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:

In this Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN.

Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

PROPOSED SYSTEM:

In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, 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.

It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.
In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

**Hardware Requirements:**

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

**Software Requirements:**

- Operating system: - Windows 7 Ultimate (32-bit) / Windows XP
- Coding Language: C#.Net
- Front End: Visual Studio 2008