International Journal of Innovative Computing, Information and Control
Volume **5**, Number **2**, February **2009**

 ISSN 1349-4198
pp. **461–466**

A LOW-COMPUTATION CONFERENCE KEY SYSTEM FOR MOBILE COMMUNICATIONS

Hui-Feng Huang, Chao-Wen Chan, Chih-Hao Lin and Hsin-Wei Wang

Graduate School of Computer Science and Information Technology
National Taichung Institute of Technology
Taichung 404, Taiwan
{ phoenix; ccwen; s18953202; s18953106 }@ntit.edu.tw

Received October 2007; revised January 2008

Abstract. *Recently, technological advances have allowed all conferees to hold a mobile conference via wireless communications. Wireless communications are more susceptible to eavesdropping and unauthorized access than conversations via wires. The traditional conference key scheme isn't suitable for participants because wireless devices are low powered and have limited computing capability. Therefore, it is crucial to ensure confidentially and authenticity in mobile teleconferencing. However, many investigations designed on conference key schemes for wireless communications have been shown to be insecure. Based on the one-way hash function and XOR operations (⊕), we propose a new low-computation conference key system which allows a participant to dynamically join or terminate a teleconference. In the proposed scheme, neither a conference bridge (trusted center) nor an interactive protocol among participants is required to construct the common conference key for each session. This can save on communication overhead.*
Keywords: Wireless communications, Mobile conference, Low-computation

1. **Introduction.** A conference key system enables a group of people to construct a secret key to hold a secure conference. The conference key is a common secret key in which one can encrypt and decrypt messages to communicate with others in the group over an insecure network. The rapid growth of technological advances has allowed all conferees to hold a mobile conference via wireless communications [8]. When holding a mobile teleconference, a conference bridge (trusted center) receives signals from conferees, operates on these signals in an appropriate way, and then broadcasts the results to conferees. A mobile teleconference is a synchronous collaboration session, shown in Figure 1, in which conferees at remote locations cooperate in an interactive procedure, such as a scientific discussion, a board meeting, or even a virtual classroom. However, wireless communications transmit conversations via radio that are more susceptible to eavesdropping and unauthorized access than transition via hard wires. The traditional conference key scheme isn't suitable for mobile or wireless participants because a mobile user's portable devices are usually low powered, low cost, and have limited computing capability [2-4,7,12], it is crucial to ensure confidentiality and authenticity in mobile teleconferences. However, many conference schemes designed for wireless communication systems have been shown to be insecure [9,13,14].

For the limited computing capability in a mobile user's portable device, Hwang and Yang proposed the conference key establishing scheme for mobile communications [4]. But they do not consider the situation that a participant may be in a conference for only a period of time. If a participant resigns or leaves the conference and he premeditatedly eavesdropped on data transmissions, he could then also decrypt the data. Thus, all messages are likely to be compromised during the span of the system. Many mobile