SAPTHAGIRI COLLEGE OF ENGINEERING

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

Department of Computer Science and Engineering

Certificate

Certified that the project work entitled **"Secure And Efficient Data Transfer in Cluster base Wireless Sensor Networks "**carried out by **ADITI KUMARI (1SG11CS005), ARJITA (1SG11CS013 JAGADEVI KORI (1SG11CS030), JYOTI KUSHWAHA (1SG11CS032)**, bonafide students Sapthagiri College of Engineering, in partial fulfillment for the award of **Bachelor of Engineeri nComputer Science and Engineering** of**Visvesvaraya Technological University, Belgaum** during t academic year **2014-15.** It is certified that all corrections/suggestions indicated for internal assessment ha been incorporated in the report deposited in the department library. The project report has been approved a satisfies the academic requirements in respect of Project work prescribed for the said degree.

Signature of the Guide	Signature of the HOD	Signature of the Principal
Mrs. Veena Gadad	**Dr.C.M.Prashanth**	**Dr.Aswatha Kumar M**
Assistant Professor	Professor & Head	Principal

Name of the Examiners	Signature with date
1……..	……..
2……..	……..

ABSTRACT

Secure data transmission is a critical issue for wireless sensor networks (WSNs).Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.