BILINEAR PAIRINGS-BASED THRESHOLD IDENTITY AUTHENTICATION SCHEME FOR AD HOC NETWORK

FENG XU 1,2, YUQI ZHU 1, HONGXU MA 1, BIN CAI 1

1College of Computer and Information
Hohai University

2Department of Computer Science & Technology
Nanjing University
Nanjing, P. R. China
e-mail: njxufeng@163.com

ABSTRACT—Aiming at specific security threats in ad hoc network, this paper presents a bilinear pairings-based threshold identity authentication scheme without the trusted center. In this work, the security of certificate has been significantly enhanced by using improved GDH signature and interactive secret-sharing, that is, any attacker cannot forge a valid certificate for the untrusted nodes. The proposed scheme can effectively reduce the storage and computation amounts of each node, and some security problems (e.g., passive attack, man-in-the-middle attack and so on) can also be solved. Compared to the congener schemes, ours is much more efficient in the process of certificate generating.

Key Words: Ad hoc Network; Improved GDH Signature; Threshold Identity Authentication; Non-Masquerading; Insecure/Common Channel