Wireless Sensor Network- An Advanced Survey
Ahmad AA Alkhatib, Gurvinder S Baicher, Waleed K Darwish

Abstract— Wireless sensor networks (WSN) are becoming extremely attractive for both telecommunication and network industry. It is the promising technology to solve a number of present problems and creates new understanding to the future applications. These sensors can influence the understanding of the physical world around us by transmitting signals by sensing the physical around the field of influence of such devices. Such devices can then transmit electrical signals from sensor to sensor through the network until the signal reaches the sink stage. This survey explores the design issues, network services and mechanisms and some applications in this field. It provides an understanding for WSN technology, WSN OSI architecture, and some popular protocols in each layer, the main problems and their solution of using OSI in sensor network.


I. INTRODUCTION

Wireless sensor networks have seen extensive proliferation of applications and interest in research and industry. Such networks can be densely deployed over a diverse geographic area ranging from 10s of meters to several hundred of kilometers through deploying small, low cost devices that can observe and influence the physical world around them by gathering status information and then transforming this into radio signals. Such signals are then transmitted to a local sink which may be connected to a gateway to send the data to an external network such as internet. The data thus received may be analyzed, and appropriate decision/action has to be taken depending on the application itself. Unfortunately, these sensors suffer from resources constraint and power limitation as these sensors are usually deployed in remote places that are not easy to reach. Inevitably, there is a finite life time duration for such devices and new sensors has to be deployed to replace the old ones. It is some of these limitations that has shown an increasing interest from the scientific community to research in such devices that would enhance the longevity and coverage of the devices by using various new technology developments in this field. The main emphasis is on maximizing the life time of sensors and to use the limited resources efficiently by adopting mechanisms, algorithms and protocols that consider these limited resources as main priorities and challenges to produce efficient and reliable network. Wireless sensor networks utilize an efficient form of technology that has no structures or rules or adhering to a specific standard. This makes it an attractive area for research. Thus, significant resources are being placed on its study by research scholars and manufacturers alike. There are a number of applications for such devices and networks such as; military, health monitoring, indoor and outdoor fire fighting applications, security applications, and environmental, agricultural, climate changes and studying animal behavior.

II. WSN DESIGN ISSUES

WSN can be defined as: “a network of devices, denoted as nodes, which can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links. The data are forwarded, possibly via multiple hops, to a sink (sometimes denoted as a controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. They can be aware of their location or not. They can be homogeneous or not”[1]. Sensor networks are distributed small sensing devices provided with short-range wireless communications, memory and processors. This kind of network differs from conventional Ad-hoc networks in the following way:

- number of nodes deployed in WSN is higher
- Sensor nodes are densely deployed and usually in harsh environment.
- sensor nodes have a limited life span
- topology of the network may change frequently
- WSN work in a broadcast fashion, while ad-hoc is point to point.
- WSN has limited power and range resources
- may not have a global ID

To build a WSN, some factors will influence the design[1, 2]:

1. Fault tolerance (reliability): is the ability to adapt node failures without affecting the network function. Fault tolerance could be calculated through the following equation:

   \[ R_k(t) = \exp(-\lambda_k t) \] (1)

   Where: \( R_k \) is the reliability (fault tolerance), \( \lambda_k \) is the fault rate for node \( k \), \( t \) is the time period.

2. Scalability: network ability to increase the size of the network or add a new number of nodes is extremely beneficial, but scalability or increasing number of nodes has to consider network density as a factor to determine the required number of sensors to cover a certain area, which depends on the nature of application as well. The density can be calculated by:

   \[ \mu(R) = \frac{(N \pi R^2)}{A} \] (2)

   Where: \( N \) is the number of sensors; \( R \) is the sensor range. \( \mu(R) \) is the density function to find the number of sensors within sensor range, \( N \) is the number of sensors, \( A \) is the area.

3. Product cost: a very important factor because sensors densely deployed up to few thousand, so little extra charge for device cost will be huge for the network cost.

4. Hardware constraints: basically, sensors consist of; sensing unit (sensor, ADC), processing unit (simple
micro-controller, small memory), transceiver unit with short range communication capability and power unit (usually it is two AA batteries). Some applications have extra components such as; location finding system (e.g., GPS device), power scavenging device (e.g. solar panels) and mobilizer. See Fig. 1.

![Sensor Node Diagram](image)

**Fig 1: Sensor Node**

5. Power consumption: WSNs consume power in three parts: a) Sensing: This is almost fixed power.
   b) Data communication: major power is used in this part. A sensor transceiver comprises of:
   - Transmitter and receiver approximately consume the same power.
   - Mixer; frequency synthesizer, voltage control oscillator.
   - PLL, power amplifier.
   All of them consume node power in addition to the START UP power. The startup power can be calculated by the eq. 3:

\[
P_c = N_t[P_r(T_{on} + T_{st}) + P_{out}(T_{on})] + N_r[P_r(R_{on} + R_{st})]
\]  

(3)

Where: PT/PR are the consumed power by transmitter and receiver respectively, POUT is the power at transmitted antenna, TON/RON is transmitter/receiver wake up time, TST/RST is transmitter/receiver start-up time and NT/NR is the number of times transmitter or receiver is switched on per unit time, which depends on the task and medium access control (MAC) scheme. Data processing: power consumption in data processing is much less than power consumption for Data communication. Due to the low cost and size requirements of sensor manufacturing, CMOS technology is normally used for micro-processors and this limits the expended power thus giving greater efficiency. Other factors that influence the WAN design are: security, network type, Quality of service, self-organizing network, data rate and throughput, routing, modeling, size and applications.

### III. NETWORK SERVICES

Some of the services carried out within the WSN networks are shown here.

#### A. WSN Storage Mechanisms [4]

The following are some mechanisms:

- GEM[5]: Graph Embedding Mechanism provides an infrastructure for routing and data centric storage, where each node has an identifier and label encoded with position and each node need to know the labels of its neighbour so the node chooses a label guest graph (receiver) then embeds that guest graph into the actual sensor topology TSAR[6]: in this method the node sends the metadata to the nearest proxy and then this metadata moves from proxy to another where the actual data is stored in the sensor, through this to reduce the overhead through sending the queries to proxies. Multi-resolution storage[7]: Multi-resolution storage system provides a hierarchy distributed storage structure and long term query data in intensive data application. This storage method is divided into three stages; wavelet process to build a multi-resolution summary to compress the data, drill-down query is a process to reduce search cost done in the highest level of the hierarchy where this stage uses the summary as a pointer for the network part that contain the required data and finally, data aging scheme to discard summaries after a certain time and make a space for the new data.

#### B. Localization

Listed here are some localization algorithms used in WSN:

- Moore’s algorithm[8]: each node becomes a centre of cluster, then measure the distance of one hop neighbour then broadcast it for each cluster to use the overlap information to localize other sensors. RIPS[9]: it uses two radio transmissions to create interference, one transmission is set slightly different than the other. By measuring the offset frequency, the location can be obtained through the use of a given formula. Secure localization[10]: sensor relies on beacon information to compute their position and for security purposes. Sensor can only accept the information from authenticated beacon. In general wireless sensor networks localization algorithm uses either GPS devices or estimation algorithms or using directional antennas with some measurement, such as AOA (angle of arrival) TOA (time of arrival) TDOA (time difference of arrival) and RSS (received signal strength) measurement to apply them in equations in order to localize them. In wireless sensor networks, the cost and size are critical issues, where adding devices like GPS devices and directional antennas or even array of antennas for localization purposes will increase the cost and size for sensor device. GPS is not efficient for indoor applications. Estimation algorithms required directional antennas and a lot of complicated calculations; this will be a problem for sensors regards to the limited resources, limited memory and buffer in addition to the inaccuracy. The Estimation techniques can be divided into [11-14]:

- Angle of Arrival measurement: AOA depends on amplitude and phase responses for the antennas, where the beam form and the maximum signal strength used to determine the Angle of reception. The problem is the signal is vary, and the antenna can’t define the received signal variation due to the amplitude and phase, but the solution is to use an Omni-directional antenna with the directional one. Because the Omni-directional antenna has a static beamform, the phase response can be defined by comparing the two
beam forms. Another way to find the AOA is to deploy two or four directional antennas to overlap the beamforms.

- Distance Related Measurements: this technique can be done by measuring one of the following:
  a) One way propagation time: require a precise synchronization for devices and measuring the time propagation in order to calculate the distance.
  b) Round trip propagation: no need for synchronization, just measuring the round trip propagation time to calculate the distance. The error is coming from signal processing in the second node.
  c) TDOA (Time Difference of Arrival): used to estimate the coordination of the transmitter by measuring the signal on multiple receiver and doing some calculations. Cross correlation is one of the most popular methods for TDOA.
  d) Received Signal Strength (RSS): it based on measuring the signal strength at the receiver to apply that on one of the propagation models and calculate the distance.

Most of these techniques can calculate the distance but can’t define the directions.

C. Synchronization[3]
The following are some synchronization protocols:
Uncertainty-driven approach: based on a long term clock drifts between all nodes for long time synchronization to minimize overhead. Where it measures the sync rate, obtain history of past sync beacon and compute the result of estimation scheme to use them in Rate Adaptive Time Synchronization protocol (RATS).
Timing sync protocol for sensor network (TPSN): this protocol is carried out in two phases: Discovery phase to create a hierarchical topology for the network, where each node is classified into levels and each node can at least communicate to one node from lower level. Synchronization phase where each node tries to synchronize with the nodes in level – 1.
Clock-sampling mutual network sync (CSMNS): relies on IEEE 802.11, periodic beacon to exchange time information. Where each node has a different, time drift coefficient and initial time. so the nodes send their timing process periodically in the beacon and then the received node computes the difference and corrects its clock.

II. BANDWIDTH CHOICES FOR WIRELESS SENSOR NETWORK [4]
These may be listed as:
  - Narrow band that focus on bandwidth efficiency and use enough bandwidth for symbol rate transmission (data rate/ BW).
  - Spread spectrum: the narrow band signal is spread into a wideband signal. This method has the ability to reduce the power and communicate effectively.
  - Ultra Wide Band (UWB): employs larger BW than spread spectrum so the interference to other radios is negligible.

Spread spectrum and UWB are more suitable for WSN because of low power utilization and robustness for multi-path fading, shadowing and interference.

III. SOME TEST-BEDS TO TEST WSN NETWORKS[4]
- ORBIT: Open access research test-bed for next-generation wireless network, useful to test new applications, protocols and algorithms, indicate on system performance and run cross-layer experiments.
- MOTELAB: is a testbed of MicaZ wireless sensor networks based web. Used to test new developed protocols, analyse signal strength, and cluster performance.
- EMULAB: a mobile robot used to test wireless sensor networks. Analyse network topology, impact of mobility on protocols, test algorithms and applications.

IV. SENSOR NETWORK ARCHITECTURE
Most common architecture for WSN follows the OSI Model. In sensor network we need five layers: application layer, transport layer, network layer, data link layer and physical layer. Added to the five layers are the three cross layers planes as shown in Fig. 2[2].

![Fig 2: WSN Architecture][2]

A. Cross layers[2, 15]
1. Mobility management plane: detect sensor nodes movement. Node can keep track of neighbours and power levels (for power balancing).
2. Task management plane: schedule the sensing tasks to a given area. Determine which nodes are off and which ones are on.
3. Power management plane: to control the power level for all nodes.

The three cross planes or layers are: power management plane, mobility management plane and task management plane. These layers are used to manage the network and make the sensors work together in order to increase the overall efficiency of the network. For example a certain node
doing the sensing transmitting and receiving and routing tasks, after a while the power level for this node will reach the threshold value, instead of loosing this node at early stage of the network life time and maybe causing coverage gap, the cross layers will make this node stop doing the routing task and inform all the neighbours that this node will save the remaining power for sensing and transmitting tasks in order to stay alive as much time as possible.

B. WSN OSI layers.

Table 1: Difference of Architectures between OSI, WLAN and WSN

<table>
<thead>
<tr>
<th>Wireless network</th>
<th>sensor</th>
<th>WLAN</th>
<th>OSI Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN Application</td>
<td></td>
<td>Application</td>
<td>Application layer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>programs</td>
<td></td>
</tr>
<tr>
<td>WSN Middleware</td>
<td></td>
<td>Middleware</td>
<td>Presentation layer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Socket API</td>
<td>Session layer</td>
</tr>
<tr>
<td>WSN protocols</td>
<td></td>
<td>TCP/UDP</td>
<td>Transport layer</td>
</tr>
<tr>
<td>WSN protocols</td>
<td></td>
<td>IP</td>
<td>Network layer</td>
</tr>
<tr>
<td>Error control</td>
<td></td>
<td>WLAN Adapter</td>
<td>Data link layer</td>
</tr>
<tr>
<td>WSN protocols</td>
<td>MAC</td>
<td>&amp; device driver</td>
<td></td>
</tr>
<tr>
<td>Transceiver</td>
<td></td>
<td>Transceiver</td>
<td>Physical layer</td>
</tr>
</tbody>
</table>

Transport layer: The function of this layer is to provide reliability and congestion avoidance where a lot of protocols designed to provide this function are either applied on the upstream (user to sink, ex: ESRT, STCP and DSTN), or downstream (sink to user, ex: PSFQ and GARUDA). These protocols use different mechanisms for loss detection ((ACK, NACK, and Sequence number)) and loss recovery ((End to End or Hop by Hop)). This layer is specifically needed when a system is organised to access other networks. Providing a reliable hop by hop is more energy efficient than end to end and that is one of the reason why TCP is not suitable for WSN. Usually the link from sink to node is considered as downstream link for multicast transmission and UDP traffic because of the limited memory and overhead avoiding. On the other hand from User to sink is considered as upstream link for mono-cast transmission and TCP or UDP traffic(2). In general, Transport protocols can be divided into[16]:

a) Packet driven: ‘all packets sent by source must reach destination’.

b) Event driven: ‘the event must be detected, but it is enough that one notification message reaches the sink’.

The following are some popular protocols in this layer with a brief description [4, 16, 17]:

STCP (Sensor Transmission Control Protocol): upstream protocol; provides reliability, congestion detection and congestion avoidance. STCP function is applied on the base station. The node sends a session initiation packet to the sink which contains information about transmission rate, required reliability, data flow. Then the sensor node waits for ACK before starting to send data. The base station estimates the arrival time of each packet, when there is a failure in packet delivery the base station checks with the current reliability meets the required criteria. If current reliability is less than the required criteria then sink send NACK for retransmission, otherwise do nothing. The current reliability is computed by the packet fractions that are successfully received.

- PORT (Price-Oriented Reliable Transport Protocol): downstream protocol; assure that the sink receives enough information from the physical phenomena. Port adapts a bias packet routing rate to increase sink information from a specific region by two methods: First method: Node price is the total number of transmissions before the first packet arrives at the sink, and this is used to define the cost of communication. Each packet is sent encapsulated with source price then the sink adjusts the reporting rate according to node price. Second method: Use end-end communication cost to reduce congestion. When congestion occurs the communication cost is increased. The sink reduces the reporting rate for sources and increases the rate of other sources that have lower communication cost. PSFQ (pump slow fetch quick): downstream protocol; data to all neighbours and the neighbour’s forward data to their neighbours and so on. One node can receive enormous amount of repeated data from different neighbours, and this data could be generated from the same origin node or even generated by redundant nodes. Since the data processing consumes less power than data transmission, we can solve that by data aggregation and data fusion to remove the redundant data. Data aggregation is described as ‘a set of automated methods combining the data that comes from many sensor nodes into a set of meaningful information and eliminate the duplication.’[20] This is mainly used in flat routing.

Reliable, scalable and robust. Three functions in this protocol are; pump, fetch and report.

a) Pump uses two timers T_{min} and T_{max}, where the node waits T_{min} before transmission to recover missing packets and remove redundant broadcast. Node waits for T_{max} if there are any packets or multiple packets lost.

b) Fetch operation requests a retransmission for the missing packets from neighbour.

c) Finally report the operation to provide feedback to the user.

Network layer: The major function of this layer is routing. This layer has a lot of challenges depending on the application but apparently, the main challenges are in the power saving, limited memory and buffers; sensor does not have a global ID and have to be self organized. This is unlike computer networks with IP address and central device for controlling. The basic idea of the routing protocol is to define reliable path and redundant paths according to a certain scale called metric, which differs from protocol to protocol. There is a lot of routing protocols available for this layer, they can be dividing according to the topology; such as flat routing (for example, direct diffusion) and hierarchal routing (for example, LEACH) or can be divided according to data delivery model; such as time driven, query driven and event.
driven. In continuous time driven protocol, the data are sent periodically, and time driven for applications that need a periodic monitoring. In event driven and query driven protocols, the sensor responds according to action or user query. In this layer, three techniques have been adopted: Data aggregation, Data fusion, Data centric. Data aggregation and data fusion: In order to provide a full coverage for a certain area, even when we have a failure, we have to deploy redundant sensors. Where these redundant sensors provide a repeated data, in addition to sensors in some cases, sends data on multi-hop style (from sensor to another till it reaches the sink) and sometimes as in flood protocols, each sensor forwards data to all neighbours and the neighbours forward data to their neighbours and so on. One node can receive enormous amount of repeated data from different neighbours, and this data could be generated from the same origin node or even generated by redundant nodes. Since the data processing consumes less power than data transmission, we can solve that by data aggregation and data fusion to remove the redundant data. Data aggregation is described as ‘a set of automated methods combining the data that comes from many sensor nodes into a set of meaningful information and eliminate the duplication.’ [20] This is mainly used in flat routing.

Data fusion is described as ‘when the nodes do some more processing on the aggregated data to produce more accurate output for example, reducing the noise in the signals’ [20].

Data Centric: because of no global ID in WSN, it’s hard to specify a set of nodes to respond for a query, which resulted in a huge number of redundant data in the network and increase the power consumption from the sensors battery. As a solution for this problem, data centric protocols have been used in order to create and manage routes between two addressed nodes in the network layer.

In this work routing protocols will be divided into five types [27, 28]: Flooding and gossiping, Data centric protocols, Hierarchical protocols, location based protocols and QoS protocols.

Flooding and gossiping [routing survey]: the first two protocols used in sensor networks. No needs for topologies or routing tables.

<table>
<thead>
<tr>
<th>Table 2: Transport Layer Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transport Protocol</strong></td>
</tr>
<tr>
<td>ESRT Event to sink reliable transport [18]</td>
</tr>
<tr>
<td>Transport Protocol</td>
</tr>
<tr>
<td>ESRT Event to sink reliable transport [18]</td>
</tr>
<tr>
<td>Ensure[20] code</td>
</tr>
<tr>
<td>RBC Reliable bursty convergecas [21]</td>
</tr>
</tbody>
</table>
Fig 3: Spin protocol

Flooding: relies on broadcasting the data to all neighbours, then the neighbours rebroadcast the data again and so on till it reaches the destination. This protocol has three main problems: Implosion caused by duplicated messages and overlap when two nodes sense the same area and the huge resource waste for the network. Data centric routing protocols: The first data centric protocols are SPIN and directed fusion. Spin: broadcast ADV message to advertise for data availability, where the only interested node sends a REQ to receive the data, then the transmission starts. Direct diffusion: where the sink broadcasts a query, then the determined node replies with the data by broadcasting it to the neighbours, the sink then chooses the best route and forces others to turn off, but if the current path is no longer efficient, then the sink sends a negative reinforcement to reduce the rate or implement time out. Hierarchy protocol: under this type of routing protocols, there are a large number of suggested protocols for routing, and considering the power saving purposes at the same time. For example, PEAS (Probing Environment and Adaptive Sleeping), GAF, SPAN, ASCENT, AFCEA, CLD (Controlled Layer Protocol), MTE (Minimum Transmission Energy), LEACH (The Low-Energy Adaptive Clustering Hierarchy). All of these protocols solve routing and energy problems by using clustering and distributing methods. The most popular hierarchy routing protocol is LEACH[22]. This divides the network into clusters then randomly each cluster selects the cluster head node to do the routing job from the cluster to the sink after carrying out data aggregation. PEAS[29] based on using a large number of sensors and specifying the working sensors, and turning off the redundant sensors, through dividing the sensors in three modes (sleeping, probing, and working). They give a deep analysis about those three modes and how the nodes sleep for a random time, after that they send a probing message to discover if there are any working nodes in their probing area, if they have a reply from the working node they back to sleep after using the new value of probing rate from the reply message -which is measured by the working node with certain process- to generate a new sleeping time. This protocol is a very robust protocol because PEAS designed to have a high performance in harsh environments, unexpected failures (up to 38% of node failure, and power depletion by using less than 1% of the total energy consumption, through functioning time in a linear proportion to the numbers of working nodes). PEAS missed the point of power balancing, in addition to the edge nodes, they have to stay wake up most of the time, which leads to consume the energy on the edge sensors quickly. Location based protocol: most of the protocols in sensor networks require the location information. Since no IP addresses used to identify the sensors, location information can be used to identify the required intermediate sensors. An example on
location routing protocol: GAF (Geographic Adaptive Fidelity) and GEAR (Geographic and Energy–Aware Routing).

a) Sink broadcast the query

Fig 4: Direct Diffusion Protocol

GAF (Geographic adaptive fidelity): protocol for Mobile Ad-hoc networks and sensor networks. This protocol relies on produces a grid map for the coverage area and indicates the sensor location on the map by using GPS devices. The main point of the map is to save energy by determining the unnecessary sensors and turning them off in order to increase the life time for the network. GEAR (Geographic and Energy–Aware Routing): This protocol uses the energy levels and geographic information in order to determine the region of where to apply the direct diffusion. GEAR reduces the energy consumption, increase the network life time and better performance of packet delivery. CLD (Controlled Layer Protocol)[30], the secret of this protocol is coming from the design method for nodes distribution. This protocol combines between PEAS, MTE, and LEACH, by using the sensing method from PEAS and the indirect transmission scheme from MTE and clustering from LEACH. The design method based on dividing the coverage area into many layers to distribute nodes (working and sleeping nodes) according to some rules, and spreading the sleeping nodes around the working node. As a result of square shape and the node distribution method, the diagonals have closer nodes than the horizontal or vertical directions, so the other nodes will choose the diagonal nodes as the shortest path to the sink, and that what cause the cascading. While the diagonals considered the shortest path, the power consumption will be increased in the working nodes around the sink, but we can solve that by increasing the sleeping sensors in those nodes. Location based protocol: most of the protocols in sensor networks require the location information. Since no IP addresses used to identify the sensors, location information can be used to identify the required intermediate sensors. An example on location routing protocol: GAF (Geographic Adaptive Fidelity) and GEAR (Geographic and Energy–Aware Routing).
still need a tremendous number of sensors in order to provide a full coverage, and we need to solve the cascading effect which results from the intermediate nodes QoS Routing Protocol: a huge number of Routing protocol consider the QoS as one of the main target, such as the life time maximization, low end to end delay, reliability and minimum cost forwarding SAR (Sequential Assignment Routing): is the first protocol considering QoS as a part of routing decision. SAR produces routing trees according to QoS metric and energy resource. The packet priority used to make the decision of which path to forward the data to. Data link layer: Responsible for multiplexing data streams, data frame detection, MAC, and error control, ensures reliability of point–point or point–multipoint. Errors or unreliability comes from[21]:

- Co-channel interference at the MAC layer. This problem is solved by MAC protocols.
- Multipath fading and shadowing at the physical layer and this problem is solved by forward error correction (FEC) and automatic repeat request (ARQ).

ARQ: not popular in WSN because of additional re-transmission cost and overhead. ARQ is not efficient to frame error detection so all the frame has to retransmit if there is a single bit error.

FEC: decreases the number of retransmission by adding redundant data on each message so the receiver can detect and correct errors. By that we can avoid re-transmission and wait for ACK.

MAC layer: Responsible for Channel access policies, scheduling, buffer management and error control. In WSN, we need a MAC protocol to consider energy efficiency, reliability, low access delay and high throughput as major priorities to accommodate with sensors limited resources and to avoid redundant power consumption.

Sources of energy waste in MAC[21, 31]
Energy waste in MAC protocols is attributed to the following: Collision: when two nodes try to access the medium at the same time.
Overhearing: when the node receives a packet belonging to another node.

![CLD protocol](image)

Fig 5: CLD protocol [30]

### Table 3: Routing Protocols

<table>
<thead>
<tr>
<th>Routing protocol</th>
<th>Data-centric</th>
<th>Hierarchal</th>
<th>Location-based</th>
<th>QoS</th>
<th>Data aggregation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPIN</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Direct Diffusion</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LEACH</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PEAS</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>GAF</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GEAR</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLD</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SAR</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SPEED</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Idle listening: this is the major source of energy waste, where the node keeps listening to medium because it does not know when it will be receiving data.

MAC families[21]:

Schedule based protocol: Usually it uses time division multiple access (TDMA). This type needs previous knowledge of network topology to establish a schedule.

Advantages: no collision, predictable delay, increases the overall throughput, fairness.

Disadvantages: not good for large network, not scalable, works with stable topology, needs precise synchronization and previous knowledge of network topology, which requires expensive hardware and large overhead.

Contention based protocol: usually uses CSMA or ALOHA, there is no need for synchronization or topology knowledge because nodes compete to access the channel and only the winner will succeed.

Advantages: good for large scale, scalable.

Disadvantages: less performance for high load traffic, data packet size usually small, RTS and CTS are more energy consuming. RTS and CTS only used for uni-cast.

Some MAC protocols [2, 21, 22, 31]:

Sensor MAC (S-MAC): uses a synchronized duty cycle and schedule periodic wake and sleep, and using very short SYNC packet to exchange periodically sleep schedules with neighbours. It contains transmitter address and the next sleep time. Advantages: reducing wasted energy by minimizing idle listening by making sleep and listen periods predefined and constant. Disadvantages: when a node lies between two awake clusters, the node has to follow two different schedules which consume more power. Furthermore, large message is divided into frames and sent in a burst to reduce overhead and latency, on the contrary it becomes unfair medium access. See Fig. 6.

Fig 6: S-MAC

Time out MAC (T-MAC): uses sleep/active duty cycle (NP), scheduling exchange protocol (SEP) and adaptive election algorithm (AEA). NP: uses the random access period for signalling, synchronizing and updating two hops neighbour information. It uses the schedule of the target node for future transmission, where the node schedule is established according to its current traffic and propagated to the neighbours. AEA: use the information from SEP and neighbours information to elect transmitter, receiver and stand by nodes for current time slot and the not selected for Trans/Receive data is removed from the election and goes to sleep. B-MAC (versatile low power MAC): uses the CSMA protocol. The node wakes up every check interval, where the radio samples the channel and checks if there is an activity during the preamble period. It stays on for receiving data, but if there are no data the time out forces the node to sleep. To transmit data, the node adds a preamble that is slightly longer than the sleep period of the receiver.

Fig 7: T-MAC and S-MAC [21]

During the preamble, the Rx will wake up and wait to receive data after the preamble. Disadvantages: overhearing and excess latency at each hop, so this implies that Rx will have to wait until the end of the preamble period to start data receiving. Other nodes have to stay in wake up status as well until the end of the preamble. All the waiting leads to pre-hop latency and for multi-hop network the accumulated latency will have effect on overall network performance. X-MAX (short preamble MAC): solves the P-MAC problems by embedding the target ID in the preamble so other node can go back to sleep. Embedding short pauses between preamble packets so if the Rx wakes up it can send an ACK during this pause and cut the preamble to start sending data. TSMP: uses TDMA and frequency division multiplex FDMA over 16 frequency channels divided into time slots so more than one node can access the medium at the same slot but with different frequency. The TSMP works under this rules: never put two transmissions in the same time and frequency, for a given node it should not receive or transmit two times. Disadvantages: complexity, tight synchronization, scalability, broadcast communication, memory. Fig. 8 explains the TSMP protocol. IEEE 802.15.4: This kind consists of Beacon to announce the frame beginning. CAP (Contention Access Period): where all the nodes compete to access the channel by using CSMA/CA to book time slots in the next period for transmission (7 TS in max). CFP (Contention Free Period) or GTS (Guaranteed Time Slots): each node booked a time slot will start transmitting at that slot. Finally, the Inactive period: where the node goes to sleep, but ends dynamically. Node in the active period sends or
receives data but when there is no action for a certain time the active period ends. Advantages: increased efficiency of the algorithm for variable traffic loads. Fig. 2 explains the difference between T-MAC and S-MAC.

![Fig 8: TSMP protocol [21]](image)

A problem of early sleep will occur when a third node supposed to be part of the next transmission process goes to sleep. This problem is solved in T-MAC by future RTS (FRTS), so the third node stays active to receive data instead of waiting for the next active period.

**S-MACL (global sleeping schedule):** This protocol solves the SMAC border node problem. S-MAC considers the whole network as one cluster and each node has a unique ID, in this protocol we have two kinds of nodes: synchronizers and followers. When nodes do not receive a SYNC frame after the first listening period, arbitrarily the network chooses one node to use its schedule as a reference for the network (synchronizer node). When node receives a schedule different than the neighbours, it compares the current ID with the new one and follows the higher ID. If the new one has a lower ID, the node will announce its own schedule in the next listening time.

**Pattern MAC (P-MAC):** It is used in a dynamic sleep/wake up schedule according to the node traffic and its neighbours. Nodes get information from its neighbour before it sends the communication packets (pattern), in other words the node derives its schedule according to its own pattern and neighbour pattern. Traffic adaptive MAC (TRAMA): using single time slotted channel access divided into random and scheduled access period. Consists of neighbour protocol Physical Layer[22]: Can provide an interface to transmit a stream of bits over the physical medium. Responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption. For the physical layer, Bluetooth is not efficient for WSN because it is only working in line of sight communication style. The available options for WSN: Zigbee[1, 4], IEEE 802.15.4[1], WirelessHart[4], ISA100.11a, 6LoWPAN[4], Wibree[4], picoRadio[24], WINS, µ AMPS, Ultra wide band (UWB).

![Fig 9: IEEE 802.15.4 [21]](image)

The most popular types in the market are:

- **IEEE 802.15.4:** Proposed as standard for low rate personal area and WSN with low cost, complexity, power consumption, range of communication to maximize battery life. Use CSMA/CA, support star and peer to peer topology. There are many versions of IEEE 802.15.4:
  - 802.15.4-2003: the slandered relies on Zigbee protocol and use DSSS technique Use CSMA/CA beacon enable or non beacon enable, support three frequencies: 2.4G (ISM): 16 channel with 5MHz guard band (2400-2483.5MHz) and 250kbps, 8QPSK+ half pulse shaping, 868MHz for Europe, 1 channel, 20kpbs, BPSK and raise cosine pulse shaping and 915 for America, 10 channels with 2MHz guard band, 40kpbs, BPSK and raise cosine pulse shaping. MICAz sensor an example for this type

  **Zigbee has to kind of devices to reduce the cost:**
  a) RED: reduced function device used for star topology. This type can’t do coordination functions and talk only to coordinators ((end point)).
  b) FFD: full function device used for any topology, can be the coordinator and can talk to all devices.
  - 802.15.4b-2006: optional improvement in data rate in 868/915 to 100 and 250kbps by increase the complexity (DSSS and O-QPSK) or (parallel sequence spread spectrum PSSS and ASK) give 250 for both frequencies. Number of channels are 27.
  - 802.15.4a-2007: relies on UWB 3.1-10.6 GHz instead of CSMA/CA it uses ALOHA
  - 802.15.4c-2009: add 780MHz to the band for China using O-QPSK or MPSK with 2MHz spacing and 8channels, 250kbps, back to CSMA/CA
  - 802.15.4d-2009: add 950 for Japan using (DSSS+BPSK) or (GFSK)
Ultra Wide Band (UWB)\cite{32]:
Wide band is convenient to WSN because:
- Resilience to multipath fading
- Low power transmission
- High capability of range determination: Ranging capability can be found by the physical meaning of the information gathered by sensors. Such as angle of arrival (AOA), time of arrival (TOA). The ranging expression for WSN is:
\[ \text{Var}(d) \leq C/(1.4\pi^2\text{SNR}^{0.5}) \] (4)
Where C is the speed of light, SNR represents the signal-to-noise ratio, and \( b \) is the effective signal bandwidth.
UWB use a baseband pulse with length range from 100ps to 1ns by using Pulse position modulation (PPM), frequency range (3.1-10.6) GHz. UWB has two existing main variants:
- Multicarrier UWB (MC-UWB): using OFDM to avoid interference. Unfortunately, OFDM use FFT processing and that leads to more complexity. In addition to the Problem in power amplifier, this is due to continuous changing in power over wide bandwidth.
- Time hopping impulse radio UWB (TH-IR-UWB): Time divided into frames to sends very short duration pulses to convey information so multi-user can access by pseudo random time hopping sequence which require fast switching time and precise synchronization.

Wireless HART: provide a protocol to control process and applications, this slandered relied on IEEE 802.15.4 for 2.4GHz, this technology secure, reliable and energy efficient, support mesh, star and combined network, channel hopping and time synchronization messages. Wireless Hart is Secure because it uses encryption, verification, authentication and key management.

ISA100.11a: to monitor low data rate application, based on OSI standard, security, and system management, the advantages of this kind is interoperable with other networks, scalable and low power consumption, 2.4GHz and channel hopping to increase reliability and reduce interference.

Application layer: Responsible for traffic management and provide software for different applications that translate the data in an understandable form or send queries to obtain certain. WSN used everywhere in our life such as; Street light monitoring, Structural health monitoring, Agricultural monitoring management, Weather information service, Health care services, Solution against climate change, Monitoring and tracking, Animal habitat studies, Security services, Indoor/Outdoor Fire control, Rescue tasks, Flood/volcano alarms, Military applications, Smart homes and uncountable number of applications depend on this technology. The following are real applied research projects for WSN:

Wearable sensors\cite{36]: where it is a smart fire fighter suite that consist of 5 sensors installed in three layer garments, to measure, blood pressure, core temperature, heart rate, O2 oximeter, heat flux and wind speed. These data are sending continuously to the team leader so he can follow every one of the team members status, and make sure they are not in danger.
Forest fire control[37]: These systems are based on an efficient and reliable wireless sensor network to detect wood fire in early stages to take action while the fire is still controllable. Sensors measure the temperature, smoke, weather, slope of earth, wind speed, speed of fire spread, flame length and many other necessary parameters to use them as input in smart programs like BEHAVEPLUS, FARSITE, or many other programs for this purpose, to be represented for the fire fighters team in a simple and understandable simulation form to help them understand the fire behaviour at the present and any time in the future. This simulation helps the team leader in decision making to choose the best plane to contain the fire and push the team performance during the fire fighting.

Zebranet[38]: is a project to study and track long animal migration. This project built by sensors provided with GPS device and attached to zebras nicks, where all sensors communicate through sending data from zebra to another until it reach the base station. See figure 16.

Max[39]: is a system to search for objects and localize there position. It based on hierarchal structure, where in the first layer each object tagged differently and then in the upper layer used to tag the land through base stations land marking, and in the last layer is the main base station to refer for the location.

CenWits[40]: This system designed especially for rescue and track passengers in the wild areas. It based on sensors with RF signals to communicate with each other occasionally, and that’s a special property for this project. When passenger heads a wild area they take CinWits device with them. Passengers move in groups or separately, so when two sensors become in the range of each other they start to change information about the position, last time seen, how many base station passed through travel and who, where and when met other passengers. all this information stored in memory for Later, when sensor become in base station range, it sends all information in memory to the base station to do some comparison between data from this passenger and data from ther passengers to come up with results if there is a passenger or group of passengers expected to be in danger and what the possible areas their position could be.

Squad fire fighter positioning system[41]: where this project used for indoor fires designed by the University of New South Wales in Sydney, and it rewarded “ the Australian
Design Award Via GizMay”. This device is similar to PDA but it able to determine the positions, track victims and even find paths and exits, all that beside the main function is to build a small map helps fire fighters to localize every member of the team inside the building and there status, for example, if one of the team member in danger he can send a special signal to announce the argent situation, where other member can localize the position by sending Ultrasonic waves. Ultrasonic wave works very efficient in fire environment without being affected by the smoke, ashes, fire flames...etc. Ultrasonic waves propagate through the air even if we have a small space, like the space between the bottom of the door and the ground, it still working without any problems.

Fig 18: Squad Positioning System [41]

- Great Duck Island[42]: this research done by the college of Atlantic for habitat monitoring in few Islands located 15 Km south Mount Desert Island. This project consist of thirty two nodes sending data to the internet through the Gateway, and they consider energy efficient protocols and adaptive to node failure or environment changes.
- Cyclops[32]: is an electronic interface between CMOS camera and Micaz mote enhance the image resolution and increase the FoV (Field of View), and enable multi-resolution View (zoom a specific part of the image for more details).

IV. CONCLUSION

This paper conducts an overview of the wireless sensor networks, their design issues, network services and developments that have recently taken place. The use of wireless sensor technology has seen proliferation in a large number of applications and this paper is towards that effort to develop a total understanding for this technology, the differences between WSN and other networks and how this change the priorities of the network design and protocols and algorithms are used in the networks layer in order to use the limited network resources efficiently.

REFERENCES


[38] Pei, Z., et al., Hardware design experiences in ZebraNet, in Proceedings of the 2nd international conference on embedded networked sensor systems. 2004, ACM: Baltimore, MD, USA.


AUTHOR’S PROFILE

Gurvinder S Baicher completed his doctoral degree in the area of optimal design of digital signal processing (DSP) systems using genetic algorithms. He has several papers published in the area of DSP, communications engineering and wireless sensor networks. He is currently a Senior Lecturer and Post Graduate programme leader at the University of Wales, Newport, South Wales, UK. Gurvinder has lectured in several countries in International forums and given keynote addresses in his research interest areas. He is presently researching in the areas of wireless sensor networks and communication systems on-board unmanned aerial vehicles (UAV) for disaster management. He is a reviewer for several Journals and is presently on International Programme Committees for several national and international conferences.

Waleed Darwish completed his Undergraduate studies in Electronics and Communications Engineering at the University of Bath, U.K. Then, he completed his Master's degree in Wireless Systems at the University of Bath, U.K. Since then, Waleed has been working in the TV broadcasting industry. Initially, he worked for Mirifice Ltd, as a Developer and Support Engineer, developing, testing and supporting STB Test Automation application known as MiriATE. Currently, he works as a Senior Engineer at Nagra Media U.K where he is involved in developing, testing and supporting difference security modules, such as CAS, multiDRM, STB and SDP.