International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **8**, August **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 4821–4831

A SECURE BILLING SERVICE WITH TWO-FACTOR USER AUTHENTICATION IN WIRELESS SENSOR NETWORKS

Chun-Ta Li[1], Cheng-Chi Lee[2,4,*], Lian-Jun Wang[3] and Chen-Ju Liu[1]

[1]Department of Information Management
Tainan University of Technology
No. 529, Jhong Jheng Road, Yongkang, Tainan 710, Taiwan
th0040@mail.tut.edu.tw

[2]Department of Library and Information Science
Fu Jen Catholic University
No. 510, Jhong Jheng Road, Taipei 242, Taiwan
*Corresponding author: cclee@mail.fju.edu.tw

[3]Department of Information Management
Yuan-Ze University
No. 135, Yuan-Tung Road, Chung-Li 320, Taiwan

[4]Department of Photonics and Communication Engineering
Asia University
No. 500, Lioufeng Road, Taichung 413, Taiwan

Received March 2010; revised July 2010

Abstract. *Recently, Das proposed a secure two-factor user authentication scheme based on hash function, which is efficient enough to be implemented on most of the target resource-constrained devices, such as low-computation smart cards and low-power sensor nodes in wireless sensor networks (WSNs). As Das claimed, the proposed scheme can resist attacks and threats such as many logged-in users with the same login identity, stolen-verifier, guessing, impersonation and replay. Unfortunately, we find that Das's authentication scheme is insecure against attacks of unknown user, password guessing and masquerade. In this paper, based on the framework of Das's two-factor user authentication, we introduce a secure billing service, and analyze our extended scheme on how to achieve imposter prevention, as well as resist against the drawbacks of Das's scheme.*
Keywords: Billing service, Hash function, Information security, Smart cards, User authentication, Wireless sensor networks

1. **Introduction.** Wireless Sensor Networks (WSNs) have become technically and economically feasible and drawn intensive interests from both academic and industrial areas [10]. They consist of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion and pollutants. WSNs have been used for a wide variety of applications such as environment monitoring, wild animal tracking, health monitoring and military sensing. To access the sensor nodes, some secure mechanisms are necessarily against unauthorized actions, and this is an extremely important security issue in WSNs. However, given the stringent constraints on processing power, memory, bandwidth and energy consumption of small devices, it is very difficult to design suitable secure mechanisms for WSNs.

Recently, a lot of secured user authentication schemes are proposed to prevent unauthorized access in WSNs. For example, Watro et al. [23] suggested a user authentication scheme using the RSA [21] and Diffie-Hellman algorithms [3]. However, it is too expensive