Chapter 3

ON THE ROLE OF WIRELESS SENSOR NETWORKS IN SUBSURFACE EXPLORATION: THE LITERATURE REVIEW

3.1 Introduction

Wireless Sensor Networks (WSN) play a noteworthy role in a wide arena of daily life, like environmental pollution control, habitat monitoring, natural disaster monitoring etc. Despite this fact, a little has been done towards utilizing this technology for the Subsurface Exploration. Subsurface exploration basically refers to the extraction of hydrocarbons from the oil field. In fact, subsurface exploration is a very established field which, has been practiced for a very long time now. It can be observed from the statistics that with the increasing rate of consumption of extracted hydrocarbons there has been no significant increase in the quantity and quality of natural resources extracted. In view of this the oil companies are not only constantly looking towards new sources of oil but also to improve the production of existing wells. This chapter presents a detailed review of research that has been carried out in this direction and also the issues that still need to be debated upon.

As already discussed in chapter 2, subsurface exploration is the process of extracting the hydrocarbons available beneath the earth crust. The term is generally being used for extraction of crude oil from the oil fields. According to Central Intelligence Authority (CIA) [75], in 2007 alone, the United States of America produced an estimated 7.46 million barrels of crude oil per day and imported 13.21 million barrels per day from other countries. This trend reflects that more oil is imported then it is actually extracted within the country like USA. Moreover, available facts [9], indicate that only 30% (approximately) of the oil is recovered from an available field & the rest of 70% remains un-extracted due to lack of information
or various other factors such as amount remaining, pressure, temperature & other real time conditions. Basically, the crude oil is refined into finer products like gasoline, kerosene, heating oil etc. To keep pace with the increased demands as well as consumption, oil companies are in ever ending pursuit for finding new sources of petroleum, as well as to improve the production of existing wells with the help of latest technologies. One such promising technology is WSN [48, 141], in which Intelligent sensors can collect and process a vast amount of data. WSN finds it traditional applications in fields like protection and control of natural and man-made environment, remote interaction with the physical world and so on. Since, sensors are capable of acquisition of parameters viz. temperature, pressure, density etc., therefore seems to be a promising candidate beneath the earth also. The upcoming section presents the motivation of deploying WSN in the field of oil exploration.

3.2 On the Role of WSN in Subsurface Exploration

Subsurface Exploration is the process of drilling exploratory holes in the ground, sampling at discrete points, and in situ or laboratory testing to confirm the presence of ores, oil or gas. In majority of the cases the minerals are deep below the earth’s surface, and drilling is very expensive. This calls for the optimization of the drilling investigation, amongst other things. Moreover the resources in the subsurface area are non-renewable and limited in quantity. Hence should be extracted in the most optimal way to make maximum utilization of the natural resources and operational instruments.

Chapter 2 outlined various methods of oil extraction highlighting the pros and cons of each of them. Also, the section highlighted the modern techniques used by geologists for interpreting features of surfaces, rocks, soil types and terrain with the help of satellite images. There exist methods like sensitive gravity meters, sensitive magnetometers, seismology that adds value and excellence to oil extraction process, however, the gravity methods are too slow and expensive for traditional exploration process. In addition, the data generated by these methods are not only difficult to
interpret; it has the added complication as well. In fact, latest oil-extraction techniques that have proved to better than their previous counterparts are still offering very low success rate in non-deterministic environments.

The above-mentioned issues prompted the researchers to look for a more promising technology to respond to the evils in subsurface engineering. As a result, WSN emerged as one of the promising candidates recently [9]. Upcoming literature aims to prove the feasibility and significance of WSN in subsurface exploration.

Advances in Micro-Mechanical Systems (MEMS) [74] have allowed integration of sensors, actuators, mechanical elements and wireless communication on a common silicon substrate with the help of micro-fabrication. These integrated units are low-cost and small form-factor embedded systems called sensor nodes [92, 36]. Wireless sensors leading to a robust and scalable WSN are being successfully used for energy management [17], medical monitoring [66], battlefield management / surveillance [132], habitat monitoring [10], and security systems [106] and so on.

![Diagram of sensor capabilities](image)

Figure 3.1: Issues Related to Sensor Capabilities [9]
In July 2008, Advance Energy Consortium [9] floated a Request for Proposal (RFP) “Oil and Gas Micro-and Nano-sensor Needs”, where in, along with other issues they discussed the need for the Required Sensor Capability [9]. The various issues under Sensor Capability are as depicted in figure 3.1.

Although proposals [9] had been invited for the deployment of sensors in oil fields but none have succeeded in deployment of sensors in subsurface exploration. The need for self-effacing and remote monitoring is the main motivation for deploying a sensing and communication network in subsurface. The call from AEC which projected the need to bridge the gap between existing exploration technologies and WSN, sowed of the seed of this work. It is apparent that the need of the hour is to exploit sensor abilities to know the presence of subsurface components, their quantity as well as quality along with the geographical area of their presence. Further, it is emphasized that although a lot of work has been done pertaining to the field of sensor networks, but most of the researchers have remained silent towards the application of WSN in subsurface exploration. In fact, available literature [10, 17, 32] reveals the fact that very few researchers have spent little time looking at the more recent work from other fields. One example of this is the lack of wireless sensor networks [48] within the community of subsurface exploration. There are many properties of sensors such as intelligent sensing, collection and processing of data, make them well suited to uncertain environments. The adoption of Mobile Sensors as architectural elements enables us to achieve the desired delegated goal of enhanced oil recovery which in turn demands the formulation and development of a novel sensor deployment strategy in subsurfaces.

The motivating factor behind this research is negligible cost of sensors as these are relatively inexpensive devices as compared to boring a well. In fact it can be presumed that the return on investment with sensors is going to be very high, since they will be instrumental in extraction of valuable crude oil from below the earth’s surface.
On the other hand, various issues still need to be debated upon and resolved like the challenge involved in deployment of sensors beneath the earth crust, techniques for communication in harsh conditions, lifetime of sensors etc. Moreover, the communication protocols, data dissemination are some other important unfolded research issues that need to be addressed.

The focus of this work is to propose deployment of sensors underneath so as to explore the depleting underground hydrocarbon resources. It is being foreseen that these deployed and hence communicating sensors would be able to provide vital information / parameters pertaining to the oil field, which further can be used by scientists around the world for real-time analysis. It must further be realized that deployed system is robust and presents a maximum lifespan. Therefore the chapter has been divided in four sections. The upcoming section explores the feasibility of deploying sensors, and hence presents the works of other authors related to the deployment of sensors in non-deterministic environments. Related works pertaining to inter-node communication, information processing, and robustness of the WSN is given in subsequent sections.

3.3. Sensor Node Deployment

The major challenge is to devise an efficient strategy for deploying sensors beneath the earth crust. The thrust is on deploying wireless sensors in the oil field so that an accurate estimate about the geo distance to which oil is spread, can be calculated. An efficient analysis would then allow the boring for the steam injector at an optimal distance such that the maximum quantity of oil can be extracted from the well.

The concept of coverage as a paradigm for evaluating multi-robot systems was introduced by [45]. Gage defines three basic types of coverage: blanket coverage,
where the objective is to achieve a static arrangement of nodes that maximizes the total detection area; barrier coverage, where the objective is to minimize the probability of undetected penetration through the barrier; and sweep coverage, which is more-or-less equivalent to a moving barrier.

The problem of exploration by a single robot in an unknown environment has been considered by a number of authors [2, 15, 16]. The frontier-based approach described in [15, 16] is particularly pertinent: this exploration algorithm proceeds by incrementally building a global occupancy map of the environment, which is then analyzed to find the ‘frontiers’ between free and unknown space.

Sensors for map-building has been explored by a number of authors [14, 20, 36, 64, 79, 100] who use a variety of techniques ranging from topological matching [64] to fuzzy inference [100] and particle filters [19].

Burgard describes an adaptive algorithm for making estimates of these otherwise unpredictable quantities. A distributed algorithm for the deployment of mobile sensors has been described by [38]. Payton introduces the concept of ‘virtual pheromones’: localized messages that are emitted by one robot and detected by nearby robots. Virtual pheromones can be used to generate either ‘gas expansion’ or ‘guided growth’ deployment models. The key advantage of this approach is that the deployment algorithm is entirely distributed, and has the potential to respond dynamically to changes in the environment. This algorithm does, however, lead to relatively slow deployment; it is also unclear, from the published results, how effective this algorithm is at producing good area coverage. A somewhat similar algorithm based on artificial potential fields is described in [6]. In a somewhat similar vein, [4] considers the problem of distributed sensing in an ad-hoc wireless network. Nodes are introduced into the environment in masses and allowed to disperse using a random-walk algorithm. Nodes are assumed to have a limited communication range, and the environment is assumed to be sufficiently large such that full network
connectivity cannot be maintained. Hence the network relies on continuous random motion to bring nodes into contact, and thereby propagate information to the edges of the network.

A mobile sensor network can also be viewed as a large-scale mobile robot formation. Such formations have been studied by a number of authors [59, 82, 130], all of whom describe methods for creating and maintaining formations via local interactions between robots. In this research, interaction with the environment is of secondary importance to interaction between the nodes themselves. In contrast, the work proposed in this thesis emphasizes interaction with environment, and attempts to minimize interaction between network nodes.

Finally, it is found that that the problem of deployment is related to the traditional art gallery problem in computational geometry [83]. The art gallery problem seeks to determine, for some polygonal environment, the minimum number of cameras that can be placed such that the entire environment is observed. While there exists number of algorithms designed to solve the art gallery problem, all of them are based on the assumption that good prior models of the environment are available. In contrast, the prior models of the subsurface environments are either incomplete, inaccurate, or non-existent. The sensor network must therefore determine the structure of the environment empirically and incrementally.

The algorithm described here is an incremental deployment algorithm [5]. The nodes are deployed one at a time, with each node making use of information gathered by the previously deployed nodes to determine its ideal deployment location. The algorithm aims to maximize the total network coverage, i.e. the total area that can be ‘seen’ by the network. At the same time, the algorithm must ensure that the visibility constraint is satisfied; i.e. each node must be visible to at least one other node. The algorithm relies on a number of key assumptions such as Homogeneous nodes, Static environment, Model-free, Full communication, Localization. The algorithm has been
evaluated using two performance metrics i.e. coverage and deployment time while the connectivity factor has been completely ignored.

Usually, static sensors [1, 121] are being used, which do not have any kind of locomotive capability, whereas mobile sensors may be deployed for better performance [17]. A mobile sensor network [1, 143] comprises of a distributed collection of nodes, which in addition to sensing, computation and communication abilities, is also possessed with locomotion capabilities.

Traditionally in WSN network application, sensors were usually deployed with aim of monitoring a specified area. In certain applications it was always easy to select sites where sensors could have been placed, e.g. sensors placed in a building for firefighting [86] purpose or to monitor intrusion detection and such a deployment is termed as deterministic deployment. But, in non-deterministic deployment like habitat monitoring [10] in hostile locations, large numbers of sensors are simply scattered via air drop with the hope that they connect with each other and start passing data within themselves. For both strategies, various, algorithms [35, 93, 148] have been developed ensuring the coverage [49, 142] and connectivity [142, 146]. However, the literature reveals the fact that neither of the strategies is suitable enough for subsurface. Therefore, an optimal deployment of finite number of sensors in oil fields that are able to communicate efficiently is in high demand.

It is recommended to ensure coverage and connectivity property where, coverage property [150] checks that sensors being deployed are adequately covering all data points which are to be sensed or monitored whereas Connectivity checks that these sensors are not placed far apart such that they are unable to communicate with each other. The section discusses various mathematical models employed for efficient coverage and connectivity in various domains.
Researchers [73, 146] proved that for a finite sensor density in k-coverage,

\[ c \geq 2r \]

is a necessary and sufficient condition for coverage to imply connectivity where “r” is sensing range of a sensor or the distance to which a sensor can monitor desired activities, while “c” is the communication range of the sensor. Also, k-coverage with \( k > 1 \) affords some degree of fault tolerance and is able to monitor all points so long as no more than \( k - 1 \) sensors fail.

Xu & Sahni [145] introduced an Integer Linear Programming (ILP) formulation assuming a set of modalities such as temperature, sound, levels of different gases, radioactivity etc. at each location. This formulation for cost calculation is fine for traditional applications of wireless sensors. However, the same cannot be applied directly in a subsurface as it comprises of relatively harsh vibration, temperature and corrosive environments. Since, sensor technology is used in a wide range of applications and in various different markets; therefore, these can be deployed in either a phased or an iterative manner. Deploying mobile sensors result in increased network coverage, better routing performance, self-deployment and self reconfiguration. This research proposes deployment of mobile sensor in subsurfaces since reconfiguration of nodes depending on real time conditions shall be far more easy and attainable.

3.4 Sensor Node Communication

It is apparent that, in order to forward the data collected, the deployed sensors shall communicate with each other efficiently. The literature is explored to its depth to find a suitable protocol for communication among the deployed sensors.
Today, WSN makes use of novel ad hoc networking technology to facilitate inter-sensor communication [67, 92]. The flexibility of installing and configuring a sensor network has been greatly enhanced. Lot of research have been carried out in the field of sensor networks, including design issues related to the physical and media access layers [7, 57, 139] and routing protocols [39, 42, 71].

Sensor nodes are always limited in resources; let it be computation, storage or power. While last decade has seen a lot of research work in the area of routing for WSN, it has been found that conservative ad-hoc routing techniques are not viable for large and intense sensor networks. In recent years, sensor networks have been the focal point of an increasing research effort and many routing mechanisms for sensor networks have been projected and developed.

As per Jiang and Manivannan in their work [113], the issues involved in designing efficient routing protocols, identifying several important desired features of a routing protocol and have compared and contrasted the existing routing protocols with respect to these features. The authors have given a very simple classification of the routing protocols based on various criteria’s. viz: (1) Depending on how the sender of a message gains a route to the receiver (like Proactive protocols, Reactive protocols and Hybrid protocols), (2) According to nodes’ participating style (like Direct communication, Flat communication and Clustering protocols), and (3) Depending on whether a routing protocol is location aware or not (like Location aware and Location-less protocols).

Bandyopadhyay and Coyle in their work [122] proposed Energy Efficient Hierarchical Clustering (EEHC), which is a randomized and distributed clustering algorithm. It is used for organizing sensors within network in a hierarchy of clusters. In the clustered setup, there exists a processing center which can be one of the normal sensors or one with extra resources available within it. The end level sensors responsible for collection of data, within the network, are connected to data
processing center through a hierarchy of cluster heads. The algorithm works in a bottom-up fashion, which makes a calculation of the communication cost involved. The cost involved between a transmitting sensor and the final receiving processing unit, consists of energy consumed for transmission from sensor node to level 1 cluster head, then from level 1 to level 2 cluster head, and so on, finally from highest level cluster head to the processing unit itself. The energy consumed as calculated in this protocol depends on the parameters \( p \) (probability that a called volunteer cluster head becomes actual cluster head) and \( k \) (used for cluster head election on each level).

Heinzelman and Chandrakasan in their work [71] presented Low-Energy Adaptive Clustering Hierarchy (LEACH). LEACH is a cluster-based routing protocol which aims at minimizing global energy consumption in sensor network by randomized rotation of local cluster heads, such as, to evenly distribute the energy load among the sensors. In each round of process, clusters are organized in a set-up phase, followed by a steady-state phase. After a definite time, which is determined in advance, the next round begins. During the process of clusters creation, every node decides in favor or against becoming cluster head for the current round. Each node chooses values, which lies between possible probability values i.e. 0 and 1. This value is then compared with \( T(n) \), which is based on the recommended percentage of cluster heads for the network and the number of times the node has become cluster head in past.

While [71, 122] had been example of cluster-based routing, having two different types of nodes (cluster heads and normal sensing nodes), researchers have proposed and implemented flat routing too [39, 152], in which all nodes are essentially designated the same responsibilities. Yu, Govindan and Estrin in [152] proposed Geographical and Energy Aware Routing (GEAR). This is an energy proficient algorithm which, makes use of energy aware neighbor selection to route a packet towards the target region without flooding.
Braginsky and Estrin proposed Rumor Routing [39], which is a well-organized technique to distribute queries to nodes that observed events of interest in the network. This method proves significant power cost reductions due to logical compromise between flooding queries and flooding event notifications within network. The idea behind Rumor Routing is to create paths leading to each event. The algorithm makes use of a set of long-lived agents that create paths directed towards the events they encounter.

In the current body of research done in the area of wireless sensor networks, attention has not been given to propose a communication technique for sensor nodes in subsurface. Most current routing protocols have been laid down for traditional applications on earth surface or even underwater. Therefore, there exists a need for networks geared towards subsurface to have an efficient routing protocol, custom defined for them. We also believe that sensor networks in subsurface should have the ability to communicate data on Query Reporting Model, which will lead to maximizing their lifetime and energy sources. So, the current work focuses on developing a communication protocol which is able to achieve the stated objectives and also can survive successfully in oil field.

3.5 Information Processing

Information processing controls the process of transforming raw data collected via sensor readings, into useful and meaningful information, to be used by scientists and researchers. Since beginning, due to energy constraints, information processing has been active research area in wireless sensor networks [25, 43, 44, 50, 53, 54, 61, 62, 67, 72, 77, 85, 87, 99].

In the past few years, innovative oil monitoring techniques deployed in oil wells or sub-surfaces have proved to be an efficient way of measuring various
parameters such as pressure, temperature, volume of oil available at various locations. Such innovative systems comprise of thousands of heterogeneous sensors which continually sense the environment. Recent works indicates that innovative deployment of sensors in subsurfaces can beneficially support the production of oil and gas. The data which is sensed by such sensors is usually corrupted with noise. 

*Filtering is desirable in such embedded systems in order to smooth out such fluctuations that otherwise would shorten the lifespan of sensors.* Moreover, since, sensors are constrained in terms of energy, therefore, in order to be efficiently benefited from such systems, information that is actually promising shall only be routed so as to avoid useless energy drain and reduced lifespan of WSN.

In order to meet, the above stated objective, one must employ the technique of collaborative signal processing [103] and filter the unnecessary noise locally. Collaborative signal processing leads to information fusion which in turn reduces the data volume to be routed. However, the authors feel that this fused information must be processed i.e. filtered before routing because sensors readings are usually imprecise due to strong variations in the environment and hence information is corrupted with noise. In order to filter the sensed data, tools known as Kalman filters [129] can be used as these are often being used in embedded control systems for estimating the accurate range of process variables.

Current research efforts include system state estimation, sensor management, collaborative signal processing, information fusion, information filtering, distributed compression, sensor querying and tasking, mobile-agent based information processing, and distributed inference and learning in wireless sensor networks just to name a few. Transmission of packets over wireless media is always a challenging task in WSN due to resource scarcity of sensor network. At the same time, data transmission always remains the highest energy consumption factor in any network, and hence needs to be controlled efficiently. The best way available for saving energy and hence increasing lifetime of networks is to implement efficient data gathering as well as information
processing techniques, so that only the minimal amount of data is transmitted over the wireless media.

Design challenges [41] of the information processing in a wireless sensor network, includes data extraction, representation, data manipulation and propagation of refined information. It aims at providing robust and efficient techniques to process high volume of data generated from large number of sensors, while remaining modest on available resource consumption. Some of biggest challenges of information processing includes, and are not restricted to data sampling, data storage, data aggregation, data fusion, data query and retrieval. Other challenges include identification of multiple concurrent physical phenomena leading to duplicate data values, estimation of state, information compression and replication.

The main challenges involved in information processing design include the organization of participating sensor nodes into various clusters, identity identification of multiple physical attributes (viz. temperature, pressure, velocity etc), estimation of these physical attributes, and aggregation / processing and transmission of estimated results.

Akbar M. Sayeed [44] developed a collaborative signal processing (CSP) framework for the detection, classification and tracking of single [25], multiple [77] and distributed targets [61, 67, 72] in wireless sensor networks. Zhao et al. proposed Information-Driven Dynamic Sensor Collaboration [43] and Information-Directed Approach [62]. These techniques calculate communication and computing cost within sensor network to ascertain which sensor nodes will be participating in information processing. Guo and Wang [44] developed dynamic sensor collaboration scheme, while Qi et al. [87] have discussed mobile agent based information processing. Towards the improvement in existing information processing techniques, many researchers have been concentrating upon algorithmic design [53], distributed
compression-estimation [54], distributed inference [50], and joint source-channel communication [99].

An in-depth evaluation of the above section indicates that researchers have been putting efforts to meet the challenges in information processing but most of them have remained silent towards the application of Kalman filter in this domain, especially in Sub-surfaces where sensors are being deployed for monitoring. The thesis contributes a unique application of Extended Kalman Filtering (EKF) technique for processing such sensitive information because sensor readings are usually imprecise due to strong variations in environment and also, computation has to be much more energy efficient than communication. Out of the various filtering algorithms available, we have chosen to apply Kalman filter, primarily because it works well both in theory and practice and moreover, it is able to minimize the variance of estimation error i.e. filters noise from the actual signal more accurately.

3.6 Fault Tolerance and Robustness

Traditionally in WSN network application, a lot of research has been undertaken for deployment, communications, security, and energy efficiency. But little has been talked about the robustness of WSN architecture. This is based on the fact that WSN are like ad-hoc networks which are designed to have capabilities of self healing. This restructuring or re-aligning of nodes are good for traditional networks deployed in public or hostile environments, but for subsurface exploration it becomes difficult to designate an alternate path in case of nodes failure.

WSN are generally used for some critical operations like battlefield surveillance, intrusion detection, or detection and tracking of chemical, biological, radiological, nuclear and explosive agents. These applications require high degree of reliability mechanism in order to significantly reduce end-to-end packet loss ratio. Drifting nodes and failing nodes due to depletion of battery power or other reasons
raise a significant number of routing issues, demanding the design and implementation of efficient routing protocols. In addition to re-routing data packets in case of nodes failure, researchers have worked on replenishment or replacement of sensor nodes too. These strategies allow the network topology to be re-instated to its original form [21], and hence making way to a smooth communication.

Tong et al. in their work [18], proposed a node replacement and reclamation (NRR) strategy, and designed an adaptive rendezvous-based two-tier scheduling (ARTS) scheme. According to this work, for long-term deployment and collection of data, the energy resources required are always less than what could be stored on a node. This leads to termination of network, even before the assigned task is complete. Though [18] presented a novel strategy for node replacement, however the ARTS scheme only considers point coverage and not area coverage, which is essential in many WSN applications. Tong et al. in their next work [19] proposed a new implementation scheme for NRR strategy, which was based on a novel staircase-based scheduling model.

Shue et al. in their work [89] considered sensor networks consisting of both static and mobile nodes. The authors designed a smart mobile robot and implemented an application of nodes replacement to demonstrate its use, via nodes replacement algorithm. This algorithm demonstrated the capability of mobile robots to navigate towards low-energy sensor nodes and replace them automatically, with new sensor nodes, having no location information.

Kuo et al. in their work [153] proposed a technique for sensor relocation in order to repair coverage holes caused by node failures. The authors proposed a fast sensor relocation algorithm to arrange redundant nodes to form redundant walls without GPS.
Parikh et al. [123] proposed several node replacement policies to improve the network lifetime and the quality of coverage while maintaining a threshold-coverage. By utilizing a minimal number of additional replacement nodes (< 10%), authors demonstrated that their proposed node-replacement policies improve the network lifetime and the quality of coverage by approximately 90% each, compared to the no-replacement policy.

Hussain et al. [127] analyzed the feasibility of using received signal strength indicator (RSSI) values measured at the receiver node to detect attacks like node replication, replacement, and man-in-the-middle. Dorsey et al. [49] proposed a replenishment control framework where additional nodes are added to an initial deployment in consecutive batches in order to meet mission lifetimes while reducing cost. The control framework consists of a failure process model used to forecast sensor failures due to energy depletion, and a two-stage limited look-ahead controller used to determine the number of nodes to be added to the network and the approximate locations of their deployment.

The above presented works enlightens the need of adding robustness to the proposed model. By proposing a novel node replenishment algorithm for wireless sensor networks in sub-surface, this work not only adds fault-tolerance to the network but also makes the system robust. The proposed strategy while collecting data from sensor nodes; will also acquire meta-information regarding their geo-location, which will be used to determine the correctness of deployed network topology. The strategy would be able to describe node replenishment policy in case the meta-information gathered reflect some deviation. The strategy is a unique contribution to subsurface exploration technology as none has proposed replacement and hence robustness strategy for this field, in particular.
3.7 Security

If sensor networks are to attain their potential, security is one of the most important aspects to be taken care of. The need for security in military applications is obvious, but even more benign uses, such as home health monitoring, habitat monitoring and sub-surface exploration require confidentiality. WSNs are perfect to detect various threats like biological, chemical, or environmental over large areas, but at the same time maliciously induced false alarms could completely negate value of the system. The extensive deployment and success of wireless sensor networks is directly dependent on their security potency. These stated facts form the basis of this study [55].

Far-reaching research is being done in the area of Wireless Sensor Networks. Researchers have been concentrating on solving a variety of challenges ranging from limited resource capabilities to secure communication. Literature indicates that sensor networks generally are deployed in public or deserted areas, over insecure wireless channels [10, 23, 66, 132]. It is therefore alluring for a malicious device / intruder to snoop-in or even infuse bad messages into the network. The traditional solution to this problem has been to take up techniques such as message validation codes, symmetric key encryption schemes or public key cryptography. However, since there are resource scarcities for motes, the major challenge here is to employ these encryption strategies in a proficient method without over utilizing already scarce resources. One method of shielding network against foreigner attacks is to apply a straightforward key infrastructure. However, it is known that global keys do not provide network resilience and pair wise keys are not a perfect solution in terms of scalability. A more intuitive solution is needed for WSNs.

TinySec [141] introduced security to the link layer of TinyOS suite [135] by incorporating software-based symmetric keying with low operating cost requirements. Unfortunately, not all vulnerabilities of TinySec could be addressed. For example
techniques to avoid insider attacks were not addressed by TinySec. In contrast, Zigbee or the 802.15.4 standard [105] introduced hardware-based symmetric keying with much success. However, in order to provide thorough security, possible use of public cryptography to create secure keys throughout network deployment and maintenance phases [37] is also being tested out. This concept has opened a vast area of research and unheard territory for the sensor network cryptographic infrastructure. Widespread research is also being carried out on topics such as key storage & key sharing [70], key preservation [137] and shared key pools [98]. Now, since sensor nodes need to cluster aiming to fulfill a particular task, it is desired that the group members’ secure communication between each other, in spite of the fact that overall security mechanism may also have been employed, where the nodes are deployed. But, contrary to this fact secure grouping has been researched to a very low extent in the past and only a few exhaustive solutions exist.

Further, although, data aggregation (sensor nodes aggregate sensed data from environment before finally transmitting it to the base station) is one of the promising strategies to reduce cost and network traffic but such data is always susceptible to attacks by intruders. A challenger with control over an aggregating node can choose to disregard reports or produce fake reports, affecting reliability of the generated data and at times whole network as well. The main aim in this area is to use flexible functions, which will be able to discover and report forged reports through demonstrating authenticity of the data somehow. Wagner [46] established a technique in which aggregator uses hash trees to create proof of its neighbors’ data, which in turn is used to verify purity of collected data to the base station. Another approach [138], takes advantage of network density by using the aggregator’s neighbors as witnesses. It is also possible to reduce amount of traffic heading to base station by using bloom filters to filter out false aggregations [60]. Latest research trends [94] towards security measures indicate development of Secure Protocols. The main research challenge in this area is to discover new defense techniques to be applied to existing routing protocols, without compromising connectivity, coverage or scalability [47]. Perrig et al
[115] made the first attempt to devise a secure protocol for sensor networks. Security Protocols in Sensor Networks (SPINS) provide data authentication, replay protection, semantic security and low overhead. Majority of overhead arises from transmission of extra data rather than any computational costs.

SPINS was later used to design a secure cluster based protocols such as LEACH. Karlof and Wagner [24] have provided an extensive analysis on the WSNs routing vulnerabilities and possible countermeasures. According to their study common sensor network protocols are vulnerable due to their simplicity and hence security should be built into these protocols right from design time. In particular, their study targets TinyOs, directed diffusion and geographic routing.

Security goals for sensor networks include the same four primary objectives as conventional networks: availability, secrecy, integrity, and authentication. Though WSN security is characterized by the same properties as compared to traditional network security, but at the same time they are prone to new attacks. Attacks are made at several levels on the network, like Physical Layer, Link Layer or Network Layer. Attacks at physical level include jamming of radio signal and tampering with physical devices. One of the most prominent attacks at this layer is Jamming [47], a well-known attack on wireless communication. In jamming, intruder interferes with wireless frequencies on which the transceivers used by a device operates. It represents an attack on the network accessibility. Jamming is different from normal radio transmission in that it is redundant and disorderly, thus creating a denial-of-service condition. The degree of jamming is determined by physical properties such as available power, antenna design, obstacles, and height above ground. Jamming is extremely successful against single channel networks, i.e., when all nodes transmits in a small single band of the wireless spectrum.

Tampering [8] is the second security issue at physical layer. Sensor nodes are generally deployed in hostile environment, away from personal monitoring. These
sensors are available for easy access to intruders, which can potentially harm these devices by tampering, duplicating or even destroying them. One available solution to this problem is manufacturing of tamper-proof sensor nodes. These nodes are smart enough to delete any cryptographic information available within them as soon as they sense some sort of tampering. But these are not economically viable since tamper-proof sensor nodes increase overall cost. Other solutions might be using of multi-key security algorithms. In these security algorithms intruders will not have access to complete data even if one of the key has been compromised upon.

Like the physical layer, link layer is particularly vulnerable to denial of service attacks. The link and media access control (MAC) layer handles neighbor-to-neighbor communication and channel arbitration. The first type of attack at this layer is known as Collision [101]. If a challenger is able to generate a collision of even part of a transmission, one can interrupt the entire packet. A single bit error will cause a Cyclic Redundancy Check (CRC) variance and would require retransmission. In some MAC protocols, a corrupted ACK may cause exponential back-off and pointlessly increase latency. Although error-correcting codes guard against some level of packet corruption, intentional corruption can occur at levels which are beyond the encoding scheme’s capability to correct. The advantage, to the challenger, of this MAC level jamming over physical layer jamming is that much less energy is required to achieve the same effect.

Another malicious goal of intruders is Exhaustion [8] of a sensor node’s battery power resources. Exhaustion may be initiated by an interrogation attack. A compromised sensor node could repeatedly transmit RTS (Request To Send) packets in order to bring forth CTS (Clear To Send) packets from a uncompromised neighbor, eventually draining the battery power of both nodes. Still more damaging attack on Link Layer is Unfairness [68]. In this type of attack at Link Layer, a compromised node can be misrepresented to sporadically attack the network in such a fashion which induces inequality in the priority for granting of medium access. This fragile form of
denial of service attack might increase latency so that protocols working in real-time miss their deadlines. Another form of this attack could target one particular flow of data in order to restrain recognition of some event. The use of tokens which avert a compromised node from capturing the channel for a long period of time has been proposed.

![A Four-Way Handshake ensures collision avoidance in 802.11 networks](image)

Due to the ad-hoc nature of sensor networks, every node eventually at some point of time assumes routing responsibilities. Since every node in a sensor network virtually enact as a router, hence WSN are highly susceptible to routing attacks at network layer. Researchers have identified a variety of routing attacks [24] and have shown them to be effective against every major sensor network routing protocol. Various classifications of attacks are summarized below and followed by a general discussion of secure routing techniques.

The most prominent attack on routing is to spoof, alter, or replay routing information. This type of attack is known as False Routing Information (see figure 3.3). The false information may allow intruder to create routing loops, attract or repel traffic, shorten or extend route lengths, increase latency, and even partition the network. Clearly, the distortion of routing information can cripple complete network. The standard solution is to require authentication for routing information, i.e., routers only accept routing information from valid routers encrypted with valid shared key information.
Another attack, known as Selective Forwarding [20] is a more clever attack in which the compromised node is made to transmit forward only some of the packets correctly, while others are silently dropped. Smart networks are capable to routing data along another path, in case of a failure of a particular node. If all packets from a node are dropped, it will be considered as a dead network. Hence only selective packets are being forwarded by compromised node, creating an illusion that it is still active, and that data can be routed via it.

Routing decisions in network are based on distance between nodes. As shown in figure 3.4, in Sinkhole Attack [78] a compromised node is made to advertise a luring route to the base station or sink. Thus all neighboring nodes are made to route their data towards the compromised node. The intruder at compromised node thus gains access to major data within its area, and might destroy, manipulate or even modify these packets.
Figure 3.5 depicts Sybil attack [56], wherein the compromised node spoof neighboring nodes by broadcasting multiple identities. The compromised node claims to be other node present within the network, hence presenting a great threat to overall routing process. The malicious effect aggravates as other nodes unknowingly further transmit routing data received from compromised node to their neighbors.

In Wormhole Attack [147], two mutually understanding malicious nodes form an out-of-bound channel or transmission tunnel in between them. The end points of this tunnel are called as Start & End point (see figure 3.6). The compromised node at Start point transmits its data via tunnel to malicious node present at End point. The End point node then re-transmits the received data packets, hence creating an illusion that these distant nodes are neighbors. This sort of attack is likely to be used in arrangement with selective forwarding or eavesdropping.
Nodes present within a network rely on acknowledgment received from neighboring nodes. In Acknowledgment Spoofing attack [63], a malicious node may respond back to a transmitting node on behest of a weak or a non-active node, and thus deceiving sensor about strength of link. This way sender unknowingly keeps on transmitting to the non-active node and data is eventually lost or captured and destroyed by malicious node.

There have been several approaches to defend against network layer attacks. Authentication and encryption are a first step, but more proactive techniques such as monitoring, probing, and transmitting redundant packets have also been suggested. Secure routing methods protect against some of previous attacks. Proposed techniques include Authentication & Encryption. Link layer authentication and encryption protect against most outsider attacks on a sensor network routing protocol. Even a simple scheme which uses a globally shared key will prevent unauthorized nodes from joining topology of the network. In addition to preventing selective forwarding and sinkhole attacks [26], authentication and encryption also make Sybil attack impossible because nodes will not accept even one identity from the malicious node.

Another technique is Monitoring, which is a more active strategy for secure routing, where-in nodes monitor their neighbors and watch for suspicious behavior. In this approach, nodes act as “watchdogs” to monitor next hop transmission of the packet. In event that misbehavior is detected, nodes will update routing information to avoid the compromised node. Another proactive defense against malicious routers is probing. This method periodically sends probing packets across the network to detect blackout regions. Since geographic routing protocols have knowledge of the physical topology of the network, probing is especially well-suited to their use. Probes must appear to be normal traffic, however, so that compromised nodes do not intentionally route them correctly in order to escape detection. Redundancy is another strategy for secure routing. An inelegant approach, redundancy simply transmits a packet multiple
times over different routes. Hopefully, at least one route is uncompromised and will correctly deliver message to the destination. Despite its inefficiency, this method does increase the difficulty for an attacker to stop a data flow.

Five of the most looked for challenges in designing security schemes for large wireless sensor networks are Wireless Medium, Ad-Hoc Deployment, Hostile Surroundings, Resource Scarcity and Immense Scale. Applications proposed for sensor networks necessitate wireless communication links. The deployment scenarios for ad-hoc sensor motes renders use of wired media communication totally infeasible [65]. This leads to more security concerns in WSN, since wireless medium is always prone to security attacks since its method of operation / transmission makes it an easy prey for eavesdropping. Wireless communication can be easily trapped, modified or even replaced by intruders. The wireless media allows intruders to destroy genuine communication packets and inject deceptive data into network, with least of the efforts. Wireless media security problem has been intrinsic to traditional networks too, but enhanced and robust solutions are required for sensor networks, owing to their unpredictable deployment and ad-hoc arrangement.

Another challenge for WSN security is its ad-hoc deployment. Sensors may be required to deploy in deterministic or non-deterministic environments. In both cases no fixed topology can be framed in advance. Even the deployed network may have to change its topology every now and then, subject to addition of new nodes, node failures etc. [34]. Under such conditions, robust security protocols are required which can adapt dynamically as per changing configuration / topology of WSN. Hence in sensor networks traditional security mechanisms based on static configurations cannot be applied.

The environment within which sensor nodes operate, collect and transmit data is hostile. Intruders might have know-about the geographical locations of sensor motes, and subsequently reach them to capture / destroy them. No security protocol can fend
WSN against such kind of physical attacks, but these needs to be kept in scenario while designing a security framework, in order to provide self-healing capabilities to network.

Another challenge in WSN is resource scarcity within sensor motes. *Due to hostile conditions and non-predictable environment sensor nodes cannot be replenished in terms of battery power.* In addition to battery, the memory size and computational powers too are low due to small size of nodes. These factors make efficient but resource extensive security mechanisms totally infeasible for WSN. A representative example of a sensor node is the Mica mote. It has a 4 MHz Atmel ATMega103 CPU with 128 KB of instruction memory, 512 KB of flash memory, and just 4 KB of RAM for data [34]. The radio operates in the range of 0 to 40 Kbps bandwidth with a transmission range of a few dozen meters. Such constraints on resources demand extremely competent security algorithms in terms of computational complexity, memory as well as bandwidth. While energy remains the most prized resource for sensor networks, earlier researchers have given little to no attention to energy efficiency. Transmission is especially expensive in terms of power, as apparent from SPINS [Figure 3.7] too.

![Figure 3.7 Energy costs from SPINS [115]](image-url)
Large scale deployment also contributes to the list of challenges for WSN. Traditional networks might be limited to an office or to a bigger geographical location but in a controlled fashion. But in case of sensors, the area being covered may be large and un-predictable. In many cases sensors are even air-dropped and hence their exact geographical location may be different than what might have been thought of. In such cases providing security to all nodes present becomes a challenging task. *Security mechanism needs to be developed which can cater to large number of nodes spread over a large scale, and at the same time maintaining computational and communication efficiency.*

### 3.8 Conclusions

A critical look at the above literature points out the need to bridge the gap between existing technologies and current needs. Therefore the need of the hour is to find the application of WSN to know the presence of subsurface components, their quantity as well as quality along with the geographical area of their presence. Although a lot of work has been done pertaining to the field of sensor networks, but most of the researchers have remained silent towards the application of WSN in subsurface exploration. In addition to the challenge of deploying sensors in subsurface, the inter-node communication, effective information processing and robustness of such an expensive system shall also be considered *apriori*. The subsequent chapters aim to provide solutions to the issues highlighted in this chapter and hence meet the stated objectives.