International Journal of Innovative Computing, Information and Control
Volume **4**, Number **8**, August **2008**

ICIC International ©2008 ISSN 1349-4198
pp. **2045–2056**

A KEY MANAGEMENT FOR WIRELESS COMMUNICATIONS

Min-Shiang Hwang[1], Cheng-Chi Lee[2*], Song-Kong Chong[3] and Jung-Wen Lo[4,5]

[1]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
mshwang@nchu.edu.tw

[2]Department of Computer and Communication Engineering
Asia University
No.500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan
*Correspondence: cclee@asia.edu.tw

[3]Department of Computer Science and Information Engineering
National Cheng-Kung University
No.1, Ta-Hsueh Road, Tainan 701, Taiwan

[4]Department of Computer Science and Engineering
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan

[5]Department of Information Management
National Taichung Institute of Technology
129 Sec.3 San-min Road, Taichung 404, Taiwan

Received June 2007; revised December 2007

Abstract. *In this article, we present a new authentication protocol to solve several drawbacks of GSM authentication protocol including: transmission overloading between Home Location Register (HLR) and Visitor Location Register (VLR); storage overhead in VLR; calculation overloading when authenticating a mobile user. Most importantly, a robust and efficient secret key management scheme for home network was proposed. The idea behind the proposed method is to introduce a simple public one-way hash function to achieve the above requirements. In addition, the method does not only apply to the GSM system, but also applies to other wireless communication systems.*
Keywords: Authentication, GSM, One-way hash function, Wireless communications

1. **Introduction.** In recent years, the roaming services provided by the Global System of Mobile Communications (GSM) [9] has been widely popular. It has been accepted as the worldwide wireless communication standard in over 70 countries around the world [20]. Owing to the widespread use of the GSM standard, people can easily communicate with each other wherever they are. Although other mobile communication systems are going to replace GSM systems, undoubtedly the number of GSM users and telecommunications will dominate the market for a long period of time.

The astonishing market growth of GSM is inseparable from people's lives because people wish to communicate with others no matter where they are [12]. The wide acceptance of GSM makes people concerned about two main security problems: authentication and privacy [12, 14]. Authentication is the process to verify the identity of a subscriber. Only