A Secure Handshake Scheme with Pre-negotiation for Mobile-hierarchy City Intelligent Transportation System under Semi-honest model

Shuai Li*, Peng Gong*, Qian Yang*, Xiaopeng Yan*, Jiejun Kong**, and Ping Li*

** National Key Laboratory of Mechatronic Engineering and Control, School of Mechatronical Engineering,*
Beijing Institute of Technology, Beijing,100081, China

*** Department of Computer Sciences, University of Florida, Gainesville, FL, USA*

lshuai@ndrc.gov.cn, {penggong,yangqian,yanxiaopeng}@bit.edu.cn, jkong@cs.ucla.edu, liping85@bit.edu.cn

***Abstract*—Mobile-hierarchy architecture was widely adopted for query a deployed wireless sensor network in an intelligent transportation system recently. Secure handshake among mobile node and ordinary nodes becomes an important part of an intelligent transportation system. For dividing virtual communication area, pre-negotiation should be conducted between mobile node and ordinary node before formal handshake. Pre-negotiation among nodes can increase the odds for a successful handshake. The mobile node negotiates with an ordinary sensor node over an insecure communication channel by private set intersection. As an important handshake factor, Attribute set is negotiated privately among them in local side. In this paper, a secure handshake scheme with pre-negotiation for mobile-hierarchy city intelligent transportation system under semi-honest model is proposed**

***(Pt9)Keyword*—Attribute-based handshake; Private set intersection; Intelligent transportation system; Wireless sensor network; Attribute Encryption**

Xiaopeng Yan received the B.E. degree in mechanical and electronic engineering and the M.E. degree in pattern recognition and intelligent system, and the Ph.D. degree in weapon system and application Engineering from the Beijing Institute of Tec hnology, Beijing, China, in 1999, 2003 and 2009, respectively. He is an Associate Professor with the School of Mechatronic al Engineering, Beijing Institute of Technology, where he has been a faculty member since 2003. His research interests are i n the areas of radio proximity detection, signal processing in proximity sensor and information security in wireless communic ation.