Abstract

Entity authentication and key distribution are very important cryptographic problems in mobile communication or in ad-hoc networks or in wireless communication at large. Mutual entity authentication is seen as the necessary process to the establishment of a secure and authentic connection. For a reliable secure communication, mutual entity authentication is very often seen as the necessity to the establishment of a secure connection. Authentication is necessary in wireless communication such as GSM or for Ad-Hoc purposes [26]. Here Latin word ad-hoc means for the specific purpose only. Authentication is also necessary in situations where we need more than two entities in the authentication exchange such as a mobile user, a local AAA (Authentication, Authorization and Accounting) server and a remote (home) AAA server [8,21]. In such situations it is essential to include authentic and secure key exchange mechanism that ensures enhancement of trust in communication. This paper provides an authenticated zero knowledge protocol which is very helpful in establishing secure wireless communication in ad-hoc networks by satisfying cryptographic goals such as authentication, data integrity etc [13].
References


Index Terms

Computer Science    Wireless
Keywords