Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks

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.
EXISTING SYSTEM:

Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network’s clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH, and RLEACH.

DISADVANTAGES OF EXISTING SYSTEM:

- Symmetric key management suffers from a so-called orphan node problem.
- It cannot participate in any cluster, and therefore, has to elect itself as a CH.
- Increases the overhead of transmission and system energy consumption by raising the number of CHs.

PROPOSED SYSTEM:

We propose two Secure and Efficient data transmission protocols for CWSNs, called SET-IBS and SET-IBOOS. It provide feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.
ADVANTAGES OF PROPOSED SYSTEM:

- The proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

- Reduce the computational overhead for security using the IBOOS scheme.

SYSTEM ARCHITECTURE:
System Requirements:

Hardware Requirements:

System : Pentium IV 2.4 GHz.
Hard Disk : 40 GB.
Floppy Drive : 1.44 Mb.
Monitor : 15 VGA Colour.
Mouse : Logitech.
Ram : 512 Mb.

Software Requirements:

Operating system : Windows 7.
Coding Language : C#.net, Asp.net
IDE : VisualStudio 2010