VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELGAUM

Project Work entitled

PRIVACY AT NETWORK LEVEL IN WIRELESS SENSOR NETWORK

Submitted by

Deepak B.	**4BB10IS002**
Keerthana N.P.	**4BB10IS003**
Namitha U.	**4BB10IS006**
Yogita M.R.	**4BB10IS012**

Under the Guidance of

Mrs. C. R. Kavitha B.E., M.Tech

Associate Professor

Department of Computer Science & Engineering

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

Bahubali College of Engineering

Shravanabelagola-573 135

2013-14

ABSTRACT

Secure data transmission is a critical issue in wireless sensor networks (WSNs) in which Clustering is an effective and practical way to enhance the system performance. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically for secure and efficient transmission of data. There are 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 and 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 results shows that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.