A CRT based encryption methodology for secure communication in MANET

Abstract

MANETs are well known for their flexibility and ease of communication. The communication is purely based on trust, without any need of authentication. This often leads to insecure communication, causing information tampering. The traditional means of security are not sufficient to safeguard against the inherent dangers of MANET. Researchers around the world are working in this issue. The preferred mode of securing data is through encryption. The process of encryption however is complex enough to increase the computational overhead. This paper proposes a secure encryption strategy using Chinese Remainder Theorem for shielding data from unauthorized access. The paper also includes a comparison of proposed method with existing methods.

References


Index Terms

Computer Science
Network Security

Keywords
Chinese Remainder Theorem Safety Key Super Key Lagrange’s Interpolation