Abstract

The Wireless Sensor Networks (WSNs) are composed of sensor nodes that are deployed in remote and hostile environments to sense, process and communicate vital information to the base station. Due to the stringent constraints on the resources in the sensor nodes, it is essential to optimally devise the WSN operational paradigms, to minimize the resource overhead. Since, communications costs always are significantly higher than that for processing the sensed data the WSNs typically, employ in-network processing, so as to minimize effectively, the total number of packets eventually transmitted to the base station. Such in-network processing is largely based on data aggregation operations that aggregate the data into a compact representation viz. a data aggregate for further transmission. However, due to the ubiquitous and pervasive deployment of the sensor nodes, the security concerns in WSNs are anyway critical. Therefore, it is necessary to ensure the security of the data aggregator nodes that depend on various other nodes for the eventual output using carefully designed approaches. In this paper, we investigate various approaches for data aggregation with a view to critically analyze the same and propose a new approach for secure data aggregation.
References


Index Terms

Computer Science Wireless

Keywords

Confidentiality, Integrity, Privacy Homomorphism, Data Aggregation, Secure Data Aggregation.