CHAPTER 1

INTRODUCTION

1.1. HEALTH MONITORING OF ELECTRICAL SYSTEM

The increasing electricity demand, together with the complex and nonlinear nature of the electric power generation, transmission and distribution network, have caused the need for including wind, solar etc. renewable energy resources into existing power grid to reduce power demand and congestion issues. The network congestion and safety-related factors, the overstressed situation in the existing power grid requires *pervasive systems*. The role of pervasive systems is for effective communications, system monitoring, fault diagnostics, and automation to reduce the possibility of region-wide grid system breakdown initiated by system malfunctioning due to overload or stress impacts or due to equipment (like Transformers, Circuit Breakers, Insulators etc) fault.

In this respect, the intelligent low-cost monitoring and control enabled by suitable sensors interfaced to embedded microcontrollers supported by special operating system, communication transceivers that are protocol supportive called *sensor motes* have become essential to maintain safety, reliability, efficiency and uptime into the network , with the application being based on *wireless sensor networking(WSN).* The impact of electrical equipment failures due to overload or capacity limitations, natural accidents or catastrophes, which would cause largely any power disturbances and outages, can be avoided by smart way of power system condition

monitoring with diagnostics using special configurations of WSN called *Wireless Personal Area Networks (WPAN for smart grid based on the IEEE 802.15.4 standard).*

1.1.1. Monitoring the Electrical Grid

Sensors based on the embedded processors operating as nodes in the WPAN need to monitor the Electrical and nonelectrical signals of Equipments of the Grid shown in the Figure 1.1, like

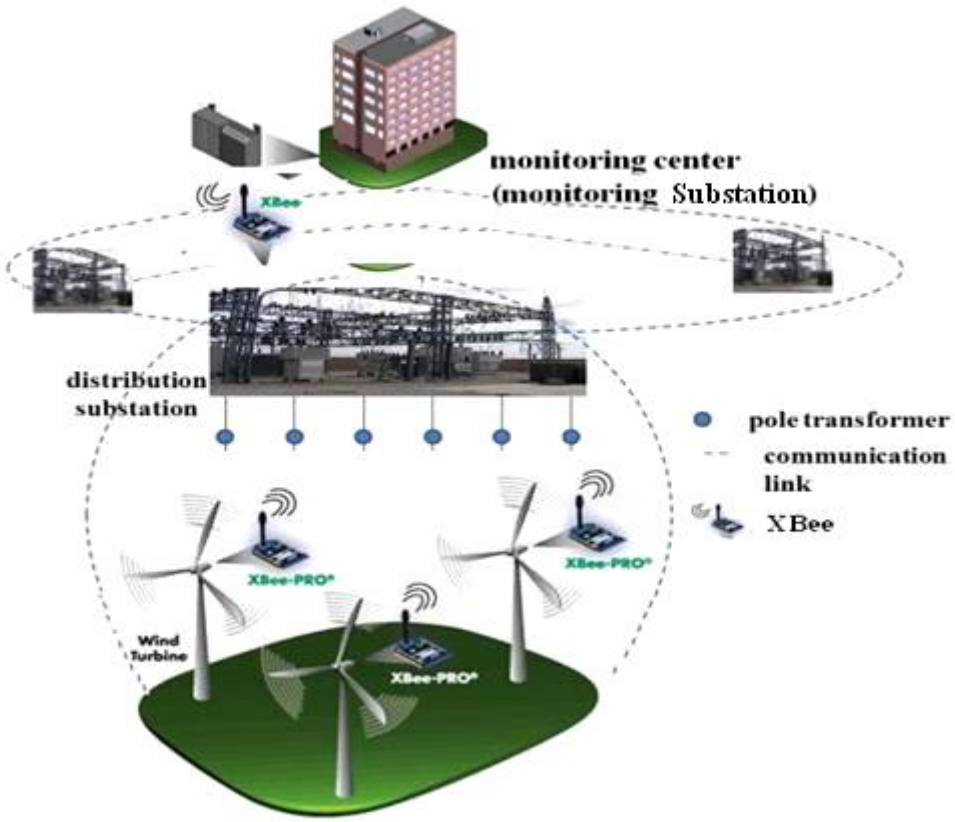

Figure 1.1 Wireless Personal Area Network (WPAN) for Electrical Grid Monitoring (Smart Energy Monitoring)

- temperature of a operating equipment
- supply and the operating frequency
- fundamental frequency upto say 21st harmonics

- power factor and Total Harmonic Distortion
- RMS/DC offset value of voltage
- RMS/DC offset value of current
- Noise in voltage or current or the high frequency noise
- Types of fault Event like short circuits, open circuits
- event time stamping

1.1.1.1. Introduction to wireless sensor network

Wireless Sensor Network (WSN) is a sub-class of wireless Ad hoc Networks that are randomly deployed in the physical environment in which small, low-power, light weight, inexpensive wireless sensor nodes deployed in large numbers to monitor the environment or health of the system by measuring the physical parameters such as temperature, light intensity etc.

A Wireless Sensor Network (Akyildiz et al 2002) is a collection of randomly distributed devices integrated with sensor module, processing module, power provision module and wireless communication module which is shown in Figure 1.2. The sensor module includes various types of sensor and analog to digital converters which senses the environment or physical parameters of the system. The processing module has a processor with memory which performs computations on the sensed data. The wireless communication module has a transceiver which connects the node to the network and exchanges the message with the neighbouring nodes. The battery powered (eg. Alkaline AA battery, Li-ion AA battery) supply is used as power provision module. The wireless sensor devices are also called ‘smart dust’, because of its size.

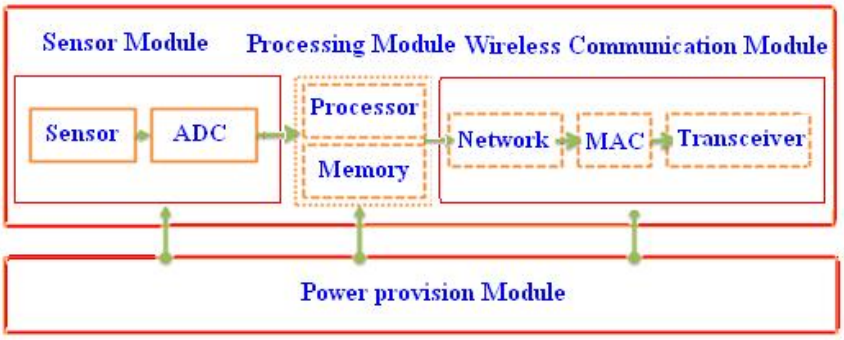

Figure 1.2 Functional Block Diagram of Wireless Sensor Node

Generally, wireless ad hoc networking techniques are used in wireless sensor network applications, even though, many proposed protocols in the literature for traditional wireless ad hoc networks are not well suited for the application requirements of wireless sensor networks. Some of the differences between the wireless sensor networks and wireless ad hoc network are addressed here.

- Wireless Ad hoc network is a self-configuring infrastructure-less network of devices connected by wireless and the network topology is not predictable. The WSN has common network topologies like star, mesh, tree etc.
- Hundreds to thousands of nodes are deployed in wireless sensor network which are higher than the nodes in wireless ad hoc networks.
- Sensor nodes are densely deployed in WSN. WSN adopts frequent topology changes and it mainly uses the broadcast communication, whereas wireless ad hoc networks use point-to-point communication.
- The main goal of WSN is not only just communication; it is also used for detection of event interest, data fusion or data aggregation. WSN can do In network data processing, but Ad-hoc network cannot do so.

The increased adoption of wireless sensor network and its applications across the world is due to some reasons like ease of implementation, ability to operate in harsh environments, used in unmanned region, easy troubleshooting and high levels of performance.

1.1.1.2. Overview of WPAN

The WPAN is a communication network variable in its organization due to variation in:

- Size of the network in terms of the number and organization of nodes in network.
- Constraints like Channel Allocation, Bandwidth utilization, energy capacity etc.
- Type of routing protocol adopted for forwarding the data across the nodes.
- Security criteria like data or route security specific to the electrical grid.
- The application for which it is deployed like whether for structural, or for environmental or for system health monitoring etc.

1.1.1.3. Role of sensor node in WSN

Depending on the design of protocols and algorithms, the sensor nodes in the network are configured to perform as various roles, based on their responsibilities. The various configurations of sensor node are:

- **Source Node:** A Sensor node which provides required information or data to the network. This Thesis configured source node as End device which contains Temp, Hall Effect sensor etc. and is connected to the Electrical System.
- **Router**: A router is a node that forwards data packets between two nodes. In this Thesis, the router nodes are deployed between sink and base station.
- **Gateway:** It is a node that serves as entrance to another network. It means that it can forward the information or data outside the network. This node is configured to perform channel switching algorithm.
- **Sink**: A node that required information is called sink node. Sink node might be a node in the sensor network or outside of the network. Sink node in this Thesis configured for interference Minimization
- **Coordinator:** It is Full-Function Device (FFD) which allows the node to talk to any other device.
- **Base Station:** The base station is a Central Supervisory System and has one or more components of the WSN with high computational, energy and communication resources.

1.2. WIRELESS COMMUNICATION STANDARDS

Different methods and standards of wireless communication have developed based on various requirements. Based on their communication range and their specific application, the wireless standards can be classified into four individual categories such as Wide Area Networks (WAN), Metropolitan Access Network (MAN), Local Area Network (LAN) and Personal Area Network (PAN) and are shown in the Figure 1.3. Some of the available wireless standards (Cooklev 2011) are discussed in the following sub sections.

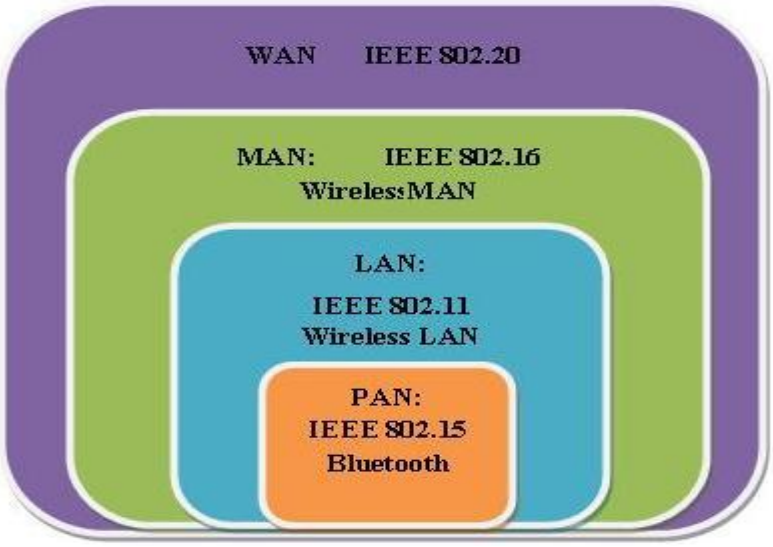

Figure 1.3 Wireless Communication Standards

1.2.1. IEEE 802.20

IEEE 802.20 is a standard (IEEE standards information) which is developed for Mobile Broadband Wireless Access (MBWA). The main features of this standard include

- Air-interface specification of PHY layers and MAC layers for interoperable MBWAs.
- Operates in frequency bands below 3.5 GHz.
- Optimized for IP-data transport provides access capability for various vehicular mobility classes.
- Supports various vehicular mobility classes.
- Peak data rates of 80 Mbps.

1.2.2. IEEE 802.16

IEEE 802.16 is a standard for the fixed and mobile broadband wireless metropolitan networks which use a one-to-many architecture and are commonly referred to as WiMAX or Wireless MAN (WMAN).

- The bandwidth specification has two frequency ranges between 10GHz and 66GHz, 2GHZ and 11GHz.
- It defines Medium Access Control (MAC) layer which supports multiple physical layer specifications for these frequency range.
- It supports very high bit rates, such as data rates of 100 Mbps for mobile and 1Gbit/s for fixed.
- Transmission range up to 30 miles.

1.2.3. IEE 802.11

IEEE 802.11 and IEEE 802.11x refer to a family of specifications developed for Wireless Local Area Network (WLAN) technology. It has the following specifications

- Maximum raw data rate of 11 Mbps.
- Operating frequency range of 2.4 GHz.
- Devices operating in 2.4 GHz include Bluetooth devices, cordless telephones and some amateur radio equipment.

1.2.4. IEEE 802.15

IEEE 802.15 is a standard which specifies the Wireless Personal Area Network (WPAN) standards. It includes Bluetooth, Body Area Network, mesh networking Low-Rate PAN, High-Rate PAN etc. IEEE 802.15.1 is the

standard which specifies Bluetooth/WPAN and it can communicate with maximum seven devices and IEEE 802.15.4 is the MAC layer and PHY layer specifications for Low-Rate Wireless Personal Area Network (LR-WPAN) that can communicate with many number of devices.

1.2.4.1. IEEE 802.15.4

ZigBee protocol over *IEEE 802.15.4* defines the protocol and interconnection of devices via radio communication in a personal area network (PAN) and also defines the specifications for Low-Rate WPAN for supporting simple devices that consume less power and operate in small distance. This protocol provides self-organized mesh networking with long battery lifetime (Lee 2006). A Full-Function Device (FFD) and a Reduced Function Device (RFD) are the two different device types that can participate in an LR-WPAN. The FFD can serve as a coordinator, or a device and it operates with complete protocol set. The FFD can talk to other FFDs or RFDs, whereas RFD can talk only to an FFD and it operates with the reduced protocol set. An RFD is an end device for applications that are extremely simple, such as a temperature sensor. The Zigbee / IEEE 802.15.4 (Krishnamachari 2005) supports four types of topologies such as star topology, peer-peer topology, mesh topology and cluster topology.

The LR-WPAN device comprises of PHY layer and MAC sub-layer. The PHY layer includes the radio frequency (RF) transceiver and MAC sub-layer which provides access to the physical channel for all types of transmission. The upper layer, which is above the MAC sub-layer, consists of network layer and application layer. The network layer provides network configuration, network management and routing protocol. The application layer provides intended function of the devices. The definition and specification of these layers are not included in the scope of the IEE80.15.4 standard.

1.3. CHALLENGES IN WSN

Wireless sensor network has a number of serious challenges due to the following reasons:

Limited Energy Source: Sensor nodes are operated on battery power, which in many cases cannot be replaced or recharged. Hence, energy efficient communication protocols need to be designed by considering the available energy which is the major constraint. Efficiently harvesting, converting and storing energy is also the most efficient way for proper utilization of resources.

Wireless Connectivity: Wireless connectivity is an important challenge which is unpredictable in both indoor and outdoor environments. The wireless connectivity in the indoor environments is more affected by the interference rather than the outdoor environments when low power RF transceivers are used.

Proper Bandwidth Utilization: Due to noisy environment and obstruction, wireless link shows the varying characteristics over time and space. Hence, the location based proper utilization of the bandwidth and channel selection algorithm has to be developed.

Security: Secured transmission of the data is one of the research challenges in WSN. The node that transmits information is to be authenticated, and also to verify the receiver node, which receives the information is an intended receiver. The information or data security can be achieved by using various data encryption schemes. The proper design of encryption algorithm helps to make the data transmission more reliable and secured.

Limited Computation Capability: Sensors have embedded processors with limited memory and computation capabilities. However, resources are all limited; there is a need to use the limited computation ability. The main challenge is to design efficient distributed algorithms for wireless sensor networks that have minimum computation abilities.

1.4. APPLICATIONS OF WIRELESS SENSOR NETWORKS

Wireless sensor networks are used in various real time applications such as Home automation, Security and Military surveillance, Acoustic detection, Seismic detection etc. Some of the applications of WSNs are:

Environmental Monitoring: Environmental monitoring is a common application of WSNs. In environmental monitoring, some phenomenon is to be monitored by deploying the WSN over a region.

Healthcare Monitoring: Wireless Sensor Networks are used for body position measurement and location identification of the person, overall patients' monitoring in hospital or at home. Monitoring the elderly people is also an important WSN application. Body sensor networks can collect information about an individual person's health, energy expenditure etc.

Industrial Monitoring: In industries, wireless sensor networks are used for monitoring the health condition of a machine or system which is one of the emerging applications of WSN. Significant cost savings can be obtained by using WSN for monitoring machine or system.

Structural Health Monitoring: Wireless sensor networks can be used to monitor the condition of infrastructure of the buildings. Nowadays, WSN are commonly used to monitor the health condition of the bridges. They are also used for data logging, using appropriately interfaced sensors.

1.5. RESEARCH MOTIVATION

The unique features of Wireless Personal Area Networks (WPAN) for smart grid applications are a promising platform for remote implementations of energy monitoring and fault diagnostic in electrical systems with dependence on energy efficient and reliable communication protocol capabilities configured onto the deployed sensor nodes of the network. WPANs have revolutionized the field of data communication with security. It offers unique advantages and has extensive applications. Still, it has certain challenges and limitation that must be overcome to achieve the best services of the network.

The battery is only the energy source for the sensor nodes which are deployed in a network. Once the sensor nodes are deployed, it is difficult to recharge or replace the battery of the sensor node, if it is deployed in the remote or unmanned region. Developing techniques to enhance the lifetime of the network and secured data transmission are the main focuses of the current research work. Different energy saving methodologies and data security mechanisms are discussed in the literature to extend the life of the battery and secured communication. The reduction of energy consumption can be achieved by efficient routing protocol design, hardware design etc. Generally, the sensor node consumes energy during various states such as sensing, listening, idle, transmission and reception. Among all these states, the node consumes more energy during data transmission; it is an obvious area of focus for energy conservation research.

Data security can be achieved by designing various encryption algorithms. Efficient energy conservation algorithm with secured data transmission is crucial in WSN. Hence there exists excellent opportunities to develop an event-driven based energy efficient multipath routing protocol to limit the amount of data to be transmitted and the pattern based encryption

algorithm to achieve data security. Thus energy efficient scheme with secured data transmission is developed for online remote monitoring of the electrical system. This Thesis is focused to develop the load balanced multipath routing algorithm with pattern based data security technique for health monitoring of electrical systems.

1.6. GOAL OF THE THESIS

The goal of this Thesis is to Research into:

- Design of a reliable WPAN algorithms (applicable for System Health monitoring of power grid) to provide high data delivery quality with the least cost of communication system installation and maintenance.
- Develop protocols suitably to enrich the Power awareness for extended Life Time of the WPAN sensor nodes which are meant for the Smart Grid (application related to power quality and equipment Health monitoring information relevant to the Grid) where it is deployed.
- Sensor signals observed by sensor nodes placed on pole transformers or other equipments require remote monitoring to inform power substations on the power quality and equipment health condition information periodically. The WPAN deployment requires the application developer/user to configure its nodes for functions as signal capture/measure and forward/ transmit to the monitoring centers that would generally be power grid substations.
- To improve the performance in terms of the data delivery rate and the distribution delay of the power quality data, the

algorithms and protocols need to be developed as customized communication protocol adoptable for the distribution pattern of the power quality information with higher data delivery rate in a timely and reliable manner.

- The concepts need to be validated though simulations and experiments for performance analysis on the feasibility of the designed system for Smart Grid Applications.

1.7. LITERATURE SURVEY

As stated by Lu & Gungor (2009), the energy efficiency of the induction motor was monitored using WSN. The motor terminal data such as voltage and current data were collected at the Motor Control Centre (MCC) and wirelessly communicated to the Central Supervisory System (CSS), and then it was processed in CSS. The author also discussed that the data was processed by the sensor node and the processed result as 'fault alarums' were only transmitted to the CSS. The noise and inference level during transmission was analyzed. Though the transmission of fault alarms minimizes the transmission energy, the nature of the fault or criticality of the occurred event is not addressed in this literature. It is an important parameter of the event-based communication, because depending on the critical level of the event, the action has to be taken in advance to avoid the accidents. The proper designing of the routing protocols also decrease the energy consumption of the node thereby, the lifetime of the network has to be increased.

Bouabdallah et al (2009) presented the continuous monitoring using event-driven reporting approach (CM-EDR). The author used the existing protocol such as Low Energy Adaptive Clustering Hierarchy (LEACH), Hybrid Energy-Efficient Distributed (HEED) clustering for event-driven

algorithm. The Contention based MAC protocol and Carrier-Sense Multiple Access (CSMA) were considered for the comparison of the cluster based and unscheduled architectures. The cluster head received the data only when an event occurred. The predefined sleep period has been allotted for cluster head. During sleep time of cluster head, the cluster member could be directly communicated to the sink. The system was analyzed using Markov process and the analytical model for the energy consumption and latency metrics were found.

Gungor et al (2010) discussed the challenges of WSN in Smart Grid applications. The monitoring of the substation, indoor power room and underground transformer vault have been done by using Tmote Sky nodes. The effect of noise interference and link quality of the signal were analysed but data transmission scheme or algorithm was not addressed in this literature.

Efficient Event Detecting protocol (EEDP) for event monitoring applications was discussed by Liang et al (2012). When an event occurred, only one single alarm packet was transmitted by EEDP. Even though EEDP minimizes the transmission energy by transmitting a single packet, the alarm packet did not have the information about the nature of the event like criticality, type of the event or fault etc. This Thesis proposes the criticality based event driven reporting approach with proper channel assignment algorithm for improving the latency and minimizing the transmission energy.

Nasirudin et al (2011) also discussed the event-driven algorithm using WSN for monitoring the quality of the fresh water. The GSM network was used for transmission between the node and the network coordinator.

The tree-based data forwarding protocol used for power quality monitoring was discussed by Lim et al (2010). Time scheduling based communication system had been designed for power quality monitoring. The

power quality data was measured for every one second but transmitted to the processing centre during every time interval. It examined the performance tradeoffs between the data delivery rate and the distribution delay of the power quality data. However, the time scheduling based communication system is unsuitable for event monitoring algorithm. One more limitation found in this literature is network traffic and congestion based communication which was not addressed.

The tree based multichannel scheme called TMCP for data collection was stated by Wu et al (2008). The fixed channel assignment algorithm was used for assigning channels to sub tree. Good link qualities with non-adjacent channel have been selected for data collection when two nodes sampled the link quality at a time. The author concluded that the time synchronization was not required because it used the minimum number of channels of IEEE 802.11. TMCP used Greedy algorithm for channel selection. The greedy algorithm always selects the good link-quality channel. One shortcoming found in TMCP is, the highest link-quality channel is frequently selected for data collection.

Time schedule based multi channel protocol called MC-LMAC was addressed by Hoesel (2007) and discussed by Incel (2011). MC-LMAC assigned timeslots for each node to access the medium for transmission. Time slot was divided into two periods, control period and data transmission period. Destination notification during data transmission could be obtained by using control period. Channel switching, joining of new nodes to the network were addressed in MC-LMAC. The synchronization can easily be maintained because of time scheduling, which is an advantage of MC-LMAC. On the other hand, when number of channels are large, the exchange of control message before data transmission causes increase in latency. When two neighbour nodes, which are operated on two different channels, try to

communicate with a node in the same time slot, only one neighbour can communicate. One more shortcoming is the time slot based channel allocation is not suitable for all applications like Event based applications.

The performance analysis of cluster-based WSNs based on LEACH protocol for different communication patterns have been carried out by Malik et al (2009). Event-driven communication models and continuous communication models were considered for performance analysis of the network. The analysis was carried out based on the ratio of the event area to sensing area. Three possibilities of the cluster position in the network such as Cluster fully confined within the Event Field, Cluster located outside the Event Field, Cluster partially confined within the Event Field were considered in case of event communication. In continuous communication model, the sensed value was reported to the Cluster Head (CH) in periodic intervals. The drawback of this algorithm is, the CH selection is based on the frames value. This means that the CH selection is random in nature.

The energy utilization and network lifetime for LEACH protocol based cluster sensor networks have been analyzed by Malik & Qureshi (2010). LEACH Protocol does not have any control over the distribution of CHs in the network. The total number of CHs for every round varied immensely. The unequal size of clusters was formed in LEACH. Thus the energy utilization of the node in the network was unbalanced. In LEACH some of the cluster-heads may be very close to each other thereby inefficient cluster head degrade the energy efficiency because LEACH depends on energy probability model for CH selection.

Kumar et al (2011) proposed cluster formation and cluster head selection in the distributed hierarchical clustering environment using fuzzy search algorithm. CH selection was done using Fuzzy Logic with three variables- battery level of node, node density and distance from base station.

The performance metric like data collection and energy consumption were analyzed. This algorithm was proposed for mobile network.

Shu et al (2010) developed the mechanisms for generating randomized multipath routes. The packets were divided into shares and transmitted over different routes. It is a secured multipath routing protocol because it could not be possible to find the routes of each packet even if the routes were known to the adversary. Even this algorithm had been designed for secured data communication, it will face the increased packet delay as packets are shared and transmitted over different routes. This Thesis proposed the optimized multipath routing with pattern based security algorithm for reduced delay and improved load balancing.

A Multipath Routing Protocol (MRP) based on dynamic clustering and Ant Colony Optimization (ACO) algorithm was proposed by Yang et al (2010). The Cluster Head (CH) was selected in the event area based on the residual energy. Multiple paths were obtained by using improved ACO algorithm. The route was dynamically selected for CH to transmit data. Dynamic clustering with ACO algorithm improves the load balancing and reducing the energy consumption. But the performance metric of the network can further be improved by using optimized multipath routing which is explained in this Thesis.

The security scheme proposed by Merhav (2013) used the finite-state encryptability of an individual plain-text sequence that guaranteed the perfect secrecy. It considered the encryption of individual sequences. The author adopted a model of a Finite-State Encrypter (FSE), which received the plain-text and the secret key bit stream as inputs, for cipher text generation. The result of this scheme showed that finite-state encryptability is equal to the finite-state compressibility. However, this secret scheme required higher processing energy because of the finite state encryption. This shortcoming is

overcome by using the pattern based viable key algorithm with less power consumption which is proposed in this Thesis.

1.8. RESEARCH OBJECTIVE

It is observed from the literature that the online system health monitoring using wireless sensor nodes could be possible with significant energy savings. Figure 1.1 shows the health monitoring of the smart grid systems by substation using wireless sensor nodes. The sensed information or event information of wind energy plant is communicated to the substation through XBee transceiver.

This research work is focused towards topology development of the WPAN applicable to electrical grid with secured data transmission using energy efficient routing protocol, for monitoring the health of the system using Wireless communication protocol. Accordingly the specific objectives of this research include:

- Development of *Cluster based Multi-sink topology* with *Multi-channel communication* to minimize packet collision.
- Development of *Fuzzy Logic scheme based Optimizing number of Cluster Head (CH) selection*.
- Design of *Optimized multipath routing* for event-driven application to achieve the network load balancing.
- Design of *Pattern based Viable Key encryption algorithm* for highly secured data transmission.

Thus, the scope of the research work is given in Figure 1.4.

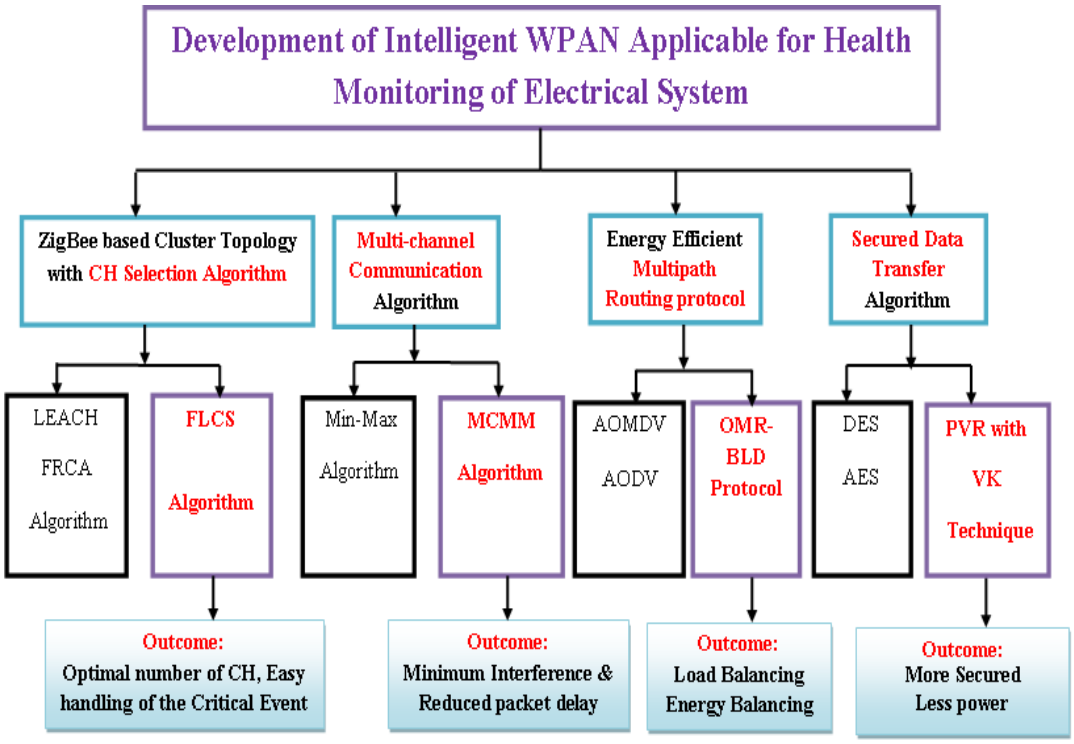

Figure 1.4 Scope of the Research Work

1.9. ORGANIZATION OF THE THESIS

This section provides an overview of the Thesis structure. In Chapter 2, Fuzzy logic based Cluster Head Selection algorithm is proposed to optimize the number of cluster heads. The three criteria considered in this algorithm are used to select the most appropriate node as cluster head candidate. Finally the cluster based network with cluster head (CH) is developed with maximum coverage range. The simulation results show that the network throughput is maximized and the lifetime of the network is increased.

The proper channel allocation for the cluster based network topology and channel switching algorithm for data transmission are discussed in Chapter 3. The Fixed Channel Assignment and proper Channel Switching algorithm are presented for minimization of the channel interference and

packet delay. The channel switching algorithm is also evaluated using *TINY-OS based IRIS mote* implementation and analyzed using *Perytons Analyzer 4.0*, a standard network analyzer.

In Chapter 4, Optimized multipath routing protocol is presented for network load balancing capability. The Modified Intelligent Water Drop optimization algorithm is used for designing the optimized multipath routing protocol. This protocol is simulated using NS2 network simulator and the performance results are compared with standard protocols and the improvement over standard protocols is also presented.

Chapter 5 proposes a novel Pattern Viable Restoration technique based on Viable Key scripts for secure data transmission. The proposed data security technique is simple and requires less processing power. This technique is also evaluated using hardware implementation. The power consumption of this technique is compared with the standard encryption algorithms. Finally, Chapter 6 focuses on the highlights of the work done, summary and conclusions, and the directions for future research.