Distinctive key management method to secure multicast IPv6 networks

ABSTRACT

Secure multicast over wireless networks is an important and challenging goal because of widespread deployment of wireless networks and the need of multicast. In this paper, we propose a new method to generate and distribute keys for multicast security function. In existing key management protocols, after join or leave a node, key regeneration and distribution is needed to provide multicast security. In our distinctive method, each node that joins the multicast group has a different decryption key with other multicast group members. Therefore key regeneration and distribution is not needed due to new node joining or leaving, which can significantly minimize the number of transmission and storage requirements required for re-key of the multicast group. It also provides protection against data tampering after node leaving.

At the end the implementation of this method has been done on the real time network test-bed and the real obtained results show the efficiency of the proposed method.

Keyword: Multicast security; Key management; Multicast IPv6; IPv6 test-bed; IPv6 security