CHAPTER 2

LITERATURE SURVEY

Security in communication channel or in routing protocol is necessary during the user communication. So, this chapter deals with the literature survey of the secure data communication and the attacks, which steal or interrupt the user communication. The literature survey contains the unconditional secure communication and the issues in wireless communication. For routing data from source to destination, any one of the efficient either proactive or reactive routing protocols is used. The BB84 [6] is the first internationally accepted QKDP, and it is used to exchange the secrets of the key to establish the secret key.

2.1 Introduction

Wireless Sensor Network (WSN) is a collection of sensor nodes with processing unit and memory. The sensor nodes are deployed in remote areas and thereby collect the environmental information to avoid unwanted happenings. In this thesis, the focus is on the secure data communication resisting different types of attacks such as BH, WH, flooding and grey hole.

Routing is a kind of process to find a path from one place to another place and security could be achieved by preventing the attacks. Since the success of QC is based on secure communication for key distribution technique, this can be used in WMN.

Routing techniques in WSNs can be divided into three categories, namely flat-based routing; hierarchical-based routing and location-based routing depending on the network structure. In flat-based routing, all nodes play the same role. In hierarchical-based routing, however, nodes will play different roles in the network. In
location-based routing, sensor nodes' positions are exploited to route data in the network.

Many different types of routing protocols have been developed for ad hoc networks and have been classified into two main categories: Proactive (periodic) protocols and Reactive (on-demand) protocols. In proactive routing protocol, nodes periodically exchange routing information with the other nodes and hereby each node always knows a current route to all destinations. In reactive routing protocol, nodes exchange routing information only when needed.

In order to reduce the computing, radio and battery resources of sensors, routing protocols in WSNs have to fulfill the following requirements like Autonomy, Energy Efficiency, Scalability, Resilience, Device Heterogeneity, Mobility and Adaptability.

Security threat in secure networks can be divided into passive attack and active attack. Passive attackers are only interested in collecting sensitive data from the sensor network, which compromises the privacy and confidentiality requirements. These are attempts to reach the owner data and make use of them without the owner realizing it. It is hard to detect this kind of attack because it does not modify the data. So, the prevention of the attack is more useful rather than struggle for detection. Active attackers are interested to modify the data during user communication.

2.2 Quantum Secret Sharing

QC utilizes states of individual quantum systems to transfer the classical bits of information. QKDPs are based on the combinations of principles from quantum physics and information theory. The impossibility of measuring quantum systems guarantees the detection of eavesdropping and hence secure information transfer is possible [3], [72], [77], [98]. QC works over distances ~10km and with bit rates
Maximum distance for QKD in practical application is currently limited by the noise of available single photon detectors and the absorption along the quantum channel, for example, in fiber to about 100 km [73]. Quantum teleportation [98] transmits elementary quantum states over short distances.

For example, with the qubit states represented by the vectors, the “bit value operator” (i.e., $B$) is represented by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. In general, $B|1\rangle=1|1\rangle$ and $B|0\rangle=0|0\rangle$. The states $|1\rangle$ and $|0\rangle$ are eigen states of the operator $B$. A system in an eigen state has a definite bit value known as the eigen value, these are obviously one and zero respectively.

Although quantum cryptosystem based on the QKDP [42] can achieve unconditional security, its key generation is not efficient in practice because the qubits transmitted in the quantum channel cannot be completely employed.

The first QKDP was introduced by Charles Bennett and Gilles Brassard in 1984, which is named as BB84. BB84 protocol is based on Heisenberg’s Uncertainty Principle. Any two pairs of conjugate states can be used for the protocol, and many optical fiber-based implementations described as BB84 use phase encoded states. In BB84, Alice sends photons one by one, in states which she chooses at random. Bob randomly chooses to measure the polarization in either rectilinear or diagonal basis. Bob records his results and keeps them secret. He then announces publicly the list of basis which he used for the measurements. They both discard photon measurements where Bob used a different basis, which is half on average, leaving half the bits as a shared key.

The Quantum Key Agreement (QKA) protocol has much significance for generating identical random numbers in remote places. If the quantum states
transmitted through the channel are altered by Eve, the results Alice and Bob obtained will absolutely be changed, with which existence of Eve can be detected. A secure transmission method is described in [77], which is used to transmit secret key between two legitimate parties with the existence of eavesdropper.

Quantum Key Growing (QKG) [30] uses properties of quantum mechanical systems to share a secret key between two sites. The purpose of the QKG system is to use the two channels and a small portion of the already shared key to generate a new key portion, larger than the one just used. The initial key only needs to be large enough to allow for the first generation sequence, typically authenticating two messages, one from Alice to Bob and one in the other direction.

QKG makes use of Wegman-Carter authentication, which is equivalent to verman cipher. In Wegman-Carter Authentication, Alice and Bob share a secret key $k$ just large enough to select a hash function $h_k \in H$; Alice wants Bob to have the message $m_A \in M$ and sends both $m_A$ and $t_A - h_k(m_A)$. Bob verifies whether $t_A$ equals $h_k(m_A)$ and accepts the message as authentic if it does. The key $k$ is then discarded and never reused. Wegman-Carter Authentication has serious impact on security that is Eve can influence the message to be sent, and together with partial knowledge of the key.

Cascaded hash functions are employed in [44], in order to generate a shared secret key locally by the communicating parties. A shared entangled pair is used for authentication according to the deterministic six-state quantum protocol (6DP). Hence, a Quantum Authentication Process (QAP) is established. The QAP task is to verify the mutual identification of the two parties. Initially, the sender prepares six quantum states randomly. Every state contains two different entangled pairs of photons. If any of the two photons is missing or has a changed state of polarization, it
denotes eavesdropping. If nothing wrong is detected, continuously the two states will be sent to the receiver. The receiver flips them by one of the four prepared quantum pauli operators and sends them back to the sender. The sender checks and compares all these states with the previous polarization states. After checking and comparison of the six states, if it is found that any state is missing or changed, the whole process is thus stopped and an investigation is carried out. Otherwise, the communication will continue as usual by enabling instruction to start another phase in the KDP-6DP protocol. This phase is called key distribution process which performs key-sharing by using cascaded hash functions.

The three modes of algorithm for KDP-6DP are compared with respect to speed, error detection and correction, and security is shown in Table 2.1. In first mode algorithm, it is easy to detect and correct error, whereas third mode algorithm is fast and more secure.

<table>
<thead>
<tr>
<th>Factors</th>
<th>First Mode</th>
<th>Second Mode</th>
<th>Third Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Slow</td>
<td>Slow</td>
<td>Fast</td>
</tr>
<tr>
<td>Error Detection and Correction</td>
<td>Easy</td>
<td>Difficult</td>
<td>Difficult</td>
</tr>
<tr>
<td>Security</td>
<td>Moderate</td>
<td>Moderate</td>
<td>More</td>
</tr>
</tbody>
</table>

### 2.3 Multi-Party Information Sharing

Quantum Three Pass Protocol (QTPP) [89] requires only quantum channels, and classical one-bit information is encoded into a “quantum bit” or “qubit”. After an \( n \)-bit message is encoded into \( n \) photons, the polarization of each photon is rotated by an angle \( \theta_i \), which is chosen randomly for each qubit. In QTPP, users generate their
own secret key and it is not shared. Each session key is used only twice in the session by the generator: once for encryption and once for decryption.

The existence of Eve increases the bit error rate up to 50%, which helps in revealing the presence of Eve. Like [89], rotation is considered as encryption in [90]. In [81], Quantum Secret Sharing (QSS) scheme is described in which the secret can be recovered only by the collaboration of all users. The goal of QSS is to share the private key and the quantum information.

Quantum information is shared among multiple parties based on entanglement swapping [88]. Entanglement swapping means to entangle quantum systems that have never interacted before. This scheme consumes Bell states [4], and the splitting of quantum information is realized by entanglement swapping.

Only Bell states [4] are employed in [96] and needed to be identified to realize the multiparty secret sharing of quantum information. The essence of a multiparty secret sharing of quantum information is that no subset of all the quantum information receivers can reconstruct the unknown state in a qubit but the entire collaborates, i.e. only with all other receivers’ helps, one receiver can reconstruct the unknown state in a qubit. In fact, before Alice distributes her secret messages to all the receivers except for Bob, this group can and should detect whether the quantum channel is attacked by Eve by using the so-called two-measuring-basis method as well as the message authentication method.

Bell states in the high dimension Hilbert space are employed in [16], and hence this scheme is the high source capacity. Securities of the two sequences transmission are assured by two batches of decoy particles. By measuring decoy particles, it can be judged whether the two sequences are transmitted securely.
A five-party Quantum State Sharing (QSTS) scheme [65] resorts to a three-particle GHZ(Greenberger-Horne-Zeilinger)-state quantum channel and three-particle GHZ-state measurements, not a five particle GHZ-state quantum channel or five-particle GHZ-state joint measurements. Moreover, this scheme is secure if the number of the dishonest agents is more than one (no more than three).

A scheme is used to verify the identity of the participants is Quantum Identity Authentication (QIA). In [57], all the users can be authenticated by a Trusted Third Party (TTP) simultaneously. In [79], a QIA protocol is based on entanglement swapping in which TTP shares a secret identity number and a secret hash function with each user. TTP and the users check eavesdropping. If they confirm that the quantum channel is safe, they continue to the next step, otherwise, they abort the protocol. TTP divides the remaining GHZ states into $M$ ordered groups. Each user performs unitary operations on their particles according to the authentication keys and each user measures particles of each group in the Bell basis. They will publish the measurement results. Then, TTP performs the Bell basis measurements of each group and authenticates the users according to the communication parties’ measurement results.

In [86], two Multiparty Simultaneous Quantum Identity Authentication (MSQIA) protocols are described. In the first protocol, the TTP shares a random key $K$ with all the users using quantum secret sharing. The $i^{th}$ share acts as the authentication key of the $i^{th}$ user. When it is necessary to perform MSQIA, the TTP generates a random number $R$ secretly and sends a sequence of single photons encoded with $K$ and $R$ to all the users. According to the users’ share, each user performs the corresponding unitary operations on the single photon sequence sequentially. At last, the TTP can judge whether the impersonator exists.
Quantum Fourier transform and entanglement swapping are used to achieve a high intrinsic efficiency and source capacity while sharing quantum information. In this approach, it is necessary to share a GHZ state between TTP and users [36]. Users can prepare some prior Bell pairs between them. They then select their subset and run the control mode. If more than an acceptable number of measurement results disagree, users think there exists an eavesdropping and abort the protocol. Finally, because he cannot attain all three particles in the entangled state during the process, Trent (the TTP) cannot obtain any information about the secret. Hence, the secrecy of this protocol is tightly kept because nobody, even Trent knows the whole secret. Eavesdropping will be detected with the probability of 50% in the control mode. Thus the intercept-and-resend strategy cannot succeed. In a QSS system, a participant generally has more power to attack than an outside eavesdropper. The inside collaborative eavesdropping attack is still detectable with a probability of 50%, and the fundamental security is retained. The efficiency of this protocol is given as \( \frac{1}{2 \max(m, n)} \), which is higher than the efficiency of Yan-Gao protocol [82] given by \( \frac{1}{2mn} \). Thus, avoiding the use of a classical channel during the message mode increases both efficiency and security of the protocol.

Two three-party QKDPs are described in [27], one with implicit user authentication (Three-Party Authenticated Quantum Key Distribution Protocol (3AQKDP)) and the other with explicit mutual authentication (Three-Party Quantum Key Distribution Protocol with Mutual Authentication (3QKDPMA)). In 3AQKDP, Alice and Bob cannot mutually authenticate each other until the session key is used in the further communications, i.e. implicit mutual authentication. In 3QKDPMA, an authenticator is added to the 3AQKDP so that explicit user authentication can be
achieved. By integrating the advantages of both the classical and quantum cryptographies, the 3QKDPMA can avoid the man-in-the-middle, passive and replay attacks. In [23], a three-party QKDP is described in which the center is responsible for generating qubits and assists the key distribution between users. The center can be either trusted or honest. While an honest center always follows the designed procedures to execute the QKDP, a trusted center never compromises the security of the protocol. Thus, a trusted center is also honest but an honest center may not be trusted. An untrusted center, who is neither honest nor trusted, is no more than an agent who is responsible for facilitating the protocol execution and could perform any attack with every possible method like a malicious user.

2.4 Performance Analysis of Quantum Key Distribution Protocols

Qubit Efficiency of existing QKDPs are shown in Figure 2.1. Qubit efficiency can be defined as the ratio of number of qubits used to the number of qubits transmitted. Qubit efficiency of BB84 and Einstein-Podolsky-Rosen (EPR) is 25%, whereas DENG scheme achieves 50% and Enhanced EPR (EEPR) achieves 100%. Unlike BB84, QTPP provides 100% qubit efficiency [89]. Like QTPP, authentication protocol using superposition states provides 100% qubit efficiency [26]. The Quantum Secret Sharing scheme achieves only 50% qubit efficiency whereas QSS with six states provides 100% qubit efficiency [17]. Also, the Threshold based QSS achieves 100% efficiency [85].

Error Rate of existing QKDPs is shown in Figure 2.2. In [89], Eve’s intercept-resend attack increases the bit error rate (BER) up to 50%. This BER caused by eavesdropping is much higher than BB84 (25%). Since EPR correlation pairs are used in [98], eavesdropping increases the BER up to 100%. In [89], the BER is found to increase up to 25% due to Eavesdropping. Unconditional security of a six state
protocol raises the BER up to 14.1% [17]. With entanglement swapping [36], the BER increases up to 50%.

Figure 2.1 Qubit Efficiency of Quantum Key Distribution Protocols

The existing QKDPs are also compared in terms of number of quantum channels required, method with which eavesdropping is detected and number of communication rounds, qubit efficiency (maximal theoretical value) as shown in Table 2.2. Three-Party QKDPs are compared as shown in Table 2.3 with respect to dishonest center attack, public discussion made in order to detect eavesdropping, dense coding attack and need for quantum memory.

Figure 2.2 Error Rate of Quantum Key Distribution Protocols
Table 2.2 Comparison of Quantum Key Distribution Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Quantum Channel</th>
<th>Public Discussion</th>
<th>Qubit Efficiency</th>
<th>Communication Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>QSS</td>
<td>3</td>
<td>Random Sampling</td>
<td>50</td>
<td>5</td>
</tr>
<tr>
<td>QKA</td>
<td>0</td>
<td>Random Sampling</td>
<td>50</td>
<td>4</td>
</tr>
<tr>
<td>EEPR</td>
<td>1</td>
<td>Random Sampling</td>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>QTPP</td>
<td>1</td>
<td>No</td>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>APSS</td>
<td>1</td>
<td>No</td>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>Three-Party</td>
<td>3</td>
<td>Checksum</td>
<td>100</td>
<td>4</td>
</tr>
<tr>
<td>QKDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Six State</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2.3 Comparison of Three-Party Quantum Key Distribution Protocols

<table>
<thead>
<tr>
<th>3PQKDP</th>
<th>Dishonest Center attack</th>
<th>Dense Coding attack</th>
<th>Operation</th>
<th>Quantum Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honest Center</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Untrusted Center</td>
<td>No</td>
<td>Yes</td>
<td>Shuffling</td>
<td>Yes</td>
</tr>
<tr>
<td>Against Dense Coding attack</td>
<td>No</td>
<td>No</td>
<td>Shuffling</td>
<td>Yes</td>
</tr>
</tbody>
</table>

With honest center, security is compromised when center acts malicious, and dense coding attack is also possible. These limitations are overcome with untrusted center, where the recipient does a shuffling operation which is unknown to the center. Hence, the attack due to dishonest center is not possible, but dense coding attack is
possible. Also, this approach requires the user (receiver) to be equipped with quantum memory.

In [15], this issue is overcome by means of performing shuffling operation by the sender before encoding the received qubit sequence. Hence this approach too requires the user to be equipped with quantum memory.

2.5 Secret Sharing in Wireless Medium

Transmitting data over a wireless network must be done with great care as traffic can be intercepted at ease in wireless networks. Although there are lots of ongoing researches to advance the task of providing secure data communication to users, they are still subjected to security attacks. QC tends to provide unconditional security, yet it has not gained attention in wireless networks with respect to secure key distribution.

The triumph of QKD over wireless optical paths is based on the transmission through a turbulent medium. Transmission over wireless atmospheres has a number of benefits compared to the use of optical fibers. The atmosphere has an elevated transmission window at a wavelength of around 770nm, where photons can easily be detected using quantum devices and the polarization state of the photon is not altered.

However, QKD with respect to free-space is showing rather slow progress. One of the main reasons for this slow progress in free-space photon transmission is the difficulty in providing Line-Of-Sight (LOS) between transmitter and receiver for long distance. Before quantum repeaters are put to use, QC offers communication over distances of more than a few hundred kilometers. In case of wireless communications, a QC link could be established between ground base stations and a low-orbit (300 to 1200 km) satellite.
In quantum wireless communication network, quantum routing mechanism can be employed to set up a route message between sender and receiver, which enables a quantum mobile device to teleport a quantum state to a remote site even if they do not share EPR pairs mutually. For quantum teleportation to work perfectly, pure EPR pairs are required. It is important to design a method to extract pure EPR pairs from polluted ones. Therefore, an entanglement purification protocol was used.

Purity testing protocol only checks whether EPR pairs are correct or not, but does not repair wrong ones. A quantum wire is used to move quantum data from one spatial location to another. Moreover, it was also pointed out that for a long distance data transmission, it is more faithful by using quantum teleportation than directly transmitting through quantum wires. Besides that, in order to avoid a fully meshed quantum wires in the networks, Tao, Wang and Cheng proposed a non-blocking digital switching architecture in the quantum domain which support unicasting and multicasting [66].

In the wireless communication network, transmitting messages from sender to receiver may traverse several intermediate nodes. Any eavesdropper can attack in the communication channel, and any malicious intermediate node can act as receiver to intercept the message. Quantum authentication protocols are aimed to achieve the secure communication network. In the quantum wireless communication network, a quantum routing mechanism is proposed. By using this mechanism, one can teleport a quantum state from sender to receiver. But, this mechanism lacks security and privacy.

The two-way secure communication protocol can set up the secure routing path from sender to receiver. The two-way secure communication protocol includes
the sender and the receiver oriented checking. By using quantum sharing table, these checking schemes investigate whether the routing path is secure or not. In the beginning, the sender and receiver pre-share a quantum sharing table to detect all the dishonest nodes. The quantum sharing table acts as a QKD which cannot be stolen by any Eve. Hence, this mechanism achieves high liar detection probability.

Security is an important issue in multi-hop WMN and not much research work has been done till now in the area of WMN security. In [58], the authors have identified the operations to be secured in WMN as corrupted and proposed some solutions to secure the operations. The authors have shown an effective way to model a node-capture attack in multi-hop WMN by formulating it as an integer-linear programming minimization problem. They claim that privacy-preserving key establishment protocols can help to prevent minimum cost node capture attack.

Zhang et al. in [95] have come up with attack resilient security architecture for multihop WMNs. They used identity-based cryptosystem for authentication and key agreement between mesh clients and routers. The authors have identified that the mesh network is vulnerable to privacy attacks because of the open medium characteristics of the wireless channel, its limited size and fixed topology. They propose an Onion routing algorithm that protects the routing information from the attackers. The authors have focused on the traffic privacy by proposing a penalty-based routing algorithm.

The mesh-based protocols try to create multiple trees among the group members such that the packets can be delivered to each receiver through multiple paths. Multichannel Multicast (MCM) algorithm [21] inherits the tree-based multicast design, but it differs from other tree-based multicasting.
The main objective of privacy-preserving of hybrid ad hoc networks is to provide anonymity and location privacy for mobile nodes in hybrid ad hoc networks. Temporary public key pairs are used by each mobile node to anonymously establish pairwise secrets with its neighbours. These pairwise secrets in turn are used to secure routes to the access point.

The structure called “Onion ring” uses “Onion encryption” in a ring structure so that it is impossible for an adversary to distinguish the source node or the destination node. This scheme is able to identify the misbehaving nodes. The protocol proposed in [97] uses multiple paths for data delivery so that an attacker is unable to observe a fraction of the traffic.

To facilitate anonymity and identity privacy, blind signature can be utilized as a part of authentication mechanism, which involves less computation overhead as it makes use of lesser public key and hash operations. The authors present an anonymous authentication scheme between mesh clients and mesh router for preserving identity privacy and security in data communication in WMN. In order to preserve traffic privacy, penalty-based routing algorithm is employed in [71], to achieve the goal of hiding traffic pattern by exploiting the richness of available paths between two nodes in WMN.

2.6 Analysis of Secure Routing Protocols

The goal of WSN is to provide an infrastructure to deliver data from a source node to a destination node. Routing protocols are the most critical components because they address the problem of how to find path from the source to the destination. If routing protocols fail under malicious attacks, the high layer application also fails and the network is useless. Therefore, secure routing is very important to guarantee the data delivery in the face of malicious attackers. The
various attacks encountered in routing protocol are Selective Forwarding attack, Sybil attack, Sinkhole attack, BH attack, Hello Flood attack, and WH attack [31].

The Cluster Based Hierarchical Routing Protocol (CBHRP) [41] scheme introduces a new concept called head set, which consists of one active cluster head and some other associative cluster heads within a cluster. When compared to Low-energy Adaptive Clustering Hierarchy (LEACH), the iteration time of CBHRP increases by several times for a given number of head-sets. The CBHRP is able to transmit higher data frame when compared to LEACH.

The Dynamic Window Secured Implicit Geographic Forwarding (DWSIGF) [22] approach uses dynamic time which can provide a good PDR even when the neighbours perform the BH attack. The Secured Implicit Geographic Forwarding (SIGF) and DWSIGF increase the end-to-end delay with 17% and 19% respectively when compared to Implicit Geographic Forwarding (IGF). IGF is considered a perfect solution to be used when there is no attacker in the communication.

In Two-Tier Secure Routing (TTSR), the transmission range of Low end-sensor (L-sensor) and High end-sensor (H-sensor) is 60m and 150m respectively [78]. TTSR has higher delivery ratio than Directed Diffusion (DD). The energy consumption of DD increases much faster than TTSR, and it becomes very large when node density is high. The TTSR also has smaller end-to-end delay than DD for all tested sensor density.

A secure routing protocol, namely Secured Greedy Perimeter Stateless Routing Protocol (S-GPSR) is proposed for mobile sensor networks by incorporating trust-based mechanism in the existing GPSR. The results show that the routing overhead achieved using the S-GPSR protocol was 73%, which is less than the
standard GPSR protocol [59]. Furthermore, improvements of 25% in the delivery ratio have been achieved in the S-GPSR protocol.

The selective forwarding attack [64] is detected by checkpoint, source node, ordinary node and node id. Once the node is identified, it is removed from the network, and the packet is routed through the alternate path. Detection accuracy also depends upon the transmission and reception range since the nodes are mobile. The undetected ratio is 20% [64] which proves that detection accuracy is 80%. The PDR of normal nodes are from 70% to 100% and compromised node is only 30%.

The Hierarchical Secure Routing Protocol Scheme (HSRBH) is used for detecting and defending against BH attack in [29]. The network density, nodes mobility and the number of BH nodes are determining factors in this solution performance [62], in terms of end-to-end delay and network load. In the presence of BH attack, PDR of Ad hoc On-Demand Distance Vector (AODV) drops by 81.812%.

To provide the security for transmitting, RSA algorithm is used at each node in [31]. The keys are used to encrypt and decrypt the data at the source and destination node respectively. RSA algorithm consumes $12.5 \times 10^{-3} J$ and ELGAMAL algorithm consumes $27 \times 10^{-3} J$. Therefore, RSA is adaptable for the WSNs as it consumes less energy. The Lightweight and Attack Resistant Authenticated Routing Protocol (LARARP) for mobile ad hoc networks supports the node to drop the invalid packets earlier by detecting the malicious nodes quickly by verifying the digital signatures of all the intermediate nodes [53]. It is also used to prevent the Denial-of-Service (DoS) attack. LARARP scheme achieves more PDR, slightly lower delay and has less routing overhead than the Secure AODV (SAODV) scheme since it has both reliability and security features.
In [2], a technique using Data Routing Information (DRI) table to identify multiple BHs, cooperating with each other, and discover a safe route, avoiding cooperative BH attack has been proposed. Detection, Prevention and Reactive AODV (DPRAODV) scheme presented in [48], uses a very simple and effective way of providing security in AODV against BH attack. This scheme [48] detects the malicious nodes and isolates it from an active data forwarding, routing and reacts by sending ALARM packet to its neighbours. The DPRAODV increases PDR with minimum increase in Average-end-to-end Delay.

To evaluate the security enhancement for routing protocols, a secured optimized routing protocol named SARO-AODV, which combines Security Awarded Routing Optimization (SARO) and AODV protocols, is used. The throughput of SARO-AODV protocol is much higher than AODV. In SARO-AODV, the malicious listening rate is greatly reduced as compared to that of AODV. The Trust-based Multipath DSR (TMDSR) protocol provides better throughput in the presence of 40% of misbehaving nodes in the network. This protocol is able to detect 90% of misbehaving nodes in the network [51]. The routing overhead of TMDSR is more than DSR when there are no malicious nodes in the network.

Heterogeneous Sensor Network (HSN) model [84] is used for key management scheme, which establishes shared keys for neighbour sensors that communicate with each other. A public key algorithm Elliptic Curve Cryptography (ECC) is used to further improve the key management scheme. The simulation result shows that the ECC key management scheme consumes much less energy than the El-Gammal scheme and the ECC scheme achieves more energy saving for larger networks. Thus, the ECC key management scheme is very resilient against node compromise attack.
The cluster-based on-demand routing mechanism also provides security by attaching multiple MAC values and increases the security level by computing keys on-demand [28]. This proposal is a dynamic routing path selection made by cluster heads, and it also provides message authentication. Distributed Secure Multipath solution is to route data across multiple paths so that intruders require much more resources to mount successful attacks [78].

Multi-path routing protocol chooses only nodes with more energy to act as cluster heads. Using trust mechanisms, it creates the credit value, and based on the credit value, the multi-path cluster head routing can finally be found. The credit value is created and exchanged among the cluster heads only. Theoretical analysis combined with simulation results demonstrate that this protocol can save the resource, prolong the lifetime and ensure the security and performance of the network.

The performance of secured path redundancy algorithm is due to the usage of a secured alternate path which involves less number of broken paths, hop count and less packet loss to reach the destination node.

2.7 Secure Localization Schemes

Localization is critical for many applications in WSN such as clustering, topology control, location-based information querying and geographical routing. Centralized localization algorithms require base station with plenty of computational power to gather network-wide environment information. Base station determines the location of each node by collected data and transport them back into network.

In distributed localization, each node independently determined its location with only limited communication and with one-hop or multi-hops neighbour nodes. Range-based localization methods depend on distance or angle between nodes to obtain unknown node’s location. Range-free localization methods use the information
of topology and connectivity for location estimation. In [40], a localization scheme with a medium access protocol based on received signal strength (RSS) that provides better localization accuracy is discussed.

In a robust positioning system, there is a Robust Position Estimation (ROPE) that allows sensors to determine their location without any centralized computation. ROPE provides a location verification mechanism that verifies the location claims of the sensors even in the presence of malicious adversaries before data collection. The attackers may attack the localization process to make the estimated locations incorrect. Incorrect locations may lead to severe consequences. In [60], the existing localization algorithms developed for sensor networks which are vulnerable to attacks in hostile environments are discussed. A general secure localization scheme to protect localization from adversarial attacks along with mobility-assisted secure localization frameworks is discussed in [87].

To eliminate the need for tight clock synchronization between anchors and locatees, a Time of Arrival (ToA) two-way ranging method is often desired [93]. In [84], an authentication technique which makes use of Elliptic Curve Cryptography (ECC) along with the ToA positioning scheme is implemented. The position of the sensor nodes in the network are determined by applying the ToA algorithm. Because of the implementation of the ECC technique, the distance estimation and positioning technique were capable of overcoming the attacks and accurate positions were obtained. It clearly indicates that ToA approach of localization along with the implementation of ECC with key exchange is well suited for WSNs.

Usage of ECC protocol in mobile networks [54] allows only the authorized base station to access the node. A suite of techniques to detect and remove compromised beacon nodes that supply misleading location information to the regular
sensors is introduced and it aims to provide secure location discovery services in WSN. The basic idea is to evaluate the suspiciousness of each beacon node based on the alerts from detecting nodes. The beacon nodes with high degree of suspiciousness are considered as compromised.

In [10], a strategy is proposed to defend against colluding malicious nodes in a sensor network. It is based on a new relaxation labeling algorithm to classify nodes into benign or malicious ones. Only reports from benign nodes can then be used to perform localization and obtain accurate results. In [9], a distributed method for localization of sensor nodes using a single moving beacon is described, where sensor nodes compute their position based on the range-free technique. Two parameters are critical to the location accuracy of sensor nodes: the radio transmission range of the beacon and how often the beacon broadcasts its position.

In [60], a scheme that performs accurate localization of the nodes in the network despite the presence of such malicious anchors is described and the way to identify most of these malicious anchors is also shown. In the presence of measurement errors, a convex optimization-based localization scheme that can accurately localize a node is proposed as long as the number of malicious anchors in its communication range is no more than the threshold. In the lifetime of a network, the possibility of anchors being tampered or compromised by an adversary is fairly high. These compromised anchors may be reprogrammed by the adversary to provide false distance estimates to the nodes that are localizing themselves. Moreover, multiple malicious anchors may collude, resulting in false localization of a node. This is a critical setback for the localization process, as incorrect localization may have serious repercussions.
Secure Integrated Routing and Localization Scheme (SIRLoS) [68] guarantees that routing and location information are protected against eavesdropping and unauthorized manipulation, while providing broadcast authentication, data confidentiality, integrity and freshness.

In [24], a secure localization scheme against WH attacks has three phases: WH attack detection, neighboring locators’ differentiation and secure localization. The main idea of the secure localization scheme is to build a so-called conflicting set for each locator according to the abnormalities of message exchanges among neighbouring locators, which is used to differentiate the dubious locators from valid locators for the secure localization. A Secure Localization scheme Against Wormhole attacks (SLAW) works well under secure localization system model. The localization accuracy of schemes of RSS and ToA are shown in Figure 2.3 and Figure 2.4 respectively.

![Comparing RSS Schemes to obtain percentage of Localization](image)

**Figure 2.3 Comparing RSS Schemes to obtain percentage of Localization.**

Comparison of various Secure Localization Algorithms is shown in Table 2.4. Location is verified efficiently in ROPE algorithm, and SPINE algorithm is found to
be more robust. HiRLoc, SeRLoc and ROPE are easier as well as these need extra hardware, that is, directional antennas in beacon nodes, but SeRLoc does not consider hostile beacon nodes. SPINE algorithm requires nanosecond clocks as described in [5].

![Figure 2.4 Comparing ToA Schemes to obtain percentage of Localization](image)

**Figure 2.4 Comparing ToA Schemes to obtain percentage of Localization**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Misbehavior Detection</th>
<th>Robust position computation</th>
<th>Location verification</th>
<th>Simple Algorithm</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiRLoc</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Directional antennas</td>
</tr>
<tr>
<td>SeRLoc</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Directional antennas</td>
</tr>
<tr>
<td>ROPE</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Directional antennas</td>
</tr>
<tr>
<td>SPINE</td>
<td>No</td>
<td>Verifiable multilateration</td>
<td>No</td>
<td>No</td>
<td>Nanosec clocks.</td>
</tr>
</tbody>
</table>

Unlike most existing key management schemes for WSNs, SHELL [43] supports rekeying, and thus, enhances network security and survivability against node
capture. SHELL distributes key management functionality among multiple nodes and minimizes the memory and energy consumption through trading off of the number of keys and rekeying messages. All nodes in the network have unique identifiers. Every gateway can detect the failure or compromise of a sensor in its cluster. In case of a sensor compromise/failure, the data keys of the entire cluster will have to be changed. This is done so that the adversary cannot decrypt future messages of the network. In SHELL, keys are reused in multiple nodes and only key combinations are unique.

A scheme based on weighted-trust evaluation is used to detect malicious nodes and reduces the communication overhead between sensor nodes by utilizing clustered topology.

Using centroid approach, the Localization error is reduced with the use of Secure Integrated Routing and Localization Scheme (SIRLoS) algorithm [75]. Accurate localization is ensured by SLS [83] despite the presence of attacks. When employing approaches like Overlapping Circles, Trilateration and Overlapping Sectors, the localization percentages drop from around 90% to around 40%, as sensor being attacked by WHs cannot obtain an overlapping region for its location. When Dynamic Anchor Regrouping (DAR), is used, the percentage is maintained.

### 2.8 Analysis of Attacks in Trusted Routing Protocols

In the optimized link state routing protocol (OLSR) [45], if a WH attack is launched during the propagation of link state packets, the wrong link information presents throughout the network which could lead to routing interruption. A method attempts to identify the links that may be a part of a WH tunnel, and it exhibits high detection rate under various scenarios.

The WH attack can be launched in hidden and participation modes. In the hidden mode, the attackers do not use their identities so they remain hidden from the
legitimate nodes. In the participation mode, it is assumed that the attackers possess valid cryptographic keys that can be used to launch a more powerful attack. In this mode, the attackers make no virtual links between the legitimate nodes. A timing-based countermeasure [32] against the WH attack over existing schemes based on timing analysis is discussed. So, the nodes do not need to have synchronized clocks to be capable of fast switching between the sent and received modes. The disjoint path-based approaches have been adopted in [52] and they use the relative frequency of each link when discovering routes within the network.

Anomaly detection is a technique that quantitatively defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. An anomaly-detection scheme [46] based on a dynamic learning process that allows the training data to be updated at particular time intervals is used. This system demonstrates an effective performance in terms of high detection rates and low false positive rates against routing disruption attack and resource consumption attack.

A novel algorithm is used in [92] to detect internal attacks by using both message and route redundancy during route discovery. As long as there are sufficiently many correct nodes, the routing protocols should be able to discover routes that go around some compromised nodes. Similar methods can be adopted into the scheme to discover multiple routes. Secure routing against collusion (SRAC) is used by a node to make a routing decision based on its trust of its neighbouring nodes and the performance provided by them. A malicious node randomly drops data packets and can be detected during topology discovery.

A secure routing protocol (SRP) with quality of service (QoS) support, called Trustworthiness-based Quality of Service (TQOS) routing, is used in [91]. The
routing control messages are secured by using both public and shared keys, which can be generated on-demand and maintained dynamically. The message exchanging mechanism also provides a way to detect attacks against internal attacks. Each node has built up an updated trust repository locally for the nodes. The routing metrics are obtained by combing the requirements on the trustworthiness of the nodes in the network and the QoS of the links along a route. The attacks can be detected by verifying various copies of a received message, which reaches a node via different paths at different times. The results on the message verification conducted by a node are used to build a trustworthiness repository.

The trust is based on previous individual experiences of the node and on the recommendations of its neighbours. The recommendations improve the ability of assessing the trust level of its neighbours and brings to detect and to isolate malicious behaviours, and cooperation can be achieved by selecting the neighbours with higher trust levels. The recommendations are only exchanged between neighbours, and there is no intermediate node to increase the uncertainty of the information. The Recommendation Exchange Protocol (REP) [76] model is used to detect the behaviour changes of nodes and is robust to slander and colluding attacks.

Non-cooperative behaviours of nodes will significantly degrade the network performance. Although a reputation system can stimulate nodes to cooperate with each other, the recommendation-based trust model may cause a decline in network performance, because of fake recommendation, convergence of iteration and node redemption. To address this issue, a topology transform-based recommendation trust model [80] is proposed to relieve the malicious effects on the accuracy of recommendation trust, which stem from fake recommendation. In this model, every node maintains a trust table, including global trust and recommendation trust.
The limitation of flooding attack prevention (FAP) is eliminated by [11] using threshold prevention. In this method, they defined the fixed threshold value for every node in the network. If any node receives the RREQ flooding packet more than the threshold value then the sender is assumed as an attacker and all the packets from the attacker are discarded by the receiver node. This method eliminates the flooding packet but if the intruder has the idea about the threshold value then it can bypass this mechanism.

Dynamic Source Routing (DSR) protocol is used in [63] along with the trust estimation function because the communication between the nodes in the MANET depends on the cooperation and the trust level on its neighbours.

A mechanism based on Packet Drop Ratio (PDRR) [69] is used to detect the BH attack in MANET with AODV protocol. Threshold detection technique compares calculated PDRR against a Threshold value. Here, threshold value is a maximum PDRR value without BH attack.

In [56] presented an algorithm to prevent the co-operative BH attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks. Besides due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

Many important applications in ad hoc networks use group oriented communication and may use multicast communication services. Most of the multicast routing protocols assume trusted, non-adversarial environment and do not take security issues into the account. Multicast Ad hoc On Demand Distance Vector (MAODV) protocol is a multicast routing protocol which is used to identify some routing attacks like BH, WH and flooding [8]. In order to multicast the data, MAODV dynamically constructs a shared multicast tree which connects the group members. A
trust-based approach maintains a log of success and failure rate of packet transmissions for each node which are then used to determine the trust values, thereby helping in the mitigation of BH and WH attacks. A new parameter trust value (TV) is used to choose the best path which ensures trustworthiness of the path by calculating the trust value of the neighbour nodes.

In [19], each node would evaluate its own trust vector parameters about neighbours through monitoring the neighbours’ pattern of traffic in network. All nodes are placed in the promiscuous mode all the time whether a node transmits control packets or data packets. After a period of time, its experience value would be extremely low as a result of malicious behaviour. The results demonstrate that modified routing protocols can effectively detect malicious nodes and mitigate their attacks.

Mobile ad hoc wireless networks are established through the mutual cooperation of their participating nodes. These nodes often operate in a physically insecure environment and as a result, are vulnerable to capture and compromise. In addition, the nature of the wireless communication medium restricts enforcement of rigorous node memberships and so a number of malicious nodes may also participate in the network. These nodes, in order to obstruct or interrupt, can undertake a variety of attacks against the network. Among these, WH attacks have unusual significance primarily due to their method of operation and typical attack pattern. In [50], a novel trust-based scheme for identifying and isolating nodes that create a WH in the network, without engaging any cryptographic techniques is presented.

Two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so is a problem. To mitigate this problem, categorizing nodes is used based upon their dynamically measured
behaviour. Watchdog is used to identify misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. The watchdog mechanism is used to detect replay attacks, but would require maintaining a great deal of state information at each node as it monitors its neighbours to ensure that they do not retransmit a packet that they have already forwarded. When watchdog and path-rater are used together in a network with moderate mobility, these two techniques increase throughput by 17% in the presence of 40% of misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

Recently, a new class of routing protocol called trusted routing protocol is determined. Trusted routing protocols consist of two parts such as routing part and a trust model. Routing decisions are made according to the trust model. Trust is used to assess the risk associated with cooperating nodes and can be derived from direct interactions. Here, the trust model for acknowledgements as the single observable factor to assess the trust can offer an effective indication of a node’s trustworthiness. An acknowledgement is a means of ensuring those packets which have been sent for forwarding. There are a number of ways that this is possible, but passive acknowledgement is the simplest. Passive acknowledgement uses promiscuous mode to monitor the channel, which allows a node to detect any transmitted packets, irrelevant of the actual destination that they are intended for forwarding. In ST-AODV [20], it uses a simple trust model, where the trust value for each node is initialised to 0. With each observation, the value is incremented for nodes that are detected to forward packets and decremented for nodes that do not appear to forward
packets. If a node is untrusted then it is not sent packets for forwarding, and any replies it gives to route requests are ignored. Once a node becomes untrusted it is excluded from the consideration of packet forwarding by dropping it from the set of neighbours, removing all routes that use it, and sending out a new RREQ to re-establish the removed routes. Nodes make routing choices based on trust in ST-AODV whereas in AOTDV [35] it makes routing based on the trust as well as the number of hops.

In [55], the survey of trust-based protocols, some techniques on trust management in MANETs and the various trust models are discussed. In the survey [1], the current state of the art routing attacks and countermeasures MANETs are reviewed. Furthermore, most of the mechanisms can work only with one or two specific attacks and are still vulnerable to unexpected attacks. Another active area of research in Mobile Ad Hoc and Sensor Network security in general is the Trust-Based Security Solutions. When a network entity establishes trust in other network entities, it can predict the future behaviours of others and diagnose their security properties. Trust helps in assistance in decision-making to improve security and robustness, adaptation to risk leading to flexible security solutions, misbehaviour detection and quantitative assessment of system-level security properties.

Figure 2.5 shows the comparison of various protocols of PDR and end-to-end delay of the packets against the routing attacks. Both the EIDS AODV and SRAC protocol has similar performance for PDR. SADEC protocol has the 55% PDR which is lower and 30ms delay of packets which is higher when compared to other protocols. AOTDV protocol has the 65% PDR which is higher when compared to the other protocols and also it has 15ms delay of packets. AOTDV protocol has a better performance when compared to the other protocols.
Figure 2.5 Comparison of Packet Delivery Ratio and Delay of Packets

2.9 Summary

In this chapter, the basics of QC and various secret key sharing schemes are reviewed. Also, secure data communication through routing protocols of WMN and wireless sensor and ad hoc networks are reviewed. In this chapter, the trust-based routing protocol in ad hoc network is analysed. Since all these methods are transmitting data through the wireless medium, it is vulnerable to various attacks. So, the BH, WH, flooding and grey hole attacks detection and prevention schemes are analysed. The ever-increasing importances of application areas such as cryptography and secure data communications have led researchers to a renovated interest in trust-based secure routing protocols and localization problems in WSN. The study of various attacks is also outlined and it is very useful to improve throughput, packet delivery ratio and to reduce control packet overhead. The outcome of this thesis is discussed in the following chapters. The proposed quantum cryptography-based unconditional secure communication protocol is presented in the next chapter.