International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **9**, September **2010**

 ISSN 1349-4198
pp. 4125–4132

AN AUTHENTICATED KEY EXCHANGE PROTOCOL FOR MOBILE STATIONS FROM TWO DISTINCT HOME NETWORKS

Hao-Li Wang, Tzung-Her Chen*, Long-Sheng Li, Yan-Ting Wu and Jhong Chen

Department of Computer Science and Information Engineering
National Chiayi University
300 University Rd., Chiayi City 60004, Taiwan
*Corresponding author: thchen@mail.ncyu.edu.tw

Received April 2009; revised August 2009

Abstract. *Authentication in Mobile IP enables authorized mobile nodes to access services within the foreign domain. However, previous research only considers communication from a mobile node (MN) to a corresponding node (CN), not the other way around. They do not support sharing of session key for communicating parties belonging to distinct home networks (HN) to encrypt secret data. This paper aims at transferring confidentiality between MNs belonging to two distinct home networks by proposing a protocol to establish the session key for communicating parties and authenticate each identity simultaneously. The proposed scheme provides confidentiality, integrity and perfect forward secrecy. It is the first attempt to supply authentication key exchange protocol for mobile stations within two HNs.*
Keywords: Authentication key exchange, Diffie-Hellman protocol, Mobile IP

1. **Introduction.** Mobile computing becomes increasingly important due to the rising number of portable devices and a desire to have continuous network connectivity to the Internet irrespective of the node's physical location. To offer continuous services in a mobile environment is a vital issue in both research and practice. In IPv4, a node's IP address is assumed to uniquely identify the node's point of attachment to the Internet; a node must be located on the network indicated by its IP address to receive a destined packet. If a node intends to change point of attachment, either the node changes its IP address or host-specific routing mechanism is used.

1.1. **Authentication to mobile IP.** Mobile IP is an IETF (Internet Engineering Task Force) standard enabling nodes to change their attachment point to the Internet without changing their IP address. A mobile device, MN, is always expected to be addressable at its home address, whether it is currently attached to its home link or not. While an MN is in the home network, packets addressed to its home address are routed to its Home Agent (HA), using conventional Internet routing mechanisms. An MN attached to a foreign link away from home is also addressable at one or more care-of addresses (CoA), a mechanism allowing mobile devices to change point-of-attachment without interrupting IP service. In detail, MN immediately sends a "binding" message to HA that associates MN's care-of address with its home address. Whenever MN changes its point-of-attachment, a binding update is required for HA. After successful binding update, HA will send a "binding acknowledgement" message to MN, called registration.

A care-of address is a uni-cast routable address associated with a MN visiting a foreign link allocated by Foreign Agent (FA) in a foreign network. A device communicating with MN refers to as CN, either a stationary or mobile node. When a CN sends a packet to