Abstract

Due to significant advancement in wireless communication, wireless sensor networks (WSNs) have attracted great attention in recent years. WSNs are randomly deployed, battery operated autonomous systems consisting of large number of sensors nodes which are responsible for transmitting the real-time sensed data for a specific application in the monitoring area to the base station where it can be further processed and analyzed. However, due to wireless communication, the network is easily compromised. Solutions dedicated to wire networks are not suited in the resource constrained wireless network. There is still a scope for wide research potential in the field of wireless sensor network security. In this paper, we analyzed the issues related to security in WSNs and also highlight the research area in the field of wireless sensor networks.

References


BLOM, R. A key-optimal class of symmetric key generation systems," in proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, Eds.):


**Index Terms**

Computer Science Wireless

**Keywords**

WSNs Attack Security Constrains Requirements Sensor node Base Station Characteristics

Forward Secrecy

Backward Secrecy