A secure authentication scheme for Internet of Things

King-Hang Wang, Chien-Ming Chen, Weicheng Fang, Tsu-Yang Wu

PII: S1574-1192(16)30436-9
DOI: https://doi.org/10.1016/j.pmcj.2017.09.004
Reference: PMCJ 889

To appear in: *Pervasive and Mobile Computing*

Received date : 14 December 2016
Revised date : 24 August 2017
Accepted date : 1 September 2017

Please cite this article as: K. Wang, C.-M. Chen, W. Fang, T. Wu, A secure authentication scheme for Internet of Things, *Pervasive and Mobile Computing* (2017), https://doi.org/10.1016/j.pmcj.2017.09.004

A Secure Authentication Scheme for Internet of Things

King-Hang Wang

Hong Kong University of Science and Technology, Hong Kong

Chien-Ming Chen, Weicheng Fang

Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China

Tsu-Yang Wu

Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fujian University of Technology, Fujian, China

National Demonstration Center for Experimental Electronic Information and Electrical Technology Education, Fujian University of Technology, Fujian, China

Abstract

Security is one of the major issues in Internet of Things (IoT) research. The rapid growth in the number of IoT devices, the heterogeneity and complexity of these objects and their networks have made authentication a challenging task. Other constraints such as limited computational ability and power, and small storage of some embedded devices make implementation of complex cryptographic algorithms difficult. So far there has been no established industrial standard to address this problem.

Recently, Kalra and Sood, and subsequently Chang *et al.* attempted to solve the authentication problem by proposing key agreement schemes for IoT devices. However, the security of their schemes were unproven. In this paper we demonstrate that these schemes are insecure. We extend upon their work to present a scheme that enables embedded devices to communicate securely with a server on an IoT network. We prove the security of this scheme using formal methods and demonstrate this under the intractability of some well-defined hard problems. We also discuss some practical aspects related to the implementation of the scheme.

Keywords: IoT Security, Authentication, Elliptic Curve Cryptography,