International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **9**, September **2009**

 ISSN 1349-4198
pp. **2657–2664**

AN AUTHENTICATION PROTOCOL WITH BILLING NON-REPUDIATION TO PERSONAL COMMUNICATION SYSTEMS

Tzung-Her Chen

Department of Computer Science and Information Engineering
National Chiayi University
300 University Rd., Chiayi City 600, Taiwan
thchen@mail.ncyu.edu.tw

Received February 2008; revised June 2008

Abstract. *The trend toward personal communication system (PCS) is perhaps the most significant technological change in the last decade. Hence, there are many articles proposed for the PCS-like authentication schemes. Recently, Stach et al. proposed a PCS-like version to provide non-repudiation for billing services. The assumption that the service provider is trustworthy is not always true. For example, the service provider potentially benefits from imputing extra charge to subscribers. Furthermore, a specious subscriber intended to deny the received services can claim that the evidence to services is illegally generated by service provider. In this paper, the author point out that their scheme lacks not only mutual authentication, backward privacy but also non-repudiation. In addition, Certain PCS authentication schemes, claiming with non-repudiation, still fail to provide this service. The proposed improved scheme will overcome these weaknesses and thus provide the billing non-repudiation service.*

Keywords: Personal communication system (PCS), Billing, One way hash function, Non-repudiation, Digital signature

1. **Introduction.** Over the past ten years, the mobile phone market has remarkable growth such that the phone itself is now regarded as daily essentials by millions of people. Personal communication system (PCS) such as GSM [1] and UMTS [2] is based on the available radio and wire networks.

However, security is still a barrier to wide acceptance of wireless communication technology, whose success depends on authentication [3], the most important premise that the service is properly used. Once security on PCS is well-addressed, the highly sensitive transactions, such as electronic trade, electronic accounting etc., can be carried out.

The common security requirements for PCS are highlighted as follows [4]:

1) *Message confidentiality*: Message transmitted over the wireless link should be kept secret in ciphertext.
2) *Mutual authentication*: Authentication, one of the major concerns, guarantees the grant of access control for services by identifying the identities of communicating parties. For higher security level, authentication between a subscriber and a service provider should be mutual.
3) *Non-repudiation*: From the side of a service provider, a subscriber should never be able to repudiate the service he has used. From a subscriber's perspective, the service provider cannot benefit from mistaken charge of a subscriber for the services he has not used.
4) *Minimum trust on visited service domains*: While roaming, the visited service domain must obtain some authentication parameters from the visitor's home service domain