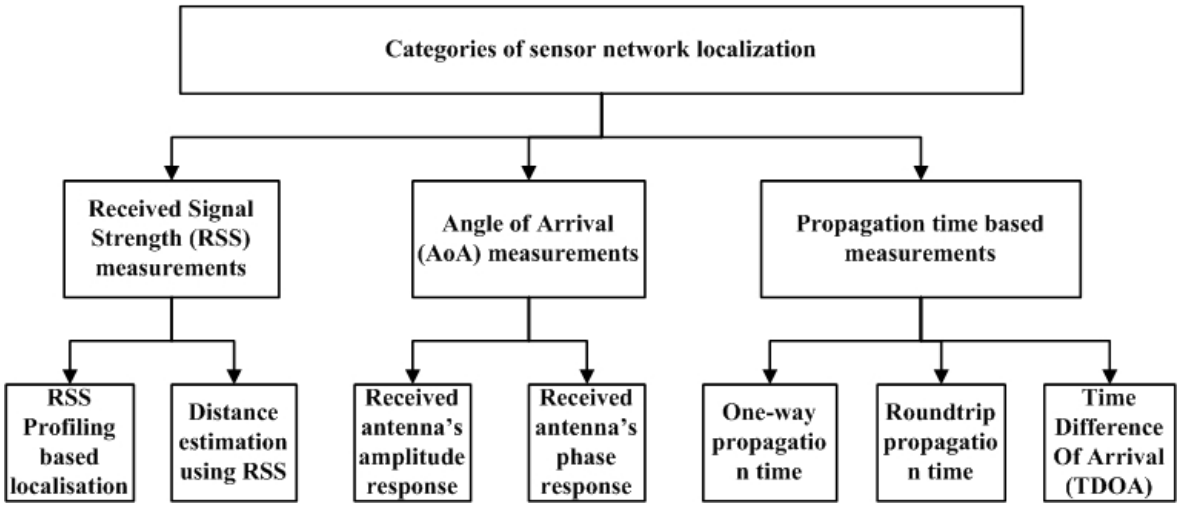

Figure 2.2: Categories of localisation measurement techniques in WSNs

To determine the location of all nodes in a WSN, various network localisation methods are used, e.g. in the work of (Krishnamachari, 2005; Bulusu et al., 2001; Savvides et al., 2001; Lederer et al., May 2008; Biswas et al., 2006; Pan et al., 2006; Patwari et al., 2005):

- Constraint-based methods: use a set of constraints and reference nodes as inputs to a semi-definite programming function. Biswas et al. describe a set of semidefinite programming (SDP) algorithms to determine the location of nodes in a WSN. The primary disadvantage of this approach is that SDP algorithms do not scale to larger densities very well.
- RSS-based joint estimation or proximity-based localisation: uses a matrix of received signal strength to estimate a location set for all nodes.
- Multilateration and iterative multilateration: on network initialisation a small number of nodes know their location. The unknown nodes determine their distance from their neighbours, using a node location technique such as received signal strength or time of arrival to estimate the distance between an unknown node and three reference neighbour nodes to triangulate its position. This node then becomes a reference node and the process iterates until all node locations are known.
- Collaborative multilateration: the location of unknown nodes within a set of collaborative subgraphs of reference and unknown nodes is obtained from a constrained set of quadratic equations.
- Multi-hop distance estimation methods: estimate distance (in terms of hops) to reference nodes, and use triangulation to determine location.
- Cooperative localisation: sensor nodes cooperate in a peer-to-peer manner to form a map of the network. The nodes use statistical models to calculate localisation performance bounds on location estimation precision; based on time of arrival, angle-of-arrival and received-signal-strength measurements.
- Anchor-free localisation: none of the nodes knows its location and a relative coordinate system of the network geometry is calculated using global rotation and translation from local knowledge of network connectivity. Typical applications of anchor-free localisation are in remote areas or indoor/underwater environments in which GPS does not work or is too expensive.
- Clustered two-tier WSN: the WSN is divided into clusters. Within each cluster is an application node. The application nodes communicate with a base station. Pan et al. describe an algorithm to calculate the optimum location of a base station in a two-tier WSN.

The above approaches are constrained by the non-renewable power supplies of sensor nodes, so the nodes should not expend excess time and energy in receiving and transmitting location-based messages.

2.5 WIRELESS SENSOR ACTOR NETWORKS

In typical WSNs, after an event occurs (e.g. temperature change), the sensing nodes activated by the event need to coordinate the messages between the nodes to send a single aggregated data message to a sink node, which then transmits the data to a remote end user for evaluation and response. The real-time response of the WSN thus depends on the reaction of the human entity in question. To enable better response to events, mobile non-human devices called actors are placed in the application area to form a WSAN. The use of mobile actors within a WSN application enables rapid response to data received from sensor(s) (Yoneki & Bacon, September, 2005).

A WSAN is defined by Akyildiz and Kasimoglu as a group of sensors and actors linked by wireless medium to perform distributed sensing and acting tasks. In such a network, sensors gather information about the physical world, while actors take decisions and then perform appropriate actions upon the environment, which allows a user to sense and act effectively at a distance (Akyildiz and Kasimoglu, 2004). Compared to the resource-constrained sensor node, actors are resource-rich mobile nodes with better processing and communication capabilities. Because of the larger costs, actors are not as densely deployed within an application area as sensor nodes. The advantage of WSAN is that sensor-actor-actor coordination will achieve a faster response time than sensor-sink-human responses.

The key differences between a WSN and a WSAN are that a WSAN has the following unique characteristics (Akyildiz and Kasimoglu, 2004):

1. *Real-time requirement* where the application requires rapid response to received sensor data, for example, a fast response is necessary in a fire application, or in the detection and seizure of trespassers or other intruders in an area.
2. *Coordination* among actors and sensors to enable rapid response to triggered events is vital. Sensor-actor coordination provides the transmission of event features from

sensors to actors. After receiving event information, actors need to coordinate with one another in order to make decisions on the most appropriate way to perform the action.

When an event is detected by a group of sensors in a WSAN, the sensors reach consensus to send a single message to one or more actors. When an actor receives a message, it informs all other actors of the event. The actors need to coordinate a response and determine the actor(s) that will respond to the event. To provide effective sensing and actuating, a distributed local coordination mechanism is necessary among sensors and actors.

Akyildiz and Kasimoglu describe four types of scenarios for single-actor and multiple-actor responses, namely (Akyildiz and Kasimoglu, 2004):

1. Single-actor centralised decision (SACD): A single actor receives data about an event and makes a decision on how to respond to the event.
2. Single-actor distributed decision (SADD): A single actor receives data about an event. The actor broadcasts this information to other actors. A collaborative decision is taken as to which actor(s) will react to the event.
3. Multi-actor centralised decision (MACD): Multiple actors receive data about an event and send the data to a central actor, which determines the best actor to react to the event.
4. Multi-actor distributed decision (MADD): Multiple actors receive data about an event and make a mutual decision on which set of actors will react to the event.

2.6 MOBILE SINKS AND MOBILE RELAYS

The application and routing challenges presented by static nodes in a dense, multi-hop WSN has led to the investigation of the use of mobile elements in WSNs for data collection and/or dissemination. The advantages of using mobile entities in WSNs include (Francesco et al., 2011; Hamida & Chelius, 2008):

1. Improved reliability as there is less contention and collisions within the wireless medium because data can now be collected directly through single or limited hop transmissions.

2. Reduced reliance on nodes located close to a static sink to route messages to the sink, resulting in increased energy efficiency and network lifetime.
3. Improved connectivity as mobile nodes can enable the retrieval of collected measurements from isolated regions of the sensor application area.
4. A sparse network architecture implies reduced application cost as fewer nodes are required and nodes can utilise mobile elements already present in the application area such as trains, cars, wildlife, and livestock etc.

The use of mobility in WSNs introduces complications not found in static WSN applications, such as detecting when nodes are within transmission range of a mobile sink, ensuring reliable data transfer as nodes may move as messages are exchanged, tracking sink location and design of a virtual backbone to store data reports so that the mobile sink can easily collect them, and managing sensor nodes to support sink mobility (Francesco et al., 2011; Hamida & Chelius, 2008).

Current strategies for data collection and dissemination using mobile elements include a rendezvous-based virtual infrastructure which uses limited and unlimited multi-hop relays to route data messages, or a backbone-based approach where mobile sinks only communicate with pre-defined cluster heads or gateways, or passive data collection where there is direct communication between the source and sink (Hamida & Chelius, 2008; Faheem et al., 2009).

The mobility patterns of mobile elements (sinks and relays) are dependent on the type of WSN application, its data collection requirements and the controllability of the mobile elements. Current mobility patterns can be classified into the following categories (Faheem et al., 2009; Francesco et al., 2011):

1. *Random mobility*: no network information required because communication does not occur regularly but with a distribution probability. This method does not provide optimal increases in network lifetime due to the need for continuous sink position updates and route reconstruction.

2. *Predictable or deterministic mobility*: mobile elements enter range of sensor nodes at regular, periodic times to collect data, and allow the sensor nodes to predict arrival of mobile entities.
3. *Controlled mobility*: the mobile elements movements are not predictable but are controlled by network parameters such as maximum and minimum residual energy of sensor nodes on a data route, event location, and the mobile elements trajectory and speed. In addition, the mobile entities can be instructed to visit individual nodes at specific times, and stop at nodes until they have collected all buffered data.

2.7 STANDARDS

A need for standardisation in WSN communication protocols was expressed in early 2000 by sensor device suppliers. It was found that most communication protocols performed inconsistently i.e. could sometimes perform better in certain applications but poorly in others. The most important standardisation bodies for WSN technology are the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the HART Communication Foundation, the European Telecommunications Standards Institute (ETSI) and the International Society for Automation (ISA). Although these organisations focus on different areas, they all provide a common platform for interoperability and low power consumption between sensor node devices. The subsections mentioned below list and discuss some of these standards.

2.7.1 IEEE 802.15.4 standard

IEEE 802.15.4 is a wireless network standard that specifies the physical and data link MAC layer protocols for low power, low rate wireless personal area networks (LR-WPAN). There are three frequency bands with 27 radio channels in the physical layer, namely (1) 868.0 to 868.6 MHz, which provides a data rate of 20 kbps, (2) 902.0 to 928.0 MHz with a data rate of 40 kbps, and (3) 2.4 to 2.4835 GHz with a data rate of 250 kbps. Routing is not directly defined by IEEE 802.15.4, because it does not define a network layer. The standard has very broad applications in the area of (but is not limited to) WSNs, industrial monitoring and control, home automation and control, automatic meter reading and inventory management (Lee et al., January 2010).

IEEE 802.15.4-compliant devices have limited power, which has to be conserved to ensure the device remains active for a lengthy time period. There are two classes of IEEE 802.15.4-compliant devices, namely (1) full function devices (FFDs), which have the capability of serving as a coordinator or associating with an existing coordinator/router and becoming a router, and can thus communicate with all other devices and reroute messages; or (2) reduced function devices (RFDs), which can only associate with a coordinator or router and cannot have children, i.e. can only communicate with one FFD (Pan et al., November 2009).

The IEEE 802.15.4 standard provides an energy-saving mechanism that uses a superframe structure in the beacon mode. This is because one of the major energy wastes is idle listening, due to the inherent nature of carrier sense multiple access with collision avoidance (CSMA/CA) MAC. The radio circuitry needs to be in the active mode for idle listening, although it is not transmitting or receiving data frames. The energy consumption of the radio circuitry in the active mode is usually higher than that of a small microcontroller (Lee et al., January 2010).

Although IEEE 802.15.4 was developed to meet the needs for low power, low data-rate wireless communication, it is potentially vulnerable to interference by other wireless technologies having much higher power and working in the same industrial, scientific, and medical (ISM) band, such as IEEE 802.11b/g (Yuan et al., 15-15 Nov. 2007).

2.7.2 6loWPAN

As mentioned previously the IEEE 802.15.4 standard is only concerned with the physical and media access control layers. To ensure effective message communication between wireless devices, the Internet Engineering Task Force (IETF) integrated an IPv6 addressing scheme with the IEEE 802.15.4 standard to provide an effective low power Wireless Personal Area Network (6LoWPAN), (Ma & Luo, 19-20 Dec. 2008). This specification allows the design of smart sensors with an end-to-end IPv6-based architecture carried over an IEEE 802.15.4 network. In addition, 6loWPAN networks are characterised as low bit-rate, short-range and low-cost networks. 6LoWPAN defines a set of compression

mechanisms that allows packets to be transported from sender to receiver and vice versa in wireless networks based on the IEEE 802.15.4 protocol (Polepalli et al., 2009).

2.7.3 ZigBee

The ZigBee Alliance was formed to promote the IEEE 802.15.4 standard, provide conformance testing and improve interoperability among devices from different manufacturers. Although the ZigBee specification is based on IEEE standard 802.15.4, it does not exactly follow every part of the standard and it adds a great deal more to the standard in the form of profiles and requirements for higher layers in the networking stack. The goal of IEEE standard 802.15.4 and the ZigBee Alliance is to provide wireless solutions that are low-cost, low data-rate, and low power. The target applications are control and monitoring systems that only infrequently send small amounts of data (Gilb, 2005).

ZigBee enables interaction between the network and MAC layers, which is fundamental for power control in mobile ad hoc networks and WSNs. The power level determines who can hear the transmission, and hence it has a direct impact on the selection of the next hop, which is a network layer issue. The power level also determines the floor that the terminal reserves exclusively for its transmission through an access scheme, which is a MAC layer issue (Muqattash et al., 2006).

The ZigBee standard defines two major protocols: The “ZigBee” and the “ZigBee PRO”. The first model is essentially designed for light-duty purposes in home and office applications, whereas the second model usually provides more reliable performance but requires implementation of a larger and more complicated protocol (Kazem Sohraby, 2007). The ZigBee offers three classes of devices: the ZigBee coordinators, the ZigBee routers and the ZigBee end. Both the coordinators and the routers participate in multi-hop routing of messages, while the ZigBee end device only addresses messages to their associated parent routing device. Although the ZigBee has found a market in home and office applications, this standard has not been as widely used in control and industrial measurement processes. The reason is that its MAC layer is unable to deliver messages efficiently in applications where data reliability is a critical issue.