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 OnlineOffline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Dife-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.

Ecient 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 ecient 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 OnlineOfine 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 ecient 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.

Modules

1. SET Protocol

2. Key management for security

a. Neighborhood authentication

b. Storage cost

c. Network scalability

d. Communication overhead

e. Computational overhead

f. Attack resilience

Modules Description

SET Protocol

In this module, Secure and Ecient data Transmission (SET) protocol for CWSNs. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher eciency. The proposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We rst introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

Key management for security

In this module, security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, oine signing, online signing and verications.

Key management

In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security. • Neighborhood authentication

In this module, used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, “limited” means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.

Storage cost

In this module, represents the requirement of the security keys stored in sensor node’s memory.

Network scalability

In this module, indicates whether a security protocol is able to scale without compromising the security requirements. Here, “comparative low” means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network.

Communication overhead

In this module, the security overhead in the data packets during communication.

• Computational overhead

In this module, the energy cost and computation eciency on the generation and verications of the certicates or signatures for security.

Attack resilience

In this module, the types of attacks that security protocol can protect against.

System Requirements

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