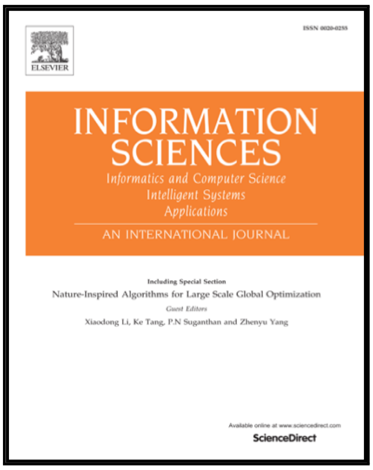

ISSN 0020-0255

ELSEVIER

INFORMATION SCIENCES

Informatics and Computer Science
Intelligent Systems
Applications

AN INTERNATIONAL JOURNAL

Including Special Section

Nature-Inspired Algorithms for Large Scale Global Optimization

Guest Editors

Xiaodong Li, Ke Tang, P.N Suganthan and Zhenyu Yang

Available online at www.sciencedirect.com

ScienceDirect

An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks

Jie Cui, Jing Zhang, Hong Zhong, Runhua Shi, Yan Xu

PII: S0020-0255(16)31051-9
DOI: 10.1016/j.ins.2018.03.060
Reference: INS 13538

To appear in: *Information Sciences*

Received date: 25 September 2016
Revised date: 28 November 2017
Accepted date: 26 March 2018

Please cite this article as: Jie Cui, Jing Zhang, Hong Zhong, Runhua Shi, Yan Xu, An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.03.060

Highlights

- The proposed signature scheme only requires a general one-way hash function, which consumes less computing time than a special one-way hash function (MapToPoint).
- A complex security analysis was performed on the proposed scheme. This analysis revealed that the proposed scheme can meet the safety and privacy requirements of VANETs.
- The communication and computation costs associated with the proposed scheme were analyzed. The results demonstrate that the performance of the proposed scheme surpasses that of previously proposed schemes for VANETs.