Secure multicast group communication scheme in wireless IPv6 networks

ABSTRACT

Key management is one of the challenging issues in group communications. It is generally used to secure multicast data transmission as well as preventing potential eavesdropping by malicious attackers. Group security key should be maintained for data encryption, while group key update and dissemination processes are required when a new user joins or leaves the group, which eventually lead to high communication and computation cost. Since eavesdrop activities can be initiated by capturing the disseminated keys, higher communication and computation cost due to frequent updates also increase the possibility of attack of multicast transmission. In this paper, a key management scheme for IPv6 networks is proposed to reduce communication and computation cost and therefore, fewer security risks. The obtained results from test-bed implementation show the efficiency of proposed scheme in terms of communication and computation cost, number of updated paths and security index due to key updating, while at the same time achieving both forward and backward secrecy.

Keyword: Group communication security; Key management; Wireless IPv6 test-bed; Path probability of attack