Abstract

In this work, the main focus is to provide Security in WSN (wireless sensor networks) as well as to provide the strategy to collect the high speed data in an efficient manner. Sensor networks are usually deployed in hostile and unattended environment where an adversary can read and modify the content of the data packet. In such situation the most popular type of attack is the external attack and replay attack. The node needs to be authenticated before data transmission takes place. In external attack the node does not belong to the network try to read and modify the packet. For that we also need to authenticate the node before data transmission. To overcome this problem we are using the concept of public and private key (Modified RSA Digital Signature Scheme). So this work tries to develop an algorithm which will form a network structure in wireless sensor network through which data can be transmitted faster to the base station without affecting life time of network and it also provide the security during communication. The cluster head in a cluster is generally involved in long distance transmission that's why its energy level decreases faster than other cluster members in a cluster. To overcome this problem we used the concept of re-clustering to rotate the responsibility of cluster head among the cluster members in a cluster so that energy can be
properly distributed among the nodes.

References

Implementation and Result Analysis of Secure Strategy for High Speed Transmission and Efficient Collection of Data in Wireless Sensor Network

3005-3014

Index Terms

Computer Science

Networks

Keywords

WSN  energy efficient  cluster head  data aggregation function  shortest path
algorithm
base
station
modified RSA digital signature scheme

re-clustering process and QoS parameters.