

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X



IJCSMC, Vol. 3, Issue. 3, March 2014, pg.155 – 160

RESEARCH ARTICLE

Source Anonymous Message Authentication Based On ECC in Wireless Sensor Networks

B.Renugadevi¹, T.John Peter²

¹PG Scholar, Department of Computer Science and Engineering, Anna University Chennai, India

²Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India

^{1,2}Roever Engineering College, Perambalur

¹renugacse12@gmail.com, ²johnthiraviam85@gmail.com

Abstract—Source Anonymous Message authentication (SAMA) is one of the most effective ways to prevent unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). A scalable authentication scheme based on elliptic curve cryptography (ECC) is introduced to allow any node to transmit an unlimited number of messages without suffering the threshold problem and provides message source privacy. For each message the sending node generates a source anonymous message authenticator for the message. The generation is based on MES scheme on elliptic curves. An efficient key management framework is introduced to ensure isolation of the compromised nodes. ECC reduces computational and communication overhead under comparable security levels while providing message source privacy.

Keywords— Hop-by-hop authentication; symmetric key cryptosystem; public-key cryptosystem; source privacy; Modified Elgamal Signature (MES)

Full Text: <http://www.ijcsmc.com/docs/papers/March2014/V3I3201443.pdf>
