Round-Robin Key Management for IEEE 802.11 Wireless LANs

Student Wen-Chun Huang Advisor Dr. Rong-Hong Jan

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE

NATIONAL CHIAO TUNG UNIVERSITY

Abstract

The IEEE 802.11 had been discovered that it is not secure. The main security problem of IEEE 802.11 standard is that it does not define the key management method. In this thesis, we propose a lightweight key management, called Round-Robin Key Management (RRKM), for IEEE 802.11 wireless networks. In RRKM, the access point will transfer semantics to the stations for key's synchronization during authentication phase. Then, the stations and access point can periodically generate a new key simultaneously. Every new key is only valid for a fixed period, thus the RRKM reduces a key long-term exposed. Although the RRKM is not solving all the security holes in IEEE 802.11, but it greatly improves the security of 802.11 wireless networks. Especially, the proposed method is suitable for small and home scale environment.