Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks

Abstract—

Mobile ad hoc networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network communications. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, we focus on the issue of certificate revocation to isolate attackers from further participating in network activities. For quick and accurate certificate revocation, we propose the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. In particular, to improve the reliability of the scheme, we recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks.