

Scalable rekeying algorithm in IEEE 802.16e

ABSTRACT

IEEE 802.16e standard provides wide coverage and high bandwidth for subscribers in a metropolitan area network. It introduces Multicast and Broadcast Rekeying Algorithm (MBRA) which is a multicasting scheme to communicate with many users concurrently. Although ELAPSE (for Efficient sub-Linear rekeying Algorithm with Perfect SEcrecy) improves on the deficiencies of MBRA, the algorithm poorly responds to scalability issue. This paper proposes a Scalable Rekeying Algorithm (SRA) based on a complete binary tree structure. SRA is introduced with linear linked list structure in order to make the system more scalable. Evaluation analysis shows that SRA manages to improve the scalability issue in MBRA for Mobile WiMAX.

Keyword: Group key managemet; Rekeying algorithm; Scalability; Unicast