Review of the Reliability and Connectivity of Wireless Sensor Technology

M. M. Ahsan[1]*, M. Hasanuzzaman[1], A. G. Olabi[2], M. S. J. Hashmi[1]

[1]Dublin City University, Mechanical and Manufacturing Engineering, Dublin 9, Ireland

[2]University of the West of Scotland, Paisley Campus, High Street Paisley PA1 2BE, UK

**Corresponding author. Tel.: +353-1-7005104, Fax: +353-1-7007148*

E-mail address: md.ahsan2@mail.dcu.ie

ABSTRACT

A wireless sensor network is used for varied important applications based on remote monitoring and target tracking. Recently sensors are manufactured smaller, cheaper, and intelligent that are equipped and interfaced wirelessly within a form of network for communication purposes. The infrastructure of wireless sensor network depends on application design structure, objectives, cost, hardware and other maintenance constraints. Sometimes it varies on weather conditions as well. This chapter reviews the technological development of wireless sensor network and specially covering the issues of connectivity and reliability.

Keywords: Wireless Sensors Network (WSN); Non-Intrusive Monitoring System; Hardware Interfacing, Healthcare and Monitoring, Vehicle monitoring; Sensor Reliability and Sensor Connectivity.

1. INTRODUCTION

Wireless sensor network (WSN) have gained worldwide popularity due to its feasibility and high level of reliability. Micro-Electro mechanical system is one of the major parts of technology to develop smart sensors like small, durable and expensive resource embedded. Different types of nodes, motes and few electronic devices are made using this system. These nodes are capable of sensing and capturing data from the particular application location according to the system procedure. Afterwards, these data are transferred to local base station and then the sensed data are transmitted to the end user in different data format.

Smart sensor nodes are equipped with sensors, processors, memory, power supply, radio etc. The sensor nodes consist of different types of mechanical, optical, biological, chemical and magnetic sensors. These sensors are used to measure different properties based on different applications. To set up a wireless network system, a base station or access point is the main point where the transmitted data will be gathered. A radio maintains this wireless communication to carry the data from the local point to the base station. Battery is usually used as a main power source. However, solar power is becoming popular nowadays, but its usage depends on the application and environment.

There are two types of WSNs: one is structured and the other one is unstructured. A dense collection of sensor nodes are used in unstructured WSN, where the sensor nodes are deployed in an ad hoc manner. Sometimes it is difficult to manage connectivity and detect failure of data in the network system as a large number of sensor nodes are used, however, a structured WSN system is cost effective and user friendly. It is easier to maintain the connectivity and data loss as few sensors are used in this system being deployed in a pre-planned manner.

WSNs have been used in different vital applications in different scenarios such as military target tracking[1], monitoring natural disaster[2], hazardous environment monitoring[3], seismic sensing[3], and health care monitoring[4]. Surgical implants as sensors are used to monitor patient's health whereas seismic sensing and ad hoc deployment can monitor earth quake and eruptions. Intrusion systems are used for military target tracking and surveillance.

On the other hand the size of the network, deployment scheme, and network topologies depend on environment. Figure 1 illustrates the connectivity within a wireless sensor network by different issues and their different layers. A few nodes are used in indoor environment, but most of nodes are required to be used in outdoor environment as it covers large scale of area.

The research work in wireless sensor network is continuing by maintaining above constraints and designing new concept, improving protocols, and developing new applications and algorithms.

This chapter contains the following aspects:

- General infrastructure of wireless sensor network (WSN).
- Recent research work on WSN.
- Different applications using WSN.

- Different types of application layers and protocols.
- Connectivity and Reliability of WSN.

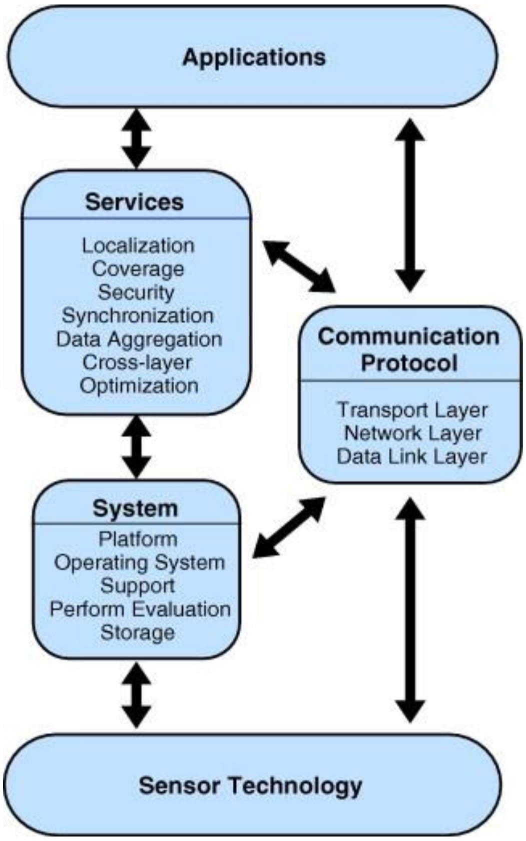

Figure 1: Classifications of different issues in wireless sensor network.[5]

2. SENSOR

2.1 Definition of Sensor

Fraden[6] suggests a generally accepted definition of sensor, and defines sensor as a device that receives a stimulus and responds with an electrical signal. A sensor acts as a converter that can measure a physical quantity and converts it into a signal which is observed or recorded by an electronic instrument, e.g. a voltmeter can read voltage which is converted signal from a thermocouple.

2.2 Types of Sensor

In day to day life, various types of sensors are used for different applications, such as cars, machines, aerospace, medicine, manufacturing, and robotics. The sensors are classified according to different categories, such as acoustic and vibration sensors, automotive and transportation sensors, chemical sensors, electric current and electric potential sensor, magnetic and radio sensors, moisture and humidity sensors, fluid flow and velocity sensors, ionising radiation and subatomic particles sensors, navigation instruments sensors, speed and acceleration sensors, optical imaging and photon sensors, pressure sensors, and thermal, heat and temperature sensors.

3.0 WIRELESS SENSOR NETWORK

3.1 Definition of Wireless Sensor

An object which can perform sensing task is called sensor. Human body can capture optical information, sounds and smell from the environment using their eyes, ears and nose. They do not need to touch the monitored object for gathering information. This is the examples of remote sensors. A sensor acts as transducer which can convert the energy into electrical or some other form of energy.[5] Figure 2 shows a schematic of sensor data acquisition and actuation.

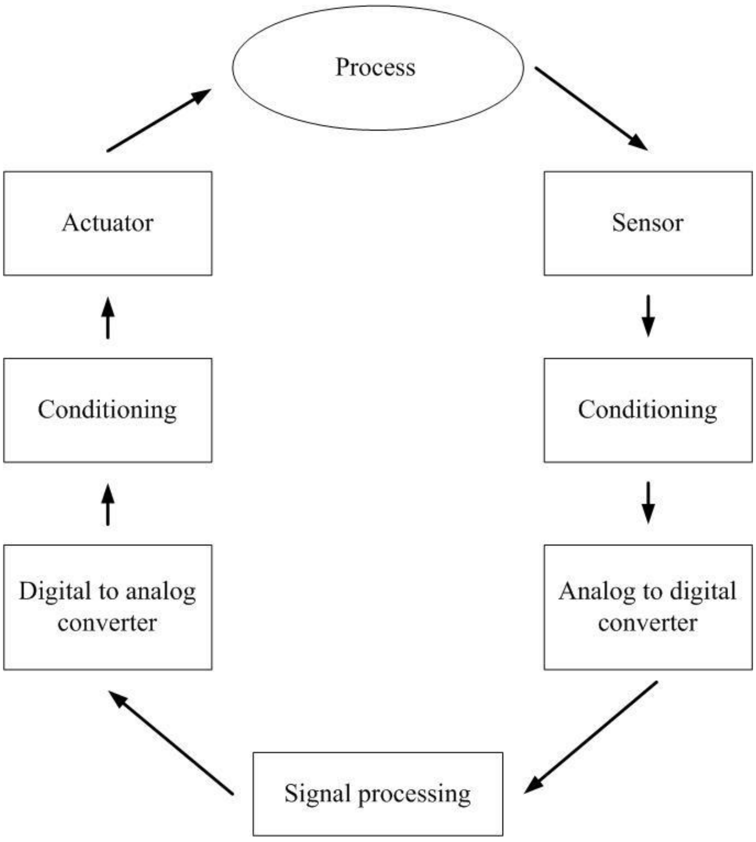

Figure 2: Sensor data acquisition and actuation.[7]

A group of smart devices that can sense and transmit information wirelessly based on application criteria and environment are called wireless sensor network. As an instance in a system data are collected using the wireless devices to the base station for analysis. Afterwards it is collected by the sink node as data collector. The sink node sends data to the gateway where the user can access those transmission data through internet. Figure 3 shows basic wireless sensor network architecture.

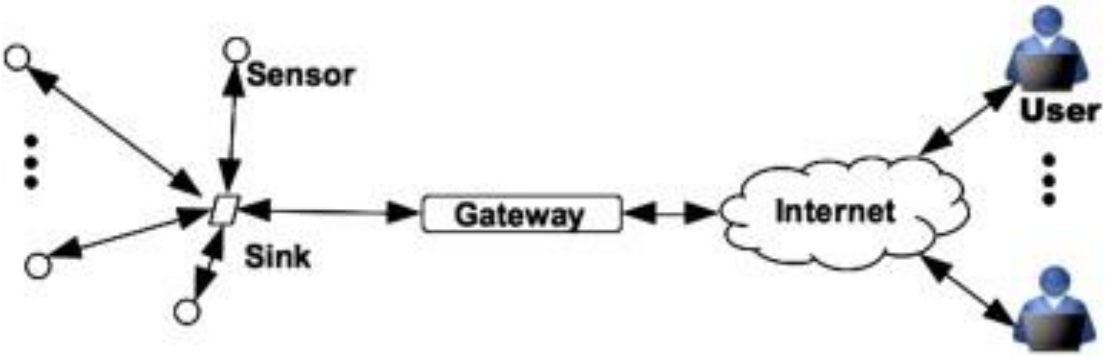

Figure 3: Architecture of wireless sensor network.[8]

3.2 Types of Wireless Sensor

There are different types of wireless sensors, such as:

Transmitter: The transmitter is used as a supporting device of scientific sensors that can transmit the data via radio signals to a receiver.

Receivers: The receiver receives the wireless data. It can receive radio signal and converts it into the desired output such as analogue output or digital display. Some receivers export the data to a software.

Controller: Controllers receive and analyse data from wireless transmitters. Moreover, they can manipulate a process based on data acquisition system. As an example, if the temperature in a furnace goes above the set temperature then controllers can identify the increased temperature and turn off heating by sending a signal.

Data logger: The wireless data logger can monitor temperature anywhere and can transmit data to receiver.

Transceiver: A transceiver consists of a transmitter and receiver within a single unit that can broadcast signal within the range of particular wireless sensor network.

3.3 Wireless sensor network

A wireless sensor network consists of distributed sensors to monitor both physical and environmental conditions of different types, such as temperature, sound, pressure, and vibration. Figure 4 describes a data acquisition system in the first part and data distribution system in the second part. In data acquisition part, the base station collects data wirelessly from different environment through wireless data collection network. Later, the base station controller sends data to the management centre for storing and analysing. On the other hand, the wireless data are distributed using wireless local area network (WLAN) through Wi-Fi, Bluetooth, and cellular network.[9]

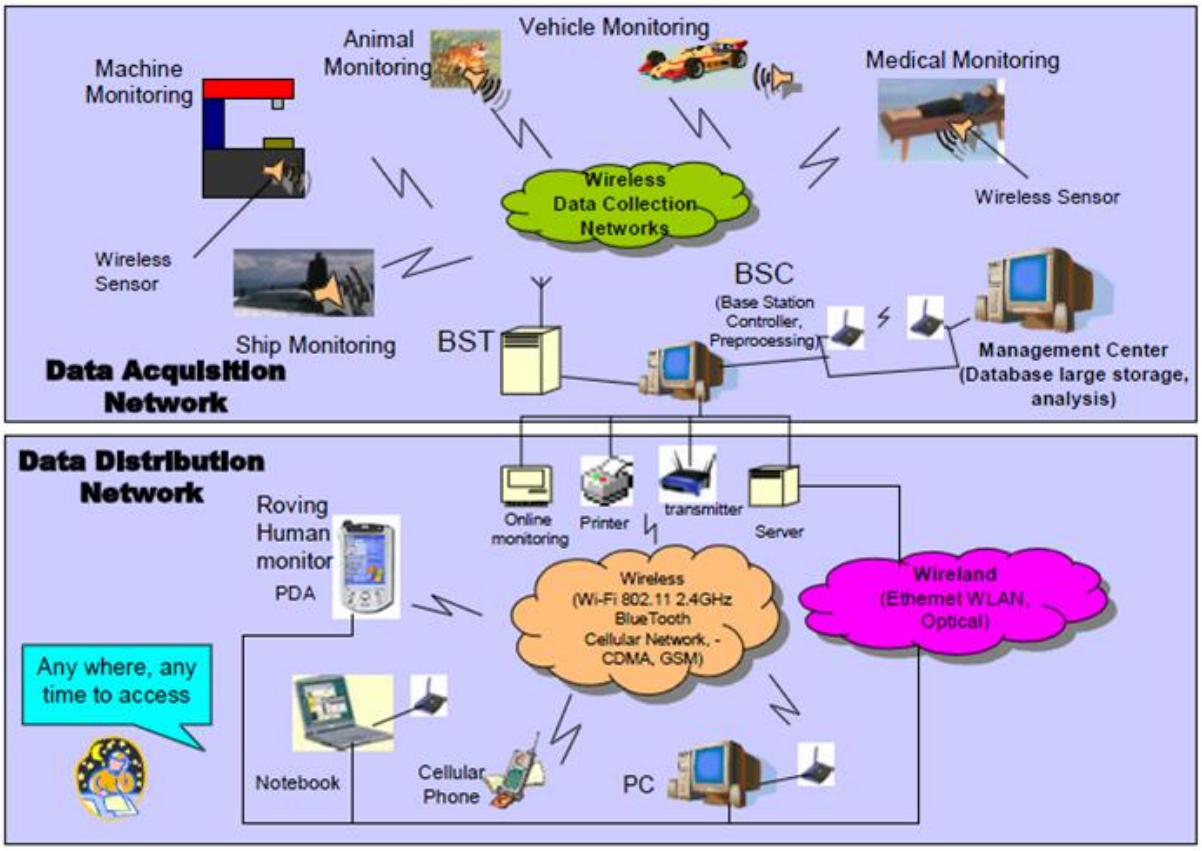
Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC
(Base Station Controller, Preprocessing)
Management Center (Database large storage, analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor
PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN, Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Figure 4: Wireless sensor network overview.[9]

3.4 History of wireless sensor networks

The Defence Advanced Research Projects Agency (DARPA) organised Distributed Sensor Networks Workshop in 1978 to disseminate the advancement of sensor technology based on networking and distributed algorithms. In the early 1980s, DARPA introduced sensor networks programme considering sensor information technology (SensIT). The concept of wireless integrated network sensors had been also developed in collaboration with the Rockwell Science Centre, the University of California in Los Angeles. Afterwards in 1996, low power wireless integrated micro sensor produced based on a CMOS chip, interface circuits, integrating multiple sensors, digital signal processing circuits, wireless radio and microcontroller on to a chip. In 1999, motes had been developed as a small sensor by the smart dust project in the University of California at Berkeley that demonstrated sensor.[10] This system can be integrated into tiny devices. The Berkeley wireless research centre, at that time, focused more on development of low power sensor devices through the Pico radio project which can power themselves from solar or vibrational energy.[11]

On the other hand, Massachusetts Institute of Technology (MIT) had developed a micro-adaptive multi domain power aware sensors project that can scale dynamic voltage to reduce power requirements at the software level using the techniques to restructure data processing algorithm.[12] Afterwards, over the last decade, a number of commercial efforts have been engaged to develop the wireless sensor system. Some companies, such as Crossbow, Sensoria, Worldsens, Dust networks and Ember Corporation provided opportunities for purchasing sensor devices which may be used for programming, maintenance, and sensor data visualisation.

3.5 Advantages of using wireless sensor network

Wireless sensor networks have many advantages over traditional cable-based monitoring systems. Wireless sensor network is handy, cost effective, and reliable. A wireless sensor network is consists of spatially distributed autonomous devices which use sensors to detect temperature, sound and other parameters in different applications. Initially wireless sensor networks were developed for military application. Nowadays, WSN is used mostly for civilian application, such as condition monitoring, healthcare, and traffic control. Furthermore, wireless sensor nodes are used to detect vehicle berth occupancy in car parks. Magnetometer is used to detect vehicle presence in hardware node. Micro radar and magnetometer are also used for vehicular tracking.

Wireless sensor network consists of large number of resources, especially with low cost sensor nodes, to establish a densely deployed network via the wireless communication module equipped on the nodes. Each sensor node is equipped with different sensors, computation units and storage devices which enable sensor nodes to sense, process and transmit all kinds of monitored information. Freeway traffic information collects through video cameras and inductive loops on the road. Wireless sensor networks are cost effective, reliable, accurate, and easy to deploy. Some characteristics of WSN are sensing accuracy, area of coverage, fault tolerance, connectivity, minimal human interaction, operability in harsh environments, and dynamic sensor scheduling.

3.6 Application of wireless sensor network

3.6.1 Volcanic monitoring

In today’s world, it is essential to monitor the volcanic situation due to the geographical change of the world. This volcanic situation can be monitored utilising the wireless sensor network. Sensor node can be used in this type of WSN setup. These nodes collect seismic and acoustic data from the volcanic area. Afterwards, the collected data can be sent to central data base station by the radio system. These nodes are power efficient and operate during a long time. Every node consists of four channels of siesmoacoustic data at 100Hz stored in a local flash memory.[13] Nodes can transmit the periodic status message. They synchronise the time as well. Once any unusual event is detected, the nodes send message to the base station laptop. If messages come within a short time interval the laptop starts for data collection by a round robin fashion. The laptop can download 30 to 60 seconds of data from each node using different data collection protocol. When data collection is completed then the nodes starts for sampling and storing again.

3.6.2 Animal tracking system

The research in biological and the geographical area are increasing day by day. Increasing the observation of species will be helpful for researcher to collect the necessary characteristics of a species, such as the understanding of their interactions and influences to each other. It is necessary to know how the species are changing both genetically and environmentally by their outer activity. Besides, the interaction between the human and animals can be identified by change of the weather patterns. Moreover, the heart rate, body temperature, frequency of feeding, and the movement of wild animals can be detected using the wireless sensor network. One of the recent animal activity tracking system is Zebra Net system which includes custom tracking collars (nodes).[14] The collars are made by Global Positioning System (GPS), flash memory, wireless transceiver, and a CPU.[14] Each node is small and has wireless computing device. It is operated by the peer-to-peer network and can send the data to the researcher.

3.6.3 Machinery monitoring

More recently, wireless sensor networks are widely used for machinery monitoring. Basically, wireless sensor nodes can be used to identify fault detection and further analysis.[15] In addition, once the sensor node is installed, it can detect machine configuration with minimal changes. Moreover, neighbouring nodes have the capability and can collaborate to monitor the overall machine condition.

3.6.4 Great Duck Island (GDI) system

The researchers from UCB Intel Research Laboratory developed a mote based sensor network on great Duck Island to monitor the behaviour of storm.[16] An Atmel Atmega 103 microcontroller which runs at 4MHz and 916MHz radio from RF monolithic is used to provide bidirectional communication at 40 kbps with AA batteries to provide energy. The mote has weather board attached with the processor connected by 51 pin extension connector. Temperature, photo resistor, barometer, humidity and thermopile sensors have been considered for this weather board. To preserve energy an Analog Digital Converter (ADC) and a 12C 8x8 power switch have been added on the sensor board.[16] The mica based motes are covered in acrylic enclosure to protect from the harsh weather. All motes are grouped into sensor patches and send the reading to gateway then the data is passed through sensor patch to the remote base station by local transmit network. Afterwards, the base station provides the data every 15 minutes to a progress data base via satellite. Finally, a small Personal Digital Assistant (PDA) size device has been used to perform local interactions activity by adjusting sampling rates and power management parameter.

3.6.5 Health care monitoring

In recent years, wireless sensor technology has been used in health care to detect and monitor different diseases and health conditions. To name a few where WST is being used are parkinson’s disease, epilepsy, heart patients, patients rehabilitating from stroke and heart attack. Substantial amount of budgetary allocations are earmarked in most of the countries for improving health care system by using up-to-date technology. In USA alone, the US centre for medicare and medical services used 2.4 trillion dollars in 2008 for health care.[17] Similar amount of budget has been estimated for many western countries. There are many sensors that have been developed acting as health care monitoring, such as Pulse oxygen saturation sensors, blood pressure sensors, blood flow sensors, blood oxygen level sensor, temperature measuring sensors, blood sugar level sensing device, electrocardiogram (ECG), respiration sensors, electromyogram etc. Figure 5 shows an architectural building block system for monitoring patients to deliver information to the central control system using wireless sensor network.

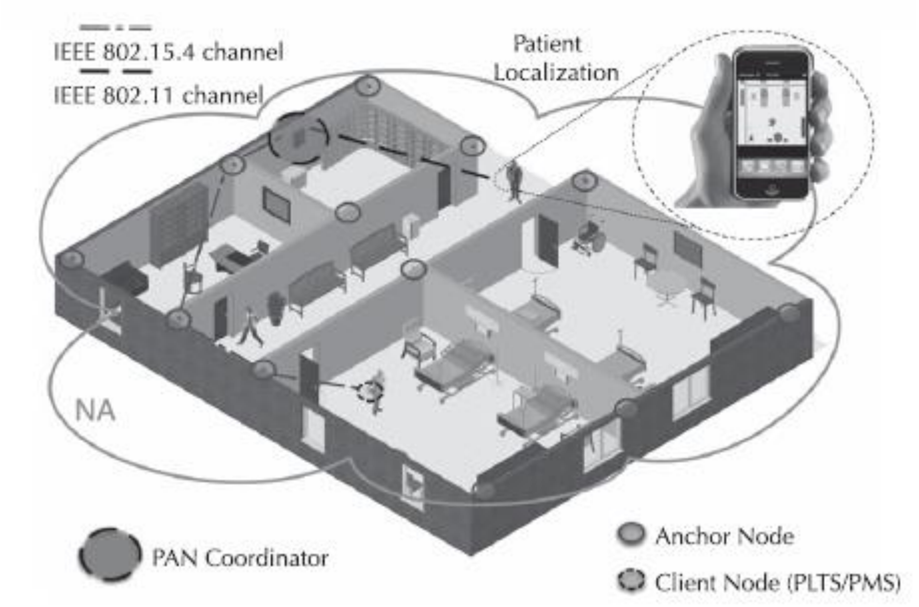

Figure 5: Health care monitoring system using wireless sensor network.[18]

3.6.6 Military surveillance

The VigilNet system is a wireless sensor network used for military surveillance.[19,20] It is self-organised and provides tripwire-based surveillance. The objective of this system is to control military command. This system can detect and classify the position of an object. After getting the information it passes the information to the nearest remote base station. The VigiNet architecture is made of the following three components – Application components, Middleware components, and TinyOS system components. The application components are specially developed for surveillance purposes. It comprises of entity-based tracking service and classification components. Time synchronisation and localisation are important for surveillance application as detection and tracking process are compiled between the tracking reports sent by multiple motes. Time synchronisation can synchronise the clock of motes in the base station. On the other hand, configuration module can reconfigure the system when it needs radio wakeup module to alert non-sentry mote. VigilNet can provide power management and collaborative detection which are two key higher-level services. VigilNet architecture has been built on top of the TinyOS. TinyOS is an event driven computation model which is written in NesC for the motes. TinyOS provides hardware drivers, a scheduler and basic communication protocols. These components are written in NesC. Afterwards, NesC compiler can process TinyOS and VigilNet applications by running executable. VigilNet runs on the XSM (and MICA2) mote platforms.

3.6.7 Environmental monitoring

Wireless sensor network is increasingly more popular in monitoring environment. Culler et al.[21] in their research described the development of design level framework for smart environment through wireless sensor network indicating the application in Bangladesh. The system they proposed describes sensor nodes. Each node has sensing unit to senses the change of parameters and the signal conditioning circuitry converts electrical signal to digital domain. Then it is sent to the processing unit. The memory can process the tasks and the transceiver is used for communicating with other sensors. Based on the sensor node properties, the authors described the flood and water level monitoring system as algorithmic diagram. WSN is now used to monitor seabird habitats, for conducting analogue studies of contaminant propagation, building comfort and intrusion detection which could help implementation of smart environment.

3.6.8 Traffic monitoring system

Many WSN systems are recently being used for traffic monitoring. Chen et al.[22] described the structure framework for traffic information collection system with problems and resolution strategies based on wireless sensor network. Traffic information collection is one of the vital parts of intelligent traffic system (ITS) associated with road design, traffic management, control, traffic design, and implementation. The current traffic information collection system is based on inductive loop detector, microwave detection, video detection, and infrared detection.[22] This system consists of embedded mobile devices for detecting and handling wireless communication function. Each node constitutes a network through ad-hoc traffic information and environmental information to facilitate collection, processing, and transmission.

Typical sensor network structure composes of sensor node, sink, internet or satellite, and task management node.[22] Sensor nodes can transmit data to sink through multi-hop route from sensor area, and sink can transmit statistics to each node in similar way. Sink is directly linked with internet and/or satellite to realise the communication between task management node and the sensor. The Sensor node is made up by power supply, perception component, embedded processor, memory, communication component, and software. The power supply provides power to the sensor. A perception component is used for perception and acquisition of outer information to convert digital signal. The processor deals and stores information from the perception component and monitor working model of the perception component and power supply. Moreover, the communication component, which communicates with other sensors and software, provides embedded operating and data base system to support the sensor. The formula for vehicle acceleration, deceleration, and merging controls has been described by Endo et al.[23] This control technique is conducted by simulation considering saturation and delay characteristics in accelerating heavy duty vehicle where desired speed and distance are calculated. This system is complex to understand clearly as it does not show experimental setup. Figure 6 illustrates traffic monitoring system equipped with GPS enabled smart phone, cellular network, data collection system and information display system.

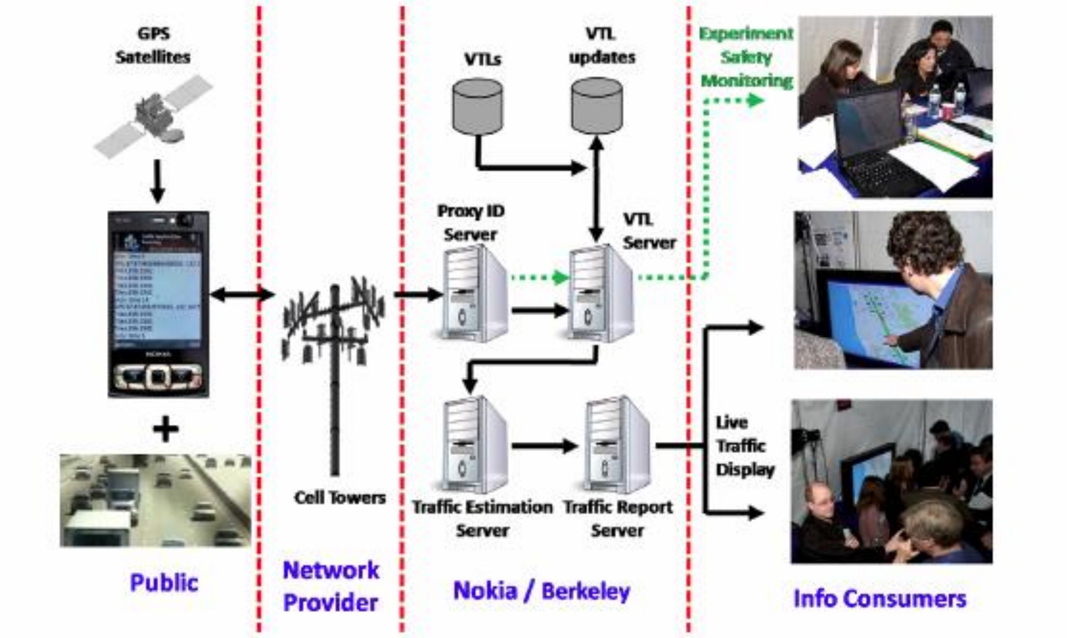

Figure 6: Traffic monitoring, data collection and displaying through wireless sensor network.[24]

4. INTERNAL INFRASTRUCTURE OF WIRELESS SENSOR NETWORK

4.1 Wireless sensor standards

Wireless sensors standards define the functions and protocols for nodes to interface with different types of networks as those developed for low power consumption. Few of the standards are 802.15.3[25], IEEE 802.15.4[26], ZigBee[27], 6LowPAN[28,29], Wibree[30], WirelessHart[31], and ISA 100.11a[32].

802.15.3[25]**:** The IEEE 802.15 is a working group of the IEEE whereas the IEEE 802 is standards committee that can specify wireless personal area network standard. The IEEE 802.15.3 is wireless standard that can operate 2.4GHz radio and data range is between 11 mbps to 55 mbps. It is a physical and MAC layer standard for high data rate wireless personal area network. The Quality of services (QoS) is maintained by time division multiple access (TDMA) in this standard. Real time video streaming and music are supported by this standard. Synchronous and asynchronous data transfers are supported by this standard. It also maintains frequency performance, data rate scalability, and power consumption. There are many devices that are conducted by using this standard, such as cordless phones, televisions, printers, wireless speaker, and connectivity for gamming, portable video electronics etc.

IEEE 802.15.4[26]: The IEEE 802.15.4 standard has been developed to operate 868 MHz, 915 MHz, and 2.45 GHz frequency bands with supporting data rate of 20, 40, and 250kbps. This standard contains two types of topology nodes – one is star that is similar to Bluetooth and other is peer-to-peer that allows the communication freely within the devices. All the communications are maintained through Personal Area Network (PAN) co-ordinator.5 Residential, industrial, environment monitoring control and automation applications are conducted by wireless sensor network using the IEEE 802.15.4. It is used for low cost of deployment, low power consumption, and low complexity. Mostly the standard is used for low rate wireless personal area networks and short range communication for maximising battery life. The formation of star and peer-to-peer topology is allowed by the standard to communicate between network devices. It supports physical and data link layer protocols. The MAC layer can validate frames, delivery, network interface, network synchronisation, secure service, and device association.5 Devices are interacted with each other through wireless network. Figure 7 shows different layers of IEEE 802.15.4.

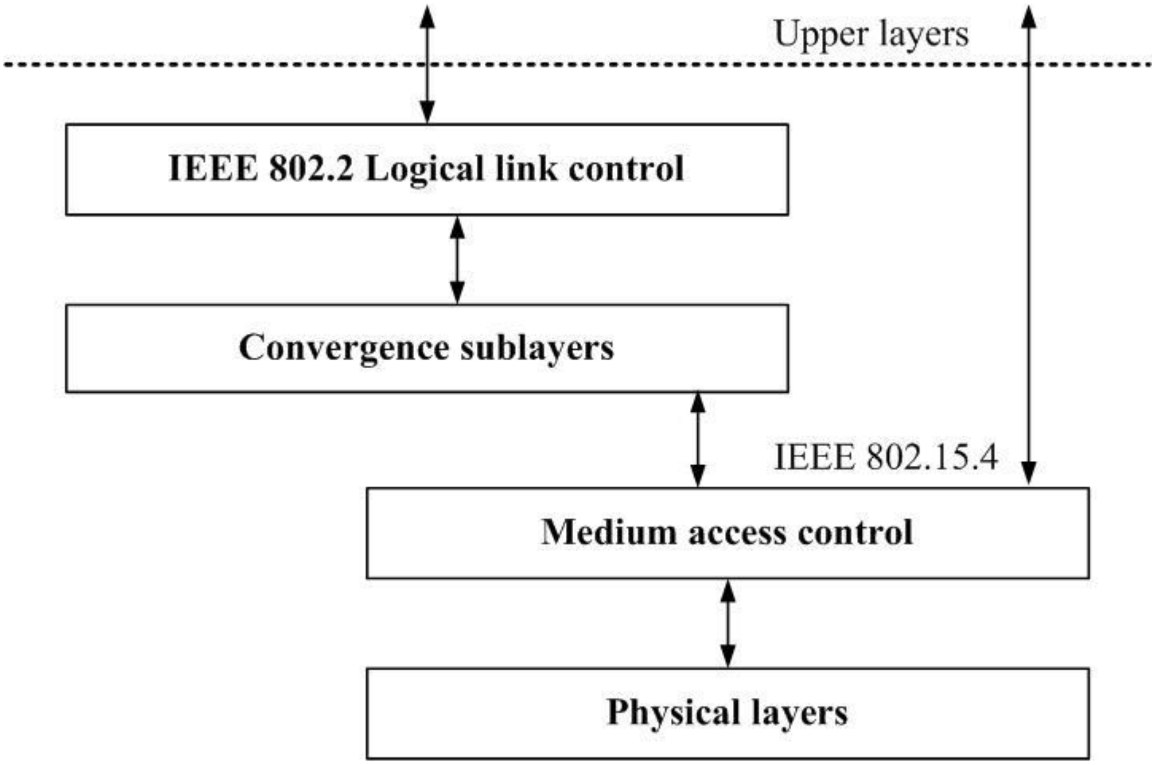

Figure 7: IEEE 802.15.4 protocol architecture.

ZigBee[27]**:** ZigBee was initially used on a low cost communication technology for low data rates and low power consumption. Afterwards, ZigBee is the commercial name for the IEEE 802.15.4 technology5. ZigBee is a simple wireless communication technology used in embedded applications. A mesh network can be consisted by ZigBee used in many devices. There are three types of ZigBee devices such as ZigBee coordinator, ZigBee router, and ZigBee end device. A very little power on cell battery is used by ZigBee device. Moreover, bridge network, store information and initiate network information are also conducted by ZigBee coordinator. Sensors, actuators and controller are main parts of ZigBee end device those can create data communication within router.

6LOWPAN[28,29]**:** 6LoWPAN is a working group's name in the internet and the name of the area is IETF. It is an IEEE802.15.4 based network designed for low data rate devices applications. It is low power wireless personal area networks based on IPV6. It can maintain communication with IP devices using IP-based protocols. New packet format, adaptation layer, and address management are provided by this standard. IPV6 packet sizes are larger than the frame size of the IEEE802.15.4. An adaptation layer is required for this IPV6. This layer maintains header compression functionality, while small packets are created to fit into the IEEE 802.15.4 frame size. The device address forming systems are controlled by the address management mechanism.

Wibree[30]**:** Wibree had been released in October 2006. It operates on 2.4 GHz and the data rate is 1 Mbps. It maintains the communication between small battery-powered devices and Bluetooth devices. Wireless keyboard, sports sensor and watches are connected to host devices such as phone, personal computer etc. and the linking distance of devices is 5-10 m. Wibree works with Bluetooth. Therefore, Wibree made devices are smaller and energy efficient. Existing Bluetooth RF is used by the Bluetooth-Wibree which enabled ultra-low power consumption.

WirelessHART[31]**:** WirelessHART network is consisted by network manager, host appliactions, gateways, and difeerent types of wireless devices. It is introduced to the industry in September 2007. WirelessHART can process plant equipment whereas communication between wireless field device and host application are developed by the gateways. On the other hand, process automation controller does continuous process system. Moreover, the network manager can manage routing, network traffic, and configure and communicate network within different devices. In addition to process automation controller, host application and the gateway are structured network managers. It is reliable, secure, energy efficient, and cost effective. It can conduct with system, tools, and existing devices. The operational power is 2.4 GHz based on the IEEE 802.15.4. This standard is used for processing and controlling the measurement applications of wireless sensor network communication protocol. There are few applications such as time synchronised messaging, mesh networking, and channel hopping which are supported by this standard. The communication of this network is more secure for authentication, encryption, and verification. Moreover, network topologies such as mesh, star, combined are supported by the wirelessHART. It can consume power to enable wireless device for providing energy efficiency.

ISA100.11a[32]**:** ISA100.11a is a wireless network technology standard that has been developed by the international society of automation and officially released in September, 2009. ISA100.11a is used for simple, flexible and scalable security functionality with star and mesh network topologies. This standard is developed for low data rate wireless monitoring and processing applications. This standard uses 2.4 GHz radio. It maintains contact with other different wireless devices in a network system. Robustness, infrastructure, scalability, interoperability and low power energy consumption are defined by this standard.

4.2 Storage allocation

Storage is needed in wireless sensor network because of the limited available storage in nodes. At the time of storage, the over data sensor optimisation is essential by aggregation and compression. Storage techniques are necessary for maintaining the proper connectivity within nodes and other devices. There are a few storage systems described in the following sections.

Graph Embedding Infrastructure system (GEM)[33]**:** GEM can store data and do the routing contact within the sensor networks. It can create guest graph in sensor network after labelling this graph for routing. Data items are mapped to a label and store different nodes. The client requests are sent to the network as query and the node will respond to that query. Lookup mechanisms are used for routing from node-to-node. A ring tree graph is applied for virtual polar co-ordinate space. Virtual angle ranges are assigned for node to recognise the number of nodes within the network.

Resolution storages[34]**:** It is used in network to store data as spatially and hierarchically decomposed storage structure. The storage system is compiled by three different ways such as wavelet process, drill down query process, and data aging. Those are used for resolution and data compression which reduce cost by discarding old data and create more space for adding new data.

Two Tier Sensor Architecture (TSAR)[35]**:** TSAR is two tier sensor storage architecture mainly used for value queries and spatio-temporal. Sensor nodes send metadata to nearest proxy. Afterwards, proxy can interact for constructing index of other communicated data to pinpoint. There are some contribution, such as index structure by interval skip graph, store data in flash memory, prototype of TSAR, and evaluation of TSAR.

4.3 Supporting operating system in WSN

There are many sensors that can be integrated on a WSN platform. Wireless Sensor Network (WSN) consists of a large number of sensor nodes. Operating systems are used to maintain this network. Network longevity, distributed programming, data management are controlled and operated by the operating system. There are few operating systems, among which most common are Bluetooth based sensor system, and detection and classification system. BT nodes are used in Bluetooth system where TinyOS is ported with BT nodes. BT node is configured as operating master and slave. They are activated before exchanging data in the network. At first the slave radio is enabled before joining the new network. Then master slave can connect the other nodes after connecting salve radio. The remaining disconnected nodes are then searching for connection. The system is organised by the network topology. On the other hand, detection and classification can detect objects. It is developed by VigiNet. More sensor nodes are deployed for this system in the environment. Magnetometer, motion sensor, and microphone are needed to build this system. A hierarchical architecture is used to sense and compute the tasks at various levels in a system. It is acted at different levels such as sensor, node, group, base etc. Operating system in WSN plays a central role and its applications are efficient and reliable. Two major existing operating systems are Contiki and LiteOS.

5.0 NETWORKING SYSTEM AND CONNECTIVITY

5.1 Localisation schemes

Global positioning system, beacon nodes, and proximity based localisation are the existing localisation nodes. The beacon method makes use of beacon nodes to help sensor for positioning purposes. Some prime localisation techniques are:

Radio Interferometric Positioning System[36]**:** The radio interferometric positioning system (RIPS) is used for two radio transmitters to create signals. Two receivers are needed to calculate the phase offset of the observed signal. The relative locations of the two receivers can be determined by measuring relative phase offset.

Process of secure localisation[37]: This can focus on the securing of the localisation process to prevent malicious beacon nodes instead of false location of the sensor. Beacon can compute the position. Sensors accept information from the authenticated beacon node. Some of the existing location techniques include SeRioc[38], Beacon suite[39], DRBTS[40], SPINE[41], and ROPE[42]. The Beacon nodes serve two processes where it provides location information to the sensor node, and also detects malicious beacon signals. Beacon nodes monitor each other for information corresponding within the sensor nodes.

Accuracy of localisation[43]**:** Spotlight can achieve the high accuracy of localisation without hardware. It uses an asymmetric architecture on a single spotlight device and a steerable laser light placed in a known terrain. The main task of the spotlight is to generate controlled events in the sensor nodes deployed field. Spotlight is more accurate and effective than other range-based localisation schemes.

Mobile Assisted Localisation (MAL)[44]: MAL technique is used to assist collection of information between itself and the static sensor nodes. The objective is to reconstruct the position of the nodes measuring distance edges. An anchor free localisation algorithm is used here. This algorithm can compute the node coordinate after building a rigid graph.

Algorithm[45]: Moore's algorithm is used for local estimation without GPS, by using a robust quadrilateral approach. This robust quadrilateral is connected four sun triangles quadrilateral. This algorithm consists of three phases – cluster localisation phase, cluster optimisation phase, and cluster transformation phase. The first phase can measure the distance of its one-hop neighbour. The optimisation phase is the second phase that can be omitted. The last phase computes the rotation, translation, and reflection. The algorithm may not be localised under low node connectivity and high noise.

5.2 Security systems in WSN

There are many security systems in the WSN based on limitations in storage, communication, and processing capabilities. Management and control services are needed to maintain wireless connection, while secure protocols are proposed for maintenance of the network securely. Few of the widely used security systems are described in the following sub-sections:

Location Aware key Establishment (LKE)[46]: This location aware key establishment by preventing node capture attacks in large scale sensor networks. The four phases in this system are pre-distribution phase, node self-configuration phase, polynomial share distribution phase, and pairwise key distribution phase. In the first phase, all sensors are programmed and configured. In the node self-configuration phase, the roles of sensors are configured. Then the sensors can determine their position based on localisation technique. The polynomial share distribution phase works in different phases and share information by using different steps. Overall this system can protect against attacks.

Key exchange protocol[47]: The decentralised key exchange protocol is mainly used for secrecy of key exchange, node disjoint path, and key shares. It can generate key shares of length and can send them to destination. The objective of this protocol is to minimise resource consumption.

TinySec[48]**:** The TinySec uses link layer security that can contribute integrity, authenticity, and confidentially by including Message Authentication Code (MAC). The MAC can be calculated using secret key. The receiver can receive the message and packet.

5.3 Coverage

The sensor coverage of designated area in wireless sensor network is important. The quality of monitoring is dependent on the application. There are some proposed techniques for the main coverage of nodes in WSN. The connectivity of few protocols in wireless sensor network is described in the following sections.

Surveillance service protocol[49]**:** This protocol provides different degrees of sensing coverage in the wireless sensor network. It is part of energy efficient sensing coverage scheme. The sensors stay in two phases in the scheme such as initialising and sensing. In the first phase, the sensor node can determine its location and synchronise time. The time is then divided into round of equal durations in the second phase.

Determination of exposure path algorithms[50]**:** The minimum exposure path is the path between two points so that the total sensor exposure is minimised along the way, while total sensor exposure is maximised for maximum exposure path. The minimal exposure path is solved by the method of calculus. To determine maximal exposure path the solution has been created for the problem NP-hard. Random path, shortest path, best point, and adjusted best points are the proposed heuristic methods. A grid based algorithm can solve the minimal exposure path.

Activity of configuration protocol[51]**:** Coverage Configuration Protocol (CCP) is decentralised protocol that can change the degree of coverage in a network according to application. It can change the degree of coverage in the network. The node has three states in the network which are sleep, active, and listen. In the sleep state, the nodes remain turned off, which then collects message at listen state. In active mode, the node updates sensing activity. CCP is connected with SPAN[52] to provide connectivity and coverage.

5.4 Synchronisation

Routing and power conservation are dependent on time synchronisation. Network’s lifetime and energy consumption are dependent on time accuracy. In the following subsection, few of these protocols are described.

Timing synchronisation protocol[53]**:** This protocol is based on conventional sender receiver synchronisation. A level discovery phase and a synchronisation phase are consisted in this protocol. The sensor node is connected with the root node. Then the root node is synchronised with the whole network and time. The node becomes timed out while a random time is retransmitting and it remains until two ways message is completed.

Lucarellis algorithm[54]: This algorithm is used to synchronise with bi-directional neighbour coupling based on local communication topology. Each node can contain state variable that is increased from 0 to 1.

Synchronisation duration[55]**:** This approach enables to empirically measure and analyse three key parameters for long term synchronisation. A rate adaptive, energy efficient, and long term time synchronisation algorithm is the rate adaptive time synchronisation protocol. Multiplicative increase and multiplicative decrease strategy is used for sampling rate and for minimising energy use.

Reach back firefly algorithm[56]**:** This algorithm is Tiny based decentralised synchronicity algorithm. The algorithm considers some mathematical model. The synchronisation can be changed by losses, adding nodes, and link changes. This algorithm works in the system with fixed time period. Every node has its internal time that is increased to 7. The node can synchronise a common phase and firing pulse function system. Delay of message, handling message, and wireless contention are major issues for the other algorithms.

Time synchronisation[57]**:** Multichannel radios are used to reduce packet collisions and interferences in time synchronisation. Pull and push mechanisms are used in this method. When a query is sent from the sensor node for getting clock information, the reference node sends the message back to a specific clock channel. The connectivity is working between different protocols and nodes.

Global synchronisation[58]**:** Node based, cluster based, and diffusion based methods are used in this system. A message is routed along the cycle path and the nodes are synchronised by all node based methods. The first message is sent along this cycle. Every node can adjust local time with error time. The sensor nodes are functioned with the clusters for synchronisation. There is connectivity visible with the sensor and the nodes which are working in a network. A sensor node can send clock values to all other neighbouring nodes for synchronisation.

Clock sampling synchronisation[59]**:** This is a network autonomous synchronisation approach. The time information changes with transmission. Every node in the network processes the beacon transmission based on time. The node can set clock for finding the value of time stamp and can calculate the gap between the time stamp of received beacon and time stamp of sensor node.

6.0 COMMUNICATION PROTOCOL AND THEIR RELIABILITY

Wireless sensor networks consist of different standard protocols. The development of reliable and energy efficient protocols are important for the improvement of different applications in wireless sensor network. In 1997, the most common wireless networking technology, the IEEE 802.11 family of standards was introduced for mobile systems. The IEEE802.11b and the IEEE802.11g protocol use 2.4 GHz band whereas the IEEE 802.11a uses 5GHz frequency band. The IEEE802.11 was used in early years and still can be found in some current networks. The high data rates are provided by this protocol. The IEEE 802.15.4 protocol has been designed for short range communication which is supported by most sensor nodes. The sensor can transmit the data directly to the base station by forming a star topology when the radio transmission ranges of all sensors are large. Then each sensor node can communicate directly to the base station using hop. Multi-hop communication is common case for sensor networks. In the mesh topology sensor nodes can serve data as relays to other nodes to propagate sensor data towards base station for further analysis. In sensor network the sensor can be failed temporarily. Sometimes this failure occurs permanently. The failure can be prevented for reliable service by deploying well designed protocol. Figure 8 shows the connectivity among the sensor nodes between different protocol layers and the task managemnet plane, mobility management plane, and power management plane within a wireless network system.

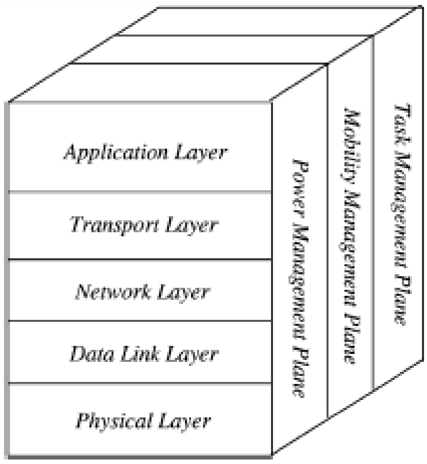

Figure 8: Protocol architecture of sensor network.[60]

6.1 Application layer

There is varied application areas defined in wireless sensor network. Application layer is the first step among few main layers in WSN. Each application layer contains some protocols that maintain connection to each other within a network. The protocols are Task assigning protocol, Management protocol, sensor query and data diffusion protocol.

Task assigning protocol: Interest dissemination is crucial operation in wireless sensor network where user and their interest regarding a certain state of sensor node are described in the network. On the other hand, advertisements of data are done by sensor nodes to the user which meets the user query. Routing can be taken as an example where software and interfacing for the user are conducted by the application layer protocol.

Management protocol: Designing management protocol has some benefits in the application layer. The lower layers transparencies are depended by the hardware and software in the management protocol layer. The interaction of the system administrators maintains using this sensor management protocol. Different types of administrative tasks are compiled by this protocol, such as: attribute based naming, clustering and data aggregation. Besides this, location finding algorithm has been developed by exchanging data. Moreover, security and key distribution in data communication, authentication, querying and reconfiguring sensor network, status of sensor node by turning on and off, moving and time synchronisation of sensor nodes are performed by using this protocol.

Sensor query and data diffusion protocol: User application with interfacing is applied to issue queries, respond to queries, and collect replies by this protocol. The attribute based and location based naming are preferred in this protocol. The sensor query and tasking language (SQTL)[61] is defined as a large set of services which supports *receive*, *every*, and *expire* events. The events is generated by the sensor node as a message by the receive keywords. On the other hand, the events are occurred for a certain period of time. When the timer has expired then it is defined by the expire keyword. When the message is being received with script then it is executed by a sensor node.

6.2 Transport layer

The transport layer protocol mainly supports multiple applications, variable reliability, and packet loss recovery. This layer can provide packet reliability and ensures the quality of data at the source. In every WSN system some packet loss occurs due to bad radio communication, packet collision, congestion, node failure, and full memory capacity. The ultimate result of this packet loss is wasted energy and reduced quality of service in data delivery; whereas, detection of packet loss and missing packets improves the energy expenditure. The development of this transport layer protocol should be independent. The hop-by-hop and end-to-end are two approaches for the packet recovery. The retransmission of hop-by-hop is performed in an intermediate node cache, and this method is energy efficient. In end-to-end transmission, the source caches are all packet information and are retransmitted when packet loss happens. The reliability is allowed by the end-to-end retransmission when the reliability requirements are high.

Congestion control mechanism can monitor and detect congestion. The source reminds alert to reduce sending packet rate before the congestion takes place. Congestion control can reduce retransmission for preventing buffer of sensor in overrun situation. In every node, the hop-by-hop mechanism is acted to monitor buffer overflows. Moreover, the hop-by-hop mechanism is faster than end-to-end system. All nodes change their behaviour after detecting congestion by the sensor nodes. The end to end mechanisms are reliable for detecting congestion at the end nodes. Packet loss recovery and congestion control mechanism trade off happens between hop-by-hop and an end-to-end approaches. This trade off depends on the application type based on reliability and sensibility. A few of the transport layer protocols are described in the following sections.

Congestion control scheme[62]**:** This is an energy congestion control scheme consisting with three components – congestion detection, hop-by-hop backpressure, and multisource regulation. The buffer occupancy and channel load are detected by this scheme. The sensor can identify the local channel load condition to detect congestion when buffer occupancy becomes high. A suppression and backpressure message is broadcasted to the node to adjust once the congestion is detected. Further congestion can be prevented by a node to drop the incoming data packets. Moreover, a closed loop multisource regulation method is used to control congestion from sources to the sink. Pre-defined event rate information is sent by the sink.

Activity of transmission control protocol[63]**:** This protocol provides congestion detection and avoidance. Variable reliability and different applications are supported within a network. The functionality of these sensors is executed at the base station which is connected with all nodes having high processing capability, storage, and power. First a packet transmission is initiated to base station containing number of flows from node, data type, transmission rate, and reliability. An acknowledgement is sent to the node from the base station before transmitting data. The base station can estimate the arrival time of packet for the each source. If any packet is missing then the base station can detect it. Reliability is maintained by successfully receiving packet of transmission, whereas a negative acknowledgment is sent if the current reliability is reduced comparing to the required level. Afterwards, the transmitted packets are saved as buffered format in the source node at the threshold position. The source node calculates the packet that reaches base station. The node will not buffer the packet to save storage if the calculated value is higher than the required value. The base station creates positive acknowledgement after receiving packet. The transmitted packets are deleted after reaching the acknowledgment. The Low and high thresholds are maintained in each sensor node. A congestion bit is set for all packets once the buffer reaches at higher threshold. Thus, the bit is working as informer while the source reduces the transmission rate or re-route packets.

Delay sensitive transmission protocol[64]**:** The major use of this protocol is for congestion control, reliability, and packet delivery. There are two components – a reliable event transport mechanism and real time event transport mechanism. To determine and ensure the desire reliability level for event-to-sink communication, the reliable event transport mechanism takes actions through observing delay constant event reliability against desired delay constant event reliability. The minimum numbers of data packets are required for detection. The event reliable is reliable when the observed delay-constrained event reliability is greater than desire delay constrained event reliability. The event-to-sink bound delay is used by the real time event to measure the event transport delay and event process delay. DST measures the buffer overflow at every node, whereas simulation experiments explain timely event detection with energy consumption and latency.

Cost reliable protocol[65]**:** This protocol minimises high communication cost and energy consumption, while the level of reliability and congestion avoidance mechanism is maintained. The amount of energy consumed is specified as end-to-end communication cost where packets are delivered from source to base station. The protocol is classified in two mechanisms to ensure reliability. The first one is dynamic source report rate feedback mechanism that can maintain the reporting rate between sink and data source. Each packet is sent according to its node price. The node price depends on the number of transmission made against successful packet delivery. The sink compares the reporting rate of each source based on source node price and the physical phenomenon. The second mechanism is to regulate the end-to-end communication cost information sending from source to the sink. Communication cost depends on congestion and the cost rises when congestion occurs respect to packet loss. The communication information cost is used to determine the ratio of reporting rate of sources.

Event to sink reliable transmission control protocol[66]**:** The reliable event detection with energy expenditure is controlled by this protocol. A congestion control mechanism is used to reduce energy consumption by running this protocol algorithm at the sink. The reliability factor and reporting frequency are calculated by the sink to measure the received data packets from source node. The ESRT increases the reporting frequency while the computed reliability is lower than desired reliability. On the other hand, the monitoring of buffer overflows indicates the congestion in the outgoing packets, which is followed by this congestion control mechanism. Afterwards, the packets with calculated reliability are received by this sink to determine the state of network.

GARUDA[67]**:** It is a data delivery transport protocol for wireless sensor network. It can identify the problem of sending data from sink to sensor. Reliability is classified by four categories, such as Guarantee of delivery to the entire field, to the sub-region of sensors, to a minimal set of sensors to cover the sensing region, and to probabilistic subset of deliveries. It is the core infrastructure for loss-recovery packet and constructed using first packet delivery method using Wait-For-First-Packet (WFP) pulse. It is also a NACK based recovery process. The WFP is a short duration pulse. The sensor node of sink receives this pulse. The core nodes are created in a network itself. An out of order strategy uses to solve the packet losses of under-utilisation. The out-of-order forwarding acts after causing the packet lost. Two loss stages are used; first the core nodes recover the packet. Once an out-of-sequence packet is received then the request is sent to the core node about the missing packet. Then the message is received by the upstream core node. The second stage is a non-core recovery phase that requests retransmission from the core node and waits to complete the retransmission before sending.

Pump slowly, fetch quickly (PSFQ)[68] protocol: PSFQ is a reliable transport protocol that can deliver data segment, data transmission and detection, data recovery operation, and provide loose delay bound for data delivery. It is operated by three sections, such as pump operation, fetch operation, and report operation. The rate of data packets are controlled while passed along into the network by this pump operation using two timers 7_{min} and 7_{max}. A packet transmits after waiting the node at least 7_{min}, whereas 7_{max} is used as loose upper delay bound. The fetch operation retrieves the packets by sending a single fetch while the packets are lost in an event. Afterwards, a feedback status is sent to the users by the report operation as a status report message. Overall, the results show reliable multicast based on tolerance and communication overhead.

Probing Environment and Adapting Sleeping (PEAS)[69]: Node failures and randomly environmental situation recovering are controlled and monitored by this protocol. A sensor can transmit probe packet where the neighbours packet will reply after a continuous backoff time while they are in probing range. The probing sensor becomes active if it doesn’t receive reply message from probing nodes. On the hand the opposite situation causes the probing sensor in sleep mode. The balance within energy savings and robustness are dependent by the probing rate of PEAS. A low probing rate occurs while unexpected node failure occurs and it creates a long delay. On the contrary the high probing rate causes huge cost by wasting energy. To keep the situation consistent probing rate should be increased at the time of node failure.

6.3 Network layer

The scalability is required in wireless sensor network as a design of network protocol. IP based routing protocols are not used in WSN as they do not have the internet protocol. This network layer controls data routing from source to destination in a network system. The protocol considers memory, computation capabilities, communication bandwidth, security, fault tolerance, and fairness. Geographical routing is used to forward a packet from source to destination. There are two types of geographical routing system: one is distance based and other one is reception based. A node can identify the distance of its neighbour by the distance based forwarding. It contains the blacklisting and greedy forwarding. The distance of the neighbour and independence of reception rate are selected by the original greedy forwarding. A number of reception based forwarding schemes are found, such as absolute reception based blacklisting, relative reception based blacklisting, best reception neighbour and best reception rate, and distance.

Secure cell relay protocol (SCR)[70]**:** This protocol provides resistance to security attacks. It is a cluster based algorithm. A common global key is shared among the sensor node and the base station for synchronising all nodes and base station before deployment. Two or more backup paths are determined by the SCR to forward packets. When a node is attacked, the backup paths forward packets. There are few attacks defended by SCR, such as Sybil, wormhole and sinkhole, and selective forwarding.

Secure routing protocol[71]**:** This protocol is a two level cluster based approach to the secure network. Each cluster has a cluster head where the sensor nodes communicate by this head. A symmetric cryptography is used to secure packets along the path. Sensor nodes contain unique identity and preloaded key, whereas the identity introduces the node and the key is used for secure message to sink. The details of the sensor nodes are known to the sink. A cluster key can help to transfer the data packet with a sensor node encrypting. The cluster head can create the cluster key by self-organising phase and can share the sensor nodes within cluster. All data are sent to the cluster head from its member and formed as a new data packet.

Location service protocol[72]**:** This is a grid and location based protocol. The routing system is maintained between multiple sources and destinations. This protocol is firstly used in a geographical grid structure for the network. The sensor node can contain the size of grid cell and the base line co-ordinates. The sensor nodes are randomly deployed to obtain location using GPS. A grid node is selected by destination node to sink agent for distributing location information using anchor system which is made by the set of grid nodes. A source node transmits data to destination node when an event occurs. Afterwards, the source node first transfer to nearest grid node as a source agent and then it locates the destination node to report the information.

6.4 Data link layer

The data link layer considers data transfer between two nodes where they can share the same link. The media access control (MAC) protocol mainly consists of fairness, bandwidth utilisation, flow control, frame synchronisation, and error control which are the keywords for effective data communication. Correction and error detection are done in the data link layer. The fixed data block sizes are agreed between sender and receiver before sending data. The 8bit CRC[73] is used for error detection. There are a few recovery techniques in wireless sensor network, such as simple packet combining, hybrid ARQ[73], and forward error detection. There are timeout and positive-negative acknowledgement used by automatic repeat request as feedback to the sender. The design of MAC protocol is consisted energy, topology, and network topology to minimise energy by extending the network lifetime. It also prevents packet collisions, overhearing, and excessive retransmission.

Berkeley media access control protocol[74]: The Berkeley media access control (B-MAC) is a protocol that controls low power processing, collision avoidance, and high channel utilisation. Clear channel assessment, packet back off, link layer acknowledgment, low power listening are functioned by B-MAC protocol. It supports the link layer acknowledgement. An acknowledgement packet is sent after receiving a packet by the receiver. An adaptive preamble sampling scheme, such as low power listening (LPL) is used to reduce power consumption. It performs both in awake and sleep period cycling.

Collaborative protocol[75]: This protocol is consisted by Event MAC and network MAC. It can prevent redundant transmission as well as correlation of data at MAC layer. For transmitting data, a single representative sensor node works when the other sensor nodes are back off for a time being. Furthermore, E-MAC protocol filters out correlated packets and N-MAC protocol routes those packets to the sink. After all energy saving, latency and packet drop rate are considered by this CC-MAC.

Power consumes distributed MAC protocol[76]**:** This protocol combines CSMA/CA and multi-channel spread spectrum techniques. In this network, a unique channel and code is assigned across each node's two-hop neighbours. This protocol is used to avoid collisions and minimise energy wastages. It also introduces a low power wake-up radio and normal data radio operation to save energy. Thus, the energy consumption of channel monitoring is significantly reduced.

Traffic adaptive medium access protocol[77]**:** The traffic adaptive medium access protocol (TRAMA) is used to increase channel utilisation and energy efficiency. The nodes start random access mode and transmit the data at random slot. TRAMA consists of three parts – neighbour protocol, schedule exchange protocol, and adaptive election algorithm. To gather neighbour updates, small signalling packets are sent out by NP. Those packets are used to maintain connectivity between the neighbours. At the time of scheduled access, the schedule information is broadcasted by the scheduled access protocol. A schedule is generated by the node after calculating the schedule interval. The last adaptation election algorithm can determine the state of node. To save energy, the nodes are switched to sleep mode.

Z-MAC protocol[78]**:** The Z-MAC is a hybrid MAC protocol that is consisted with high channel utilisation and low latency under high contention. It can combine the strength and enhance the contention resolution of the time division multiple access (TDMA) and carrier sense multiple access (CSMA). It can reduce the collision between two hop neighbours thus limiting cost. This protocol can change time synchronisation failures in the network. For slight assignment and channel reassignment, an efficient and scalable channel scheduling algorithm of this protocol is used. A node can transmit the packet data when the channel is clear. The main objective is to re-use of a slot when the data is not transmitted. To improve timing failures, channel conditions, and slot assignment failures, the CSMA, TDMA and Z-MAC are mixed.

Power reservation-based protocol[79]**:** This protocol is used for the issue of energy conservation and adaptation to traffic. The slot reservation, schedule establishment, and data transmission are functioned by the TDMA-like frame structure. The probability of successful data transmission depends on adopting the TDMA with fixed frame size. Moreover, the frame size will decrease while failure's numbers are small. By increasing throughput the nodes can transmit high data rate.

6.5 Physical layer

The physical layer describes interface for transmitting bit streams using physical communication medium. It can interact with MAC layer and control transmission and reception. The WSN physical layer is used for maximising the network lifetime and minimising the energy consumption. Energy is used to run radio circuitry and to transmit data. The maximum probability of successful transmission depends on different modulation schemes. At present, the researchers are working on low power radio design and power aware transmission schemes[80]. The physical layer design is based on digital communication and existing hardware technology. Interfacing, synchronisation, and multicasting are performed at this layer. A few of the physical layers are described in the following sections.

Schemes of modulation: The energy efficient modulation schemes are used to reduce energy consumption in the following categories.

a) Optimisation[81]: Optimising transmission time and modulation parameters can increase the energy savings. The encoded M-ary quandrature amplitude modulation (M-QAM) and M-ary frequency shift keying (M-FSK) are more efficient than encoded M-FSK. But M-FSK is used in power limited applications as it needs less power than M-QAM**.**

b) Energy-per-useful-bit (EPUB) metric[82]: This modulation scheme is used to compare different physical layers in WSN. The layers which have similar network scenarios, same channel model, average transmission distance, and bit error rate are compared by EPUB. The different costs of the transmitter and receiver are synchronised by this EPUB.

c) Binary and M-ary modulation[83,84]: M-ary modulation uses set of M distinct waveforms to transmit symbol, whereas binary modulation uses two distinct waveforms. Log_2M bits are used per sample and M-ary modulation is better than binary modulation based on energy consumption. Moreover, M-ary frequency shift keying is more efficient than M-ary phase shift keying.

Radio architecture[85]: Low power operations are needed at physical layer for reduced energy consumption. The energy is required for the transmitter and receiver to run their circuitry. The architecture of fractional-N frequency synthesiser with modulator makes the start-up time faster. As a result, the data rate using loop bandwidth increases. Power consumption can be reduced by using this loop bandwidth. On the other hand, WiseNet[86]is used to reduce power consumption and low voltage operations by using duty cycle radio and low power

MAC protocol design. Afterwards, the system runs by different transceiver blocks in a sequence.

Bandwidth specification[80]**:** Narrow band, spread spectrum, and ultra wide band are used as bandwidth of physical layer. The radio band width by the order of symbol rate is used in narrow band. The measurement of data as a bandwidth efficiency is used in narrow band. Spread spectrum can reduce power and communicate effectively. On the other hand, ultra wideband spreads signal over large bandwidth such as GHz. The spread spectrum technologies are better than the narrow band technology. However, both spread spectrum and ultra wideband can save energy.

7.0 Future research contribution issues of WSN

Federated system: A federated sensor network (FSN) is consisted by combining several networks due to maintaining the querying and tracking services. This system can detect the events activity using node from one network to another network. However, there are some problems arise in the FSN. Irregular interval with lost communication and delay in configuring take place in this system.[87]

Mobile devices: The uses of smart phones are increasing day by day. It is user friendly, handy, reliable and smoothly connected. Recently, mobile devices are used for different aspects, such as routing guidance, data collection, processing and distribution. The collected data can be saved in mobile device for further analysis. The mobile sensing unit is used for tracking objects. Mostly it is used to detect people and vehicle in crowded place. To collect data actively, images are taken instantly by the user from the mobile devices. The vibration measurements are also performed by the devices.

Robot networks: Robot networks are the modern invention of WSN systems. It is controlled remotely. It has the ability to act as human being by embedded software system. It is used for different security purposes as well as collecting environmental data. This network is also utilised to detect and recover failure data.[88]

8.0 CONCLUSION

The recent advances in hardware and software have driven the diversified usage of wireless sensor networks for applications that were not practical previously. Wireless sensor networks are widely deployed for monitoring purpose in healthcare, traffic, environment, military, and seismic sensing. To meet the recent practical applications' requirements, new communication protocols, algorithms, designs, and services are developed. Two different categories related to wireless sensor networks have been discussed in this chapter: (1) Internal infrastructure and networking, and (2) communication protocols and its reliability. Communication architectures, operating system, security, and management are other issues highlighted in this chapter. The future prospect of wireless sensor networks depends on availability of low-cost, energy efficient, long-term reliable, scalable, programmable, and fault tolerant wireless sensing system.

References

[1] Simon, G; Maroti, M.; Ledeczi, A.; Balogh, G.; Kusy, B.; Nadas, A.; Pap, G.; Sallai J.; Frampton, K. *Sensor network-based countersniper system*, Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD, 2004.

[2] Castillo-Effen, M.; Quintela, D. H.; Jordan, R.; Westhoff, W.; Moreno, W. *Wireless sensor networks for flash-flood alerting*, Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits, and Systems, Dominican Republic, 2004.

[3] Wener-Allen, G.; Lorincz, K.; Ruiz, M.; Marcillo, O.; Johnson, J.; Lees, J.; Walsh, M. *Deploying a wireless sensor network on an active volcan*; Data-Driven Applications in Sensor Networks (Special Issue), IEEE Internet Computing, March/April 2006.

[4] Gao, T.; Greenspan, D.; Welsh, M.; Juang, R.R.; Alm, A. *Vital signs monitoring and patient tracking over a wireless network*, Proceedings of the 27th IEEE EMBS Annual International Conference, 2005.

[5] Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Computer Networks*. **2008**, 52, 2292-2330.

[6] Fraden, J. *Handbook of modern sensors – Physics, Designs, and Applications,* 3rd ed.; Springer: Newyork, 2003.

[7] Dargie, W.; Poellabauer, C. Fundamentals of Wireless Sensor Networks - Theory and Practice, In *Wiley Series on Wireless Communications and Mobile Computing*, Shen, X, Pan, Y., Eds.; Wiley: London, 2010, P 4.

[8] Diallo, O.; Rodrigues, J.P.C.; Sene, M. Real-time data management on wireless sensor networks: A survey. *Review Article Journal of Network and Computer Applications*. **2012**, 35, 1013-1021.

[9] Mukhopadhyay, S. C.; Gaddam, A.; Gupta, G. S. Wireless Sensors for Home Monitoring - A Review. *Recent Patents on Electrical Engineering.* **2008**, 1, 32-39.

[10] Kahn, J.M.; Katz, R.H.; Pister, K.S.J. *Mobile networking for smart dust,* Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 1999.

[11] Rabaey, J.; Ammer, J.; da Silva, Jr J.L.; Patel, D. *Picoradio: Ad hoc wireless networking of ubiquitous low-energy sensor/monitor nodes,* Proceedings of the IEEE Computer Society Annual Workshop on VLSI, 2000.

[12] Calhoun, B. H.; Daly, D.C.; Verma, N.; Finchelstein, D. F.; Wentzloff, D. D.; Wang, A.; Cho, S. H.; Chandrakasan, A.P. Design considerations for ultralow energy wireless microsensor nodes. *IEEE Transactions on Computers*. **2005**, 54, 727-749.

[13] Marcillo, O.; Allen, G. W.-; Ruiz, M. *Deploying a wireless sensor network on an active volcano,* IEEE Internet Computing, Special Issue on Data-Driven Applications in Sensor Networks, March/April 2006.

[14] Oki, H.; Juang, P.; Wang, Y.; Martonosi, M. *Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet*, ASPLOS-X conference. San Jose, CA., October, 2002.

[15] Sundararajan, V.; Redfern, A.; Schneider, M. Wireless *sensor networks for machinery monitoring*, ASME International Mechanical Engineering Congress and Exposition, (82224), November 2005.

[16] Mainwaring, A.; Polastre, J.; Szewczyk, R.; Culler, D.; Anderson, J. *Wireless sensor networks for habitat monitoring*, In ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'02), Atlanta, GA, September 2002.

[17] Kulkarni, P.; Öztürk, Y. Requirements and design spaces of mobile medical care. *SIGMOBILE Mob. Comput. Commun. Rev*. **2007**, 11, 12-30.

[18] Redondi, A.; Chirico, M.; Borsani, L.; Cesana, M.; Tagliasacchi, M. An integrated system based on wireless sensor networks for patient monitoring, localization and tracking. *Original Research Article Ad Hoc Networks*. **2013**, 11, 39-53.

[19] He, T.; Krishnamurthy, S.; Stankovic, J.; Abdelzaher, T.; Luo, L.; Yan, T.; Stoleru, R.; Gu, L.; Zhou, G.; Hui, J.; Krogh, B. VigilNet: An Integrated Sensor Network System for Energy Efficient Surveillance. *ACM Transactions on Sensor Networks*. **2006**, 2, 1-38.

[20] He, T.; Vicaire, P.; Yan, T.; Cao, Q.; Luo, L.; Gu, L.; Zhou, G.; Stankovic, J.; Abdelzaher, T. *Achieving Long Term Surveillance in VigilNet*, Infocom, April 2006.

[21] Culler, D.; Estrin, D.; Srivastava, M. Overview of sensor networks. *IEEE Computer Magazine*, August 2004, pp 41-49.

[22] Chen, X; Zhang, J.; Qian, S.; Xu, P. Applied Research on Traffic Information Collection Based on Wireless Sensor Networks. *Energy Procedia*. **2012**, 17, Part A, 602-606.

[23] Endo, S.; Ukawa, H.; Sanda, K.; Kitagawa, A. Simulation of speed control in acceleration mode of a heavy-duty vehicle, *JSAE Review*. **1999**, 20, 81-86.

[24] Herrera, J. C.; Work, D. B.; Herring, R; Ban, X.; Jacobson, Q.; Bayen, A. M. Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment. *Original Research Article Transportation Research Part C: Emerging Technologies*. **2010**, 18, 568-583.

[25] Ullah, S.; Zhong, Y.; Islam, R.; Nessa, A.; Kwak, K. S. *Throughput Limits of IEEE 802.11 and IEEE 802.15.3*, October 12-14, 2008, Incheon, South Korea, pp 1-4.

[26] Howitt, I.; Gutierrez, J. A. *IEEE802.15.4 low rate-wireless personal area network coexistence issues Wireless Communications and Networking*, 2003, 3, pp 1481–1486.

[27] Wireless control that simply works, ZigBee StandardsOverview. http://www.freescale.com/webapp/sps/site/overview.jsp?nodeId=01J4Fs25657725 (accessed November 10, 2010)

[28] Mulligan, G.; Group, L.W. *The 6LoWPAN architecture*, Proceedings of the EmNets, Cork, Ireland, 2007.

[29] Montenegro, G.; Kushalnagar, N.; Hui, J.; Culler, D. *Transmission of IPv6 packets over IEEE 802.15.4 networks*, Network Working Group, RFC-4944, 2007.

[30] Wibree. http://www.wibree.com/ (accessed January 18, 2011)

[31] WirelessHART specification. http://www.controleng.com/article/CA6427951.html (accessed November 12, 2010)

[32] ISA100.11a. http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891 (accessed October 12, 2010)

[33] Newsome, J.; Song, D. *GEM: Graph EMbedding for routing and data-centric storage in sensor networks without geographic information*, Proceedings of the Sensys'03, San Diego, CA, 2003.

[34] Ganesan, D.; Greenstein, B.; Perelyubskiy, D.; Estrin, D.; Heidemann, J. *An evaluation of multi-resolution storage for sensor networks*, Proceedings of the Sensys'03, Los Angeles, CA, 2003.

[35] Desnoyers, P.; Ganesan, D.; Shenoy, P. *TSAR: a two tier sensor storage architecture using interval skip graphs*, Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[36] Maroti, M.; Kusy, B.; Balogh, G.; Volgyesi, P.; Nadas, A.; Molnar, K.; Dora, S.; Ledeczi, A. *Radio interferometric geolocation*, Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[37] Srinivasan, A.; Wu, J. A survey on secure localization in wireless sensor networks. In *Wireless and Mobile Communications*, Furht, B., Ed.; CRC Press/Taylor and Francis Group: Boca Raton/London, 2007.

[38] Lazos, L.; Poovendran, R. *SeRLoc: secure range independent localization for wireless sensor networks*, First IEEE International Conference on Mobile Ad hoc and Sensor Systems, Fort Lauderdale, FL, 2004.

[39] Liu, D.; Ning, P.; Du, W. *Detecting malicious beacon nodes for secure location discovery in wireless sensor networks,* Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDC'05), 2005.

[40] Srinivasan, A.; Teitelbaum, J.; Wu, J. *DRBTS: Distributed reputation-based beacon trust system*, Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), 2006, pp 277–283.

[41] Capkun, S.; Hubaux, J.-P. *Secure positioning of wireless devices with application to sensor networks*,Proceedings of the IEEE INFOCOM'05, 2005.

[42] Lazos, L.; Poovendran, R.; Capkun, S. *ROPE: robust position estimation in wireless sensor networks*, Proceedings of the IPSN'05, 2005.

[43] Stoleru, R.; He, T.; Stankovic, J. A.; Luebke, D. *A high-accuracy, low-cost localization system for wireless sensor networks*, Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[44] Priyantha, N.B.; Balakrishnan, H.; Demaine, E. D.; Teller, S. *Mobile-assisted localization in wireless sensor networks*, Proceedings of the IEEE INFOCOM, Miami, FL, 2005.

[45] Moore, D.; Leonard, J.; Rus, D.; Teller, S. *Robust distributed network localization with noisy range measurements*, Proceedings of the Sensys'04, San Diego, CA, 2004.

[46] Liu, F.; Rivera, M. J. M.; Cheng, X.; *Location-aware key establishment in wireless sensor networks,* Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC), Vancouver, Canada, 2006.

[47] Wacker, A.; Knoll, M.; Heiber, T.; Rothermel, K. *A new approach for establishing pairwise keys for securing wireless sensor networks*, Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[48] Karlof, C.; Sastry, N.; Wagner, D. *TinySec: a link layer security architecture for wireless sensor networks*, Proceedings of the Sensys'04, Baltimore, MD, 2004.

[49] Yan, T.; He, T.; Stankovic, J. A. *Differentiated surveillance for sensor networks,* Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

[50] Veltri, G.; Huang, Q.; Qu, G.; Potkonjak, M. *Minimal and maximal exposure path algorithms for wireless embedded sensor networks,* Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

[51] Wang, X.; Xing, G.; Zhang, Y.; Lu, C.; Pless, R.; Gill, C. *Integrated coverage and connectivity configuration in wireless sensor networks*, Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

[52] Chen, B.; Jamieson, K.; Balakrishnan, H.; Morris, R. *Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks,* Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, 2001.

[53] Ganeriwal, S.; Kumar, R.; Srivastava, M. B. *Timing-sync protocol for sensor networks,* Proceedings of the Sensys'03, Los Angeles, CA, 2003.

[54] Lucarelli, D.; Wang, I.-J. *Decentralized synchronization protocols with nearest neighbor communication*, Proceedings of the Sensys'04, Baltimore, MD, 2004.

[55] Ganeriwal, S.; Ganesan, D.; Shim, H.; Tsiatsis, V.; Srivastava, B. *Estimating clock uncertainty for efficient duty-cycling in sensor networks*, Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[56] Allen, G. -W.; Tewari, G.; Patel, A.; Welsh, M.; Nagpal, R. *Firefly-inspired sensor network synchronicity with realistic radio effects,* Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[57] Dai, H.; Han, R. *TSync: a lightweight bidirectional time synchronization service for wireless sensor networks ACM SIGMOBILE*, Mobile Computing and Communications Review, January 2004, pp 125–139.

[58] Li, Q.; Rus, D.; *Global clock synchronization in sensor networks*, Proceedings of the INFOCOM, 2004, pp 564–574.

[59] Rentel, C. H.; Kunz, T. *A clock-sampling mutual network synchronization algorithm for wireless ad hoc networks*, Proceedings of the IEEE Wireless Communications and Networking Conference, 2005.

[60] Akyildiz, I. F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: a survey. *Original Research Article Computer Networks*. **2002**, 38, 393-422.

[61] Shen, C.; Srisathapornphat, C.; Jaikaeo, C. Sensor information networking architecture and applications. *IEEE personal Communications*. **2001**, 52–59.

[62] Wan, C.-Y.; Eisenman, S. B.; Campbell, A. T. *CODA: Congestion detection and avoidance in sensor networks*, Proceedings of the Sensys, 2003.

[63] Iyer, Y. G.; Gandham, S.; Venkatesan, S. *STCP: a generic transport layer protocol for wireless sensor networks*, Proceedings of the 14th IEEE International Conference on Computer Communications and Networks, San Diego, CA, 2005.

[64] Gungor, V. C.; Akan, O. B. *DST: Delay sensitive transport in wireless sensor networks*, Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN), 2006, pp 116–122.

[65] Zhou, Y.; Lyu, M. R. *PORT: a price-oriented reliable transport protocol for wireless sensor network*, Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering (ISSRE), Chicago, IL, 2005.

[66] Sankarasubramaniam, Y.; Akan, O. B.; Akyilidiz, I. F. *ESRT: event-to-sink reliable transport in wireless sensor networks*, Proceedings of the MobiHoc, Annapolis, MD, 2003

[67] Park, S.-J.; Vedantham, R.; Sivakumar, R.; Akyildiz, I. F. *A scalable approach for reliable downstream data delivery in wireless sensor networks*, Proceedings of the ACM MobiHoc'04, Roppongi, Japan, 2004.

[68] Wan, C.-Y.; Campbell, A.T.; Krishnamurthy, L. *PSFQ: a reliable transport protocol for wireless sensor*, Proceedings of the 1st ACM International workshop on Wireless Sensor Networks and Applications, 2002, pp 1–11.

[69] Ye, F,; Zhong, G.; Cheng, J.; Lu, S.; Zhang, L. *PEAS: A robust energy conserving protocol for long-lived sensor networks.* In Proceedings of the Twenty-Third International Conference on Distributed Computing Systems (ICDCS), 2003.

[70] Du, X.; Xiao, Y.; Chen, H.-H.; Wu, Q. Secure cell relay routing protocol for sensor networks. *Wireless Communications and Mobile Computing*. **2006**, 6, 375–391.

[71] Yin, J.; Madria, S. *SecRout: a secure routing protocol for sensor networks*, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), Vienna, Austria, 2006.

[72] Zhang, R.; Zhao, H.; Labrador, M. A. *The anchor location service (ALS) protocol for large-scale wireless sensor networks*, Proceedings of the First International on Integrated Internet Ad hoc and Sensor Networks, Nice, France, 2006.

[73] Ganti, R. K.; Jayachandran, P.; Luo, H.; Abdelzaher, T. F. *Datalink streaming in wireless sensor networks*, Proceedings of the Sensys'06, Boulder, CO, 2006.

[74] Polastre, J.; Hill, J.; Culler, D. *Versatile low power media access for wireless sensor networks*, Proceedings of the Sensys'04, San Diego, CA, 2004.

[75] Vuran, M. C.; Akyildiz, I. F. Spatial correlation-based collaborative medium access control in wireless sensor networks. *IEEE/ACM Transactions on Networking*. **2006**, 14, 316-329.

[76] Guo, C.; Zhong, L. C.; Rabaey, J. M. *Low power distributed MAC for ad hoc sensor radio networks*, Proceedings of the IEEE Globecom, 2001, pp 2944-2948.

[77] Rajendran, V.; Obraczka, K.; Garcia-Luna-Aceves, J. J. *Energy-efficient, collision-free medium access control for wireless sensor networks*, Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

[78] Dubois-Ferriere, H.; Estrin, D.; Vetterli, M. *Packet combining in sensor networks,* Proceedings of the Sensys'05, San Diego, CA, 2005.

[79] Mishra, S.; Nasipuri, A. *An adaptive low power reservation based MAC protocol for wireless sensor networks,* Proceedings of the IEEE International Conference on Performance Computing and Communications, 2004, pp 316–329.

[80] Ganeriwal, S.; Ganesan, D.; Shim, H.; Tsiatsis, V.; Srivastava, B. *Estimating clock uncertainty for efficient duty-cycling in sensor networks*, Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, 2005.

[81] Cui, S.; Goldsmith, A. J.; Bahai, A. Energy-constrained modulation optimization. *IEEE Transactions on Wireless Communications*. **2005**, 4, 2349-2360.

[82] Ammer, J.; Rabaey, J. *The energy-per-useful-bit metric for evaluating and optimizing sensor network physical layers*, Proceedings of the IWWAN'06, 2006.

[83] Wang, A.Y.; Cho, S.; Sodini, C. G.; Chandrakasan, A. P. *Energy efficient modulation and MAC for asymmetric RF microsensor systems*, Proceedings of the ISLPED'01, Huntington Beach, CA, 2001.

[84] Shih, E.; Cho, S. -H.; Ickes, N.; Min, R.; Sinha, A.; Wang, A; Chandrakasan, A. *Physical layer driven protocol and algorithm design for energy efficient wireless sensor networks,* ACM SIGMOBILE, Rome, Italy, 2001.

[85] Wang, A. Y.; Cho, S.; Sodini, C. G.; Chandrakasan, A. P. *Energy efficient modulation and MAC for asymmetric RF microsensor systems*, Proceedings of the ISLPED'01, Huntington Beach, CA, 2001.

[86] Enz, C. C.; El-Hoiydi, A.; Decotignia, J. -D.; Peiris, V. WiseNET: an ultralow-power wireless sensor network solution. *Computer*. **2004**, 37, pp 62-70.

[87] Demirbas, M.; Can, Z. *Investigation of querying techniques for federated sensor networks,* in: 7th International Wireless Communications and Mobile Computing Conference (IWCMC), 2011.

[88] Mei, Y.; Xian, C.; Das, S.; Hu, Y.; Lu, Y.-H. *Replacing failed sensor nodes by mobile robots*, in: 26th IEEE International Conference on Distributed Computing Systems, 2006.