CHAPTER 3

OBJECTIVE AND RESEARCH FRAMEWORK

3.1 Objective of the Present Work

Confidentiality and authenticity are two important security services required for almost every WSN application. However, small memory, weak processor and limited battery power of the sensor nodes are the major obstacles to implement traditional security primitives in them. Confidentiality, integrity and freshness of data as well as source authentication are the essential security parameters in WSN [De et al. 200; Sun et al. 2007; Szczechowiak et al. 2009].

Wireless Sensor Networks exist in conditions such that it cannot be continuously monitored by the users for malicious activity. These are sometimes areas of high vulnerability, or the areas that have very less human interaction. Due to the large number of sensors that are present in the WSNs, it becomes almost impossible to track every sensor and prevent attacks. Hence we focus towards improving the security by providing various routing mechanisms that becomes impractical for the adversary to compute. Of the various possible security threats encountered by a WSN, our objective is to counteract the threats occurring due to CN, DoS and Black-holes or Sink-holes attacks, since these are the major attacks that are present in the WSNs.
The conventional security methods alone cannot provide satisfactory solutions to these problems. This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. Likewise, an adversary can always perform DOS attacks even if it does not have any knowledge of the underlying cryptosystem. Sensor networks are especially vulnerable against external and internal attacks due to their peculiar characteristics. The devices of the network (i.e. sensor nodes) are constrained in terms of computational capabilities, memory, communication bandwidth, and battery power. As a result, it is challenging to implement and use the cryptographic algorithms and protocols required for the creation of security services. In most cases, it is easy to physically access sensor nodes: they must be located near the physical source of the events. Since nodes are not tamper-resistant, due to cost constraints, any human user or machine can reprogram them or simply destroy them. Any internal or external device can access to the information exchange because the communication channel is public. Besides, attacking the availability of the wireless channel is not a complex task. It is a difficult task to monitor and control the actual state of the elements of the network due to the inherent distributed nature of sensor networks.

Any failure in any of its elements may remain unnoticed, or the actual cause of the malfunction may not be known. Besides, a sensor network can be attacked at any point. In our current proposal, the following security mechanisms are made available in the sensor network.

- **Confidentiality.** This property tries to fulfill the following principle: A given message must not be understood by anyone other than the desired recipients. While confidentiality is an important security property, it may be not mandatory in certain scenarios where the data is public by itself (i.e. the temperature of a street) and no other information can be derived from it. However, there are particular situations and scenarios where the physical data obtained by the network can be deemed as sensitive, and should not be read by external entities. Data can be considered sensitive due to its inherent nature (e.g. patient data such as temperature), the nature of the context (e.g. a private household, a military
setting), or the nature of the sensed entities (e.g. a protected animal like a panda). Besides, certain control data exchanged by the nodes, such as security credentials and secret keys, must be hidden from unauthorized entities.

- **Integrity.** This property states that the data produced and consumed by the sensor network must not be maliciously altered. Unlike confidentiality, integrity is, in most cases, a mandatory property. The wireless channel can be accessed by anyone, thus any peer (outsiders and insiders) can manipulate the contents of the messages that traverse the network. Even more, data loss or damage may occur due to the harsh communication environment, and in the worst case the network will accept corrupted data. As the main objective of a sensor network is to provide services to its users, the sensor network will fail in its purpose if the reliability of those services can not assured due to inconsistencies in the information.

- **Availability.** The users of a sensor network must be capable of accessing its services whenever they need them. As a result, the different hardware and software elements of the network must be robust enough to be able to provide services even in the presence of malicious entities or adverse situations. Nevertheless, this property is related not only to the protection of the services, but also to the security mechanisms themselves: all protection mechanisms should be as energy efficient as possible in order not to quickly drain the batteries of the nodes.

- **Auditing.** The elements of a sensor network must be able to store any significant events that occur inside the network. This property is necessary due to the autonomous nature of the nodes. As users do not operate the sensor nodes directly, but through the base station, they may not be able to know about the existence of a certain event unless the nodes store it. Besides, if the whole sensor network fails, auditing information can be used to analyze the behaviour of the system prior to the failure. This property is also closely related to self-organization: in order to adjust their behaviour, sensor nodes must be able to know the state of their surroundings. Note that the inherent memory constraints of sensor nodes complicate the task of storing audit data.
• **Privacy and Anonymity.** These security properties are very important in those scenarios where the location and identities of the base station and the nodes that generated information should be hidden or protected.

### 3.2 Research Framework

The current research concentrates on safe transmission of data in a wireless sensor network. Figure 3.1 describes the security mechanisms in WSN. The initial methodology concentrates on providing security to the transmitted data using encryption. The Random number Addressing Cryptography provides a common key cryptographic security solution for a Wireless Sensor Network. The two main components of this process are the Address Generation and the Transposition Blocks. The Address Generation block reads the current data value, generates a random number corresponding to that value and returns the transposition address.

Even though this method provides hardware level encryption, the encrypted packets have the probability of being intercepted by the adversary. The black holes/sink holes present in the network might consume the information and destroy it. This can only be overcome by using an efficient routing methodology. This process is performed by the next method. The data from a sensor network is usually available as bulk information. All these data are read and are encrypted using the technique of Privacy Homomorphism. The aggregator node then combines this information using Concealed Data Aggregation [Dirk et al. 2006]. Now the entire data is combined to form a single data. Secret sharing approach is employed for dividing the shares for transmission.
Here the packet is broken into M shares (i.e., components of a packet that carry partial information) using a (T, M) threshold secret sharing mechanism such as the Shamir’s algorithm [Douceur J, et al. 2002]. The original information can be recovered from a combination of at least T shares, but no information can be guessed from less than T shares. This approach of secret sharing cannot be effective for both Compromised nodes and DoS attacks because, if (T, M) secret sharing allows us to evade Compromised nodes i.e., only when the attacker has T shares he can get the information, the same applies to sink where T shares are required to rebuild the information. But it is enough for the attacker to block (M-T+1) shares which will be small, resulting in a DoS attack, where we cannot rebuild the information. All these shares are transmitted to the sink using NRRP [Ravi et al. 2012c].

Even though the shares are encrypted, and a fixed number of shares are sufficient for the rebuilding of the original information, the packets still have the probability of getting...
lost in a black-hole, if the adversary manages to capture most of the nodes in the direction of
the source and the sink. This can be solved by using dynamic routing methodologies. The data
is initially transmitted to the intermediate nodes using backpressure routing. Then, the
intermediaries transmit data to the sink using reactive routing methodologies. Hence the data
is initially dispersed within the network, later focused to the sink. The routes taken by the
packets differ considerably, hence capturing of the packets becomes more complicated.