International Journal of Innovative Computing, Information and Control
Volume **5**, Number **4**, April **2009**

ICIC International ©2009 ISSN 1349-4198
pp. **1069–1080**

A ROBUST AUTHENTICATION SCHEME WITH USER ANONYMITY FOR WIRELESS ENVIRONMENTS

Ren-Chiun Wang[1], Wen-Shenq Juang[2] and Chin-Laung Lei[1*]
[1]Department of Electrical Engineering
National Taiwan University
No.1, Sec. 4, Roosevelt Rd., Taipei, Taiwan 106
rcwang@fractal.ee.ntu.edu.tw; lei@cc.ee.ntu.edu.tw
*Corresponding author

[2]Department of Information Management
National Kaohsiung First University of Science and Technology
No.2, Jhuoyue Rd., Nanzih District, Kaohsiung 811, Taiwan
wsjuang@ccms.nkfust.edu.tw

Received November 2007; revised April 2008

Abstract. *Due to the openness of data transmission over wireless environments, the wireless networks are susceptible to various security menaces. Authentication and key agreement become a basic and most important procedure before a mobile user can obtain the desired services. Apart from the security threats, in a limited bandwidth and the openness wireless environment, low computation and communication cost with privacy should be taken into considerations. Recently, Zhu and Ma proposed an authentication scheme with user anonymity for wireless environments based on hash functions and smart cards. In their scheme, the communication and computation cost is very low. However, Lee et al. pointed out that Zhu and Ma's scheme is vulnerable to several security problems. The perfect backward secrecy and mutual authentication are not provided and the forgery attack can work in Zhu and Ma's scheme. At the same time, Lee et al. proposed an improvement to solve the above weaknesses and to keep the efficiency. However, in this paper, we show that Lee et al.'s scheme cannot provide the anonymity for a mobile user and the key agreement procedure is not correct. Also, if a smart card is stolen by an adversary, the adversary could launch the impersonation attack on Lee et al.'s scheme. We then propose a new authentication scheme. Our scheme not only provides more security criteria but also requires low communication and computation cost. Finally, we use the logic analysis method to prove our scheme.*
Keywords: Anonymity, Authentication, Password, Logic analysis, Smart card, Wireless communications.

1. **Introduction.** Since the rapid developments of wireless communications, there are many opportunities to obtain desired services through wireless networks using small mobile devices at any time and any place [12, 16]. Due to the openness of data transmission over air interface, several security problems and requirements must be considered in the developments [4]. Apart from the security threats, the resources of the small device are limited, where the limited resources include memory, power supply and bandwidth. A secure authentication and key agreement scheme with low computation and communication cost is urgently required for wireless environments. Now, we introduce these security threats and requirements as follows: