Chapter - I

Introduction
CHAPTER I

INTRODUCTION

1.1 Introduction

A Wireless Sensor Network (WSN) is a highly distributed network of small wireless nodes deployed in large numbers to monitor the environment or other system by the measurement of physical parameters. Sensor network is defined as being composed of a large number of nodes which are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes collects data and its purpose is to route this information back to a sink. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined [5].

The WSN designs are classified into five classes.

- Fault Tolerance: Individual nodes are prone to unexpected failure with a much higher probability than other types of networks. The network should sustain information dissemination in spite of failures.
- Scalability: Number in the order of hundreds or thousands. Protocols should be able to scale to such high degree and take advantage of the high density of such networks.
- Production Costs: The cost of a single node must be low, much less than one dollar.
- Hardware Constraints: A sensor node is comprised of many subunits (sensing, processing, communication and power, location finding system, power scavenging and mobilizer). All these units combined together and these must consume extremely low power and be containing within an extremely small volume.
- Sensor Network Topology: Must be maintained even with very high node densities.
In this chapter, an introduction to wireless sensor network is explained in section 1.2 and single node architecture is provided in section 1.3. Applications of WSN are discussed briefly in section 1.4 and challenges in wireless sensor network discussed in section 1.5. The benefits of data collection and aggregation are explained in terms of quality improvements in section 1.6 and the motivation of the thesis is briefed in section 1.7. The chapter’s overview is presented in section 1.8.

1.2 Wireless Sensor Network

Wireless Sensor Network (WSN) is spatially distributed autonomous sensors shown in Figure 1.1 to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. It is usually composed of hundreds or thousands of inexpensive, low-powered sensing devices with limited memory, computational, and communication resources [5]. The development of wireless sensor network was motivated by military applications such as battlefield surveillance. Today this kind of networks are using in many industrial and consumer applications, for example its using for industrial process monitoring and control, machine health monitoring, and so on.

![Figure 1.1 Sensor Networks Architecture](image)

WSN usually consist of a large number of sensor nodes, which are battery-powered tiny devices. These devices perform three basic tasks: (i) sampling a physical quantity from the surrounding environment, (ii) processing (and possibly...
storing) the acquired data, and (iii) transferring them through wireless communications to a data collection point which is called sink node or base station.

The WSN application usually requires different functionalities such as sensing, storing data, and data communication. Sensing typically requires a large number of nodes to ensure coverage and a few resources on each node whereas, data transmission and data storage require more system resources. Therefore deploying a homogeneous network tends to result in unnecessarily high cost of the network. Prolonging sensor network lifetime is critical due to the slow improvement of battery capacity and the constraints of sensor physical sizes and cost.

1.3 Single-Node Architecture

A sensor is mote (self-organize) (chiefly in North America), WSN build of nodes [Table 1.1] from a few to several 100 or even 1000. The cost of sensor node is similarly variable, ranging from hundreds of (100) dollars few pennies, depending on the complexity of the individual node [5]. Where in nodes are connected with one or several sensor. Each Sensor network node has several parts

- Radio transceiver
- Antenna
- Micro controller
- Battery
- Embedded energy harvesting

The hardware components shown in Figure 1.2 for a wireless sensor node, evidently the application’s requirements play a decisive factor with regard mostly to size, costs, and energy consumption of the nodes – communication and computation facilities are often considered to be an acceptable quality, but the trade-offs between features and costs is crucial. In some extreme cases, an entire sensor node should be smaller than 1 cc, weight (considerably) less than 100g, be substantially cheaper than one dollar and dissipate less than 100μW.
A basic sensor node comprises of five main components:

- **Controller**: A controller to process all the relevant data, capable of executing arbitrary code.

- **Memory**: Some memory to store programs and intermediate data usually, different types of memory is used for programs and data.

- **Sensors and actuators**: The actual interface to the physical world: devices that can observe or control physical parameters of the environment.

- **Communication**: Turning nodes into a network requires a device for sending and receiving information over a wireless channel.

- **Power supply**: As usually no tethered power supply is available, some forms of batteries are necessary to provide energy. Sometimes, some form of recharging by obtaining energy from the environment is available (e.g. solar cells).
Table 1.1
Sample list of the wireless sensor node

<table>
<thead>
<tr>
<th>Sensor Node Name</th>
<th>Micro Controller</th>
<th>Transceiver</th>
<th>Data Memory</th>
<th>External Memory</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arago system</td>
<td>MSP430F5</td>
<td>CC2520</td>
<td>RAM:16K Bytes</td>
<td>Up to 8 MB</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Flash:256 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arago Wis Mote Mini</td>
<td>ATM EGA 128 RFA2</td>
<td>ATMEGA 128RFA2</td>
<td>RAM:16K Bytes</td>
<td>PROM:4K Bytes</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>flash:128 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tiny node</td>
<td>Texas Instruction MSP43</td>
<td>Semtech Sx1211</td>
<td>8kRAM</td>
<td>512K FLASH</td>
<td>C</td>
</tr>
<tr>
<td>T-Mote sky</td>
<td>Texas Instruction MSP43</td>
<td>250k bits</td>
<td>10k RAM</td>
<td>48K Flash</td>
<td>TinyOS SOS</td>
</tr>
<tr>
<td>Sense node</td>
<td>MSP430 F1611</td>
<td>Chipcon Cc2420</td>
<td>10k RAM</td>
<td>48K Flash</td>
<td>nesC</td>
</tr>
</tbody>
</table>

Sensor node equipped with cameras and Microphonesshown in Table 1.1. The sizeable over heads to each node sending this report to the base station and sending updates whenever new node joins the network. Every node estimates the state of its surroundings in this network, the calculated result are converted into signal.

1.4 Applications of Sensors

Military Applications

Sensor networks are applied very successfully in the military sensing. Now wireless sensor network can be an integral part of military command, control,
communications, computing, intelligence, surveillance, reconnaissance and targeting systems. There are two example important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defence Advanced Research Project Agency (DARPA)is applied very successfully in the Military sensing Environmental [5].

- **Medical Application**

  Sensor networks are also widely used in healthcare area. In some modern hospital sensor networks are constructed to monitor patient physiological data to control the drug administration track and monitor patients and doctors and inside a hospital.

- **Home Application**

  Many concepts are already designed by researchers and architects, like "Smart Environment: Residential Laboratory and Smart Kindergarten. Some are even realized.

- **Traffic Monitoring**

  The sensor node has a built-in magneto-resistive sensor that measures changes in the Earth's magnetic field caused by the presence or passage of a vehicle in the proximity of the node. A low-power radio relays the detection data to the AP at user-selectable periodic reporting intervals or on an event driven basis. By placing two nodes a few feet apart in the direction of traffic, accurate individual vehicle speeds can be measured and reported.

- **Robotics Control**

  Robotics has matured as a system integration engineering as "the intelligent connection of the perception to action". Programmable robot manipulators provide the "action" component. A variety of sensors and sensing techniques are available to provide the "perception".
Habitat Monitoring

The intimate connection with its immediate physical environment allows each sensor to provide localized measurements and detailed information for habitat environment [29].

1.4.1 WSN Application Examples

A WSN application usually requires different functionalities: sensing, storing data, and data communication. Sensing typically requires a large number of nodes to ensure coverage, and few resources on each node whereas, data transmission and data storage requires more system resources. Therefore deploying a homogeneous network tends to result in unnecessarily high cost of the network. Prolonging sensor network lifetime is critical due to the slow improvement of battery capacity and the constraints of sensor physical sizes and cost.

- Disaster relief operation
- Drop sensor nodes from an aircraft over a wildfire
- Each node measures temperature
- Derive a “temperature map”
- Biodiversity mapping
- Use sensor nodes to observe wildlife
- Intelligent buildings (or bridges)
- Reduce energy wastage by proper Humidity, Ventilation, and Air Conditioning (HVAC) control shown in Figure 1.3.
- Needs measurements about room occupancy, temperature, air flow.
- Monitor mechanical stress after earthquakes.
1.5 Challenges in Wireless Sensor Network

1.5.1 Challenge in the end device

All Security approaches require a certain amount of resources for the implementation, including data memory, code space and energy to power the sensor during the run of the approach [5]. However, currently these resources are very limited in a tiny wireless sensor node. This challenge refers interested readers to the mini hardware survey done by Tatiana Bokareva for more information about the hardware specification of more types of sensor node. The challenges in the sensor’s hardware are discussed as follows:

Limited Memory

A sensor node is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

Limited Energy Resource

The energy resource is the biggest challenge in WSN. It is assumed that once sensor nodes are deployed in a WSN, their batteries cannot be easily deployed due to the high operating costs of being deployed in remote areas.
Limited CPU Performance:

The CPU used in MICA2 sensors, for example, is the 16 bit, 8 MHz Texas Instruments MSP 430 microcontrollers. Embedded processors are generally not as powerful as those in nodes of a wired network. As such, complex cryptography algorithm should be avoided in WSN.

1.5.2 Sensor Network Challenges

Wireless sensor network uses a wide variety of application and to impact these applications in real world environments, WSN needs more efficient protocols and algorithms. Designing a new protocol or algorithm address some challenges which are needed to be clearly understood. These challenges are summarized below:

**Physical Resource Constraints:** The most important constraint imposed on sensor network is the limited battery power of sensor nodes. The effective lifetime of a sensor node is directly determined by its power supply. Hence lifetime of a sensor network is also determined by the power supply. Hence the energy consumption is the main design issue of a protocol. Limited computational power and memory size is another constraint that affects the amount of data that can be stored in individual sensor nodes.

**Deployment:** Many applications are required the ad-hoc deployment of sensor nodes in the specific area. Sensor nodes are randomly deployed over the region without any infrastructure and prior knowledge of topology. In such a situation, it is up to the nodes to identify its connectivity and distribution between the nodes. As an example, for event detection in a battle field the nodes typically would be dropped in to the enemy area from a plane.

**Fault-Tolerance:** In a hostile environment, a sensor node may fail due to the physical damage or lack of energy (power). If some nodes fail, the protocols will work upon it but these changes accommodate in the network.
Unattended operation: In many application sensor networks is deployed once and after deployment have no human intervention. Hence the nodes themselves are responsible for reconfiguration in case of any changes.

Scalability: Most of the applications are needed; the number of sensor nodes deployed, these must be in order of hundreds, thousands or more. The protocols must be scalable enough to respond and operate with such large number of sensor nodes.

Security: Security is a very critical parameter in sensor networks, given some of the proposed applications. An effective compromise must be obtained, between the low bandwidth requirements of sensor network applications and security demands for secure data communication in the sensor networks [2][5].

1.6 Data Collection and Aggregation

Data collection capacity reflects how fast the sink can collect sensing data from all sensors with interference constraint. It is critical to understand the limit of many-to-one information flows and devise efficient data collection algorithms to improve the performance of Wireless Sensor network [66]. The collection of data from a set of sensors toward a common sink over a tree-based routing topology is a fundamental operation in Wireless Sensor Network (WSN). There are two types of data collection [56]: 1) Aggregated converge cast where packets are aggregated at each hop and 2) Raw-data converge cast where packets are individually relayed towards the sink. For periodic traffic, it is well known that contention-free medium access control (MAC) protocols such as Time Division Multiple Access (TDMA) are better fit for fast data collection, since they can eliminate collisions and retransmissions and provide guarantee on the completion time as opposed to contention-based protocols.

Due to the low deployment cost requirement of wireless sensor network, the sensor nodes have simple hardware and severe resource constraints [5]. Hence, it is a challenging task to provide efficient solutions to data gathering problem. Among
these constraints, “battery power” is the most limiting factor in designing wireless sensor network protocols. Therefore, in order to reduce the power consumption of Wireless sensor network, several mechanisms are proposed such as radio scheduling, control packet elimination, topology control and most importantly data aggregation [79].

In-network aggregation deals [24] with this distributed processing of data within the network. In this scheme, the sensor networks is divided into predefined set of regions. Each region is responsible for sensing and reporting events that occurs inside the region to the sink node. In a typical sensor network scenario, different node collects data from the environment and then send it to some central node or sink which analyse and process the data and then send it to the application. But in-network data aggregation, data produced by different nodes can be jointly processed while being forwarded to the sink node. [Elena Fosolo et al] in defines the in-network aggregation process as follows: In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime. In this approach, the sensor with the most critical information aggregates the data packets and sends the fused data to the sink. Each sensor transmits its signal strength to its neighbours [24]. Data aggregation may have effective technique in this context because it reduces the number of packets to be sent to sink by aggregating the similar packets.

In wireless sensor network, the benefit of data aggregation increases, if the intermediate sensor nodes perform data aggregation incrementally, when data are being forwarded to the base station. However, while this continuous data aggregation operation improves the bandwidth and energy utilization, it may negatively affect other performance metrics such as delay, accuracy, fault-tolerance and security. Reports transmitted by these sensors are collected by observers (e.g., base stations). In this case, sensors in different regions of the field can collaborate to aggregate their data and provide more accurate reports about their local regions. For
example, in a habitat monitoring application [29], the average reported humidity values may be sufficient for the observer.

In military fields where chemical activity or radiation is measured, the maximum value may be required to alert the troops. In addition to improving the fidelity of the reported measurements, data aggregation reduces the communication overhead in the network, leading to significant energy savings. In order to support data aggregation through efficient network organization, nodes can be partitioned into a number of small groups called clusters. Each cluster has a coordinator, referred to as a cluster head, and a number of member nodes. The member nodes report their data to the respective CHs [20]. The CHs aggregate the data and send them to the central base through other CHs. Because the CHs often transmit data over longer distances and they lose more energy compared to member nodes. The network may be reclustered periodically in order to select energy-abundant nodes to serve as CHs, thus distributing the load uniformly on all the nodes. Besides achieving energy efficiency, clustering reduces channel contention and packet collisions, resulting in better network throughput under high load [1].

In WSN, computing aggregates in-network (i.e., combining partial results at intermediate nodes during message routing) significantly reduces the amount of communication and hence the energy consumed. An approach used by several data acquisition systems for WSN is to construct a spanning tree rooted at the base station, and then perform in-network aggregation along the tree [24]. The important aggregates considered by the research community include Count, and Sum. Note that it is straightforward to generalize these aggregates to predicate Count (e.g., number of sensors whose reading is higher than 100 units) and Sum. Furthermore, average can be computed from Count and Sum. Sum algorithm can be also extended to compute Standard Deviation and Statistical Moment of any order.

1.7 Motivation

In Wireless Sensor Network (WSN), there are several challenges. The main challenges are how to maximize network life time and how to provide secure data
collection and aggregation in the network. As sensor network totally rely on battery power, the main aim for maximizing lifetime of network is to reduce battery power conservation or energy with some security considerations.

In sensor network, the energy is mainly consumed for three purposes: data collection, data aggregation processing and hardware operation. So a maximizing the network lifetime, the process of data transmission should be optimized. The data transmission can be optimized by using efficient routing protocols and effective ways of data collection and aggregation.

Major operation takes place in the sensor network is to monitor the environment and send the monitored data to the sink node. In case of static sensor networks all sensors are static with the sink node. When the data communication takes place all the static sensors send their sensed data to the sink which is far away from the sensors. In that situation those sensors are close to the sink and participate more times in the data collection than any other sensor. The result is to deplete their energy faster than any other nodes, the premature disconnection of the networks.

This problem, here termed as the “network attack problem”. It leads to a premature disconnection of the network [12]. With the data collection process sink gets the data from the sensors. During the data collection node may be participate in these process and drop the packets also. Routing protocols provide the secure data collection route from the sensor nodes to sink for saving energy of nodes in the network. Here data aggregation plays a vital role in energy conservation of sensor network. Data aggregation methods are used not only for finding an optimal path from source to destination but also to eliminate the redundancy of data, since transmitting huge volume of raw data is an energy intensive operation, Thus it helped to minimize the number of data transmission.

Moreover when data aggregation is performing the data is compressed as it is passed through the network, thus occupying less bandwidth. This also reduces the
amount of transmission power expended by nodes. Hence secure data aggregation
[5] can be considered as a very challenging problem in wireless sensor network.

1.8 Overview

The remaining document is divided into four chapters: The second chapter
presents survey of wireless sensor network. The third chapter elaborates the problem
description of the thesis. The fourth chapter discusses the methodology of the
research work. The fifth chapter is Grid Based Dynamic (GBSD) keying protocol
for establishing a key between all sensor nodes that must exchange data securely and
also it facilitates the node addition / deletion should be supported. The sixth chapter
details the secure energy efficient schema for wireless transport layer sensor
network; describe a key management schema Protocol [97] which secures
communication between sensor nodes and base station by considering vulnerabilities
that associated with WSN. The seventh chapter discusses about secure data
collection and aggregation in wireless sensor network. The eighth chapter presents
the implementation, results and discussions. The ninth chapter elaborates the finds
as conclusion and the future work of the research.