CHAPTER 1

INTRODUCTION
1.1 INTRODUCTION

Wireless sensor network has recently captivated the significant attention of the research community owing to its potential applications in the area of communication as well as its ongoing problems that are more or less unsolved. The standard research work does take the assistance of sensor nodes e.g. Mica-Z, TelosB, Imote2, etc., whereas in reality there are multiple forms and types of sensors being manufactured and used in reality [1]. A sensor node captures the data using Time Division Multiple Access (TDMA) and forwards the aggregated data either to the base station or to other sensors, which ultimately reaches the users. A sensor node may also use Frequency Division Multiple Access (FDMA) for the purpose of sensing; however, it calls for permanent allocation of frequency resulting in wastage of spectrum especially at the situation of non-transmission from any other nodes. This calls for increased operational cost. Hence, TDMA benefits WSN from lowered operational cost and hence is much preferred over FDMA for sensing over large scale of application. A normal routing mechanism of sensors always considers three types of nodes i.e. cluster head (the node that performs data aggregation), member node (that forwards data to cluster head), and a base station (that forwards aggregated data to the user for analysis) [2]. Although, this mechanism of routing and cluster might sounds easier, it has exponential challenges when sensors are studied on modern and upcoming technology i.e. IoT (Internet-of-Things), Reconfigurable Networks, etc. [3].

Supported with potential advantages in commercial usage, sensors are also shrouded with significant loopholes right from the quality of service to security factor. As wireless sensors network is one of the economical ways
to capture the information from the human-unreachable area, hence, the topic is worth for investigating its prolonging issues that are still unsolved after an archive of potential research-based literature and some breakthrough inventions. The next section will discuss the background of the study to elaborate further on it.

1.2 BACKGROUND

Normally a wireless sensor network is deployed in an area where there is less feasibility of continuous monitoring without an aid of human’s intervention. The applicability of the wireless sensor network could also be the cases where the area to be surveilled is massive and requires to be monitored unattended for a long duration of time. Hence, even in the event of an adverse environment, the monitoring of the physical data must be carried out.

A wireless sensor node is a typical electronic device that has the capability of sensing some of the physical attributes e.g. thermal, pressure, moisture, smoke, dust, motion, etc. Consider a possible situation of one application in wireless sensor network e.g. forest fire detection as shown in Figure 1.1. The figure shows a simple application of sensor technology where various sensors implanted on trees senses the climatic data (e.g. precipitation, humidity, temperature, seismic activity, etc.). The Base station collects the aggregated data, which forwards the data via global satellite to the meteorological departments [4].
A sensor node is an electronic device that is capable of perceiving the surrounding information in the form of signals e.g. pressure, motion, smoke, moisture, thermal, etc. Selection of a sensor is always carried out based on resolution, cost, potential in calibrating, range, sustenance in environmental condition, etc. However, a typical sensor is capable of perceiving any one form of surrounding signals. Hence, a modern sensor-based application chooses to integrate two or more sensors in order to trap more information of the surrounding. After collecting the sensed data, it is required that such data should be converted to an application-readable signal that can be estimated electrically. Hence, the sensor can only perform this task of processing in
conjunction with other subsidiary electronic components e.g. processing unit, power source, a communication interface, analog to digital converter, memory, etc. [5, 6]. Therefore, conglomeration of all these components with sensor is called as sensor node (Figure 1.2)

![Diagram of a typical sensor node with components labeled: Communication Interface, Sensors, PU, Power, Temperature Sensor, Motion Sensor, Smoke Sensor, Light Sensor, Accelerometer, Pressure Sensor.]

Figure 1.2: A Typical Sensor Node


A sensor-based application carries out its operations using communication interface, power source, Processing Units (PU) along with specific forms of sensors. The brief descriptions of essential components of the sensor nodes are as follows:

- **Communication Interface**: The communication interface is responsible for using RF antenna configuration in order to channel the perceived signal. It assists one node to communicate with other nodes.
Although the communication interface could be wired (USB, IEEE, 802.3, RS-232) but the majority of applications prefers wireless (IEEE 802.15.4) [7]. However, such communication interfaces are more likely to suffer from interference problems, bandwidth problems, data loss, or even highly prone to malicious attacks.

- **Processing Unit**: A sensor node has two forms of processing unit viz. microcontroller and central processing unit. A microcontroller processing unit provides the memory privilege, timer operations, and general-purpose input-output interface. On the other hand, the central processing unit will be responsible for executing the programs written in the firmware specific to the application. Frequently adopted microcontrollers in sensor networks are i) ATmega328 (Arduino1), ii) ATmega128L (For MicaZ), iii) dsPic33FJ256MC710 (For FlexBoard), and iv) PIC32MX795F512L (For IPM board).

- **Power Sources**: The source of power supply in sensors can be from both battery and AC. However, the majority of the large-scale sensor network uses battery-operated sensor nodes. A normal sensor will require around 1.2-5 volts for operation, where the intake potential difference can be within the range of 2.1-19 volts also. The switching mechanism of the input potential difference work on the mechanism of either of linear converter or switching-mode converter.

1.2.2 About Applications

The usages of the sensor in modern technology have the higher scope of utility viz. detection of a forest fire, habitat monitoring, industrial monitoring, defense, combat field, underwater monitoring, natural calamities
monitoring, etc. (Figure 1.3). The applications are designed depending upon the requirements of the users. Apart from conventional application in wireless sensor network, some of the new applications are viz. i) biodegradable sensors for assessing nutrient quality from soil [8], ii) self-healing sensors which are used in locations with adverse climatic conditions [9], iii) smart dust used for monitoring, defense or covert operations [10], iv) micro-sensors used as implants in healthcare sector [11]. Such applications could be used for continuous operations or priority-based applications. It is to be noted that more sophisticated the sensor node is regarding the application, more resource utilization and energy drainage will be there.

Figure 1.3: Applications of Wireless Sensor Network

1.2.3 About challenges

As sensor node is quite a small device with the lower computational capability and less availability of resources, hence it does pose some
significant challenges when deployed in particular operations. Some of the challenges that have captured the attention of research community in last decade are as follows:

- **Energy Consumption**: Every sensor node is powered by a battery with finite lifetime. At the same time, the impact of battery life within a sensor affects multiple operations during routing process. A node consistently depletes energy even it is not transmitting data. At the same time, implementation of any form of algorithm initially affects power consumption itself. Hence, it is really a challenging task to design and develop any algorithm that understands this energy problem.

- **Performing Data Analysis**: Usually, an aggregated data is obtained using TDMA scheduling by a sensor and such data is quite raw and massive difficult enough to understand and interpret a real meaning out of it. With the evolution of IoT, a sensor accumulates a massive data and stores it in cloud clusters. The only way to perform the analysis is by using mining technique which doesn’t give 100% accuracy in its inference mechanism.

- **Energy Efficient Routing**: Although 80% of the research works till date are only focused on developing an efficient routing protocol, but still a robust security protocol is yet to witness to ensure better network lifetime retention. The routing protocols are equally focused on addressing the correlated problems of bandwidth, energy consumption, resource allocation and security.

- **Heterogeneity**: It is one of the associated problems related to routing. Although two sensors of same hardware and network features find
quite easy to process the routing data, it is quite difficult in the case when two sensors differ from each other regarding both hardware or network features. Therefore, processing data in heterogeneous network very often gives rise to delay, which is an ideal condition for an intruder to initiate an attack.

- **Security**: Owing to poor availability of resources (memory, energy, bandwidth etc.) and lower computational complexity, a sensor cannot support a complex cryptographic operation. Hence, security features of any sensor application are quite questionable for its effectiveness. The biggest problem of security rises from the preliminary routing mechanism which calls for broadcasting the control message while performing routing. Hence, adhering to standard routing protocols in sensor network, it is quite difficult to address a robust security protocol in wireless sensor network.

### 1.3 RESEARCH PROBLEM

Even though there are various forms of problem in wireless sensor network, it is found that some problems are persistently being addressed in research manuscripts. There are various forms of scattered problems on which the researchers till date have been investigating on. The amount of research work carried out till date pertaining to all the problems in wireless sensor network can be visualized in Table 1.1. The numbers highlighted in Table 1.1 are approximately 95% correct in terms of technical relevancy to its specific problem found in reputed research journals e.g. IEEE, Springer, and Science Direct. The idea behind highlighting the table is to basically show that there are two categories of problems being considered for investigation
viz. category-A, which is the found most frequently and category-B, which is found in irregular period of publications time.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Available</th>
<th>Research</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Manuscript</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research</td>
<td>IEEE</td>
<td>Springer</td>
<td>Science</td>
</tr>
<tr>
<td>Problems</td>
<td>1496</td>
<td>14, 473</td>
<td>6724</td>
</tr>
<tr>
<td>A</td>
<td>Optimization</td>
<td>12, 717</td>
<td>7073</td>
</tr>
<tr>
<td>A</td>
<td>Routing</td>
<td>15, 590</td>
<td>7460</td>
</tr>
<tr>
<td>A</td>
<td>Energy</td>
<td>18, 355</td>
<td>9528</td>
</tr>
<tr>
<td>B</td>
<td>Bandwidth</td>
<td>11669</td>
<td>5913</td>
</tr>
<tr>
<td>B</td>
<td>Resource allocation</td>
<td>4936</td>
<td>2679</td>
</tr>
<tr>
<td>B</td>
<td>Load balancing</td>
<td>5677</td>
<td>3683</td>
</tr>
</tbody>
</table>

Normally, a new research idea should consider some less repetitive concept to show uniqueness in its research ideology. However, it is felt that category-A problems has been the pivotal point of attention for researchers till date and unfortunately, no such robust or benchmarked system has been evolved or witness about the problems mentioned in category-A. Therefore, it is wise enough to consider the problem mentioned in category-A to explore the best solution till date. A closer look at all the problems mentioned in category-A is that all the problems (i.e. security, optimization routing, and energy efficiency) are inter-related to each other. Therefore, the proposed study emphasizes on security problems in wireless sensor network.
Another significant problem associated with the proposed research problems is that the solution towards security issues are normally cryptographic in nature and will have potential dependability on resources and energy for executing it, which is quite scarce in a sensor network. This gives rise to secondary problem which is energy efficiency that can be possibly achieved only using hierarchical routing protocol in contrast to data-centric and location-based routing protocols in a sensor network. Based on this, the following problems have been identified.

- Ineffective usage of cryptography
- Imbalance between security and energy efficiency
- Study specific to adversary
- Lack of an effective benchmark

Therefore, the problem statement of the proposed study can be stated as “*It is a computationally challenging task to develop a robust security technique that can balance the trade-off between security, routing, and energy efficiency in a large scale wireless sensor network.*” The next section discusses research aim and objectives.

1.4 RESEARCH AIM AND OBJECTIVES

The proposed investigation addresses the issues explored and briefly discussed in prior section. The prime aim of the proposed study is to formulate a tree-based approach for modeling the new secure and energy efficient hierarchical routing protocol in wireless sensor network. To accomplish the above-mentioned research aim, following objectives are targeted:
• To design a tree-based routing approach using probabilistic theorem that ensures superlative energy efficiency and robust authentication mechanism in wireless sensor network, also to compare the accomplished outcome of the study with standard SecLEACH routing protocol.

• To design a delay based, optimal decision making routing technique using multi hop technique along with node-to-node authentication mechanism and to compare the accomplished outcome of the study with standard SecLEACH routing protocol.

• To incorporate a robust security measures using advanced public key cryptography and digital signature for securing the routing techniques discussed in Objective one & two and also to compare the accomplished outcome of the study with LEACH, SecLEACH, and PEGASIS routing protocol.

The next section discusses the research methodology being adopted for developing the proposed system.

1.5 RESEARCH METHODOLOGY

The proposed system considers analytical research methodology that consists of both empirical methodology and mathematical approach. Figure 1.4 shows the research methodology adopted considering three sequential stages of the investigation, where the sequential accomplishment of each stage leads to meet the research objectives specified in the prior section.
Figure 1.4: Adopted Research Methodologies.

- Simulation tool used: MATLAB
- Development of WSN model using Graph theory
- Usage of standard radio-energy model for network communication
- Evolving New cluster head method
- Applying Keccak for Encryption
- Developing Mathematical Modeling the unique network
- Evolution of Superior Aggregator Node
- Developing New Public Key Cryptography for the developed network model
- Using Elliptical Curve Cryptography.
- Creating New digital signature for authentication
The brief discussions of research methodology corresponding to the three sequential stages of investigation are as follows:

- **Secured Tree-based Routing with Energy Efficiency (STREE):** The stage of the study addresses the problem of incorporating lightweight cryptography in secure routing over sensor network. The technique adopts graph theory over standard radio-energy model to accomplish an efficient routing. This phase contributes a new algorithm for encryption achieved using the latest cryptographic protocol called as keccak. The study also uses a multi-valued logic approximation to provide number of decisive parameters for selection of aggregator node.

- **Secure Authentication-based Routing (SABR):** The design of SABR is based on strengthening the authentication while performing routing, which means every participating node for one message delivery will be authenticated. The mechanism also applies a delay-based routing that authenticates even the data packet in transmission.

- **Secured Anonymous Routing with Digital Signature (SARDS):** This study phase essentially focuses on strengthening the usage of public key cryptography and also develops a mechanism to further provide a dual layer of security using new digital signature.

### 1.6 THESIS ORGANIZATION

The organizations of the thesis are as follows:

1. **Chapter-1: Introduction:** This is a preliminary chapter that discusses about the background of the study following by brief discussion of
research problem. The chapter also highlights research aim and objectives as well as brief discussion of research methodology.

2. **Chapter-2: Review of Literature**: This chapter discusses about the prior research work being carried out in the area of secure routing protocols in sensor network. The chapter will study the work being carried out with respect to secure routing, energy efficiency. The study will also discuss elaborately the research gap after reviewing literatures.

3. **Chapter-3: Secure Routing Protocols of Wireless Sensor Network**: This chapter will act as a theoretical backbone of the proposed study towards secure routing. The chapter will discuss about forms of vulnerabilities and its existing countermeasures. The chapter will also discuss the advantages and disadvantages of the existing solutions towards secure routing and will justify the need of study in this regards.

4. **Chapter-4: Secured Tree-based Routing with Energy Efficiency**: This chapter essentially introduces a new secure routing protocol that uses graph theory and multi-valued logical approximation for enhancing security. The chapter will have elaborated discussion of research methodology, algorithm description, followed by result discussion.

5. **Chapter-5: Secure Authentication-based Routing**: This chapter will introduce a new node-to-node authentication using delay-based routing. The chapter will have elaborated discussion of research methodology, algorithm description, followed by result discussion.
6. **Chapter-6: Secured Anonymous Routing with Digital Signature:**

   This chapter will present a new algorithm that can maintain a higher degree of privacy, confidentiality, and non-repudiation in routing for sensor network. The chapter will have elaborated discussion of research methodology, algorithm description, followed by result discussion.

7. **Chapter-7: Conclusion & Future Work:** This is a concluding chapter and will discuss about core findings of the entire investigation. This chapter will also discuss about the potential thesis contribution towards secure routing over sensor network and finally the chapter will conclude with discussion of scope and limitation followed by future direction of study.