Efficient Privacy-Preserving Authentication in Wireless Mobile Networks

Abstract:

Secure authentication in roaming services is being designed to allow legal users to get access to wireless network services when they are away from their home location. Recently, to protect the location privacy of users, there have been researches on anonymous authentication. In particular, anonymous authentication without the participation of home servers has attracted considerable interest owing to its influence on the communication efficiency. Unfortunately, the previously proposed anonymous authentication schemes have serious practical shortcomings, such as high communication and computation costs and huge revocation lists. In this paper, we propose a novel three-round anonymous roaming protocol that does not require the participation of home servers. The proposed protocol uses a pseudo-identity-based signcryption scheme to perform efficient revocation with a short revocation list and efficient authentication. The use of a signcryption algorithm minimizes the number of pseudo-identities stored in a Subscriber Identification Module (SIM) card with limited storage capacity. The authentication efficiency is also higher than that of existing protocols. The proposed protocol is formally proved in the Canetti-Krawczyk (CK) model.