SAPTHAGIRICOLLEGE OF ENGINEERING

14/5, Chikkasandra, Hesaraghatta Main Road, Bangalore-560057

Department of Computer Science and Engineering

Certificate

Certified that the project work entitled **"SECURE HOP-BY-HOP MESSAGE AUTHENTICATION IN WIRELESS SENSOR NETWORKS"** carried out by **PRIYANKA N L (1SG11CS058), SHASHIKALA R (1SG11CS075), SOUNDARYA V (1SG11CS081), VIDYASHREE S (1SG11CS092),** bonafide students of **this institute**, in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering** of **Visvesvaraya Technological University, Belgaum** during the academic year **2014-15** It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the department library. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said degree.

23/5/15

Signature of the Guide

Mrs. Poornima G J

Associate Professor

28/5/15

Signature of the HOD

Dr.C.M.Prashanth

Professor & Head

Signature of the Principal

Dr. Aswatha Kumar M

Principal

Dr. Aswatha Kumar. M
Principal
Sapthagiri College of Engineering
No. 14/5, Chikkasandra,
Hesaraghatta Main Road,
Bangalore -560 057.

Name of the Examiners **Signature with date**

1…………………….. ……………………..

2…………………….. ……………………..

Scanned by CamScanner

ABSTRACT

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, scalable authentication scheme based on elliptic curve cryptography (ECC) is proposed. While enabling intermediate nodes authentication, the proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, the scheme can also provide message source privacy.

Scanned by CamScanner