CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

A Wireless Sensor Network (WSN) is a distributed network and it comprises a large number of distributed, self-directed, tiny, low powered devices called sensor nodes alias motes [1]. WSN naturally encompasses a large number of spatially dispersed, petite, battery-operated, embedded devices that are networked to supportively collect, process, and convey data to the users, and it has restricted computing and processing capabilities. Motes are the small computers, which work collectively to form the networks. Motes are energy efficient, multi-functional wireless device [7]. The necessities for motes in industrial applications are widespread. A group of motes collects the information from the environment to accomplish particular application objectives. They make links with each other in different configurations to get the maximum performance. Motes communicate with each other using transceivers. In WSN the number of sensor nodes can be in the order of hundreds or even thousands. In comparison with sensor networks, Ad Hoc networks will have less number of nodes without any infrastructure. The differences between WSN and Ad hoc Networks are presented in the Table 1.1 [9].

Now a days wireless network is the most popular services utilized in industrial and commercial applications, because of its technical advancement in processor, communication, and usage of low power embedded computing devices. Sensor nodes are used to monitor environmental conditions like temperature, pressure, humidity, sound, vibration, position etc. In many real time applications the sensor nodes are performing different tasks like neighbor node discovery, smart sensing, data storage and processing,

data aggregation, target tracking, control and monitoring, node localization, synchronization and efficient routing between nodes and base station [4].

Table 1.1 Wireless Sensor Networks Vs Ad hoc Networks

Parameters	**Wireless Sensor Networks**	**Ad Hoc Networks**
Number of sensor nodes	Large	Medium
Deployment	Densely deployed	Scattered
Failure rate	Prone to failures	Very rare
Topology	Changes very frequently	Very rare
Communication paradigm	Broadcast communication	Point-to-Point communications
Battery	Not replaceable / Not rechargeable	Replaceable
Identifiers	No unique identifiers	Unique identifiers
Centric	Data centric	Address centric
Fusion / aggregation	Possible	Not suitable
Computational capacities, and memory	Limited	Not limited
Data rate	Low	High
Redundancy	High	Low

Wireless sensor nodes are equipped with sensing unit, a processing unit, communication unit and power unit [5]. Each and every node is capable to perform data gathering, sensing, processing and communicating with other nodes. The sensing unit senses the environment, the processing unit computes the confined permutations of the sensed data, and the communication unit performs exchange of processed information among

neighboring sensor nodes. The basic building block of a sensor node is shown in Figure 1.1.

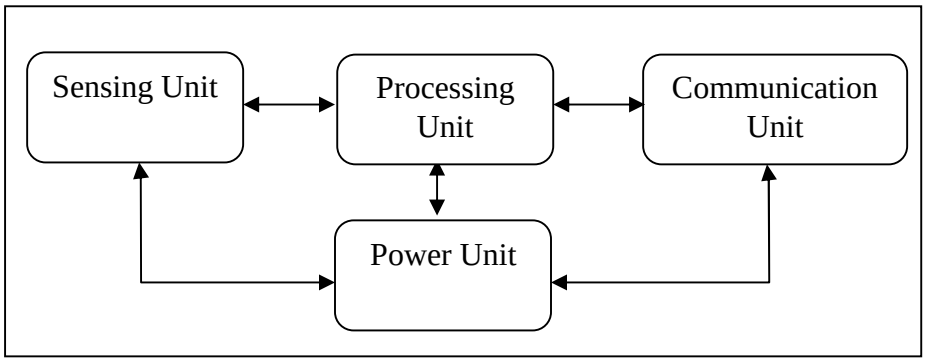

Figure 1.1 Basic Building Blocks of Sensor Node

The sensing unit of sensor nodes integrates different types of sensors like thermal sensors, magnetic sensors, vibration sensors, chemical sensors, bio sensors, and light sensors. The measured parameters from the external environment by sensing unit of sensor node are fed into the processing unit. The analog signal generated by the sensors are digitized by using Analog to Digital converter (ADC) and sent to controller for further processing.

The processing unit is the important core unit of the sensor node. The processor executes different tasks and controls the functionality of other components. The required services for the processing unit are pre-programmed and loaded into the processor of sensor nodes. The energy utilization rate of the processor varies depending upon the functionality of the nodes. The variation in the performance of the processor is identified by the evaluating factors like processing speed, data rate, memory and peripherals supported by the processors. Mostly ATMEGA 16, ATMEGA 128L, MSP 430 controllers [7] are used in

commercial motes. The computations are performed in the processing unit and the acquired result is transmitted to the base station through the communication unit.

In communication unit, a common transceiver act as a communication unit and it is mainly used to transmit and receive the information among the nodes and base station and vice versa. There are four states in the communication unit: transmit, receive, idle and sleep. In general the functionality of the sensor node is shown in Figure 1.2.

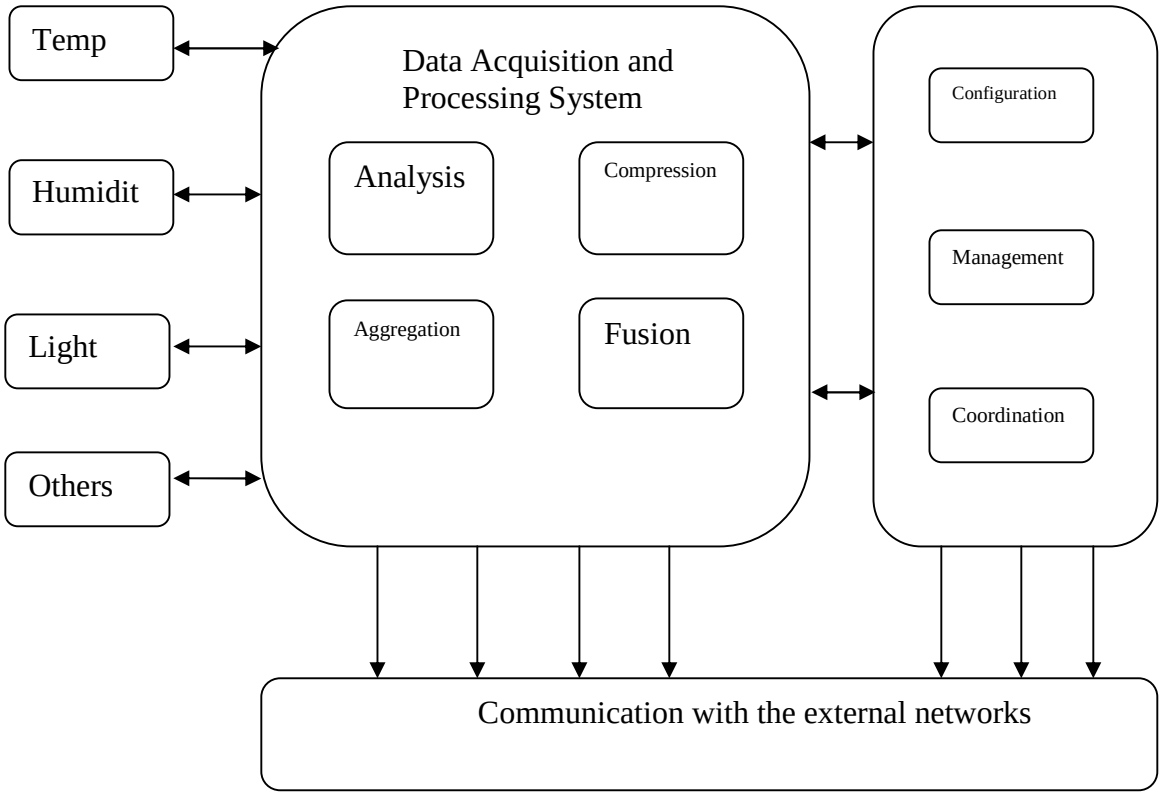

Figure 1.2 Functionality of A Sensor Node

The major characteristics of the sensor node used to evaluate the performance of WSN are [6]

1. **Fault tolerance**: Each node in the network is prone to unanticipated failure. Fault tolerance is the capability to maintain sensor network functionalities without any break due to sensor node failures.
2. **Mobility of nodes**: In order to increase the communication efficiency, the nodes can move anywhere within the sensor field based on the type of applications.
3. **Dynamic network topology**: Connection between sensor nodes follows some standard topology. The WSN should have the capability to work in the dynamic topology.
4. **Communication failures**: If any node in the WSN fails to exchange data with other nodes, it should be informed without delay to the base station or gateway node.
5. **Heterogeneity of nodes:** The sensor nodes deployed in the WSN may be of various types and need to work in a cooperative fashion.
6. **Scalability**: The number of sensor nodes in a sensor network can be in the order of hundreds or even thousands. Hence, WSN designed for sensor networks is supposed to be highly scalable.
7. **Independency:** The WSN should have the capability to work without any central control point.
8. **Programmability:** The option for reprogramming or reconfiguring should be available for the WSN to become adaptive for any dynamic changes in the network.
9. **Utilization of sensors:** The sensors should be utilized in a way that produces the maximum performance with less energy.

10. **Impracticality of public key cryptosystems:** The limited computation and power resources of sensor nodes often make it undesirable to use public key algorithms.
11. **Lack of aprior knowledge of post-deployment configuration:** If a sensor network is deployed via random distribution, the protocols will not be aware of the communication status between each nodes after deployment.

The following metrics are used to evaluate the performance of a WSN [8]: network coverage, node coverage, efficiency in terms of system lifetime, effortless deployment, data accuracy, system response time, fault tolerance, scalability, network throughput, sample rate, security, the cost of the network and network architecture used. The individual sensor node in the WSN is evaluated using flexibility, robustness, computation, communication, security, synchronization, node size and cost.

The components of WSN system are sensor node, rely node, actor node, cluster head, gateway and base station which are explained below [2].

Sensor node: Capable of executing data processing, data gathering and communicating with additional associated nodes in the network. A distinctive sensor node capability is about 4-8 MHz, having 4 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Relay node: It is a midway node used to communicate with the adjacent node. It is used to enhance the network reliability. A rely node is a special type of field device that does not have process sensor or control equipment and as such does not interface with the

process itself. A distinctive rely node processor speed is about 8 MHz, having 8 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Actor node: It is a high end node used to perform and construct a decision depending upon the application requirements. Typically these nodes are resource rich devices which are outfitted with high quality processing capabilities, greater transmission powers and greater battery life. A distinctive actor node processor capability is about 8 MHz, having 16 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency [7].

Cluster head: It is a high bandwidth sensing node used to perform data fusion and data aggregation functions in WSN. Based on the system requirements and applications, there will be more than one cluster head inside the cluster. A distinctive cluster head processor is about 4-8 MHz, having 512 KB of RAM, 4 MB flash and preferably 2.4 GHz of radio frequency [7]. This node assumed to be highly reliable, secure and is trusted by all the nodes in the sensor network.

Gateway: Gateway is an interface between sensor networks and outside networks. Compared with the sensor node and cluster head the gateway node is most powerful in terms of program and data memory, the processor used, transceiver range and the possibility of expansion through external memory. A distinctive gateway processor speed is about 16 MHz, having 512 KB of RAM, 32 MB flash and preferably 2.4 GHz of radio frequency.

Base station: It is an extraordinary type of nodes having high computational energy and processing capability.

Attractive functionality of sensor nodes in a WSN includes effortlessness installation, fault indication, energy level diagnosis, highly reliablity, easy coordination with other nodes in the network, control protocols and simple network interfaces with other smart devices. In WSN, based on the sensing range and environment, the sensor nodes are classified into four groups, namely specialized sensing node, generic sensing node, high bandwidth sensing node and gateway node. The radio bandwidth for the sensor nodes are <50 Kbps, <100 Kbps, ≈500 Kbps and >500 Kbps respectively. On board processing, computational rate and communication ranges differ from node to node in WSN. Particularly for some dedicated application sensor nodes with different capabilities are used. For example, smart specialized sensing nodes are preferred for special purpose devices, intelligent generic sensing node preferred for generic functions. For interconnectivity functions high end smart bandwidth sensing node and gateway nodes are preferred.

Sensor networks are clustered with gateway, relay node, actor node and cluster head, and every other node within the communication range. Cluster is a collection of group of sensor nodes in that particular sensor field. There may be more than one cluster in WSN. Based on the parameters like computation rate, processing speed, storage, and communication range, sensor nodes are identified and selected for WSN formation [9]. Based on the node properties the sensor networks are classified into two types, homogenous sensor networks and heterogeneous sensor networks. In homogenous sensor networks, all sensor nodes have the same property in terms of computation, communication, memory, energy level and reliability. In heterogeneous sensor networks, the nodes are of different capabilities in terms of computation, communication, memory, energy level and reliability. If all the sensor nodes within the cluster are having the same

properties (homogenous) it is referred as distributed WSN (DWSN). Otherwise if the sensor nodes have different properties (heterogeneous) it is called as hierarchical WSN (HWSN). The distributed and hierarchical WSN is shown in Figure 1.3.

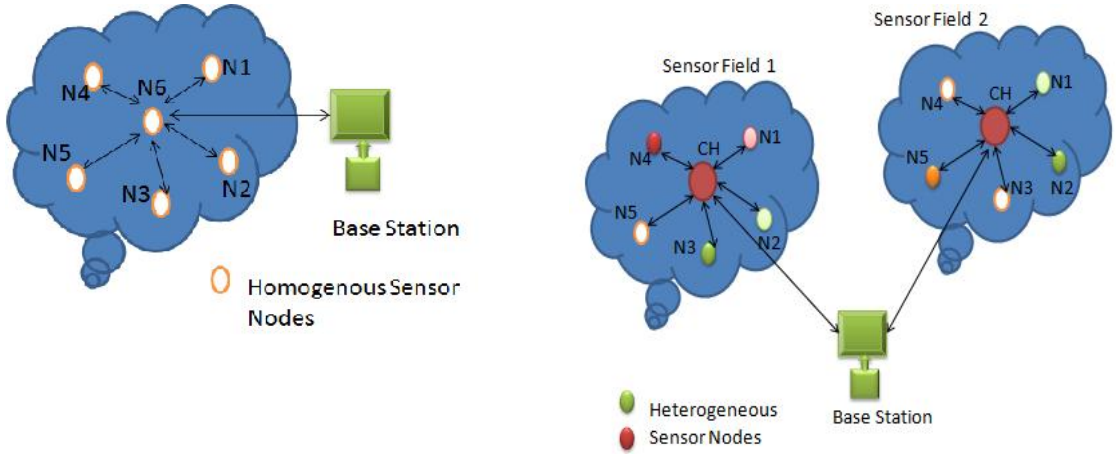

Figure 1.3 Distributed and Hierarchical WSN

Senor nodes in an open environment regularly sense the physical and environmental changes and transmit the information to the centralized server called a gateway. The computational rate and interaction of sensor nodes with the physical environment is different for different nodes in the network. In real time, sensor nodes are more constrained in its computational energy and storage resources.

The sensor nodes are intelligent to observe an extensive diversity of ambient circumstances that includes flow, temperature, pressure, humidity, moisture, noise levels, mechanical stress, speed, etc. Many novel applications are being developed due to the new concept of micro sensing and wireless networking for these smart sensing devices. Some of the possible assorted applications [24] of WSN ’s are temperature control, inventory management, physiological monitoring, habitat monitoring, precision

agriculture, forest fire detection, nuclear, chemical, and biological attack detection, military, transportation, disaster relief, and environmental monitoring.

1.2 WSN ORGANIZATION

Any WSN can be configured [24] as a five layered architecture as explained below

- The physical layer is responsible for frequency selection, modulation and data encryption.
- The data link layer functions as a pathway for multiplexing of data streams, data frame detection, Medium Access control (MAC) and error control.
- The network layer is used to route the data supplied by the transport layer using special multi-hop wireless routing protocols between sensor nodes and sink nodes.
- The transport layer maintains the flow of data if the application layer requires it.
- The application layer makes the hardware and software of the lower layers transparent to the end user.

1.3 ISSUES AND CHALLENGES IN DESIGNING WSN

- Sensor networks do not fit into any regular topology, because while deploying the sensor nodes they are scattered [8] [9] [10]
- Very limited resources
    - Limited memory,
    - Limited computation

  - Limited power
- It comes under fewer infrastructures and also maintenance is very difficult.
- Unreliable communication
  - Unreliable data transfer
  - Conflicts and latency
- Sensor node relies only on battery and it cannot be recharged or replaced. Hardware design for sensor node should also be considered.
- Unattended operations
  - Exposure to physical attack
  - Remotely managed
  - No central control point
- Achieving synchronization between nodes is also another issue.
- Node failure, topology changes and adding of nodes and deletion of nodes is another challenging issue.
- Because of its transmission nature and hostile environment, security is a challenging issue.
- Based on the applications, sensor node has to be chosen with respect to computation rate.

1.4 SECURITY IN WSN

Sensor networks pretence exclusive challenges, so conventional security techniques used in traditional networks cannot be applied directly for WSN. The sensor devices are

inadequate in their energy, computation, and communication capabilities. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. WSN works together closely with their corporal environments, posing new security troubles [11]. As a result, existing security mechanisms are insufficient, and novel ideas are needed.

- Sensor nodes are randomly deployed in an open and unattended environment, so security is critical for such networks
- WSN uses wireless communication, which is predominantly easy to eavesdrop on.
- An attacker can easily inject malicious node in the network.
- WSN involves a large number of nodes in the network. Enforcing security in all the levels is important and also too complex.
- Sensor nodes are resource constraints in terms of memory, energy, transmission range, processing power. Hence asymmetric cryptography is too expensive and symmetric cryptography is used as alternatives.
- Cost of implementing tamper resistant software is very high.

WSN's general security goals [12] are confidentiality, integrity, authentication, availability, survivability, efficiency, freshness and scalability as described in Table 1.2. WSN is susceptible to many attacks because of its transmission nature, resource restriction on sensor nodes and deployment in uncontrolled environments. To ensure the security services in WSN many crypto mechanisms like symmetric and asymmetric

methods are proposed. To achieve security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent between sensor nodes.

Table 1.2 Security Services

Confidentiality	Keeping node information secret from others but authorized users see it.
Integrity	Possible for the receiver node of a message to confirm that it has not been customized in transit.
Device authentication	Justification of the identity of the device.
Message authentication	Justification the source of information
Validation	To provide correctness of authorization to use or manipulate resources.
Access control	Restricting access to resources.
Revocation	Renunciation of certification or authorization.
Survivability	The lifetime of the sensor node must be extended even the node is compromised.
Nonrepudiation	Preventing the denial of a previous commitment.
Availability	High availability systems in sensor node is aim to remain available at all times preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.
Data freshness	Data freshness objective ensures that messages are fresh, meaning that they are in proper order and have not been reused.

In a distinctive circumstance, any two nodes (A and B) exchange data over an insecure channel. A and B want to make sure that their data exchange remains incomprehensible by anyone who might be listening. Furthermore, because A and B are in remote locations, A must be sure that the information it receives from B is not been modified by anyone during transmission. In addition, it must be sure that the information really does originate from B and not someone impersonating B. Cryptography is used to achieve above mentioned problems.

The art and science of keeping communication secure is called cryptography, and it is experienced by cryptographers. Cryptography is a process [27] associated with scrambled plain text (ordinary text, or clear text) into cipher text (a process called encryption), then back again (known as decryption). It is a mathematical techniques connected to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The two components required to encrypt data are an algorithm and a key. The algorithm is generally known and the key is kept secret. The key is very large number that should be impossible to guess, and of a size that makes an exhaustive search impractical. In a symmetric cryptosystem [26], the same key is used for encryption and decryption. In an asymmetric cryptosystem, the key used for decryption is different from the key used for encryption. In WSN, cryptographic systems are characterized as which type of operations used for transforming the data, how many numbers of keys used, key size and the way in which the sensor node process the data.

The possible threats [20] among the sensor nodes in WSN are tabulated in Table 1.3.

Table 1.3 Threat Model of WSN

Threat Model	**Action**
False Node insertion	Feed false data Prevent the true data flow among the nodes
Routing Attack	Alteration of Routing Path Sinkhole, Wormhole Attack
Malicious data	False Observation
Subversion of Node	Extraction of original data from node Misbehavior

The schematic view of crypto functions is shown in Figure 1.4. The taxonomy of cryptographic primitives is shown in Figure 1.5.

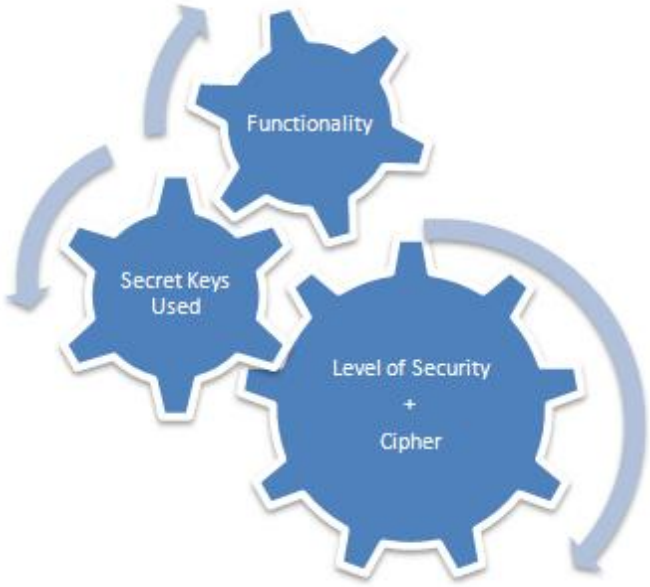

Figure 1.4 Cryptographic Systems

Lars [27] classified and proposed some categories of breaking sensor node information in WSN. These are total break, global deduction, local deduction and information deduction. Total break means, the cryptanalyst finds the key value (K) used in the sensor node, it's very difficult and also time consuming process. Global deduction means cryptanalyst finds the alternate algorithm, local deduction means cryptanalyst finds the equivalent original text and make it try to get the original data from the node. Information deduction means the cryptanalyst gain some information about the key and the data from the sensor node. The security strength of the entire crypto system mainly depends on the secret keys used, not in the algorithm.

To provide secure communications [13] between the sensor nodes in the WSNs, all the messages should be encrypted and authenticated with different secret keys. The total number of keys processed in the sensor node and the network is too high. For that reason,

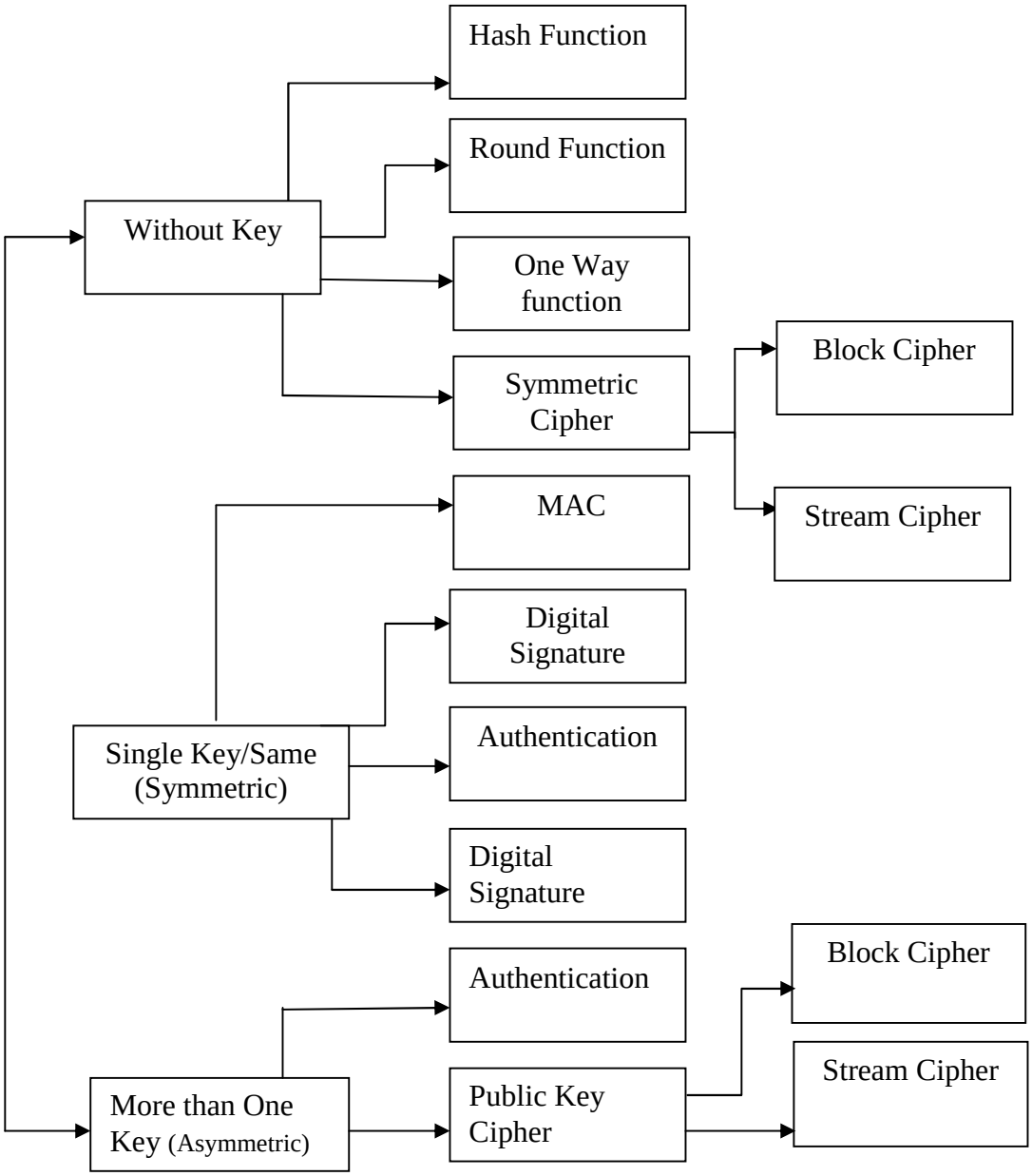

Figure 1.5 Taxonomy of Cryptographic Basics

it is important to design strong and efficient Key Management Schemes (KMS) for WSNs. In an uncontrolled environment, which enable the sensor nodes to communicate

securely with each other nodes using crypto techniques. The reason of key management [26] for WSN is to load, distribute and handle the secret keys in sensor nodes to establish a secure communication among sensor nodes. Security critical applications depend on the key management scheme because it has to provide high fault tolerance when a node get compromised. Whenever the new node wants to add or leave from the network the key management schemes play a vital role. The key updating process during node addition and node deletion are discussed and shown in Figure 1.6.

While designing the key management schemes, the important metrics [35] to be evaluated are 1. **Local / global connectivity:** Each node communicates with every other node in the sensor field region.

2. Resilience: Whenever a sensor node is compromised, the key management scheme assures in securing the remaining communication link against node capture.

3. Scalability: Capability to support when large numbers of nodes are added to the sensor network.

4. Efficiency: In terms of storage, communication and computation.

Managing efficient cryptographic keys [14] is a difficult problem in case of large dynamic sensor groups. Each time a member is evicted from or added to the group, the group key must be changed. The members of a group must be able to compute a new key efficiently, at the same time forward and backward security must be guaranteed. Forward securing means that any evicted member node cannot determine any future group key, even when

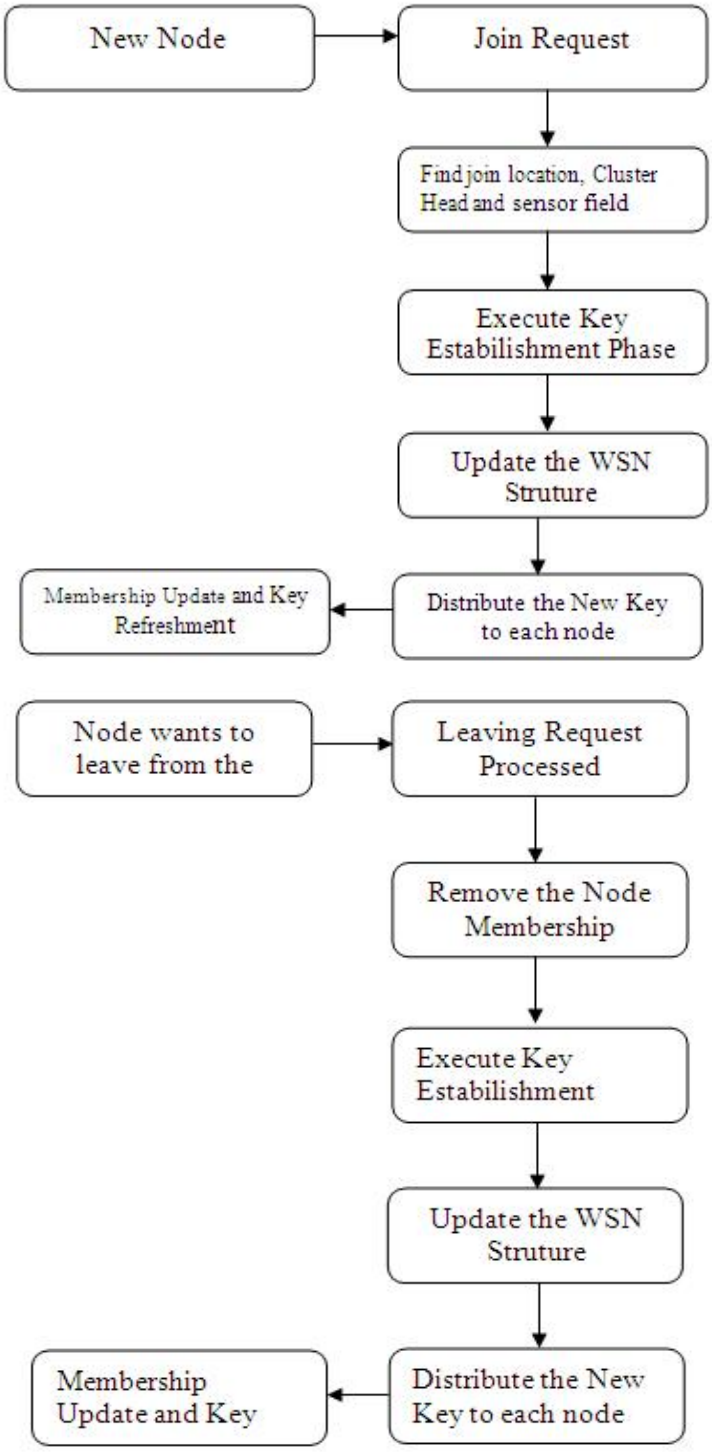

Figure 1.6 Key Refreshment Process In Node Addition and Deletion

performing other tasks. Backward security means that a newly added member node cannot determine any past key, even when working with other new members. Key management for large dynamic group communications raises a problem with scalability. Keys for encryption and authentication purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial. Many key agreement [15] schemes used in general networks, such as Diffie-Hellman and public-key based schemes are not suitable for WSN. Pre-distribution of secret keys for all pairs of nodes is not feasible due to the large amount of memory used when the network size is large. In WSN, keying mechanism is classified into two types, these are static and dynamic keying. The comparison between static and dynamic keying are described in Table 1.4 [16]

Table1.4 Static Vs Dynamic Key Management

Parameters	**Static keying**	**Dynamic keying**
Network lifetime	Short	Long
Key pool	Very large	Small size
Key assignment	Once predeployment	Post deployment
Key generation	Once predeployment	Post deployment
Key distribution	All keys are predistributed to nodes prior to deployment	Subsets of keys are re-distributed to some nodes as needed
Handling node capture	Exposed keys are lost	Exposed keys are altered
Communication cost	Not applicable for administrative keys (Key pre distribution).	High
Storage cost	More keys per node	Fewer keys per node
Handling node addition	Hard	Easy
Network resilience	High	High
Network connectivity	Less	More

During node deployment, the sensor node is clustered into different groups. The node that is placed in restricted areas is called a sensor field. Using key generation server, the keys are generated and loaded into each sensor node; the key storage server is used to store the keys. A node deployment process is described in Figure 1.7.

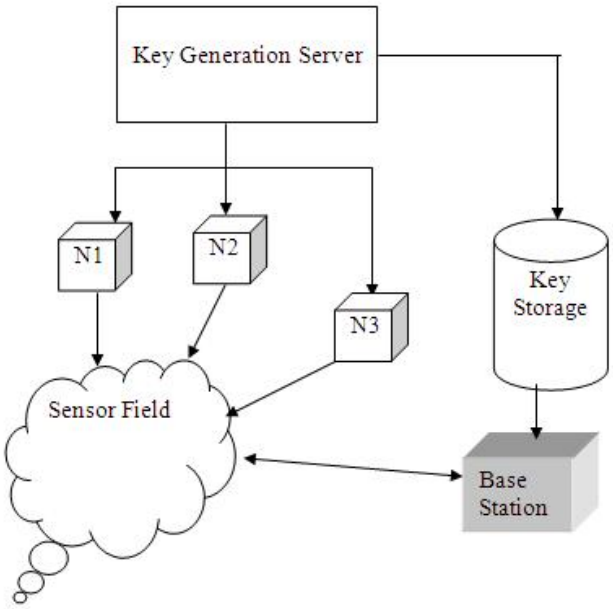

Figure 1.7 Node Deployments

Typical communication pattern in WSN is shown in Table 1.5.

Table 1.5 Communication Pattern in WSN

Source	**Purpose**
Node to Node	Sensor Readings, Queries
Node to Group Head, Node to Cluster Head	Sensor Readings, Queries
Node to Base Station	Sensor Readings, Queries
Base Station to all the nodes in the WSN, Cluster Head & Group Head	Queries, Reconfiguration and Routing
Intra Cluster	Among Neighboring Sensor Node, To minimize the total amount of message shared, for Network data processing and data aggregation.

1.5 SCOPE OF THE RESEARCH

The research reported in this thesis pertains to authenticated KMS in WSN. From literature survey, the matrix based keying mechanism is suitable for KMS in WSN. All the metrics related to KMS such as key connectivity between nodes, resilience, efficiency and scalability are evaluated against the a proposed work and achieved at an accepted level compared with existing schemes. Authentication at each layer of cluster also implemented using congruence techniques. Depends upon the applications, sensor node has to be incorporated into the network. Various types of sensor nodes are also designed using LPC 2149, LPC 2378 and AT91SAM9263 to set up the efficient WSN.

The research carried out encompasses the following objectives:

- The parameters which affect the quality of key management in WSN are to be identified.
- The problems with existing key management scheme are to be identified.
- Efficient key management protocol along with its competency with sensor node constraints are to be developed and implemented along with an efficient node to node authentication protocol is designed.
- To develop a WSN in real time using ARM processors and implement the proposed hybrid KMS to achieve maximum throughput.

The entire process of the thesis work is consolidated and shown in Figure 1.8.

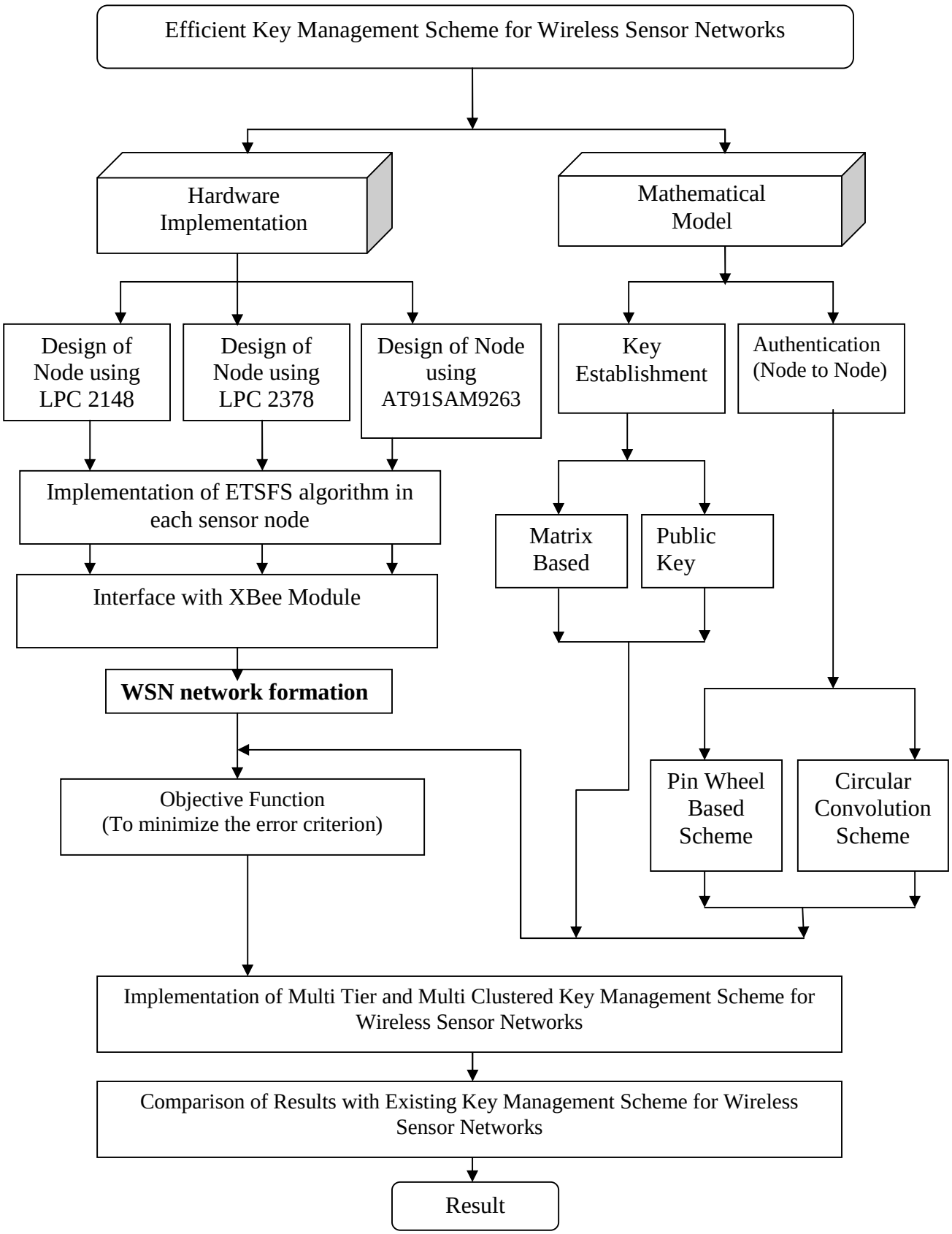

Figure 1.8 Research Scheme

1.6 ORGANIZATION OF THESIS

Chapter 2 presents the literature review with reference to this work. It also presents the relevant research works in KMS for WSN.

Chapter 3 presents 'LU decomposition based KMS. It describes the matrix based KMS techniques for WSN and the performance evaluation is done.

Chapter 4 entitled 'Congruence based pin wheel authentication protocol for WSN' describes how the node authentication has been employed in the proposed WSN and security analysis is performed.

Chapter 5 entitled 'Multi Tier & Multi Clustered WSN using LL^T, deals with the analytical model of an integrated KMS with authentication, and provides better optimization using matrix based key distribution approach for providing an efficient KMS for WSN. The results are compared with the existing KMS.

Chapter 6 entitled 'Implementation of ARM based sensor nodes' describes the hardware information related to the processing unit of sensor nodes and TSFS implementation in ARM node. The timing analysis for key generating and data encryption are done.

Chapter 7 finally concludes with the contributions of this research work.