CHAPTER 1

INTRODUCTION TO SECURITY ON DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

1.1 INTRODUCTION

Wireless sensor networks (WSNs) is an emerging technical approach for many real life applications such as military sensing, tracking objects, structural and environmental monitoring. It is a system of networked sensor nodes along with predefined functions for sensing and processing event information through real-world applications. Each sensor node resource is constrained with small memory, low processing power and limited battery power. In application domain sensors nodes are deployed in a specific region to monitor the environmental phenomenon such as temperature, pressure, humidity, sound and vibration. In the specified region the sensor nodes can observe and report the events that occur with its transmission range. During operation sensor nodes are left unattended to function autonomously without human intervention. Sensor nodes are allowed to sense the events that occur within their transmission range and report the sensed event information to the BS through multi-hop communication. An event is detected by multiple sensor nodes. Next the detecting sensor nodes collaborate among themselves to generate an aggregated event report before forwarding the event information.

The wireless link used for establishing communication in WSNs is open to everyone. Hence, an adversary is able to eavesdrop the information in
transit and may cause damage to the data and may prevent the data from safely reaching the Base Station (BS). Moreover, the self-organizing feature owned by the sensor node leads to frequent changes in the network topology. Therefore it is impractical to monitor and protect each individual sensor from physical or logical attack by means of traditional security mechanism. As a result it is important to secure the communications done in WSNs to achieve the benefits of the WSNs faultlessly (Akyildiz et al. 2002). The mechanisms used for achieving security requirements in WSN should be energy efficient with minimum resource consumption such as reduced storage requirement (Wang & Liu 2011; Nejati & Khoshbin 2010).

1.2 **NEED FOR SECURITY IN WIRELESS COMMUNICATION**

Wireless network is a network of wireless nodes that communicates with each other through radio waves or infrared waves. In wireless mode of message transmission the medium used for communication is invisible to the users. The nodes involved in wireless communication own short transmission range and mostly they are mobile nodes. Nodes within each other's transmission ranges are allowed to communicate with one another. The main security issue caused in wireless network compared to wired network is the ease of accessing the transmission medium. The transmission medium is open to everyone and anyone can monitor or participate in communications performed in a wireless network. An adversary is able to listen to the information on transit or interfere with wireless communication. Further, the short transmission range owned by sensor nodes led to hidden station problem which results in the collusion within the communications performed and may affect in loss of data.

Any communications neglecting the basic security features such as confidentiality, authentication and integrity may pave the way for the unauthorised users to retrieve and disrupt the communications in transit. In
addition, it may be possible for the attacker to intercept, interrupt and modify the communications received (Karlof & Wagner 2003). Hence it is important to provide security measures to control and manage accesses performed in wireless network to prevent unauthorised access and modification of wireless communications (Hyun-sung Kim & Lee 2009). This may results in the success of applications done through wireless network. So, an important issue to be focused when moving from wired network to wireless network is its security issue. It is necessary to provide effective security policies to protect the important resources against unauthorised access (Uluagac et al 2008).

1.3 CHALLENGES ON COMMUNICATIONS IN WIRELESS SENSOR NETWORKS

Wireless sensor networks uses air as the transmission medium that allows easy access to transmitted data by any potential eavesdropper. The wireless communication offered is open to everyone and it provides a way for the adversary to perform passive eavesdropping and active interception through false data injection, false endorsement and other Denial of Service(DoS) attacks over the event report in transit (Deng et al 2006). In general during operation sensor nodes are deployed in hostile environment where they are left unattended. It is practically impossible to monitor and protect each individual sensor node when deployed in large number (Samarah et al 2011). Moreover WSNs can scale to thousands of sensor nodes and demand for simple and scalable security protocols. However designing such scalable security protocols is a difficult task for resource constraint sensor network.

An important function to be performed in any application of WSNs is the collection of event information and directing the sensed event information towards the BS. In any application of WSNs it is expected to report event information accurately to the trusted entity the BS. In some
critical applications such as an application for forest fire detection and tracking the movements of enemy in surveillance it is important to report the event information accurately in a timely manner. Hence to achieve secure communication it is crucial to address the vulnerabilities caused by the adversaries to the communications and the nodes involved in communications.

In addition, due to the short transmission range owned by sensor nodes, any communications carried out between the sensor node and the BS is through multiple hops. The multiple intermediate nodes along with the communication path act as an entry points for the adversary to perform false data injection and other DoS attacks in WSNs. To achieve efficient communication with maximum performance it is essential to determine authentic and trusted nodes to function as next hop in forwarding the communications performed in WSNs. Furthermore the communications performed within the network can be affected through compromised en-route nodes in the communication path. A compromised en-route node is capable of monitoring the network traffic to collect the information about the nodes involved in communication. The compromised nodes are allowed to compromise other en-route nodes which may result in network capture attack.

Therefore it is important to detect and drop the compromised en-route nodes as early as possible. Event information collected by the sensor nodes of WSNs may be accessed by the users outside the network. Hence, it is necessary to provide data authentication and source authentication information along with the data because data collected from sensor nodes should be confidential and only authorised users are allowed to access the information. Also the users should accept communication received from only legitimate nodes to avoid false and invalid information. The traditional security mechanisms are unable to provide privacy for the communications
performed because cryptographic mechanisms are able to protect the data part of the packet but the header part of the packet is kept open. Therefore it is necessary to have certain security mechanisms to protect the privacy of the communication in transit.

1.4 ISSUES IN DESIGNING SECURE COMMUNICATION SCHEMES FOR WIRELESS SENSOR NETWORKS

Due to the resource limitations of sensor nodes and the design constraints followed in WSNs, it is difficult to use the traditional security mechanisms for WSNs applications. Hence, it is necessary to propose simple, flexible and scalable security mechanisms to provide strong security over the communications performed in WSNs. The issues to be addressed in designing secure communication schemes for WSNs can be classified into four types. They are resource related issue, communication related issue, environmental issue and issues regarding the design constraints to be considered in constructing WSNs (Liang et al 2011; Zhou et al 2008).

Resource related issue: One of the problems that occur while designing security protocol is to propose security mechanism with high security features making use of the limited resources owned by sensor nodes. WSNs are cheap with each sensor node containing small memory, low battery power, low processing power and limited bandwidth. Security approaches designed for providing security in traditional network is not applicable to WSNs due to their complexity in computation, communication overhead and the large memory requirement. Further, these algorithms consume more power. Hence it is essential to design light weight energy efficient security mechanisms suitable for WSNs.
Communication related issue: The wireless link used to establish communication between sensor nodes in WSNs is unreliable and open to everyone (Ren et al 2011; Lopez et al 2009). The occurrence of frequent node failure and bad link quality maintained by intermediate sensor nodes involved in communication results in unreliable data transmission. Further, adversary denies the communications performed in WSNs through compromised en-route nodes. The compromised nodes perform false data injection attack, false endorsement attack and path based denial of service attack. By means of these malicious activities compromised node or an adversary prevent the data from safely reaching the BS (Sarkar & Mandal 2009). Hence, it is essential to authenticate the nodes along with the communication path to identify legitimate nodes involved in communication. On the other hand it is necessary to ensure the principle of unabsorbability and unlinkability during communication to enhance security. Traditional end-to-end security mechanism failed to guarantee secure communication in WSNs due to the weakness that exists in the multi-hop links of WSNs.

Environment related issue: During operation sensor nodes are deployed in a hostile open environment and are susceptible to physical attacks. Attackers can extract the cryptographic credentials, tamper with the associated circuitry, modify the programming in the sensors and replace the source code maintained by malicious codes. The close interaction of the sensor nodes with the surrounding deals with node capturing attack. Lack of tamper-proof hardware and software subjects the sensor nodes to physical node capture attack (Zhou et al 2008; Zhu et al 2011). It is necessary to have security approaches to determine physical tampering and withstand the damages caused to sensor nodes from the surroundings (Pietro et al 2009a; 2009b; Zhu et al 2011).
Design constraints related issue: Designing security mechanism for WSNs requires a detailed knowledge of wireless sensor networking technology and its characteristics in providing security measures. Confidentiality, authentication, integrity are the basic and essential security services used to achieve security in WSNs. Ensuring security in such an environment becomes a critical issue because strong security algorithms have to be implemented to ensure security in WSNs as weak security mechanisms can be easily broken by an adversary. Implementing strong security algorithm requires more resources, which is difficult in WSNs due to the limited resources maintained in sensor network (Pradeepa et al 2012). Further, this creates a disagreement between minimizing resource consumption and maximizing security (Hyun & Kim 2006). In addition, the security protocol designed for WSNs should be scalable because the network extents to thousands of sensor nodes.

1.4.1 Issues in Present Security Mechanisms

An important requirement of WSNs operation performed by critical application is to secure the communication performed in WSNs. Security in communication can be ensured through cryptographic operation. Cryptographic operation is based on the principle of key management. An important issue to be addressed in achieving security through key management is to distribute or share the secret key between the source and destination (Kavitha & Sridharan 2010). The second issue to be addressed is the hop by hop encryption and decryption of the data to be exchanged between the source and destination.

1.4.1.1 Key sharing issues

Security in WSNs is achieved through key management schemes (Zhen & Guan 2010). Key management includes key generation key distribution and key revocation (Zhihong Liu et al 2009) Key generation
algorithm should be simple and resource efficient. Before ensuring secure communication, the key used to perform cryptographic operation should be securely and efficiently shared with the entities involved in communication. Sharing key securely in unreliable WSNs is an issue. Different kinds of keys can be shared between the communicating parties by different security mechanisms (Mittal & Novales 2010; Jang-ping et al 2007). But some of the present security mechanisms are impractical for WSNs due to the limited power, low memory, low processing power and limited transmission range owned by sensor nodes. Key revocation is an issue due to the dynamic topology owned by WSNs. Issues faced through key management in present security mechanism can be described as follows.

Asymmetric key cryptography: In asymmetric cryptographic schemes (Zhihong Liu et al 2009) each node should maintain two related keys in that one of the key is made public and other is made private. The data should be encrypted with the public keys and decrypted with the private key (Su et al 2007). Asymmetric cryptography is unsuitable for low power devices like wireless sensor network due to the intensive computation and communication performed in ensuring security (Amin et al 2008).

Single network wide key: Here a single common key is shared among all members involved in the communication (Alcaraz et al 2012; Tian et al 2009). By means of this mechanism the key space occupied by individual sensor node for storage is reduced. While establishing security no need to perform key discovery or key exchange between sensor nodes. Even though this scheme ensures reduced memory and computation, this scheme suffers from node compromisation problem since compromise of a single node results in compromise of the entire network.

Pair-wise key establishment scheme: In this scheme keys are distributed to nodes in such a way that each node is assigned a unique key. For a WSN with ‘n’ nodes each node needs ‘n-1’ unique keys to be stored in
its memory (Jang-ping et al 2007, Kwon et al 2009). This scheme is suitable for small network and limits its applicability for large network.

Key pre-distribution scheme: In achieving security a set of keys from a key pool are distributed to each sensor node before deployment (Liu et al 2008; Delgosha & Fekri 2009). After deployment sensor nodes determine the common keys shared between the source and destination for establishing secure communication (Zhou et al 2009; Zhang et al 2009). This scheme consumes more key space for storing a set of keys and may be subjected to compromisation of uncompromised nodes by compromised node due to key sharing probability and cannot be used in situation which demands for achieving perfect security (Hussain et al 2009). In these schemes even though security is increased the probability of breaking the secure network connectivity gets increased due to the key sharing probability among neighbour nodes (Yu et al 2010). In this scheme rekeying is complex hence addition or deletion of a node to WSNs is impossible. Disadvantages of key pre-distribution scheme are Poor scalability and high storage requirement.

Symmetric key cryptography: Symmetric key cryptography is preferred than asymmetric key cryptography due to minimum computation and communications performed in key sharing. But traditional end-to-end symmetric key sharing mechanisms (Azarderskhsh & Reyhani 2011) are not suitable for WSNs due to the issues faced by compromised node on the path of communication. Compromised en-route node can modify or add false information to the secret key in transit or even prevent the key from reaching the intended destination.

1.4.1.2 Data sharing issues

The multi-hop communication followed in WSNs allows multiple entry points for the adversary to participate in the communication performed.
As the topology of the network changes frequently, it is necessary to choose efficient alternate paths each time while establishing communication with a destination node. Also en-route nodes may be compromised by an external adversary and the compromised nodes are forced to perform malicious activities (Zhang et al 2006; Ozdemir & Cam 2010). Compromised nodes inject false messages, perform false endorsement and deny the communications from safely reaching the BS. Cryptographic keys shared with one or more nodes find the way for a compromised node to compromise other uncompromised nodes through key connectivity (Ruan & Sun 2011).

Further untrustworthy en-route nodes with low link quality perform routing attacks such as packet dropping, route misdirection and increase the delay which occurs during transmission. Hence it is necessary to determine trusted next hop to ensure reliable data transmission in WSNs. Along with reliability to ensure security it is necessary to use authenticated nodes to forward the data in transit (Daojing et al 2011). Assigning authentication information along with the dynamic path is also considered as an issue.

1.4.2 Contributions of the Thesis

The main concept contributed in the thesis is to establish secure communication between a sensor nodes and the BS. To perform this in an effective manner it is important to identify the challenges faced in existing secure communication schemes. The first study analyse about the issue that arise along en-route while establishing secure communication. In secure communication schemes (Chia-Mu et al 2011; Hong et al 2013a) the secured data is transmitted through a single path and the data in transit is exposed to the compromised en-route node along the communication path. The compromised en-route node is able to retrieve the data in transit, inject false data and prevent the data from safely reaching the BS. The affected data if allowed to reach the BS wastes the energy of the en-route nodes and the BS.
To overcome the issues faced in the existing schemes proposed scheme focus on multipath data transmission and en-route authentication mechanisms.

The second study investigates about the issues that arise in group communication and how to strengthen security in group communication. In group communication schemes the authentication keys used to generate the group key is derived through a key chain (Yuan et al 2013; Katz & Yung 2003). The key dependency property that exists among the nodes in a group show the way for node compromisation problem (Sivaraman & Ostry 2011). The compromised nodes try to compromise other nodes and collude with themselves to perform illegal sub group generation. The problems that arise during group communication in existing schemes have been addressed in the proposed mechanism. Proposed scheme uses a secret sharing mechanism and a collusion detection technique to ensure secure group communication. The proposed scheme is highly resilient to insider and outsider attacks.

The third study focuses on the problem that arises due to the involvement of unauthorised intermediate nodes along a multi-hop path during data transmission. In schemes (Chin-Fu Kuo et al 2009; Alshawi et al 2012) the involvement of unauthorised nodes may perform replay attack, false data injection attack and other path based DoS attacks. To increase the performance of end-to-end data transmission in WSNs, it is essential to involve trusted en-route nodes along the communication path or determine efficient next hops for forwarding the data. The proposed scheme is able to achieve reliability and security during data transmission. The proposed routing scheme selects trusted next hop for forwarding the data.

The fourth study analyses about the problems that arise against privacy during data transmission. The security mechanisms (Uluagac et al 2010b; Luk et al 2007) provide cryptographic operation to provide security of the payload part of the packet. The header portion of the packet is kept open.
Hence the compromised node along the communication path may be able to gain the traffic information and damage the header portion of the packet by changing the identity of the source and destination and may perform route misdirection attack. The proposed scheme is able to ensure privacy along with security. Instead of using real source and destination identity, pseudonyms are used to represent the source and destination information.

1.5 OBJECTIVES OF THE THESIS

Objectives of the thesis are:

- To achieve secure communication through multipath data transmission by addressing the issues such as eavesdropping, packet dropping and false data injection attacks caused by adversaries through compromised en-route nodes.

- To establish secure group communication through secret sharing for large scale WSNs with minimum computation and communication overhead.

- To determine trustable forwarding nodes to enhance the security and reliability of a query based communication performed in WSNs.

- To design and implement anonymous secure communication scheme to achieve end-to-end security and to find an optimal for establishing secure communication.

The brief introduction about each of them is given below.

Secure communication through multiple disjoint paths: The key used for securing the data should be efficiently distributed through two disjoint paths. Further the secured data is also send through the same paths.
used for key sharing. For the real-life application carried out by WSNs, it is essential to make sure that the sensed or observed information can be correctly and accurately delivered to the destination. This can be achieved by the proposed mechanism by filtering the false data injected by a compromised node and prevent the direct exposure of data to compromised en-route node. Reliable data transfer can be done efficiently by reducing the chance for data compromisation.

Secure group communication through secret sharing mechanism: For WSNs applications where the sensor nodes are densely populated, it is necessary to perform key sharing and data sharing in an energy efficient manner. This can be achieved through group communication. Here the group members collaborate among themselves to generate the group key for each and every session. Secure data transfer can be achieved through inter and intra cluster communication.

Secure query based communication through trusted forwarding nodes: In infrastructure-less WSNs random selection of next hop forwarding node would result in malicious activities or get exhausted quickly. To increase the lifetime of the forwarding nodes and to protect the data from damaging this research focus on selecting trustable node for forwarding the data. Further, the proposed method resists the denial of service attack that occurs in the path of data transfer. This scheme enhances the security of query based request response send by the communicating entities.

Anonymity and security in data transmission: In some critical situations such as forest fire detection through WSNs, it is very important to report the authenticated event information immediately without any delay. This can be achieved through proposed scheme by performing the cryptographic operations encryption and authentication through pre-defined secret credentials for every session. Further, the proposed scheme support for
achieving anonymous communication to protect the privacy of the data on transit.

1.6 ORGANISATION OF THE THESIS

The thesis is organised in seven chapters.

Chapter 1 ‘Introduction’ gives a brief idea about the security issues in WSNs. The need for security requirement in WSNs has been discussed and existing key management mechanisms and problems that occur when applying traditional security mechanism for WSNs have been explained. The main objective of the thesis is explained in detail. The focused objectives are designed and evaluated as secure communication schemes in the area of multipath data transmission, secure group communication, trustable next hop selection and anonymous secure communication.

Chapter 2 ‘Literature Survey’ presents a literature review to provide necessary background for a general understanding of challenges faced while establishing communication in WSNs. This chapter presents an overview of latest literatures in the following areas. Various secure multipath data transmission schemes and literatures related to false data detection mechanism through en-route filtering have been reviewed. Security mechanisms for group communication have been studied. In establishing secured and reliable data transmission various trustable forwarding node selection mechanisms have been studied. Fuzzy based optimal path selection schemes have been discussed and different ways for ensuring anonymity during communication have been surveyed and analysed.

Chapter 3 deals with “Energy efficient secure multipath data transmission scheme”. This scheme aims at improving the packet delivery ratio and to prevent the direct exposure of secured data to compromised en-route node. This chapter explains about how end-to-end security is achieved
in key sharing and data sharing. Mechanisms used for generating multiple disjoint authenticated paths are also explained. Further, it describes how false data injected by compromised en-route node can be filtered en-route other than detecting and dropping by the base station. This scheme is energy efficient in terms of computations and communications performed in providing security for WSNs. The outcomes obtained from this work are: data compromisation probability is very low, efficient false report filtering at en-route and achieves unabsorbability.

Chapter 4 deals with “Authenticated group communication scheme”. This scheme aims at resisting collusion and related attacks that occur during group communication. This chapter explains about an inter cluster, intra cluster key sharing mechanism and explains the involvement of compromised node within the cluster or a group in key sharing and data sharing. An efficient authentication mechanism which authenticates the node involved in communication is discussed. This scheme prevents the involvement of outside and inside attacker. Further the proposed scheme is able to achieve key refreshing, node authenticity, forward and backward secrecy.

Chapter 5 deals with “Secure and trust-aware communication scheme”. This scheme aims to secure query request response message communicated in WSNs. This chapter explains how a trustable next hop is selected for effective packet delivery and how the data and a symmetric key are securely routed through trustable intermediate nodes. The factors considered in next hop selection such as residual energy and link quality are suitable for fault tolerant data transmission. The following outcome has been derived in this work: high packet delivery ratio with maximum network lifetime, resilient to replay attack and path based denial of service attack.
Chapter 6 deals with “Anonymous secure communication scheme” which ensures anonymity along with security through key management operations. This chapter explains how security is achieved through pre-defined secret credentials and receiver anonymity by mixing destination address with encrypted event information. Also, it defines about how an optimal path is constructed from source towards the BS through fuzzy based approach. This scheme is able to achieve strong confidentiality against breakage of event report to get the secret key. Also compromising a node does not provide the chance for compromising other uncompromised nodes due to low key sharing probability with the neighbouring nodes. This scheme is able to achieve unlinkability and unabsorbability of the communications performed.

Chapter 7 “Conclusion and future work” summarizes the outcomes of the research work and outlines possible direction for future research. The first work concludes that data cannot be exposed to adversary in multipath data transmissions and en-route nodes verify the authenticity of data. In the second study energy efficient key sharing mechanism is explained. It resists the effect of compromised nodes during group communication and ensures strong security. Third study points out secure and reliable data forwarding through trustable next hops. It achieves high throughput and increased network lifetime. Fourth study proves how anonymity and security is maintained in communication. This work shows strong network connectivity during data transmission.