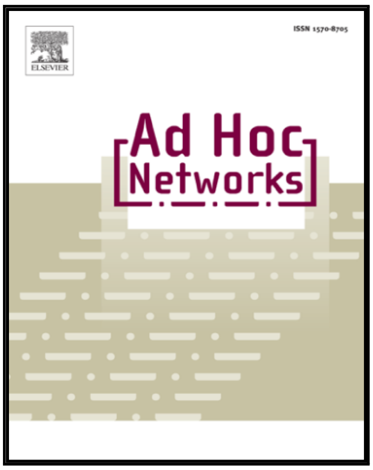

Bandwidth Efficient Designated Verifier Proxy Signature Scheme for Healthcare Wireless Sensor Networks

Girraj Kumar Verma, B.B. Singh, Harendra Singh

PII:	S1570-8705(18)30529-8
DOI:	10.1016/j.adhoc.2018.07.026
Reference:	ADHOC 1727
To appear in:	*Ad Hoc Networks*
Received date:	21 January 2018
Revised date:	12 July 2018
Accepted date:	25 July 2018

Bandwidth Efficient Designated Verifier Proxy Signature Scheme for Healthcare Wireless Sensor Networks

Girraj Kumar Verma[a,*], B. B. Singh[b], Harendra Singh[c]

[a]*Hindustan College of Science and Technology,*
Farah, Mathura, India
[b]*Government K. R. G. (P.G.) College*
Gwalior, India
[c]*Hindustan College of Science and Technology*
Farah, Mathura, India

Abstract

Recently, big data collection of e-healthcare monitoring using wireless sensor networks (WSN) have become common in practice. These WSN collect the data such as blood pressure, pH-value, pulse rate, etc. from a remote location based patient and then send to hospital/medical server. Since, the e-healthcare data is associated to a patient and thus, the confidentiality and authentication of data are critical issues. This article introduces a provably secure message recovery designated verifier proxy signature (MRDVPS) scheme to eliminate the issues. The proposed MRDVPS scheme is proven existential unforgeable (EUF) in the random oracle model (ROM), under the intractability of computational Diffie-Hellman (CDH) problem. Efficiency comparison shows that the scheme is the most appealing towards healthcare wireless sensor networks (HWSN).

Keywords: Proxy Signature, Designated Verifier Signature, e-healthcare, Wireless Sensor networks, Message Recovery Signature.
2010 MSC: 94A60

[*] Corresponding author
Email address: girrajv@gmail.com (Girraj Kumar Verma)