CHAPTER 2

REVIEW OF LITERATURE
2.1 PREAMBLE

The prior chapter introduces the concept of the secure routing protocol that aims to conserve significant level of battery among the sensor nodes in wireless sensor network. The study particularly stresses on the hierarchical routing protocol. This chapter will discuss the existing approaches that are formulated to address the security loopholes in the communication of wireless sensor network.

2.2 STUDY TOWARDS ROUTING PROTOCOLS

Study towards routing protocols in wireless sensor network is more than a decade old, and various series of security solution have been evolved. One of the interesting facts in this regards is that with an increase attention towards security, there has been a parallel evolution of various types of adversaries too apart from the common and frequently heard adversaries in wireless sensor network. Routing protocol will play a significant role in implementing the security features

2.2.1 Techniques for Energy Efficient Routing Protocol

Energy is one of the scarce resources residing within a sensor node and is highly essential for operation. The hardware design of the sensor wireless node is developed in such a way that to retain a better performance of the communication among the sensor nodes, a sufficient amount of transmittance as well as receiving energy is required to be retained by the sensor nodes. Hence, there is a close connectivity between the routing and the energy consumption pattern. Owing to routing principles, a sensor will require to be ready for allocating the certain specific amount of energy to
perform a certain specific task related to route discovery and data transmission within a defined channel. Therefore, the majority of the existing literatures towards energy efficiency were connected with the routing protocols. It is also well known that hierarchical routing protocols [12] in sensor wireless network e.g. LEACH, PEGASIS, TEEN, and APTEEN are the only standard routing protocols introduced by the research community almost a decade ago. All these algorithms have certain benefits, but however, they were all found to be associated with certain loopholes that cannot address the consumption energy problem so efficiently. Hence, there were a series of research work being carried out to explore more hidden reasons, and various studies were also found to show robust solution towards the problems of consumption energy issues in wireless sensor network. This section will discuss the existing literature and their effectiveness about energy efficient routing protocols in sensor wireless network.

Wang et al. [13] have presented a study where the routing protocol is designed using network coding technique for meeting an objective of energy-efficient communication in sensor network. The study implemented an arbitrary and linear-based network coding where the re-encoding of the messages is carried out by an intermediate node simulated over OMNet++, the outcome of the study for its energy effectiveness with increased error rate in transmission with inconsideration of interference.

Chang and Ju [14] have developed a unique clustering scheme that is essentially meant for conserving the energy depletion in wireless sensor network. The technique uses a distance calculation between the nodes and considers the highest residual energy to elect cluster head during rounds of
data aggregation. The cluster location is maintained uniform throughout the simulation study. The presented system is developed in C#.net and the outcome of this paper is compared with conventional energy efficient routing protocol with respect to energy on increasing rounds to find its higher effectiveness with respect to energy conservation.

Villada and Donoso [15] have discussed a routing protocol that have the claimed supportability of multiple path and energy factor in wireless sensor network. Supported by mathematical modelling, the presented paper is designed in Java using heuristics approach towards finding its neighbor nodes and minimum number of hops available. The system also introduces a concept of backup nodes that can highly support the failure rate of dying nodes thereby enhancing the network lifetime.

Jiang et al. [16] have presented an enhanced routing protocol using fuzzy logic for improving the communication performance of wireless sensor network. The prime purpose of this paper is to address the problem of inequality of energy consumption among the sensor nodes during data aggregation. New form of parameters like shortest distance between the nodes, node-sink etc. is considered to develop membership function in fuzzy logic. The outcome of the study is found to posse’s better energy efficiency.

Machado et al. [17] have developed a unique routing protocol that is responsible for upgrading the quality of the links in wireless sensor network. The presented system put forward a route selection mechanism based on link quality, remnant energy, and total number of hops. The technique is capable of maintaining a well equilibrium between energy drainage and load balancing for any scale of wireless sensor network. Simulated over OMNet++, the
outcome of the proposed study was evaluated with respect to existing reactive communication protocol

Thayananth and Alzranhi [18] have developed a routing technique that has the capability to maintain maximum energy efficiency using thresholding scheme. The study uses trust as well as the cross layer approach in order to evaluate the trust values along with acknowledgment data. The author has used a standard simulation tool called as TRMSIM [22] where the result was assessed for its new performance parameters e.g. ratio of malicious detection, mean energy drainage, mean length of route, and standard deviation.

Kumaramangalam et al. [19] have presented a new and standard protocol called as zone-based routing protocol in wireless sensor network. The author developed a unique topology-based routing considering the partitioning scheme for allocating the sensors of same numbers in clusters. The prime aim of this routing protocol was to minimize control overhead and energy depletion during transmission stage. Developed over Castalia simulator, the outcome of the study was evaluated with energy factor.

Patooghy et al. [20] have developed a scheme of load balancing as an indirect mechanism for controlling energy drainage and manage the incoming traffic in wireless sensor network. Considering mobile sink, the system keeps a track of the partitioned density as well as mean residual energy. Architecture have been developed that partitions the entire sensing area into four zone and keep the data collector in the centroid of the entire 4 zone. The data collected that forwards the aggregated data to the mobile base station. Simulated over NS2, the presented technique is tested for
energy factor and partition density to find the effectiveness of load balancing and energy efficiency.

Ahmad et al. [21] have presented a technique for developing a routing protocol using multiple chain of communication in order to fine tune number of hops to be communicated in this regards. The technique uses greedy approach as well as mobile sinks for preventing the hopping operation that are really not required in this process thereby saving a massive amount of energy in this regards. Simulated over Matlab, the outcome of the proposed study was testified with respect to data and energy factor mainly.

Bahazaq and Thayananthan [22] have presented a study on energy conservation and standardizing the communication system using topology-based concept in wireless sensor network. The author have presented a three dimensional topology where the unique routing system was created. The authors have also used conventional swarm intelligence based technique to enhance the quality of link while performing routing. The outcome of the study was tested with respect to energy for increasing number of nodes.

Kannan and Paramasivan [23] have presented a routing scheme using gradient-based approach of optimized communication in wireless sensor network. The study concentrates on formulating a strategy that can extract the optimized route with minimized energy consumption. Developed over an elliptical clustering region, the presented technique focuses on reducing the transmission energy for enhancing the network lifetime. The outcome of the study was evaluated with respect to ratio of deadline delivery and energy consumption.
Padhi and Pattnaik [24] have introduced a routing protocol that using a concept of symmetric clustering in order to maintain energy efficiency in wireless sensor network. The author has developed an algorithm that formulates sensor nodes distributed in simulation area in order to form a cluster. It also has a step to select an efficient cluster head based on highest residual energy. This step is also followed by data transmission stage and again re-election of cluster head. The presented algorithm is just a simple enhancement of LEACH.

Raza et al. [25] have presented an architecture that can perform routing with using a particular sensor mote called as Sun Spot motes. The technique uses a feedback based mechanism from its receiving signal strength value using a thresholder scheme to estimate the transmittance power, output power of transmitter, current drawn etc.

Zhang et al. [26] have developed a unique technique for addressing energy consumption considering the mobile sinks in wireless sensor network. The uniqueness of this recent study is that it focuses on the energy efficiency of the sink, which very few studies were found to be emphasizing in the literature. The author has considered the mathematical modeling of the proposed study considering the moving sinks as well as scheduling algorithm along with constraint of the gradient. The outcome of the study was evaluated on the network lifetime along with the energy analysis of the base station.

Sharma and Jena [27] have studied the problem of cluster-based energy consumption problem in wireless sensor network and have addressed this problem using multiple path routing approaches considered over the
conventional clustering. The idea of the presented paper was inclined over the solving the problem of the load balancing in a wireless sensor network by introducing a proactive-based routing protocol. Developed over OMNet++, the presented idea was designed and assessed on performance parameters e.g. energy consumption, packet overhead, delivery ratio, latency, etc.

Gherbi et al. [28] have presented a study that focuses on the load balancing problems in wireless sensor network and closely associated with energy depletion problems too. The approach presented by the author basically controls the state of sleep and awake mode of transmission of the sensor motes that can indirectly control the energy consumption of the entire communicating nodes. Simulated over NS2, the proposed system is evaluated with respect to energy consumption and number of alive nodes during the varying number of test-scenarios.

Dehghani et al. [29] have introduced a study that focuses on the effectiveness of the clustering algorithm with respect to the energy consumption in the wireless sensor network. Although, the study has presented a theoretical discussion of the available energy protocols published most recently, the study has discussed some important findings e.g. i) Existing energy-efficient hierarchical routing protocols in wireless sensor network doesn’t have better scalability factor, ii) the hierarchical routing protocols have good transmission delay iii) the mode of distribution of hierarchical routing protocols is very often randomly studied, iv) the overhead of control message in hierarchical routing protocols is sometime very high and sometime medium, but doesn’t witnessed much with lower
value of it, v) energy efficiency of hierarchical routing protocol is quite poor, and vi) complexity of the hierarchical routing protocol is quite high.

Fouad et al. [30] have presented a technique where the focus of energy efficiency is laid over localization of the sensor node in wireless sensor network. The presented study has introduced a topology control mechanism considering the monitoring and optimization of the energy of the sensor nodes depleting power. Developed in Java environment, the presented technique was assessed on number of alive nodes, time, number of topologies, etc.

Zhigui et al. [31] have developed an algorithm that could perform an efficient routing in wireless sensor network considering the constraints of mobile routing. The study has formulated a conventional mechanism with need energy efficiency by introducing a grid-based concept considering the selection problem of the cluster head. The technique performs scheduling of the mobility of the sink for aggregation the data from the cluster head. The study also introduces a relay node for serving the data transmission along with the cluster head in a sensor network. Simulated over NS2, the outcome of the study was assessed using cumulative energy value, number of alive nodes, and the amount of data aggregated by the sink.

Prabha et al. [32] have presented a unique communication technique that is built over the trust factor of the sensor node in the wireless sensor network. The study also uses multi-hop routing for enhancing the communication performance of the wireless sensor network. Simulated over NS2, the outcome of the study was evaluated on energy and throughput.
Kiani et al. [33] have developed a unique routing protocol using the intelligence-based technique for ensuring the energy efficiency among the wireless sensor network. The study develops such potential features using learning algorithm of reinforcement type along with the introduction of a new clustering scheme. Developed over C#.net, the effectiveness of the study was assessed suing number of packets, loss of data packets, delivered packets numbers, time, with increasing number of nodes.

Rahhala and Ramadan [34] have developed a routing technique that has the capability to maintain maximum energy efficiency using thresholding scheme. The study uses trust as well as the cross-layer approach in order to evaluate the trust values along with acknowledgement data. The author have used a standard simulation tool called as TRMSIM where the result was assessed for its new performance parameters e.g. ratio of malicious detection, mean energy drainage, mean length of route, and standard deviation.

Du and Xiao [35] have developed a very unique form of clustering called as chessboard clustering that is meant to support the routing mechanism over heterogeneous wireless sensor network. The study also considers issues of scalability. Simulated over QualNet, the outcome of the proposed system was also assessed for its network lifetime and packet delivery ratio.

Zong et al. [36] propose secure data aggregation method combining homomorphic encryption with Digital signature techniques for increasing energy efficiency in wireless sensor networks. It achieves in network data filtration to minimize unnecessary data transmission energy transmission
energy. The result performs effectively in terms of communication overhead, computational overhead, energy consumption and delay.

Jiao et.al. [37] Proposes a novel load balancing clustering method which the objective function is to increase the overall minimum lifetime of the cluster heads. Authors propose estimation of distribution algorithm based dynamic clustering approach (EDA-MADCA) it could reduce energy consumption of the nodes and prolong the network lifetime.

Tiloca et al. [38] proposes JAMMY a distributed and dynamic solution to selective jamming in TDMA-based WSNs. Time division multiple access (TDMA) is often used in wireless sensor networks (WSNs), especially for critical applications, as it gives high vitality productivity, ensured transmission capacity, high energy efficiency, limited unsurprising idleness and absence of collisions.

Summary of all the above approaches are shown in Table 2.1
Table 2.1: Summary of existing energy efficient routing protocols

<table>
<thead>
<tr>
<th>Authors</th>
<th>Benefits</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zong et al. [36], Bahazaq and Thayananthan [22], Wang et al. [12], Marco Tiloca et al. [38]</td>
<td>Reduce energy consumption</td>
<td>Doesn’t focus on computational complexity</td>
</tr>
<tr>
<td>Jiao et.al. [37], Kiani et al. [33], Rahhala and Ramadan [34], Thayananthan and Alzranhi [18]</td>
<td>Reduce energy consumption</td>
<td>Not suitable for large network</td>
</tr>
<tr>
<td>Zhang et al.[26], Zhigui et al.[31]</td>
<td>Supportive of mobile sink</td>
<td>Latency increases with increase in incoming traffic</td>
</tr>
<tr>
<td>Sharma and Jena [27], Dehghani et al[29], Padhi and Pattnaik [24], Chang and Ju [13], Du and Xiao[35]</td>
<td>Effective clustering</td>
<td>Not suitable for large network</td>
</tr>
<tr>
<td>Gherbi et.al.[28], Patooghy et al.[20]</td>
<td>Good load balancing</td>
<td>Not benchmarked</td>
</tr>
<tr>
<td>Fouad et al.[30], Kumaramangalam et.al.[19]</td>
<td>Good Topology Control</td>
<td>Packet delivery ratio diminishes in speedy rate</td>
</tr>
<tr>
<td>Prabha et al. [32], Ahmad et al. [21], Villada and Donoso [17]</td>
<td>Supports multihop communication</td>
<td>Iterative nature leading to complexity</td>
</tr>
<tr>
<td>Machado et al. [16]</td>
<td>Ensures link quality</td>
<td>Throughput is not increased</td>
</tr>
<tr>
<td>Kannan and Paramasivanan [23], Jiang et al. [15]</td>
<td>Ensures optimization</td>
<td>Uses iterative process</td>
</tr>
</tbody>
</table>

2.2.2 Techniques for Secure Routing Protocol

Majority of the security policies have been found to be formulated by adoption cryptographic approach in wireless sensor network. Normally, cryptographic technique is applied in order to perform authentication of the communicating sensor nodes. Owing to the malicious and unpredictable
intention of an adversary, the encryption of the control message as well as the data is carried out in order prevents the access by an adversary. It is not necessary that an adversary should always steal the data but it could also tamper the data thereby disrupting the normal traffic behavior. Hence, directly or indirectly, secure routing protocol are usually meant to prevent authentication of such malicious nodes and there maintain integrity, privacy, confidentiality, and non-repudiation etc. However, still it is an open end question to find presence of any such robust routing protocol. This section discusses about some of the recently studied secure routing protocol in wireless sensor network.

Maleh and Ezzati [39] have presented a technique for the purpose of identifying the intrusion points in sensor network. The authors make use of supervised learning algorithm e.g. Support Vector Machine along with digital signature for studying the malicious behavior of a sensor node. A simple mathematical model was mechanized for identifying the probability of malicious nodes. The effectiveness of the proposed system was evaluated with respect to energy consumption, rate of false positives, detection rate,

Cheikhrouhou et al. [40] have adopted graph-based theory for securing communication in groups for wireless sensor network. The study uses re-keying concept without any need to use multicast routing. The outcome of the study was assessed with respect to multiple performance parameters e.g. latency, cost of storage, and cost of communication with increasing number of nodes. The assessment of the study was carried out using homogeneous wireless sensor network.
Guermazi and Abid [41] have presented a scheme that supports secured routing in wireless sensor network using cryptographic key management. However, the study is focused on using key distribution mechanism exclusively for available energy efficient hierarchical routing protocols. The technique have used pairwise key distribution and is meant to thwart replay attacks and flooding attacks mainly. Simulated over TinyOS, the outcome of the study was evaluated with respect to response time of key distribution.

Si et al. [42] have developed a security scheme that is mainly meant for link layer of wireless sensor network. The authors have emphasized on the stream ciphers (Sosemanuk, RC4, and Salsa). The outcome of the study was evaluated with respect to CPU cycles as well as cycles per byte, which is an outcome of encryption.

Zhijie and Ruchuang [43] have developed a statistical framework in order to secure the routing system from intrusion in wireless sensor network. The authors have adopted Markov modelling to develop a new traffic system using predictive scheme. The scheme was majorly meant for resisting denial of service attack and forwarding attack in sensor network. Simulated over NS2 with 400 nodes, the outcome of the study was assessed using rate of detection and packet loss rate comparison.

Khan et al. [44] have developed a unique key management protocol for the purpose of strengthening the authentication operation between two communicating sensors. The author uses Elliptical Curve Cryptography or this purpose and performed simulation over Cooja with nodes ranges from 4-20. The study was carried out especially for sniffing attack, denial-of-service
attack, stolen ID attack, and node replication attack. The outcome of the study was assessed using response time to perform exchanging of secret keys.

Huang et al. [45] have presented a scheme that emphasizes on cryptographic key management from storage viewpoint in wireless sensor network. The study uses Exclusion Basis System for performing key management in sensor network. The core concept of the presented technique uses pre-distribution of keys along with re-keying mechanism for ensuring dual level of security for selected cluster head. The outcome of the study was evaluated with respect to number of keys required to perform encryption in one node, key messages, etc.

Zhang et al. [46] have presented a technique to circumvent an adverse effect of sinkhole attack in sensor network. The technique formulates new control message and perform an efficient selection of routes using multi-path routing techniques. A threshold-based technique is used to realize the presence of sinkhole attack and mitigate it effectively. Simulated on NS2, the outcome of the study is evaluated with respect to positive rate of detection.

Chatterjee et al. [47] have used elliptical curve cryptography for the purpose of maintain utmost level of privacy in wireless body area network. The presented system is found to support adding up new sensor nodes where the authentication can be carried out without the base station. The system develops a secret session key among different users while allows the user to perform involuntary validation of various protocols supported by the sensor nodes involved in communication. The outcome of the study was tested with
respect to energy consumption and computational cost involved in the entire process.

Chowdhury et al. [48] have presented a scheme that focuses on security of the routing in wireless sensor network. The authors have discretely used cryptographic hash function and the algorithm is claimed to be resistive of collision significantly. The technique was compared with the standard cryptographic algorithm e.g. MD5 and SHA-1. The outcome of the study was found to be quite lower computational overhead for presented technique with respect to existing system.

Elhoseny et al. [49] have presented a scheme of public key cryptography in order to maintain security in communication standards of wireless sensor network. The author particularly uses Elliptical Curve Cryptography for carrying out the encryption in sensor network, which is further strengthened using homomorphic encryption too. The study implements a key size of 176 bit which is done by integrating secure key of Elliptical Curve Cryptography, distance with respect to aggregator node, and node identity. The outcome of the study is assessed with respect to network lifetime (or energy) mainly to find presented technique is better than existing secure routing technique.

Gaur and Pant [50] have presented a study that attempted to understand the influence of received signal strength on security factor of the routing in wireless sensor network. The study uses cluster formation with trust-based calculations. An interesting observation found in this study is usage of mobile routing protocol in sensor network using OPNet simulator. The outcome of the study is evaluated with respect to quantity of sensors
present in one cluster, potential signal strength, and total number of intruders present in one cluster.

Mariammal and Gayathri [51] have introduced a technique most recently for ensuring security during data aggregation process. The authors have used caching information for reducing the data provisioning cost in sensor network. The study was focused on developing an application of sensor network using social networking aspect of it in order to prevent replay and jamming attack mainly.

Naik and Shekokar [52] have presented a technique for maintaining a better balance between energy conservation and security threats. The study introduces a new form of attack called as Denial-of-Sleep attack which mainly targets to disrupt the normal behavior of MAC protocol. The study also uses zero knowledge protocol for authenticating the sensor nodes after receiving the control message for sleep synchronization. Using mobile routing protocol and simulated over NS2 with 11 sensor nodes, the study have implemented the security using RSA algorithm.

Rizk and Alkady [53] have used extensive cryptography for securing the communication in wireless sensor network. The study also uses Advanced Encryption Standard, Elliptical Curve Cryptography, MD5, and RSA algorithm. The outcome of this hybrid cryptographic scheme is tested with respect to size of encrypted text in bytes along with time consumed in performing encryption / decryption. The study was also testified using energy consumption and rate of dropped packets too. The interesting point of the study is its testing with image and various added performance parameters e.g. correlational analysis.
Roy et al. [54] have studied and emphasized on incorporating privacy towards source location using secured routing scheme in wireless sensor network. The authors have presented a scheme called as phantom routing this attempts to hide the location of source node by broadcasting the forged request message on the network. It is based on the response messages; the source node will come to know if the other node is suspicious node or regular node. The outcome of the study was assessed using a performance metric called hit ratio.

Said and Elnashar [55] have introduced a security-based solution for evaluating the wireless sensor network. The presented study uses Gaussian distribution and statistical analysis for the three dimensional environment. The implementation of the study was carried out in NS2 to provide better efficiency from intruders. The outcome of the study was assessed using mean lost packet, throughput, end-to-end propagation delay, and efficiency.

Tang et al. [56] have presented a secure communication scheme that also goes well with reduced energy consumption in wireless sensor network. The technique ensures that privacy of the source location which means denied access for every malicious node to do so. This privilege is only retained by the base station who can only track the location of the source node. The technique presented is meant for resisting jamming attacks mainly.

Monika and Upadhyaya [57] have presented a technique for securing the communication system for wireless sensor network. The authors have used conventional secure socket layer, which is normally used in conventional network traffics. The presented techniques have used complex
cryptography along with usage of Secured Socket Layer to ensure robust authentication, integrity, and confidentiality mainly.

Xiao et al. [58] have presented another motivating works in security of sensor network. A specific case study of visual sensors was used in this study where the problems of network vulnerability evolve when the sensed data are transmitted in wireless medium. Using hardware-based approach, the proposed system develops a sophisticated encryption scheme of such forms of multimedia data over sensor network.

Therefore, it can be seen that there are good number of research work (summarized in Table 2.2) being dedicated towards using secure routing protocol in wireless sensor network, where there exists various forms of techniques with its own advantages as well as limitations. However, the present chapter is more focused on extraction of missing gap at the end of this chapter.
Table 2.2: Summary of Existing Secure Routing protocols.

<table>
<thead>
<tr>
<th><strong>Authors</strong></th>
<th><strong>Benefits</strong></th>
<th><strong>Limitation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Elhoseny et al. [49], Khan et al [44], Rizk and Alkady [53], Chatterjee et al. [47], Guermazi and Abid [41], Chowdhury et al [48], Monika and Upadhyaya [57], Si et al. [42]</td>
<td>Enhanced public key cryptography, ECC, reduced key size</td>
<td>Geometrically complex structure</td>
</tr>
<tr>
<td>Gaur and Pant [50]</td>
<td>Effective trust computation</td>
<td>Doesn’t focus on resource saving</td>
</tr>
<tr>
<td>Maleh and Ezzati [39]</td>
<td>Effective machine learning, good attack detection</td>
<td>Highly iterative</td>
</tr>
<tr>
<td>Mariammal and Gayathri [51]</td>
<td>Reduces cost of data provisioning</td>
<td>Cost factor doesn’t include computation attribute</td>
</tr>
<tr>
<td>Naik and Shekoker [52]</td>
<td>Lesser inclusion of dependable parameters</td>
<td>Uses largest size of key</td>
</tr>
<tr>
<td>Roy et al. [54]</td>
<td>Good privacy</td>
<td>Not effective if topology changes</td>
</tr>
<tr>
<td>Said and Elnashar [55], Tang et al. [56]</td>
<td>Better energy efficiency</td>
<td>Not resistive against node capture attack</td>
</tr>
<tr>
<td>Zhang et al [46]</td>
<td>Resistive against sinkhole, supports multipath</td>
<td>Iterative process</td>
</tr>
<tr>
<td>Huang et al. [45], Cheikhrouhou et al. [40]</td>
<td>Good re-keying, supports clustering</td>
<td>Iterative process</td>
</tr>
<tr>
<td>Zhijie and Ruchuang [43]</td>
<td>Supports large network</td>
<td>Not benchmarked/less energy efficient</td>
</tr>
</tbody>
</table>

2.2.3 Techniques for Optimization Principle

The optimization principles adopted in wireless sensor network are always on the lookout of exploring an elite outcome from the set of problems. The motive of the optimization principle under discussion will be how it has
enhanced the energy conservation as well as other factors that positive enhances the communication performance of sensor network. Although, optimization is a deeper concept from theoretical and implementation viewpoint, so this section will only limit its discussion toward the pattern of optimization techniques adopted by existing researchers.

Fayed et al. [59] have presented a simple optimization technique to enhance the security features. The authors have emphasized on the using Kerberos and elliptical curve cryptography using mathematical modelling aided by Galois field of cryptography.

Zhou et al. [60] have adopted tree-based technique for large scale wireless sensor network using ant colony optimization. The study also uses multiple base stations for improving the data transmission performance. Existing studies towards optimization-based approach are summarized as follows:

Taherian et al. [61] have presented a secured communication model using particle swarm optimization. The entire technique initiates with occurrence of an event from the sensing environment followed by clustering technique that significant assists in conventional process of data aggregation in wireless sensor network. The technique than performs minimizing the duplicated data and thereby enhances the quality of data. The processed data is then forwarded using particle swarm optimization.

Marzi and Li [62] have presented an optimization mechanism exclusively meant for enhancing security features in wireless sensor network. The study implements a trust-based model along with reputation
factor also focusing on the energy-efficiency of the sensor nodes simulated over TRMSim, a simulator for assessing trust and simulation in sensor network. The outcome of the study was evaluated with respect to accuracy, energy consumption, path length, etc.

Sahoo et al. [63] have developed a unique clustering technique that is meant for addressing both security and energy problems in wireless sensor network. The clustering technique has supportability of both trust as well as energy factors using Honey Bee mating technique. Developed in Matlab, the presented technique consistently monitors trust rewarding / penalty factor. The outcome of the study was assessed with respect to energy factor mainly.

Dhivya and Sundarambal [64] have addressed the problems of energy drainage in wireless sensor network using Tabu search-based optimization algorithm. The idea was basically to integrate both particle swarm optimization and tabu search algorithm together. The outcome of the study was assessed using percentage of sensor death

Lu et al. [65] have also carried out work towards data aggregation in sensor network using particle swarm optimization. However, the author brings difference in swarm intelligence using heuristic-based approach jump particle. The authors have presented a dual layer of encoding operation using tree-based approach and the outcome of the study was evaluated with respect to fitness value.
Ye and Mohamadian [66] have developed a routing protocol using conventional ant colony optimization for enhancing the clustering performance. The routing approach presented is more of adaptive type for the purpose of minimizing the data redundancy as well as the energy efficiency.

Liu et al. [67] have adopted a convex optimization approach for addressing the problem of localization in wireless sensor network. The study is particularly focused on anchor nodes. Simulated over Matlab, the study show an outcome to prove that adoption of optimization techniques leads to an efficient identification of anchor nodes which could be adversaries.

Arya and Sharma [68] have developed a framework that performs enhancement of the energy-efficient communication in sensor network using ant colony optimization. The prime goal of this study is to find the best routes using optimization principle considering gradient-based routing for performance comparative analysis. The outcome of the study was evaluated with respect to residual energy in Joules with increasing number of sensors. The outcome show better energy conservation using ant colony optimization.

Barekatain et al. [69] have presented a technique for the purpose of enhancing the communication pattern in wireless sensor network. The study uses integration of conventional k-means algorithm along with genetic algorithm for the aim of minimizing the energy consumption in sensor network. The outcome of the study was testified with respect to throughput, network lifetime to find presented system has better energy conservation with respect to existing energy-efficient routing protocol.
Gajjar et al. [70] have introduced a routing protocol using cross-layer based approach. The authors have implemented fuzzy logic as well as ant colony optimization for the purpose of minimizing energy conservation during clustering operation. The outcome of the study was assessed using number of dead nodes, time, data delivery, and energy consumption of aggregator node.

Pal et al. [71] have also carried out similar category of work for optimizing the selection process of cluster head in wireless sensor network. The author have used genetic algorithm in order to explore the best solution to clustering. The outcome of the study was evaluated with respect to number of alive nodes with increasing number of rounds.

Rajarajeshwari et al. [72] have presented a technique of optimization for conserving the energy drained during the data aggregation process in wireless sensor network. The authors have used cognitive behavior of termite as a supervised learning procedure to perform optimization. The study also focuses on addressing malicious activity where the outcome is analyzed using data transmission performance, energy, and overhead.

Salehian and Subraminiam [73] have enhanced the conventional particle swarm optimization for the purpose of improving the clustering operation in wireless sensor network. The technique addresses the unequal power dissipation that takes place during clustering phase. The outcome of the study shows better energy conservation.

Patel et al. [74] have developed an optimization scheme of assisting the problems associated with multicast routing protocol. The techniques uses
hybrid version of ant colony optimization along with particle swarm optimization. Supported by mathematical modelling, the presented system uses tree-based approach for developing multicast tree-based routing. The study outcome is evaluated with respect to execution time, cost of multicast tree, and delay etc. with increasing number of network nodes.

Devi and Rao [75] authors performance evaluation of clustering enhancement of SEP (stable election protocol enhancement) is compared with DEC and SEP, and the simulation parameters were measured for no of nodes Vs average residual energy. It has been observed that the average residual energy in SEP-E have more energy available than DEC and SEP protocol

Dhote and Asutkar [76] have proposed routing technique in wireless sensor network using queue management the paper describes the enhancement in the utility of the wireless communication sensor network applications using routing techniques by optimization of QOS parameters. Hence optimization of Quality of Service parameters leads to optimization of the wireless communication sensor network system for power efficient application also paper focuses on better performance of routing protocol by optimization in the QOS parameters with the help of Traffic Sensitive Queue management.

Nayak and Vathasavai [77] authors proposed Genetic Algorithm (GA) based clustering algorithm which evaluates the fitness function by considering the two major parameters distance and energy. GA is a probabilistic search based algorithm based on the principle of natural
selection and evolution. Simulation result proofs that the proposed protocol performs better than LEACH protocol and enhances the network lifetime.

Sharma and Kanika [78] tries to summarize all modified latest methods in terms of CH selection, new mathematical formulations, balancing of cluster loads, number of static sinks, linear clustering etc. Paper includes optimized LEACH-C, advanced MODLEACH, improved PEGASIS, P-LEACH, DAPTEEN, SEECH, LCH, and REACH-IN.
Table 2.3: Summary of Existing Optimization Routing protocols

<table>
<thead>
<tr>
<th>Authors</th>
<th>Benefits</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taherian et al.[57], Lu et al.[65], Pal et al. [71], Salehian and Subraminiam [73], Sahoo et al. [63]</td>
<td>enhanced clustering</td>
<td>Iterative process</td>
</tr>
<tr>
<td>Arya and Sharma [68], Gajjar et al. [70], Rajarajeshwari et al. [72]</td>
<td>Enhanced energy efficiency</td>
<td>Iterative process</td>
</tr>
<tr>
<td>Barekatain et al. [69], Ye and Mohamadian[66], Zhou et al. [60]</td>
<td>Good throughput and energy efficiency</td>
<td>Poor convergence performance</td>
</tr>
<tr>
<td>Patel et al. [74]</td>
<td>Support multi-cast routing</td>
<td>Highly iterative, not suitable for large network</td>
</tr>
<tr>
<td>Liu et al. [67]</td>
<td>Solves localization problems</td>
<td>Not energy efficient</td>
</tr>
<tr>
<td>Fayed et al. [59]</td>
<td>Offers good security</td>
<td>Complex internal structure</td>
</tr>
</tbody>
</table>

2.3 DISCUSSION OF RESEARCH GAP

The prior sections have discussed various studies focusing on energy efficiency as well as security issues.

Although there are various studies on various other issues in wireless sensor network, it was seen that majority of the communication-based problems arises from energy depletion problems, which also leads to security breaches. Although, there are various significant research works being carried out addressing the issues of energy consumption and security loopholes, there are various unsolved issues or research gap that is discussed
in this section. Therefore, the significant research gap explored after studying the literatures are as follows:

- **Specific to Adversary**: There are various types of routing-based attacks in wireless sensor network i.e. Sybil attack, black hole attack, denial of service attack, wormhole attack, grey hole attack, etc. [79]. There are also various attacks that compromise the data integrity and confidentiality e.g. node capture attack, denial of service attack, eavesdropping attack, etc. [80]. The attacks related to energy drainage are denial of sleep attack, collision attack, de-synchronization attack, etc. [81]. Similarly, adversaries related to bandwidth consumption are flooding attack, jamming attack, replay attack, selective forwarding attack, etc. [82]. At present, the existing solutions for mitigating the adversaries are quite specific. It is a well-known fact that each form of attacks has their own attacking strategies, which differ from each other’s. Hence, a solution for one attack may not be suitable for addressing another type of attacks. However, a closer look into all the types of attacks shows that every adversary node starts looking for a node that shows weak performance of data delivery. Hence, energy is one of the prime assets of a sensor node to stay resilient against any form of compromisation attacks. It was seen that all the existing solutions are targeting only the fundamentals and one type of attacks that reduces the affectivity as well as scope of such solution. This is one of the significant problem to understand that although all the types of attacks have their own tactics of intrusion but they start from one common pattern i.e. node with weak data communication due to energy drainage or weak security protocol implementation or
defective routing strategy with less focus on authentication. All these problems can be handled if a robust authentication policy be designed with faster mechanism of updating the routing information to other nodes in the simulation environment. Hence, existing studies are more specific to cases of adversaries poses a significant research gap.

- **More focus on Complex Cryptography:** Majority of the existing studies acting as solution towards security breaches in wireless sensor network uses the means as complex cryptographic mechanism. It is strongly believed that cryptography provides a better encryption technique that is highly required for preliminary authentication of sensor nodes. However, usage of complex cryptographic mechanism as a means of security may poses serious issues in communication performance. The problems associated with using complex cryptographic mechanism are as follows:
  
  o Iterative encryption / decryption technique may not be suitable for some real time data transmission. It is just good for single hop communication especially in case of authenticating the communicating nodes. However, with increasing hop distance, the processing time due to encryption will be highly increasing that may lead to excessive energy consumption as well as dropping of data packet. Hence, cryptographic algorithm with complex architecture is not preferred.

  o Usage of cryptographic programs will also lead to generation of keys that will be required to be stored. With variable sizes of keys from 128-512 bits, it is not possible for a cryptographic
technique for ensuring that number of keys to be generated will be reduced down although the size of the key to be stored may be constant. This process of generation of cryptographic key will need increasing memory consumption, which will excessively drain the resources that may be otherwise used in communication.

- **Less Balance between Energy and Security and Routing**: The existing studies doesn’t combinely address the issues of energy drainage, security breaches, and routing performance altogether. Although there are some studies that claim energy efficient routing in wireless sensor network, but they fail to answer many unsolved questions e.g. i) what is the computational complexity involved in the process, ii) is it compared with existing hierarchical routing protocol with security. iii) How much it affects the performance for various types of network with different values of performance parameters. Hence, if the security issue is addressed than energy and routing issues have would have been ignored. So, a very less balance between energy problems, security problems and routing problems are found to be addressed in existing system.

### 2.4 CONCLUSION

This chapter has discussed about the various existing studies being carried out for addressing the issues of energy efficiency and security breaches in wireless sensor network. The chapter has discussed all the work being done from reputed international journals focusing on latest publication on this issue. The discussion of the existing techniques towards energy and security
is then followed by discussion of research gap, where it was found that although there are massive archives of literatures towards energy problems, routing problems, and security problems, but no cost-effective studies with capability of addressing multiple forms of adversaries are seen by any routing protocol that equally addresses energy issues and security problems. The next chapter discusses about the theoretical background of security and energy problems in proposed system.