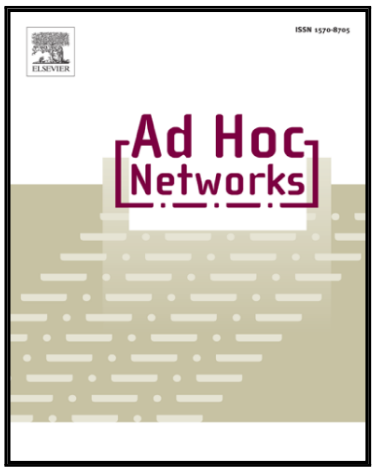

Secure and Efficient User Authentication Scheme for Multi-gateway Wireless Sensor Networks

Jangirala Srinivas, Sourav Mukhopadhyay, Dheerendra Mishra

PII: S1570-8705(16)30298-0
DOI: 10.1016/j.adhoc.2016.11.002
Reference: ADHOC 1483

To appear in: *Ad Hoc Networks*

Received date: 15 October 2015
Revised date: 23 October 2016
Accepted date: 2 November 2016

Please cite this article as: Jangirala Srinivas, Sourav Mukhopadhyay, Dheerendra Mishra, Secure and Efficient User Authentication Scheme for Multi-gateway Wireless Sensor Networks, *Ad Hoc Networks* (2016), doi: 10.1016/j.adhoc.2016.11.002

Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks xx (2016) 1–32
Ad Hoc Networks

Secure and Efficient User Authentication Scheme for Multi-gateway Wireless Sensor Networks

Jangirala Srinivas[a], Sourav Mukhopadhyay[a], Dheerendra Mishra[b]

[a]*Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India*
E-mail: jangiralasrinivas@maths.iitkgp.ernet.in, sourav@maths.iitkgp.ernet.in
[b]*Department of Mathematics, LNM Institute of Information Technology, Jaipur, India*
E-mail: dheerendra@maths.iitkgp.ernet.in

Abstract

By utilizing Internet of Things (IoT), the collected information from the sensor nodes in wireless sensor networks (WSNs) could be provided to the users who are permitted to get access of sensor nodes. As the information from the sensors are transmitted via public network and sensor nodes have limited battery, shift the focus on security and efficiency in WSNs. User authentication is the security task for limiting the access. It is achieved by equipping authorized users with passwords, tokens or biometrics. However, password and token are easy being stolen and forgotten; even biometrics inherit some limitation. More suitable approach is to combine both password and biometric authenticator to harvest benefits in security. This paper proposes a novel authentication and key agreement scheme for WSNs using biohashing. Biohashing facilitates elimination of false accept rates without increasing occurrence of false rejection rate. Additionally, biohashing has highly clear separation of imposter populations and genuine, and zero equal error rate level. The proposed scheme also supports dynamic node addition and user friendly password change mechanism. Using the BAN-logic, we prove that the proposed scheme provides mutual authentication. In addition, we simulate proposed scheme for the security against man-in-the middle attack and replay attack using the AVISPA tool, and the simulation results show that our scheme is safe. Through the informal security analysis, we show that the proposed scheme is secure against the known attacks for authentication protocols.

Keywords: Internet of Things (IoT), Wireless sensor networks(WSNs), Authentication.