Accepted Manuscript

A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring

Rifaqat Ali, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah, Mauro Conti

PII: S0167-739X(17)30386-2
DOI: http://dx.doi.org/10.1016/j.future.2017.06.018
Reference: FUTURE 3516

To appear in: *Future Generation Computer Systems*

Received date : 11 March 2017
Revised date : 4 May 2017
Accepted date : 16 June 2017

Please cite this article as: R. Ali, A.K. Pal, S. Kumari, M. Karuppiah, M. Conti, A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.06.018

A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring

Rifaqat Ali

Department of Computer Science and Engineering,
Indian Institute of Technology (Indian School of Mines), Dhanbad-826004,
Jharkhand, India
rifaqatali27@gmail.com

Arup Kumar Pal

Department of Computer Science and Engineering,
Indian Institute of Technology (Indian School of Mines), Dhanbad-826004,
Jharkhand, India
arupkrpal@gmail.com

Saru Kumari

Department of Mathematics,
CCS University, Meerut-250004, Uttar Pradesh, India
saryusiirohi@gmail.com

Marimuthu Karuppiah

School of Computer Engineering,
VIT University, Vellore-632 014, Tamilnadu, India
marimuthume@gmail.com, k.marimuthu@vit.ac.in

Mauro Conti

Department of Mathematics,
University of Padua, Via Trieste, 6335131, Padua, Italy
conti@math.unipd.it

Abstract

Agriculture is the backbone of our economic system and plays an important role in the life of an economy. It does not only provide raw material and food, but also provides large employment opportunities. Therefore, agriculture requires modern technology for increasing the productivity. In this context, wireless sensor networks (*WSNs*) could be utilized for monitoring the climatic parameters such as (temperature, humidity, light, carbon dioxide, soil moisture, acidity etc.) in an agriculture field. The climatic parameters are very important in terms of growth, quality and productivity of crops. But, any kind of interception, modification, insertion, and deletion on these parameters can have negative effect on crop. Therefore, security and privacy are important issues in agriculture field. In this regard, we design a novel remote user authentication scheme using wireless sensor networks for agriculture monitoring. The protocol is validated through Burrows-Abadi-Needham *(BAN)* logic and also simulated using Automated Validation Information Security Protocols and Applications (*AVISPA*) tool. We formally analyze the security of the scheme using random oracle model. In addition, the informal security analysis shows that the proposed protocol is secure and resists various kinds of malicious attacks. As a results, the proposed protocol is applicable in a real life application.

Keywords: Agriculture monitoring, *AVISPA*, Random oracle model, Wireless sensor networks