CHAPTER 2

LITERATURE SURVEY

2.1 WIRELESS SENSOR NETWORKS

This chapter deals with the survey of the vast literature contributing to the development of secure communication schemes. The literature on improving security in routing and data transmission has been reviewed. A brief review has been made to different security modules to improve security in data transmission. The initial part of this section gives an overview of WSNs characteristics, security related issue, challenges to be faced in designing WSNs for various fields. The literature survey emphasizes the importance of different secure communication schemes which shows the way for improving security during data transmission.

WSNs attract significant interest from research community due to their wide range of applications in environmental sensing, battle field sensing and hazard leakage detection. Sensor nodes are deployed in an unfriendly area in an ad hoc manner. No centralized authority is there to control and co-ordinate the activities performed by sensor nodes in WSNs. When a particular sensor node is compromised or captured all the information preserved in the sensor node is disclosed to the adversary (Giruka et al 2009). In addition, end-to-end communications done between sensor nodes and the Base Station (BS) may be affected by compromised intermediate nodes. An intermediate node on the path can be compromised by an adversary. Hence, the secured information preserved in the compromised sensor node can be disclosed to the adversary.
Further, if the compromised node owns the secured information for determining the secret key, the information about key generation can also be disclosed to the adversary. This creates a chance for more number of nodes to be compromised which result in the compromisation of entire network. Therefore, it is necessary to secure the data on transit from the malicious activities of the adversary.

In general in any WSNs application, sensor nodes collect data from the sensing field and periodically report the sensed information to the BS. It is impossible to prevent node compromisation attack in WSNs due to the unattended nature of sensor nodes. But the consequences of the compromised node can be reduced through security protocols without affecting the entire network. Hence, it is necessary to include security mechanisms at the design stage in any WSNs application. One method to ensure data security in WSNs is through key management (Lee & Cho 2010; Liu & Cheng 2008). The objective of key management is to generate, distribute and revoke keys as required to the sensor nodes for establishing secure communication. This key is used to encrypt or decrypt the data to be communicated within the WSNs.

Along with end-to-end security it is necessary to establish link level security (Eissa et al 2012; Pelaez et al 2010) between intermediate sensor nodes on the path of data transfer. So, it is necessary to distribute pair-wise key between intermediate nodes to ensure link level security (Delgosha & Fekri 2009; Khan& Alghathbar 2010). Different secure communication schemes have been developed to resist the vulnerabilities caused by adversary to data in transit in multi hop WSNs.

Shi & Perrig (2004) discussed about the security issues that occur due to unreliable wireless communication and resource limitation of WSNs. They described the mechanisms to be followed for establishing secure communication. Moreover, they explained about how the proposed
mechanisms address the issues. The authors described about the security threats that occur within the network and the vulnerabilities caused by attackers outside the network. The countermeasures to overcome the insider and outsider attacks are clearly described. They also expressed the need for secure routing protocols for WSNs.

Wang & Liu (2011) performed a study on recent advances in WSNs and their application in collecting sensitive information from the surrounding. The researchers explained in detail about sensor data collection in three different stages named as deployment stage, control message distribution stage and data delivery stage. They gave details about the challenges faced during data collection in different stages. Authors discuss about the existing approaches to overcome the challenges faced in different stages. Further they not only reviewed about the problems faced in the existing approaches by an analysis, but also proposed new techniques to address the problems faced in the previous methods.

Gungor & Hancke (2009) discussed the benefits achieved through WSNs in industries and their advantages over wired network. Further they described the challenges faced by industrial WSNs. They described design goal to be followed to overcome the challenges faced in industrial WSNs. Technical approaches to be explored in hardware development, software development, protocol design and system architecture are clearly explained.

Chee-Yee Chong & Kumar (2003) described about the research issues on WSNs in different applications and analyzed about the sensor nodes created and used in three different generations. Moreover they explained describe about the technical challenges faced in sensor network on hardware and software level due to their application specific nature. The authors described about the development to be performed to overcome the technical issues faced in earlier stages of sensor network developments. Developments
to be made in sensing, computing and communication to face the technical challenges are described.

Shi-Chun Tsai & Tzeng (2009) proposed a scheme to defend key storage depending adversaries. The authors described about the need for communication security since adversaries can eavesdrop the communication and store the revealed information in their memory for future use. This lays the foundation for key sharing between two unauthorized sensor nodes and the revealed key can be used for sharing authentication information. The key can also be used to break the secure message received in succeeding communications. To overcome such problems the authors proposed two key sharing mechanisms. One technique uses beacon nodes for broadcasting random bits used as authentication measure which prevent retrieving the secured key. In the second method the sensor nodes perform the role of beacon nodes.

Jaydipsen (2010) discussed about the security issues during routing with the sensor nodes in WSNs. The author enumerated the attacks or vulnerabilities occurred in wireless communication. He described the security issue and the physical attacks happened to resource constraint sensor nodes. Further he described the mechanisms to withstand the issues and resist the misbehaviours of the unauthorized nodes that are involved in communication. The author described the layer-wise attacks that occur in WSNs during routing and the countermeasures to overcome the attacks. In addition he carried out a study on the topics key management, secure data aggregation, secure routing and intrusion detection in WSNs. Some future trends in WSNs security were identified and defined.

Alcaraz et al (2012) carried out a study on key management schemes for WSNs. The authors specified the requirements and properties of key management schemes and provided a review about a suitable scheme and
its related application. The authors focus on establishing link layer security and explained about KMS in four frameworks. The frameworks are key pool framework, public key framework, mathematical framework and negotiation framework. They provide information about advantages and disadvantages of different schemes. Further, they described how to design a new protocol to overcome the issues of existing approaches.

Zhou et al (2008) performed a review on identifying security issues in WSNs and how to overcome these issues. The author’s discussed the characteristics of WSNs which are vulnerable to various attacks and classify the attacks in different point of view. They described about the solutions to defend against these attacks such as key management schemes, authentication schemes, integrity protection and protection based on availability. The authors studied about the advantages and disadvantages of each schemes. They provided the direction for future research to overcome the drawbacks of the existing schemes.

Xiao et al (2007) studied about key management schemes for WSNs which considers secrecy along with resistance, revocation and resilience in key management. The researchers described about single network-wide key, pair-wise key establishment schemes with trusted base station. Further, they described the key pre-distribution schemes, hierarchical key management scheme and key management schemes for heterogeneous sensor networks. They discussed each of the techniques along with their advantage and disadvantages which provides suggestion in selection of a suitable key management scheme based on the available resource. The tradeoffs that lie between minimum resource consumption and maximizing security were discussed.

Chen et al (2009) performed a study on securing sensor network and identified the threats and vulnerability to WSNs and described the
defence based on networking protocol. Security issues were divided into seven categories. Advantages and disadvantages of current security schemes are determined and analysed. The authors used certain metrics such as reliability, scalability to measure the performance of security protocols and further classified the attacks into internal and external attacks and explained about the security issues related to energy, compromised node and unreliable transmission. In addition, they discussed about the problem that are not yet solved and should be given more attention.

Yick et al (2008) described the WSNs and its application in different environments. Further, described the characteristics of sensor nodes and their usage in applications due to their salient features. They compared the characteristics of WSNs with traditional wired networks. Herewith discussed about the issues in wireless networks and how they can be overcome. They identified the different issues faced when performing different WSNs application. In addition, they categorized the applications and determined the advantages and disadvantages of sensor node in each application.

Pantazis et al (2012) discussed about a study on routing protocols in WSNs. They classified the routing protocols based on four different views such as network structure, communication model, topology based and reliable routing. Based on network structure the protocols were classified into flat and hierarchical routing protocols. Based on topology they are categorized into location based and mobile agent based. Authors described about route selection policy through the routing metrics residual energy, transmission power and link distance. Further, description is made about the term used to evaluate the performance of routing protocol. The common factors affecting routing in WSNs were discussed. The authors described different routing protocols and their usage in different circumstances and application specific.
Camtepe & Yener (2005) evaluated the performance of deterministic, probabilistic and hybrid type of key pre-distribution schemes. Also dynamic key generation algorithms for pair-wise, group-wise and network-wise keys were described. The authors mainly focused on evaluating the key pre-distribution schemes based on network architecture into distributed and hierarchical key pre-distribution schemes and based on communication styles into pair-wise, group-wise and network-wise schemes. They described more than one solution for a key pre-distribution scheme and compare the related schemes with each other based on scalability, key connectivity, storage complexity and identified an efficient mechanism at particular instant. Further efficiency can be achieved by measuring storage, computation and communication complexities.

Lee et al (2007) described the issues of key management schemes for WSNs. They explored the need for key management, operational requirements for key management and discuss about some of the existing key management schemes. The different stages of key management include key setup, key pre-distribution and key revocation are given in detail. The author’s analysed about five different key management protocols and compared their performance, advantages and disadvantage. Further, they discussed about the recent trend towards the development of the existing key management schemes.

2.2 SECURITY THROUGH MULTIPATH COMMUNICATION

Wenjing Lou & Kwon (2006) presented H-SPREAD, a scheme to share a data securely through multiple node disjoint paths. Secrecy and reliability can be achieved through the proposed scheme. The investigator achieved resiliency against data compromisation since a single compromised node cannot reveal the message even if a path is attacked. Branch-aware flooding mechanism and extension of the flooding mechanism is used to
generate multiple node disjoint paths. However the technique followed here cannot provide enhanced security. The adversary can perform attacks to prevent destination from receiving the original information. Further, no authentication mechanisms were followed in this scheme.

Ling & Znati (2005) described about end-to-end key sharing between sensor nodes through multiple disjoint path. In this scheme single key to be shared is divided into fragments and each fragment is sent through a disjoint path. Adversaries could not reveal the original key even if a single path was compromised. The performance evaluation shows that even though secret key is protected by splitting into fragments, yet this scheme is subjected to denial of service attacks. The energy of the intermediate nodes can be reduced by performing replay attack through compromised en-route nodes.

Liu et al (2012) proposed a secure and energy-efficient disjoint multipath data transfer scheme to prevent eavesdropping of the secured information. The researcher used a secret sharing mechanism to share the data fragments through randomly selected disjoint paths. The performance evaluation shows that the proposed scheme is efficient in terms of low energy consumption and strong security against black hole attack. They provide suggestions to improve the performance of the proposed scheme by mitigating the effect of packet loss and occurrence of delay.

Xu et al (2012) described about the issues in acoustic communication and proposed a mechanism for reliable and energy efficient communication in Underwater Sensor Networks (USNs). In this scheme every forwarding node detects and corrects the errors in the received packet by an error correction mechanism. Performance has been evaluated by comparing with single path communication scheme in terms of decoding efficiency, delay and energy efficiency.
Kohno et al (2012) described a mechanism to show the benefits of disposed data transmission in small or large network. Authors followed a tree based routing mechanism and multiple paths are constructed from source towards destination. Performance improvement has been assured in terms of secrecy, timelines and flexibility to heterogeneous sensor nodes with dynamic topology. The performance of the proposed scheme is measured by changing the factors such as node density and hop count between source and destination.

Challal et al (2011) discussed about the benefit achieved through a fault tolerant routing mechanism. The authors focused on two different approaches to improve security in routing. One approach used for generating multiple nodes-disjoint paths and other mechanism to enhance security by distributing keys along the path. The authors give importance to security by authenticating every node along the path using a one way hash-chain. Authors analyzed the proposed scheme and found that this scheme offer increased network lifetime. Also the simulation results show that the proposed scheme is highly tolerant to failure caused by intermediate nodes. They identified some issues that occur due to the limited number of disjoint paths generated for data transmission.

Nasser & Chen (2007) proposed an energy efficient routing scheme. Authors used this scheme in occasions where routing is initiated the routes by the BS. It is found that the proposed scheme is more secure. Authors focus on the parameters residual energy of a node and hop count in selecting the route nodes. The proposed scheme resists worm hole attack and selective forwarding attack. Performance of the proposed scheme was evaluated in terms of throughput, control overhead and network lifetime by comparing with direct diffusion protocol.
Stravrou & Andrea (2010) analyzed the security feature and performance of multipath routing schemes. The authors surveyed different multipath routing schemes and categorized the reviewed schemes into three classes based on their security-related operations handled. The security features were categorized based on multipath transfer, security based on resilience to different types of routing attacks and based on the security services performed. They developed performance comparison charts based on the security requirements, insider and outsider attacks for the different multipath routing schemes.

Deng & Han (2008) identified the issues of random pre-distribution schemes and their weakness in path attack. In the proposed scheme authors mainly focused on increasing the secrecy of secret key transmitted along the multiple paths. They achieved the secrecy by encoding the secret key using a maximum distance separable (MDS) code. However, the mechanism followed here did not provide complete security. The proposed scheme was affected by node capture attack and congestion along the path due to retransmission of packet as requested by destination node and found that the proposed scheme has performance efficiency in terms of reduced transmission cost and security efficiency by preventing the disclosure of secured information on transit.

Zhang & Jiang (2012) discussed about a mechanism to detect the vulnerabilities caused during communication and focus on detecting the false data injected by a compromised en-route node. The security and efficiency of the proposed scheme is increased by detecting and dropping the false data injected by compromised en-route node as early as possible along the en-route before reaching the BS.

Ye et al (2005) proposed a statistical en-route filtering scheme to address false data injection problem caused by an adversary through compromised node. The scheme was designed in such a way that only few
intermediate nodes verify the packet during report forwarding. This scheme has low filtering probability and a complicated mechanism for key sharing among neighbouring nodes.

Zhu et al (2004a) proposed a hop-by-hop authentication mechanism to authenticate the packets before forwarding. The authors used this mechanism to large scale WSNs since authentication is performed in an interleaved hop-by-hop manner and all the forwarding nodes were not involved in authentication process. Further, they generated association among the forwarding nodes by producing upper and lower associated keys. This scheme could not be used in environments where topology changes dynamically since the change in topology led to development of different paths for varying associations.

Uluagac et al (2010a) discussed about a security protocol used to enhance security during communication and used virtual energy to generate the keys used for encryption or decryption. One time dynamic keys were used for each session to overcome the issues caused by using stale keys. The authors followed an approach to secure the data during transmission. Intermediate nodes along the path of data transfer verify the authenticity and integrity of the packet before forwarding the packet. The receiving node verifies the authenticity by means of the key computed using sender’s virtual energy.

No special messages were used for dynamically generating the key for each session. The authors used this scheme to detect and drop false data packets injected by attackers outside the network. If the packet is found to be illegitimate the packet is dropped immediately. They determined that the energy spend for rekeying is very low with little computation and communication overhead. The authors evaluated the performance of the proposed scheme through theoretical analysis and simulation results. They
have specified the enhancements to be made in the future with an approach to overcome insider attacks and dynamic paths with varying topology.

Lu et al (2011) studied about a bandwidth efficient authentication technique to address false data injection attack performed by compromised sensor node. Before sending the event information to the BS, source node generates some authentication information for the event information from a fixed number of neighbours. The authenticated information is compressed into a single bit and endorsed along with event information. The authors generated the event report containing the authentication information and a timestamp value. They determined that by means of the timestamp value replay attacks are avoided. The authors analyzed the filtering efficiency of each en-route node along the path and concluded that the proposed scheme has high filtering efficiency with a simplified security mechanism.

Kraub et al (2007) followed a ticket concept for identifying a valid packet and used this scheme to resist replay attack and path based denial of service attack during data transmission in WSNs. Here three different types of keys are preserved by different sensor nodes. The forwarding nodes hold a ticket and the ticket measures the authenticity of the packets to be forwarded. This scheme is suitable for cluster based environment and for securing query based data transmission. As the authors used the ticket as the authentication measure, the event report with invalid ticket is dropped immediately. The authors did not use any key sharing mechanism to enhance the secrecy. They evaluated the performance and confirmed that the proposed scheme is implemented with low energy consumption and minimum computations.

Yang & Songwo (2004) presented an en-route filtering scheme to detect false reports generated by malicious nodes within the network. The authors used authentication key, session key and witness key for ensuring security in the proposed scheme. Forwarding node verifies the validity of the
received packet by means of the witness key and drops the packets without witness key. The authors noticed that the false data packet sent by compromised cluster head could not be detected in this scheme. As the forwarding node does not verify the content of the event report, false report send by compromised cluster head is delivered to the base station.

Wenjun et al (2011) proposed a secure communication scheme to overcome the security relevant issues during communication between pair of sensor nodes. They described how to pre-distribute different types of keys to different sensor nodes and share keys between pair of sensor nodes. One of the possible attacks performed during data transfer between sensors is eavesdropping. This scheme increases the resiliency against node capture attack through end-to-end key sharing. Authors randomly distributed the sensor nodes into different classes and distribute different key to nodes belonging to different classes. After distributing the keys they tried to find out the neighbours of nodes. They identified their one hop and two hop neighbours. Each node share pre-distributed keys with one hop and two hop neighbours.

During transmission encryption or decryption is performed hop-by-hop. Thus false data injection and denial of service attacks are prevented. This scheme is subjected to biased node capture attack. Here secret information maintained in node near the base station can be disclosed. This particular node receives or forward more traffic. The authors evaluated the scheme and observed that the heterogeneity in topology such as more traffic for the node near base station and non uniform distribution of keys has high impact of attack.

Ren et al (2008) discussed about a technique proposed to provide data security in WSNs. The authors used the location information to generate the keys. This scheme is applicable to static WSNs and authors collect the
location information of the sensor nodes after deployment using a localization scheme. The deployment area is divided into grids and each grid consists of number of cells. Three different types of keys are assigned to each sensor nodes. This location based scheme resists the impact of compromised node on the event report generated by the neighbouring sensor node. The authors observed that this scheme provided the security features such as confidentiality, authenticity and availability. Authors evaluated the performance of the proposed scheme based on false data filtering efficiency, high resiliency against selective forwarding and node compromisation attack.

Zhiong Liu et al (2010) proposed an asymmetric key pre-distribution scheme for heterogeneous WSN consisting of users with different task. The authors performed the key distribution in two phases. Distribution phase and computation phase. During distribution phase the secret key is assigned to users by a trusted authority and public keying material is assigned to the different keying material servers. During computation phase session key is generated by the privileged users. Other users are not able to generate the session key. This method of key pre-distribution increases the communication cost and requires more memory for storing the keying material.

McCusker & O’ Connor (2011) described a symmetric key distribution scheme and identity based cryptography to ensure access control along the WSN. The authors mainly focused on preventing unauthorized access and unauthenticated node to join the network during communication. The authors applied this scheme for static WSN and pre-distribute private keys to nodes before deployment. They used key generation centre (KGC) to distribute public key to nodes. The nodes with valid signature were allowed to join the network. Further identity and timestamp are assigned by KGC to the valid nodes to avoid replay attack. This scheme has high resilience to the
impact of compromised nodes and achieves enhanced development in implementing security.

2.3 SECURITY DURING GROUP COMMUNICATION

Group communication is proven as an effective concept to implement applications of WSNs. If the WSNs under consideration are densely populated then it is essential to organize the sensor nodes into clusters. This helps to achieve energy efficient operations. Moreover, grouping nodes into clusters has been the most accepted approach for supporting scalability and energy efficiency in WSNs (Camtepe & Yener 2007; Traynor et al 2007). Further, cluster-based WSNs are considered robust because compromise of a node in a cluster will affect that cluster alone and not the entire network. When implementing wireless sensor network applications there exists a strong interaction between sensor nodes and the physical world. To make use of the benefits of group communication, it is necessary to protect the communication done within a group. One method of securing the group communication is through group key management.

Group key management protocols are classified into centralized group key management and distributed group key management (Liu et al 2013). Group key management protocols allow the communicating entities within a group to generate a common secret group key (Wei-deng et al 2013; Kumar et al 2009). Group key establishment protocols can be classified into group key agreement protocols and group key transfer protocols. In group key agreement protocols each group member contributes its part to generate the group key for the particular session. In group key transfer protocols a trusted entity of a group generate and distribute the group key to the group members for the particular session. Distributing the key to the authorized member is a problem in distributed systems like WSNs. Further, in group-oriented applications it is necessary to ensure authenticity and confidentiality of
messages communicated within the group. The data communicated in the group of authorized members should be secured and inaccessible to the outsiders. Various mechanisms have been proposed to secure key sharing and secure group communication for WSNs. This section reviews works regarding secure group communication in WSNs.

Dini & Savino (2011) discussed about an authenticated rekeying scheme for cluster-based WSNs. The authors used this scheme for applications where group members are selected on a logical basis and not based on their physical closeness. The secrecy during communication for such applications can be achieved through key graph and key chain. Key graph has been used to specify the group which supports for efficient group re-keying. The authors described about achieving forward and backward secrecy through the proposed scheme. The proposed scheme follows a centralized key distribution based on key graph and key chain. The Key Management Server (KMS) performs the role of generating and distributing the keys to the group members. Session key for a group is generated by a mixing function using the keys obtained from the key chain.

Authentication during key sharing is achieved by a key chain and an inverted key chain. The authors used this scheme to achieve secure communication at single group level in highly dynamic WSNs. This scheme is resilient to collusion attack caused by compromising more than one sensor node within a group. The authors evaluated the performance of the proposed scheme and observed that this scheme is suitable for devices with minimum computation and communicational overhead. Communication overhead is analysed based on the size of the re-keying messages and the number of messages used in key generation. This scheme does not require location information or assigning prior security service before deployment of sensor nodes.
Zhu et al (2004b) proposed a Localized Encryption and Authentication Protocol (LEAP) for WSNs. The authors proposed this scheme with the objective of generating different types of keys for different application specific sensor nodes to enhance the security requirements. This scheme is used to establish secure communication with static set of neighbouring nodes. The authors used an authentication mechanism μTesla (Perrig et al 2002) to identify the source that sends the message. Through the authentication mechanism LEAP prevent the participation of unauthorised node in group communication. LEAP achieves security within a group by preventing outsider attack through combined use of authentication keys along with cluster key.

Khan et al (2007) carried out a work on rekeying scheme for cluster-based WSNs. This is a dynamic key management scheme and used on demand for rekeying due to the node capture attack occurred in a cluster. The authors used Lagrange’s interpolation formula for rekeying. Prior to rekeying, information about compromised node in a cluster is given to the BS by the cluster head. BS selects a polynomial and computes share for the uncompromised nodes in the cluster. The nodes which hold share are able to generate the key. The authors evaluated the performance and determined that the proposed scheme requires minimum communications and computation in terms of O (1) for rekeying.

Younis et al (2006) discussed a scalable cluster-based key management scheme for WSNs. The authors used Exclusion Basis Systems (EBS) along with location information for generating keys. They considered disjoint clusters for their experimentation. The process of key generation is distributed to cluster head, gateway node and command node and this avoids single point of failure. Also the information required for key generation is stored in multiple nodes. The key assignment technique followed reduces the
chance for collusion among compromised nodes because in the proposed scheme location information is also considered for key assignment. In this scheme the chance for collusion among compromised node decreases as the number colluding nodes required to reveal the combined set of key increases.

Eltoweissy et al (2004) developed EBS for key generation sharing in WSNs. The authors followed a combinatorial optimisation methodology in secure key sharing in group communication. Each node was assigned a set of keys based on combination of administrative keys (k) and rekeying messages (m). The authors evaluated the performance of the proposed scheme and determined that proposed scheme requires low memory for storage because the storage of secret information is distributed among different types of node. Further the computation and communications performed for rekeying is very much reduced.

Huang et al (2005) described about a secure and efficient group communication scheme used in WSNs. The authors achieved effectiveness of the proposed scheme by subdividing the tree structured network into number of levels and each level can have number of branches. Each level uses its level key to encrypt or decrypt the data packets forwarded across the level. Data confidentiality along the level is achieved through hop-by-hop encryption. Member join and member leave operations are allowed in the proposed scheme and are controlled by the BS. The authors analysed the security of the proposed scheme and determined that proposed scheme is resilient to replay attack. To get rid of this attack, in the proposed scheme the BS block the area to which the node belongs.

Dahai et al (2012) proposed a dynamic key management scheme for cluster based WSNs. This scheme was proposed to overcome the drawbacks of probabilistic key management mechanism and key management using deployment knowledge. In this scheme the session keys used for
communication were created by CH on demand. The session key was generated by congruence property of modular arithmetic and this mechanism is suitable for heterogeneous WSNs. Through simulation results the authors determined that the time consumption and energy consumption of the proposed scheme were very much reduced.

Harn & Lin (2010) proposed a key transfer protocol for securely sharing a secret key with each of the authorized member in the group. Here a trusted entity shared a secret with each of the registered member of a group. This scheme used Shamir’s secret sharing scheme to share the session key among the members of a group. The secret share is generated by Lagrange’s interpolation polynomial. Here the authors used a trusted entity called key distribution centre (KDC). Each user of a group should get registered to the KDC which provides the key distribution service to the registered user. Through the proposed scheme the authors were able to achieve key refresh, key confidentiality and authentication. The proposed scheme is highly resilient to outsider attack.

Jungh Yun et al (2011) described Harn and Lin’s secret sharing scheme and proposed a technique to overcome the drawback of Harn and Lin’s scheme. In Harn and Lin’s scheme is vulnerable to replay attack performed by a compromised node within a group. This led to the disclosure of secret information shared within a group. In the proposed scheme KDC and the valid members of the group exchange a random value. These random values are used as a measure of confirming the secret information received along both sides. The changes made through the proposed scheme enhance the security and prevent any compromised node from eavesdropping the secret information communicated in the group. Further replay attack is not allowed in the proposed scheme.
Cheikhrouhou et al (2011) proposed a ring based group communication scheme. Here the group is represented by a logical ring topology with a group controller and number of member nodes. Each group member has to store the address of next node and the previous node. Secrecy can be achieved by means of the key generated by the controller and shared with group members. Further the proposed scheme maintains forward secrecy and backward secrecy during member join and member leave operation. Security against node capture attack can be achieved by the proposed scheme. Compromised group controller can be detected by the BS and compromised node in a group can be detected by the group controller. The authors determined that proposed scheme function well for small and medium sized network.

Guo et al (2010) developed a secure group-based communication to address the problems that occur during key generation and distribution of session keys in a group. The authors followed Diffie- Hellman approach for key exchange in inter-cluster and intra-cluster communication in ad hoc networks. The communications done by the nodes are trusted by exchanging certificates and one-way hash function. The mechanisms followed in the proposed scheme support for integrity and authentication through a nonce and challenge response message. The receiver checks the integrity of the secret information received through the message digest endorsed along with the message.

Shaikh et al (2009) proposed a group based trust management scheme to determine trust values of individual sensor nodes involved in inter-cluster and intra-cluster communication. Trust values were measured by direct and indirect observations observed for a specific node. Direct observation determines the number of successful and unsuccessful transmissions performed. Indirect observation is by collecting information about a specific
node from a trusted node. Trust values may be determined at node level, cluster level and BS level. By using the trust information the authors were able to determine the malicious node and avoid using these nodes in a secure communication. Further, they observed that the proposed scheme provided security in communication against malicious, selfish and faulty nodes.

Guo & Leung (2010) proposed a scheme to resist node capture attack during group rekeying in WSNs. The polynomial used for rekeying is updated periodically. Even if a compromised node exists in the group, the key received by the compromised node expire quickly. Compromised node further cannot perform any attack within the group. Further communications are done in the group by eliminating the compromised node. Additional information is not required for rekeying. The cluster head is responsible for group key generation without collecting information from member nodes. The cluster head and BS are able to detect intrusion within a group. The authors observed that the proposed scheme is suitable for large scale WSNs.

Oliverira et al (2007) described how to provide secure communication in LEACH (Heinzelman et al 2002). The authors used a key pre-distribution scheme and an authentication scheme to enhance the secrecy of the communications performed in a cluster. Pools of keys are generated before deployment and a ring of m keys selected randomly from the pool are pre-distributed to each node in the cluster. Authentication is achieved by keys generated using the protocol μTesla. The proposed scheme provides authenticity, integrity and confidentiality to communication thus preventing unauthorized node from participating in the communication. Further the proposed scheme provides necessary control measures to prevent unauthorized node from becoming a cluster head.
Chia-Yin Lee et al (2011) proposed a key sharing protocol using a trusted KDC to overcome the drawbacks of secure key agreement schemes. The proposed scheme uses one-time session key for establishing secure communication. To overcome single point of failure the proposed scheme uses one of the group members as an initiator of group key generation. The proposed scheme resists insider and outsider attack. Further a compromised group key does not reveal any information about the future group key to the adversary. Thus the proposed scheme holds high resiliency to insider attack.

Konstantinou (2011) proposed a study to describe and evaluate the performance of group key agreement protocols used for WSNs. The author initially discussed the benefits achieved through clustering as clustering technique can be used for large-scale WSNs and for time critical real-time application. Further through clustering bandwidth and energy efficient communication can be achieved. Author described the advantage of cluster-based group key management and how node compromisation within a cluster does not affect the entire network. The author grouped the application oriented WSNs environment into infrastructure based WSNs and infrastructure less WSNs environment. In addition they determine which of the group key agreement protocols are suitable to a particular environment. They also evaluated the performance of the group key agreement protocols described in the study based on the energy consumed during operation.

Zhang & Cao (2005) described a mechanism for filtering false data in group communication. Through compromised node adversary can inject false data or modify the data send by a legitimate node within a group. The authors proposed a method by which neighbouring nodes of a compromised node collaborate together to use the pre-distributed key for rekeying. In the proposed mechanism authors pre-distribute keys to the sensor nodes before deployment. This prevents storage overhead that occurs in the centralised
trusted node. The new group received after rekeying can be authenticated using the old group key. The authors analyzed the security of the proposed scheme and observed that proposed scheme outperform the existing schemes by high filtering efficiency.

Rafaeli & Hutchison et al (2003) discussed about a study on secure group communication. The author classified group key management approaches into three categories such as centralised group key management decentralised group key management and distributed group key management. The author evaluated the performance of the protocols belonging to each approach separately by means of the secrecy maintained by the protocols and their computation communication and storage overhead.

Chi-Yuan Chen & Han-Chieh Chao (2011) described about some of the key distribution approaches illustrated through literatures. The author classified the key distribution schemes into two categories. They are Location independent key distribution schemes and location dependent key distribution schemes. The authors evaluated the performance of the key distribution schemes based on resiliency against node compromisation, efficient utilization of the resources, the probability that pair of nodes can compute their shared key and adaptability of the key distribution scheme according to the network settings.

2.4 SECURITY THROUGH TRUSTED FORWARDING NODES IN QUERY BASED COMMUNICATION

WSNs consist of battery-powered sensor devices. Each sensor node is tiny sized with limited memory, processor with low processing power and short communication range. Sensor nodes function in an ad hoc manner in a hostile environment. Secure routing is a challenging task faced by sensor nodes when forwarding the sensed data to the BS due to the limitations in the
communication range. Further, uneven distribution of energy among the intermediate nodes in the path drains out of energy of some nodes quickly which causes failure of path. To address these issues qualified nodes have to be selected for routing. Various mechanisms have been proposed for secured and reliable route identification and communication using secured routes (Babu et al 2011). This section reviews works regarding secured routing and data transfer.

Deng et al (2006) described a mechanism to secure multi-hop data transfer for WSNs. The authors were motivated to resist denial of service attacks that occurs in the path of data transfer. The authors used a one way hash chain to generate a sequence numbers which is used as an authentication measure. During data transfer intermediate node verifies the validity of the packet through key generated using a hash chain. The one-way hash chain is periodically refreshed to resist replay attack that occurs due to compromised intermediate node. Further each intermediate node along the path contains history about the packets transmitted which helps them to resist replay attacks along the path. In addition an unauthorized node is not able to generate a valid hash chain number. Thus the proposed scheme resists the attack in the path of data transfer.

Kraub et al (2008) described a mechanism used to resist false endorsement based denial of service attacks during data transfer in WSNs. The authors experiment the proposed scheme in WSNs organized into clusters. In clustered WSNs cluster head generate a report about the event that occurred within the cluster. Event report should be endorsed by the member nodes within a cluster. If a cluster node is compromised by an external adversary, compromised cluster node endorse false endorsement which invalidates the generated report. The authors analyzed the security of the proposed scheme and observed that proposed scheme can absolutely resist
insider attacks that occur due to report endorsement by compromised cluster nodes.

Dong et al (2008) discussed about a mechanism to filter bogus message that cause denial of service attack along the communication path. The authors used a key-chain based approach for authentication of legitimate sensor nodes. The first key in the chain is called commitment or seed key. As the hash chain is irreversible, authors determined that node which has the key from a key chain can verify the later keys in the key chain but former keys cannot be verified. Further the authors used pair-wise keys to be shared by the neighbouring nodes to verify bogus message during data forwarding. The authors analyzed the security of the proposed scheme and proved that the key-chain based method can effectively reduce denial of service attack in data transfer.

Saifan & Al-jarrah (2010) described a mechanism to defend against denial of service attacks that occur in the path of data transfer. The author discussed about the security issues that occur in end-to-end secure protocols and express the need for security along the path of data transfer. Adversary can inject or endorse false information and perform replay attack in the path of the data transfer and this insists for link layer security. The proposed scheme achieves link layer security by sharing pair-wise keys between neighbouring hops. The proposed scheme deals with vulnerabilities that occur in the path from node to BS and BS to node during communication.

Authentication is achieved for each packet transferred by means of a sequence number endorsed in the packet. Each en-route node has the verifier for verifying the sequence number. The author demonstrated through simulation that proposed scheme can achieve security services such as authentication, confidentiality and integrity of packet in transit. Further the packet can be authenticated by en-route node as well as BS.
Sun et al (2009) proposed a scheme to overcome the issues addressed because of path change in statistical en-route filtering scheme. The author used a mechanism to select a secure path for data transfer in WSNs. The security of a path can be determined using an evaluation function. Evaluation function includes distance of the path based on node count, weight in terms of security and partition id values maintained in an array. BS broadcast control message to the source node. Source node receives the control message from the neighbouring node and selects the one which has the highest evaluation value. Thus the path selection scheme enhance the false data detection probability of statistical en-route filtering scheme.

Yang & Songwo (2004) discussed about a mechanism used to detect false data inject attack. The author used this mechanism to secure query request and query response received by BS. BS initiates a query request towards a sensor node for specific information along with a session key to be shared with the sensor node and a witness key to be received by all intermediate and destination node. The proposed scheme delete false event message by means of authentication using MACs generated using session key and witness key. By means of this mechanism the authors were able to detect the false data as early as possible.

Lee et al (2010) proposed a scheme for filtering false data along the path of data transfer. The author followed an authenticated scheme in which interleaved hops contain the authentication key and the key derived from the upstream node towards the BS. By this way false data can be detected and dropped at en-route nodes without forwarding to BS. Hence large amount of energy can be saved.

Yuan et al (2008) proposed a scheme to verify the packet endorsement along the path of data transfer. It is easy for an adversary to compromise and access all secret information maintained in the compromised
node. Further adversary can inject false data through the compromised node. So it is necessary to authenticate a legitimate report by number of sensor nodes. This scheme is applied for clustered WSNs. Author assigned key chains for the node in a cluster. After deployment commitments from different node in a cluster will be sent to the BS. En-route nodes receive some of the commitments and then forwards to the BS. Event reports when received by an en-route node will be verified by the en-route node if it contains the authenticated information.

Mao et al (2011) proposed a scheme to select efficient forwarding list of node for forwarding the data. Authors’ objective of using the proposed scheme was to minimize the energy required for transmission and to increase the lifetime of the forwarding node along the selected path. The authors proposed a mechanism to identify the neighbour of a node through which the data has to be transferred. Further they determined the expected cost for forwarding the packet through determined neighbour. They found an optimal forwarding list by arranging the node in an increasing order according to the expected cost. The node with minimum cost gets selected. Authors evaluated the performance of the proposed scheme by determining the throughput delay rate and packet delivery ratio. They observed that the proposed scheme achieved reliable and routing with low delay.

Alshawi et al (2012) described a routing mechanism to achieve maximum life. Authors used soft computing approach and A-star algorithm (Kim & Cho 2008) to select a suitable path. Authors focused on achieving the efficiency by considering the factors such as minimum number of hops, minimum traffic and high residual energy. As the sensor nodes have short communication range data collected by sensor node travel through multiple hop. If a node along the route has been drained the node is said to be dead and further the path is not used for data transfer. To increase the duration of the
path used for data transmission the energy of the intermediate should be maximum and evenly distributed along the path. This can be achieved in the proposed scheme. The proposed scheme selects an optimal path with maximum energy and minimum hop count.

Babu et al (2011) proposed a scheme to select indispensable nodes for routing in WSNs. Authors focus on nodes trust level, residual energy and distance from the BS for selecting a suitable route. Authors calculated trust level based on geometric mean based trust management system. Further they consider the energy consumption by nodes for communication during trust management and residual energy. They used soft computing techniques on the given input value and based on their priority level author evaluated the performance and observed that proposed scheme can increase node lifetime and network lifetime.

Jai-Hwan Chang & Tassiulas (2004) proposed an approach to increase the lifetime of the path used for communication. Authors studied about the problems occurred in routing schemes for fixed information and arbitrary information generated in periodical rate commodity. They determined that in these routing schemes shortest cost path is used for routing and cost of the path will be determined afterwards. Author’s objective in the proposed scheme is to select the best link cost path for routing. The authors achieved the benefit of increasing the amount of data transfer along a path by increasing the path lifetime and system lifetime.

Hussain et al (2009) proposed a secure mechanism for distributing session using a keyed hash chain in WSNs. Authors determined the problems that occur due to key pre-distribution in resource constrained WSNs. Authors overcame the problem in the existing schemes by distributing generation keys to the sensor nodes after deployment. Neighbouring sensor nodes identify the common generation keys among the received keys. The nodes which have
common keys are determined as secured neighbours. They used a hash chain to generate different keys using the common key for each session. The authors observed that proposed scheme is more secure and highly resilient against the attacks that occur in the path.

Leligou et al (2010) proposed a routing scheme to defend against routing attacks by combining trust information along with the location information for routing. Authors described the drawbacks that occur due to the lack of trust information in routing. Authors generated four trust aware routing rules to identify a trusted next hop as trusted for routing. Though the rules include minimum processing steps they highly resist the involvement of malicious node in routing. The authors evaluated the performance of the proposed routing scheme by computing the packet delivery ratio and delay that occur during packet transfer in the presence of malicious node. They observed that even though large number of malicious nodes is present in the network the system can survive with outstanding performance compared with related schemes.

Moon & Cho (2012a) discussed about a scheme used to select reliable and uncompromised intermediate nodes to detect and drop false event messages for every sessions. The authors focused on a deterministic approach to address the problems that occur in probabilistic approach of selecting en-route nodes. In probabilistic approach it is difficult to predict accurately the false traffic and energy inefficiency that occur to intermediate nodes on the path. Further, the selection process of filtering nodes is based on false traffic ratio, communication overhead due to MAC size and residual energy of the node. All these values are given as input to a fuzzy controller. By means of soft computing approach fitness values for different nodes on the path are determined (Moon & Cho 2012a, 2012b. Authors evaluated the performance
of proposed scheme and observed that false event messages can be filtered without a doubt if the count of selected suitable nodes is increased.

Zhang & Jiang (2012) described about a proposed scheme used to detect any false data injected by compromised en-route node while sending query message from BS to sensor node. This scheme is also used to detect PDoS (Path based Denial of Service) attack by means of timestamp and queryid endorsed in the query message. Bs generates a symmetric key to be shared with information specific sensor node to continue with secure data transfer. Authors evaluated security features of the proposed scheme and determined that proposed scheme is resilient to false data injection attack, false endorsement attack and PDoS attack. Further the proposed scheme is performed with minimum storage requirements and low energy consumption for data transmission.

Chin-Fu Kuo et al (2009) proposed new routing scheme to overcome the issues that occur in communication in wireless networks. The authors objective was to generate a dynamic routing algorithm based on distance vector based routing scheme to achieve security in data transmission. Each node maintains routing table which holds information about the neighbouring nodes. During data transmission the node with minimum cost is selected as the next hop. To reduce eavesdropping and other attacks due to compromised en-route, by selecting a next hop randomly from the suitable list of nodes maintained in the routing table. The performance of the proposed routing algorithm has been evaluated by means of the metrics delay, traffic load and packet delivery ratio. It has been determined that proposed scheme perform well when compared to shortest path and minimum cost routing algorithms.
Tao Shu et al (2010) discussed about a scheme for secure communication in wireless sensor network using randomized routes. The authors’ objective of using the proposed scheme is to prevent DoS attack in communication. In related existing routing approaches once the adversary is able to compute the routes with the knowledge of routing algorithm, he may be able to retrieve the information transmitted through the route. The authors followed a multipath routing scheme by randomly selecting multiple paths and different paths are selected for different sessions. Each shares are send in a dispersive manner. Four different techniques are followed for dispersive transmission. By means of the proposed scheme authors observed that the packet interception probability of the proposed scheme is low compared to existing scheme.

Chachulski et al (2007) proposed an opportunistic routing scheme for wireless sensor network. Here the routing path is selected based on link quality and the node which can overhear the transmission can forward the transmission. Hence more than one node can forward the same packet. Issue faced in this scheme is to use appropriate mechanisms to select efficient forwarding list of node to minimize energy cost.

Chia-Mu Yu et al (2011) proposed a polynomial function based authentication scheme to defend against false data injection and path-based denial of service attacks for WSNs. By means of the proposed scheme the other than the BS the intermediate nodes along the path has the ability to check the authenticity of the forwarding message packet. Authors used two types of polynomials namely, the authentication polynomial and the verification polynomial. Authors observed that the proposed scheme is resilient to en-route node compromisation by an adversary. Further, the
proposed scheme can perform immediate authentication with high filtering efficiency.

2.5 SECURITY THROUGH ANONYMOUS COMMUNICATION

Delgado-Mohatar et al. (2011) described about an authentication scheme using simple cryptographic operations with low computational requirement. The author mainly focused on node authentication and pair-wise key establishment. This scheme is highly resilient to node capture attack. This scheme achieves maximum security with minimum storage in each node and avoids key pre-distribution. Security analysis shows that the proposed scheme is highly resilient to denial of service attack and other physical attack. The author compared the results obtained through the proposed scheme with related schemes and determined that the proposed scheme is energy efficient compared to SPINS (Perrig et al. 2002) and BROSK (Lai et al. 2004).

Huang et al. (2013) presented an effective mechanism to establish secure data transmission in cluster-based WSN. The author proposed two Secure and Efficient data Transmission (SET) mechanisms: SET-IBS and SET-IBOOS using Identity-Based digital signature Scheme (IBS) and identity-Based Online/Offline digital signature (IBOOS). The basic idea used in the scheme is to encrypt and authenticate the sensed data using node ID and the symmetric secret key shared with BS. The sensor nodes are able to get their keys without requiring auxiliary data exchange. This scheme solves the orphan node problem through identity based cryptographic (IBC) operations. In this scheme the sensed data is encrypted by means of homomorphic encryption operation.

The entire operations performed are divided into two phases namely setup phase and steady-state phase. The former is used for construction of clusters while the latter is used for secure data transmission.
Further this scheme prevents the occurrence of delay by means of a timestamp endorsed along with the signature generated. The author assigned the scheduling to access the medium for data transmission through TDMA (Time Division Multiple Access) control. This node resists the involvement of a compromised node by refreshing the IDs of compromised nodes at the initial stage of each transmission round.

An authentication scheme was proposed by (Yasmin et al 2012) to address the problem of authentication such as delayed authentication and DoS attack that occur in µTESLA (Liu & Ning 2004) and other schemes use message authentication code for authentication. This scheme is highly resilient to insider and outsider attacks. This scheme use IBC operations to generate the authentication message to be endorsed along with the packet. Here the authentication message is generated by each and every sensor nodes without the involvement of BS. During data transmission the authenticity of the packet is identified by means of the signature endorsed in the packet and legitimacy of the outside user is also authenticated without requiring any information from the sender. This scheme is efficient in terms of energy consumption, computation time and the memory requirement. This scheme is highly resilient to replay attack, node compromisation and false data injection attack.

Hong Yu et al (2013b) developed a mechanism for end-to-end secure communication between sensor nodes in WSNs and internet nodes. The authors used two models to connect WSNs to internet. In the first model, BS is used as an interface between internet users and the sensor nodes. When an encrypted data was received by BS it decrypts the received information. Further, it provides the required security mechanism before directing the data towards the specified destination security. In this scheme the BS is involved in decrypting and re-encryption before re-directing the data to the specified
sensor node. Hence this model reduces the scalability and increases computation complexity.

The second model is used to overcome the drawback of first model. The entire communication between internet users and sensor nodes are done with the help of IP protocol. Here routers or forwarders are used to connect internet with WSNs. The security mechanism used to enhance the secrecy in internet is through the existing transport protocol and in WSNs link layer security was achieved through shared keys between the neighbouring nodes. Here authentication is achieved through signcryption and confidentiality is through symmetric encryption. Before forwarding between internet and WSNs authentication and access control is done through where user information is maintained. The author observed that the performance of the proposed scheme is efficient when compared with Elliptic Curve Cryptography (ECC) scheme.

Collier et al (2009) proposed TinyIBE an identity based scheme for WSNs. This scheme is mainly applicable for heterogeneous sensor network to establish secure communication between cluster head and other low level sensor nodes. Even though this scheme uses an asymmetric cryptographic mechanism to provide authenticated key exchange it reduces the computation involved in key exchange and certificate exchange. This scheme requires only minimum number of keys and do not need to maintain shared keys between neighbouring nodes. This reduces computation and storage overhead. The performance of the proposed scheme is evaluated and determined that Identity Based Encryption (IBE) is a suitable technique for WSNs. The proposed scheme is protected against compromised cluster heads and is resilient to identity theft and other identity based issues through mechanisms used for identity check.
McCusker & O’ Connor (2011) illustrated a concept to distribute pair-wise symmetric key between sensor nodes in WSNs. In the proposed mechanism authentication is achieved through identity based digital signature. Here the keys are generated using Tate pairing and keys are distributed using an identity-based non-interactive key distribution scheme. This scheme had access control measures which prevented unauthorized third party from accessing the network. The author observed the performance of the proposed scheme by comparing with related schemes and confirmed that the proposed identity based cryptography provides a simple, scalable mechanism for distribution of symmetric keys and is highly resilient against node capture attack. Moreover, the proposed scheme resist Sink hole, Worm hole, Sybil and identity replication attack.

Sarkar & Mandal (2012) described about a secure communication scheme which uses fuzzy logic for cryptographic operations. In this scheme the authors determined the limitations of conventional Elliptic Curve Cryptography (ECC) and propose a new mechanism to address the issues determined. During experimentation they observed that proposed scheme is performed with reduced memory space, minimum computational complexity and low power consumption. However the proposed scheme is not scalable to large key size and works only with integer values.

Haider & Yusuf (2009) proposed an optimised routing mechanism through fuzzy based approach. This scheme was used for performing energy-aware routing and the routing metrics considered for route generation are residual energy, transmission energy and the energy consumption rate. In this scheme routing is done based on the link cost between consecutive sensor nodes. This scheme does not consider about the security measures in route generation but focused only on efficient data forwarding.
Mehta et al (2011) described a mechanism for protecting location privacy in wireless sensor networks. Most of the mechanisms designed for ensuring security in wireless sensor networks support for achieving confidentiality for the content of the message but the contextual information remains exposed to the adversary. The authors focused on protecting the privacy against a global eavesdropper. They discussed about two mechanisms one for source location privacy and the other for sink location privacy. These mechanisms were efficient and effective against communication overhead. But through this scheme the global eavesdropper is able to compromise set of sensor node and may perform traffic analysis. This work did not guarantee strong resiliency against traffic analysis attack.

Ei Defrawy & Tsudik (2011) described anonymity in proactive routing. In this scheme each node broadcast its location information to its authenticated neighbours. Each node builds a map for later anonymous route discovery. But construction of this map leaks the location of the intended destination and compromises the route anonymity. Thus this scheme is unable to protect location anonymity of source and destination.

Shen & Zhao (2013) discussed about an anonymous location based routing protocol for ad hoc networks. This scheme partitions the network into number of zones and randomly selects node from zones to function as forwarding nodes. Anonymity is achieved in this scheme by hiding the source information destination information and the identity of the intermediate nodes. Even though this scheme hides the location information, it is unable to determine efficient forwarding nodes due to random selection of forwarding nodes.

Sun et al (2009) discussed a mechanism for enhancing the false data detection probability of en-route nodes. The authors described that the false data detection probability is affected by the path that has been selected for
forwarding the event information. So to improve the detection power it is necessary to evaluate the detection power of the forwarding nodes. This work paved the way for early detection of false data. But selection of path based on partition ID (identity) alone does not reflect the possession of forwarding node. Hence it is essential to consider other factors to determine efficient forwarding nodes.

Pushpender & Garg (2013) explained about a technique for routing based on fuzzy logic. In this work the authors described about the issues faced in routing by means of single constraints and the benefits achieved by using more than one constraint in routing. In this scheme the authors use fuzzy based approach for efficient node determination. The constraints considered are bandwidth, throughput delay and mobility. This scheme is not scalable for large networks since the practical effectiveness of the work is not achieved for large networks.