Abstract

Seamless connectivity for the roaming users is highly desirable to all kinds of wireless communications, for example, Cellular Networks, 3GPP and Wireless Mesh Networks (WMNs) etc. In the situations, when a mobile node roams and enters into other foreign domains; to make the mobile user get ubiquitous services without geographic limitations, a roaming authentication is very much needed. The traditional three-party roaming authentication approach requires home server′s participation during the authentication between the roaming user and the foreign server. If large numbers of roaming requests are to be processed, the heavier burden will be on the home server. Therefore, the home server may not be able to deal with all the authentication requests in time, which yields authentication delay and hence not desirable for seamless connectivity. Meanwhile, there have been growing researches on anonymous roaming authentication to protect the privacy of users. In particular, anonymous roaming authentication without participation of the home servers has been attracting considerable amount of interest because of its efficiency in terms of communication overhead and security.

In this dissertation we have investigated the problem of roaming authentication in WMNs and proposed a *pairing based authentication protocol with anonymous roaming for Wireless Mesh Networks* which avoids the requirement of home server′s participation. The protocol uses pairing-based cryptography to secure roaming authentication and provide user anonymity, while minimizing computation cost and communication overhead. In addition, the protocol efficiently mitigates the effects of DoS attacks at the foreign servers. Implementation results show that it has better performance in terms of computation cost and security compared with the similar existing roaming authentication protocols whose authentication do not need home server′s participation.

Keywords: Wireless Mesh Networks, Roaming Authentication, Anonymity, Efficiency, Security, Denial of Service Attack.