ABSTRACT

A wireless sensor network (WSN) consists of a large number of small and low cost sensor nodes. Usually a sensor node is resource constrained in terms of energy, memory, limited communication range and processing power. Recently, WSNs became popular among researchers due to wide range of its applications like environment monitoring, healthcare, military operations, weather forecasting, fire detection, transportation, real time applications and so on.

Prolong network lifetime and security are important requirements for resource constrained WSNs. Clustering is an effective approach to achieve energy efficiency in the network. In clustering, data aggregation is used to reduce the amount of data that flows in the network. Clustering is formed by grouping several nodes based on some common criteria where one node is elected as a cluster head from a group of nodes in the network. Several groups are formed in the network and each group elects a different cluster head. The role of cluster head is to collect data from the sensor nodes for onward transmissions to the base station.

Security is achieved by using cryptography in the network. A node encrypts data with a secret key and forwards encrypted data to the cluster head. Cluster head now re-encrypt this collected data with a different key and forward this re-encrypted data to the base station. If the role of cluster head and cluster members is fixed then security is not a major issue because one key is fixed and shared between cluster members and cluster head and other key is fixed and shared between cluster head and the base station. To avoid the risk of compromised key, both of these keys are refreshed at regular intervals.

In homogenous WSNs where all nodes have uniform but limited resources, it is essential to rotate the role of cluster head from sensor to sensor. Hence key management becomes very difficult as every time a new cluster head is elected and a new key is required to be shared between all the new cluster members and new cluster head and also between new cluster head and the base station. If both of these keys are managed and refreshed by the base station, then control traffic is increased more than data traffic in the network. At this stage, maintenance cost becomes higher than network operating cost in terms of network resources. This reduces the network lifetime.

In this thesis, a security framework for WSNs has been presented. The main contributions of this study are secure data aggregation, multi key management and key refreshing scheme, removal and replacement of compromised sensor node from the network, a lightweight dynamic encryption scheme to achieve forward and backward secrecy and pairing based encoding scheme for WSNs.