

## **Reliable key management and data delivery method in multicast over wireless ipv6 networks**

### **Abstract**

Multicast is an efficient way to reduce the required bandwidth of transmitting data simultaneously to a group of users in wireless IPv6 networks. Nevertheless, multicast suffers from two main drawbacks which can be looked from two perspectives, namely security and QoS. With regard to security, the main challenge is to provide security protection to multicast data, which can be achieved by using a secure key management process. Considering a highly dense environment where connection of users to the network is changing frequently due to join or leave operations, key updating approach may burden a network devices with a huge amount of complex encryption/decryption processes. From the QoS perspective, multicast transmission over WLAN offers a tradeoff between the transmission rate and the coverage. The transmission rate of multicast is confined by the user with the lowest data rate in the group which is called fixed base rate problem. To address the above mentioned problems, we propose and implement a lightweight key management and data delivery scheme for multicast over wireless IPv6 networks. The proposed solution is envisaged to reduce the complexity of key updating, while at the same time is able to address the fixed base rate problem. The performance evaluation (by means of analytical and test-bed implementation) of the proposed key management method indicates its efficiency in reducing communication, computation, and storage costs, while maintaining both forward and backward securities. Moreover, the proposed data delivery method is able to improve the throughput and QoS, with low packet loss and transmission delay.

### **Keywords**

Data rate transmission; Key management; Multicast IPv6 Test-bed; Multicast over WLANs; Multicast security; Quality of service