Abstract
The applications of the Wireless Sensor Networks (WSNs) comprising of resource constrained sensor nodes are increasing day by day. However, the pervasive environments in which the WSNs are deployed and the criticality of the available resources therein make the applicability of the security protocols therein, non-trivial. Amongst various panaceas pursued in research, one of the attractive ones is using privacy homomorphism based secure data aggregation. Indeed one can find several algorithms based on either Symmetric Key Cryptography or Asymmetric Key Cryptography in the literature that supports either additive or multiplicative homomorphic encryption. In this paper, we attempt to survey the existing algorithms with a view to highlight the characteristics of the same. However not limiting ourselves to only theoretical review of the existing literature, we also implement the algorithms. Our work principally focuses only on the support for confidentiality and privacy, the solutions for supporting message integrity and entity authentication are beyond the purview of our survey in this paper.

References

A Survey of the Privacy Homomorphism in Wireless Sensor Networks


Index Terms

Computer Science Wireless Networks

Keywords

Wireless Sensor Networks Secure Data Aggregation Privacy Homomorphism