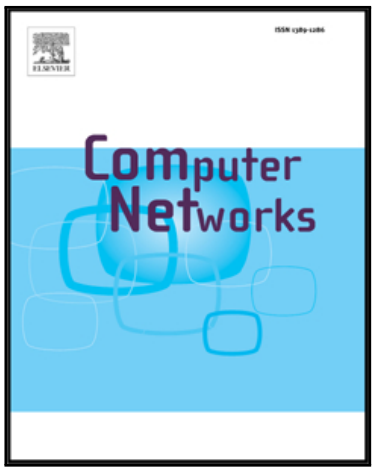

Analysis of Handover Authentication Protocols for Mobile Wireless Networks Using Identity-Based Public Key Cryptography

Debiao He, Sherali Zeadally, Libing Wu, Huaqun Wang

PII: S1389-1286(16)30428-5
DOI: 10.1016/j.comnet.2016.12.013
Reference: COMPNW 6076

To appear in: *Computer Networks*

Received date: 16 July 2016
Revised date: 28 October 2016
Accepted date: 20 December 2016

Please cite this article as: Debiao He, Sherali Zeadally, Libing Wu, Huaqun Wang, Analysis of Handover Authentication Protocols for Mobile Wireless Networks Using Identity-Based Public Key Cryptography, *Computer Networks* (2016), doi: 10.1016/j.comnet.2016.12.013

Analysis of Handover Authentication Protocols for Mobile Wireless Networks Using Identity-Based Public Key Cryptography

Debiao He [1,2], Sherali Zeadally [3], Libing Wu [1], Huaqun Wang [4]

[1] *State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan, China*

[2] *Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Gulin, China*

[3] *College of Communication and Information, University of Kentucky, USA*

[4] *School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China*

Abstract

The handover authentication protocol plays an important role in mobile wireless networks where mobile devices often need to securely and seamlessly roam among different access points. To satisfy various security and privacy requirements of practical wireless applications, many handover authentication protocols for mobile wireless networks have been proposed in the last decade. In particular, the handover authentication protocol using the Identity-based Public Key Cryptography (ID-based PKC) has better security and has attracted a lot of attention recently. Here, we discuss the security and privacy requirements of handover authentication protocols for mobile wireless networks and we present a brief review of handover authentication protocols using the ID-based PKC technique. Our security analysis shows that only one of the recent protocols proposed can satisfy all security and function requirements. We also implement and compare the communication and computation costs associated with these protocols on a specific mobile device.

Keywords: anonymity, handover authentication, protocol, provable security, wireless network

2010 MSC: 00-01, 99-00