Abstract

Wireless Sensor Networks (WSN) has experienced an explosive growth during the last decade. Energy efficiency and security issues remain as central issues in the practical deploy ability of these networks. Wireless Sensor Networks are usually deployed for gathering data from unattended or hostile environment both in civil and military applications. Several factors like – physical exposure of the sensor nodes to the adversaries, ad-hoc network connections etc. make WSN more prone to security threats. Providing security solution to the WSN is a very difficult task due to inherent resource constraints with both node and networks like – limited processing power, limited shared bandwidth, smaller memory and fixed battery power etc. Security solutions based on public key cryptography are usually not recommended for WSN due to their high computational overhead. Several application specific security protocols for authentication and encryption of data in WSN have been proposed during the last decade. However, most of them have paid little or no attention towards internal attacks. In this report we have explored possible security threats in WSN and proposed an energy efficient security protocol by using symmetric key cryptography.