Due to advancement in technology, sensor networks and wireless communication give rise to a new technology known as wireless sensor networks (WSNs). This technology is growing rapidly in recent years. The network operates on wireless medium. This medium is open for all, i.e. the chances of wireless network to be compromised in comparison with wired networks are more in WSNs. So the solutions dedicated to wired network are not sufficient for resource constrained wireless sensor network. There is still a scope for wide research potential in the field of wireless sensor network security. In this chapter, we analyze issues related to security in WSNs and highlight research objectives implemented in this thesis in the field of wireless sensor networks.

Rest of the chapter is organized as follows

Rest of the chapter is organized as follows. Section 1.1 presents overview to wireless sensor networks. Problem definition is presented in Section 1.2. Work carried out in this thesis is given in Section 1.3 followed by organization of thesis in Section 1.4. Finally, chapter has been summarized in Section 1.5.

1.1 OVERVIEW TO WSNs

Wireless sensor network (WSN) consists of large number of battery-operated sensor nodes. These sensors are very small in size. They have also a built-in processor that is used for the computing functions. In case of wireless sensor network, communication among the sensors is done using wireless transceivers. So every sensor is equipped with a built-in antenna that helps them in communication to other sensors in their limited communication range. Each sensor consist of four subsystems: Power Supply subsystem, sensing subsystems, processing sub systems and communication Subsystems. So with the help of these subsystems, sensors are able to sense the environment, compute simple tasks and exchange data among each other. But all the sensors are resource constrained in terms of memory, energy, processing power and communication bandwidth. Every subsystem uses energy for their working. Once the battery is drained, sensor nodes are useless. The situation of network disconnection is also arises if battery is drained in few of the nodes. So energy consumption by a node is a critical aspect, in order to increase the lifetime of
Chapter 1: Introduction

the network. In most of the cases it is very difficult to recharge or replace the battery. Thus it is necessary that a protocol in WSN must be energy efficient. Sensor nodes are usually deployed in harsh or hostile environments such as battlefield, environmental monitoring or disaster area where they are operated without any attendance. Thus unattended operation makes the secure data aggregation even harder.

Figure 1.1: Randomly deployed WSNs

Figure 1.1 shows a network of wireless sensors which are randomly deployed in the area of interest. The range of every node is very limited, so it can communicate only with those nodes that are within its communication range. In Figure 1.1 the connectivity of every sensor node with its neighbors that are within the communication range of this sensors are shown with the help of a link. Some nodes are disconnected in the network because they have no connectivity with the network as the network is randomly deployed.

Figure 1.1 shows a randomly deployed wireless sensor networks in a two dimensional coverage area ‘A’ that is 100 meter square. This network consists of a set of sensor nodes \( S = \{s_1, s_2, \ldots, s_{100}\} \). Each sensor \( S_i, i=1..100 \) located at random coordinate \((x_i,y_i)\) inside ‘A’. Each sensor has a sensing range of \( r_i \), i.e. 15 meters. All the sensors communicate with each other and establish a routing topology to form a single network. They can sense the environmental conditions as a data and then transmit this data back to
Chapter 1: Introduction

a collection point known as base station which is shown with ID number 101 at X=50 and y=50 area in Figure 1.1.

![Figure 1.2: Characteristics of WSNs](image)

**1.1.1 Characteristics of WSNs**

Wireless sensor networks have the following unique characteristics as shown in Figure 1.2. The network consists of sensor nodes. These nodes are deployed randomly in the network area. So there is no need for any careful planning and engineering to deploy the network. All the nodes in the network are battery operated. It is completely impossible to change or recharge the battery of sensor node after its deployment because the nodes are deployed in unattended area. So once deployed, sensor nodes have to autonomously configure themselves into the communication network. Battery is consumed when a sensor node performs any type of operation like sensing, transmission and processing etc. Every node in the network is resource constrained in terms of energy, computation and
Chapter 1: Introduction

Storage space these constrains make it very difficult to implement strong security algorithms.

A network is usually designed for a specific application and operation. The design requirements of a network are different from one application to other. Due to limited energy and small size of sensor nodes, there are always chances that a node fails or physically damage. This is the cause of unreliability in the network. Node failure, damage, addition, energy depletion or channel fading is frequently occurring in the network that results in frequent topology updating in the network.

Due to the large number of sensor nodes, it is impossible to build a global addressing scheme for the entire network because it would introduce a high overhead for the identification of every sensor.

In most of the sensor network applications, the data sensed by any sensor node flowed in the direction of a Base station. This behavior exhibits many-to-one traffic pattern. In most of the sensor network applications, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of redundancy.

1.1.2 Security Constrains in WSNs

A wireless sensor network has many security constraints as compared to a traditional wired network. Due to these security constraints, it is very difficult to directly employ the existing security approaches of wired network into the wireless sensor networks. Therefore, to develop an energy efficient security mechanism, it is necessary to know and understand these security constraints first. This section describes security constrains in WSNs as shown in Figure 1.3.

Wireless channels are open to everyone. It provides a convenient way for attackers to break into the network. Also most of the protocols used in wireless sensor networks are publicly known. For these reasons, attackers can easily launch attacks by exploiting security holes in the network.

The security of a network depends upon the protocol which itself depends upon the communication medium. Even if the protocol is reliable, the communication medium may still be unreliable. This is due to the open channel access. So a weak radio link supports unreliability in the network.
Chapter 1: Introduction

It is very complex task to build a simulator to be used in WSNs. But the solution of this problem is that there are several popular simulators freely available to be used in wireless sensor networks. Some of them are NS-2 [63], TOSSIM [64], GloMoSim [65], USNeT [66], SENS [67], COOJA [68], Castalia [69], Shawn [70], EmStar [71], SENSE [72], VisualSense [73], OMNeT++ [74], J-Sim [75], Avrora [76]. But every simulator has its own limitations. Some simulators supports only a limited number of protocols while others are limited to use in IP networks only. It is very complicated to use and learn a simulator as it takes a lot of time. Second thing is that it requires special training to use the simulator. It is an art that is learned with experience over time. So people like to use a simple language like Mat Lab as a replacement of simulators.

All the sensors used in the network are resource constrained in terms of memory, energy, processing power and communication bandwidth. So the security protocols used in the traditional wired networks are not compatible with the resource constrained wireless networks.

Figure 1.3: Security constrains in WSNs
Chapter 1: Introduction

Sensor nodes are usually deployed in an unattended and harsh environment that is open to attackers, hard environments and so on. The chances that a sensor node physically captured in such environments are much higher than the traditional wired network which is located in a secure place in a controlled manner.

Traditional security protocols are designed only for point to point settings. So if these traditional protocols are applied in the wireless sensor networks where the number of sensors is very-very large, then it increased large number of overheads in the system that is uncontrolled to manage.

The size of sensor nodes is so small that it is practically impossible to add a temper-proof hardware unit in the small size sensor node where all the sensitive information like symmetric key or other secrets are stored that are always safe from the adversary by physically capturing the node.

Key distribution is also a problem in symmetric key cryptography algorithms. Similarly permanent unique key stored in each sensor is also not a solution as if the key is compromised then all the future communication and data used by that sensor is compromised. So we need a lightweight encryption algorithm that uses the concept of dynamic key, i.e. the key used by any sensor is update regularly and the problem of key distribution is not required in the network.

1.1.3 Security Requirements in WSNs

The basic goal of security in WSNs is to protect the information stored in the memory of sensor and also to keep track of the information and resources from attacks and misbehavior. Security requirements in WSNs are shown in Figure 1.4.
Whenever some malicious node attacks the network then this normal communication changes and the security is compromised. A normal communication between sending sensor ‘S’ and receiving sensor ‘R’ is shown in Figure 1.5.

A. **Confidentiality:** This ensures that the classified data should be accessible and understood only by the authorized sensors. Figure 1.6 shows a loss of confidentiality. The data is disclosed by the attacker when the data is travelled from sender to receiver over the wireless medium. This attack is known as interception.
Chapter 1: Introduction

B. Availability: This ensures that the desired network services like flow of data in both directions i.e. from sensors to base station and from base station to sensors is available all the time even in the presence of denial-of-service attacks. Figure 1.7 shows a loss of availability by the attacker to stop using the services given to some authorized sensor ‘S’ given by the other authorized sensor ‘R’. This attack is known as interruption.

C. Integrity: This ensures that changes need to be done in the message only by the authorized sensors and through authorized mechanisms. Or in other words the message is not modified during transmission by malicious intermediate nodes. Figure 1.8 shows a loss of integrity by the attacker where the attacker has change the ideal route of the message and after change the message sent it to receiving sensor. This attack is known as modification.

D. Authentication: This ensures that origin of the received message or packet in the network is correctly identified before using it in the network. Figure 1.9 shows the scenario where a malicious sensor ‘M’ sent the information to receiving sensor ‘R’ to impersonate itself as a sensor ‘S’. This attack is known as fabrication.
Chapter 1: Introduction

Figure 1.9: Loss of authenticity

E. Non-repudiation: which ensures that a node cannot deny sending a message it has previously sent. Figure 1.10 shows non-repudiation attack where the sender of the message ‘S’ later deny that it has never sent the message to the receiver ‘R’.

Figure 1.10: Non-repudiation Attack

F. Freshness: This ensures that the data is recent and ensures that no adversary can replay old messages. Figure 1.11 shows replay attack where the attacker ‘M’ stores packet ‘P1’ send by the sensor ‘S’ to sensor ‘R’ through intermediate sensor ‘A’ in its memory and later sent this stored packet ‘P1’ to sensor ‘A’ which forwards this packet one more time to sensor ‘R’.

Figure 1.11: Replay Attack

G. Forward secrecy: This ensures that a compromised current secrets or keys should not be able to compromise any secret or key in future.

H. Backward secrecy: This ensures that a compromised current secrets or key should not be able to compromise any earlier secret or key.
Chapter 1: Introduction

The concept of forward and backward secrecy is given in Figure 1.12. Figure 1.12 (A) shows that the second key (K1) is generated with the help of a first key (K0) and third key (K2) is generated with the help of second key (K1) and similarly Ki is generated with the help of a Ki-1 key and so on. In Figure 1.12 (B) a single key (Ki) is compromised at time tk that result in exposing all keys of the system as shown in Figure 1.12(C). In Figure 1.12(D) the concept of forward secrecy is shown which secure all keys that are generated after time tk+1. In Figure 1.12 (E), the concept of backward secrecy is given which secure
all keys by exposing that are generated before time $t_k$ when a key has been exposed at time $t_k$.

I. **Location awareness:** This ensures that the damage cannot be spread from the victimized area to the entire network by security attack even if the sensor node is compromised.

### 1.1.4 Security Attacks in WSNs

Sensor networks are vulnerable to several types of attacks. These attacks can be performed in a variety of ways which includes:

![Attacks on WSNs](image)

**Figure 1.13:** Attacks on WSNs

A. **Denial-of-Service Attack:** In the Denial-of-Service (DoS) attack, a malicious node attempts to disrupt the network services partially or completely. The result of this attack is that the network stops functioning or the services of a network slow down. A variant of Denial-of-Service attack is Distributed Denial-of-Service Attack (DDoS). The functioning of DDoS attack is similar to that of DoS attack. But the difference
Chapter 1: Introduction

between both of them is that, in DDoS attack there is more than one attacker, performing DoS activity from different location.

Figure 1.14: Black Hole Attack

B. **Black Hole Attack** [18]: Black Hole is a region which prevents anything from escaping. In this type of attack, a malicious node drops all the packets passing through it. Figure 1.14 shows the working of a Black Hole Attack. In the network shown in the figure, an ID is assign to every node. A malicious node number 37 discards all the packets that are received by it. Gray shade represents attack area in the figure. In the network malicious node number 37 position itself on the point where it can receive data sent by other nodes (12, 13, 27, 37, 42, 45, 60, 81 and 99). In this case a malicious node creates a Black Hole for these nodes. There are some other nodes (31, 34, 56, 71 and 75) which are aware of this attack but their packets have been passed to base station by other nodes through this path. So overall the packets send by these nodes also lost in the black hole region. At this stage, all of these nodes are disconnected from the network.

C. **Selective Forwarding Attack**: The functioning of this attack [18] is also similar to that of black hole attack but the difference between both of them is that in selective forwarding attack, instead of dropping all the packets like in black hole attack, the malicious node drops only those packets that are matched within certain criteria, i.e.
drop selected packets of a node or to drop all packets from a selected node. Figure 1.15 shows the working of a Selective Forwarding Attack. In the network shown in the figure, a malicious node number 18 discards any packet receive from one path but pass all the packets received from other path. Gray shade in the figure represents the attacked area. Since it is very difficult to distinguish between packet losses due to mobility or channel errors and packet drops due to malicious node. So selective forwarding attack is even harder to detect than black hole attack.

![Selective Forwarding Attack](image)

**Figure 1.15: Selective Forwarding Attack**

D. **Sinkhole Attack:** In Sinkhole attack [18], a malicious node claims to be a base station. The aim of malicious node is to collect maximum network data by position itself on the point where maximum traffic flows in the network. The working of Sink Hole attack is shown in Figure 1.16. A network as shown in figure, a malicious node number 61 pretends to be a sink among its neighboring nodes (74, 87 and 91). The data of neighboring nodes (10, 14, 15, 22, 24, 26, 30, 49, 57, 65 and 67) of these neighbors (74, 87 and 91) is also collected by the malicious node because (74, 87 and 91) nodes are also act as gateway nodes for their neighbors.
E. **Sybil Attack:** In this type of attack, a malicious node presents a more than one identity at different locations in the network. Figure 1.17 demonstrates the working of a Sybil
Chapter 1: Introduction

Attack. In the network shown in the figure, malicious node number 37 pretends to be more than one identity at different location in the network.

F. Wormhole Attack: This attack is performed by more than one collaborating malicious nodes. In this type of attack, one malicious node collects packets at some location and tunnels them to another location to other malicious node in the network through a high quality out-of-band link. Other malicious node further retransmits these packets to some other location in the network. Figure 1.18 demonstrates the working of a Worm Hole Attack. In the network shown in the figure, malicious node number 40 collects packet at one end and tunnel them to other end at malicious node number 55 which again retransmit these packets to some other location in the network.

![Figure 1.18: Worm Hole Attack](image)

G. Hello Flood Attack [19]: Many WSNs protocols use the exchange of HELLO messages to update their one hop local neighborhood information. But a powerful malicious node broadcast a single HELLO message to every node in its wide communication range. The result is that every node receiving this HELLO message thinks that the attacker is within one-hop radio communication range to this malicious node.
1.2 RESEARCH OBJECTIVES

Due to the limited networking solution in wireless sensor networks, there is a still several applications that have not yet been fully investigated in the field of WSNs security. So it is very crucial to identify and authenticate each node participating in the network and all the data delivered to the network. Otherwise it is very easy for a malicious node to modify the collected information or to inject false information into the network. When the information provided by the networks increases, the risk of secure transmission of information over the networks also increases. To achieve the security requirements in wireless sensor networks, it is necessary that proposed mechanism is lightweight in nature for resource constrained wireless sensor networks. So to achieve the above WSNs security challenges the mechanism includes data encryption, secure key management, malicious node detection and Node revocation & replacement scheme. A brief introduction of the solutions that achieve the described security goals are given below:

• There is need to develop an efficient and secure data aggregation technique essential for cluster based WSNs for eliminating data redundancy to reduce energy consumption and hence to extend lifetime of the entire network.

• A secret key establishment between the source and destination by multiple intermediate nodes can require multi key requirement scheme where more than one key is required and used for the proper functioning of the network. Therefore, multi-key management schemes without communication overheads is a core requirement in wireless sensor networks.

• To achieve performance efficiency and reduce resource requirements in wireless sensor networks an encryption mechanism is required which is lightweight and dynamic in nature i.e. it produces different output irrespective of the similar input for different runs. Proposed technique eliminates the requirement of key distribution and establishment.

• There is need to design an efficient security mechanism that is used to revoke the functioning of a malicious nodes in the network. The basic idea of revoking a malicious node is key replacement scheme in such a way that the updated key is unavailable to the malicious node in the network.

• To increase the power of the system, an encoding scheme is require that along with a lightweight encryption function gives same complexity that can be achieved by heavy cryptography algorithm with no encoding scheme.
Chapter 1: Introduction

1.3 WORKS CARRIED OUT

Security is very important research objective in the field of wireless sensor networks. There are still many goals and open problems in the field of WSNs security. The need for security grows significantly with the rapid use of WSNs. Existing solutions are not suitable for resource constrained devices, so new techniques are required to make them secure. A simple model is required that would enable fully functional security in WSNs. A brief summary of the works carried out in the field of WSNs security are given below:

- Analyze security issue in wireless sensor networks.
- Investigate the application of Cryptography in wireless sensor networks.
- Design an efficient key management scheme that solves many of the shortcomings of existing protocols in the wireless sensor networks.
- Design secure data aggregation mechanisms for wireless sensor networks.
- Develop a model for removing & replacement of compromised Sensor Nodes from Wireless Sensor Networks.
- Develop a model to achieve the principle of forward secrecy, i.e. a sensor should not be able to read any future data.
- Develop a model to achieve the principle of backward secrecy, i.e. a joining sensor should not be able to read any past data.

The presented work considers the above challenges in this research work. The challenges include data encryption, secure data aggregation scheme, secure key management, malicious node revocation scheme.

1.4 THESIS ORGANIZATION

This thesis is organized into eight chapters. Chapter 2 provides literature review including the background for the subject of WSNs, secure data aggregation, key management, lightweight encoding scheme and removing and replacement of compromised sensor node from WSNs. Chapter 3 describes a model for secure data aggregation in WSN using class intervals. A virtual location based key management scheme has been presented in Chapter 4 for multi-key requirement scheme in WSNs. In Chapter 5, a key replacement scheme has been demonstrated for removing and replacement of compromised sensor nodes from the network using guard nodes with static clustering. Chapter 6 presents dynamic encryption function to convert the plain text message into cipher text message followed
Chapter 1: Introduction

by a light weight encoding scheme in Chapter 7. Finally, Chapter 8 concludes the work by re-evaluating the contributions followed by the future research directions opened by the mechanisms presented in this thesis.

1.5 SUMMARY

Security issues and remedies have been described in detail in this chapter. This chapter includes the justification and motivation behind the work presented in the form of doctoral thesis followed by the description of problem and thesis organization. In chapter-2, state of the art literature survey has been presented in detail.