Abstract

Wireless Sensor Networks is made of a large number of low-cost and low power sensor nodes that contains strictly limited sensing, computation, as well as communication abilities. Because of resource restricted sensor nodes, it is very important to reduce the amount of data transmission so the average sensor lifespan and also the total bandwidth utilization are generally increased. Data aggregation is the process of summarizing and merging sensor data to be able to minimize the number of data transmission in the network. Cluster based Data Aggregation approach, the data sensed by the sensor nodes are transferred to the cluster head and in the cluster head performs data aggregation and forwards results to the sink. Data aggregation could conserve energy (power) as well as bandwidth of the networks. As wireless sensor networks are generally used in remote and hostile environments in order to transfer very sensitive information, sensor nodes are susceptible to node compromise attacks and security problems such as data confidentiality and integrity are extremely crucial. Therefore, Secure Data aggregation protocol, must be designed with security in mind and investigates the relationship between security and data aggregation process within wireless sensor networks. In this paper, the secure data aggregation schemes are categorized into hop by hop aggregation and end to end aggregation. Here we explore a Homomorphic aggregation system based on a public key encryption (PKE) scheme to protect sensor data secure is proposed. Security
analysis shows that our proposed protocol can guarantee end-to-end confidentiality and privacy.

References

- Wenbo He, Hoang Nguyen, Xue Liu, Klara Nahrstedt, Tarek Abdelzaher, "SPDA: Secure and Privacy-preserving Data Aggregation in Wireless Sensor Networks.
- C. Castelluccia, E. Mykletun, and G. Tsudik. "Efficient Aggregation of Encrypted Data

Index Terms

Computer Science
Networks

Keywords
Wireless Sensor Network  Data Aggregation  Data Confidentiality  Data Integrity
Public Key Encryption
Homomorphic Encryption.