Abstract

For dense deployment of sensor nodes required in many environmental monitoring applications, an hierarchical network organization offers distinct advantages over flat networks. Broadcast and multicast, being the principle modes of communication in these networks, require confidentiality and authentication to prevent adversaries from broadcasting false messages. In this work, an authentication framework for hierarchical networks is proposed that permits authenticated and secure broadcast from base station as well as middle tier nodes using Chinese remainder theorem (CRT). The proposed protocol uses different prime numbers in each cluster to generate unique CRT solutions for authenticating multicast messages by cluster head. We shall describe our strategy for the distribution of prime numbers to establish initial trust in the network. Further, we shall prove that multicast authentication using CRT is ideal for clustered network organization in terms of energy efficiency and tolerance to attacks.
Multicast Authentication Framework for Hierarchical Networks using Chinese Remainder Theorem

- Hu Xiangdong and Feng Rui. Message broadcast authentication in utesla based on double filtering mechanism. In Internet Technology and Applications (iTAP), 2011 International Conference on, pages 1–4, 2011.
- Mathias Bohge and Wade Trappe. An authentication framework for hierarchical ad hoc
Multicast Authentication Framework for Hierarchical Networks using Chinese Remainder Theorem


Index Terms

Computer Science Wireless

Keywords

Wireless Sensor Networks  Multicast  Authentication  Chinese Remainder Theorem