Chapter 2
Secure and Energy-Efficient Routing for Cluster-Based Wireless Sensor Networks

Meenakshi Tripathi
Malaviya National Institute of Technology, India

M. S. Gaur
Indian Institute of Technology Jammu, India

Vijay Laxmi
Malaviya National Institute of Technology, India

Ramesh Battula
Malaviya National Institute of Technology, India

ABSTRACT

Security is a prime concern in the resource constrained wireless sensor networks. Traditional cryptographic mechanisms cannot be used with these networks due to their limited battery. Clustering is one of the popular methods to improve the energy efficiency of WSN. In this chapter, the authors propose a secure routing protocol for cluster-based wireless sensor networks. A hierarchical topology is formed by the base station, which is also responsible for distributing the cryptographic keys among the nodes. Security analysis of the proposed protocol is done against various security attacks. The efficiency of the proposed protocol is explained through mathematical calculations and simulations. The proposed protocol also performs better than other existing secure protocols for cluster-based WSN regarding battery life and security overhead.

INTRODUCTION

Technological advancement coupled with the reduced cost of Micro-Electro-Mechanical Systems (MEMS) components is driving organizations to design smaller wireless products such as miniaturized sensors, actuators etc. Huge manufacturing and miniaturization are making them popular even for the smallest device such as a smartphone now may consist of the motion detector, thermometer, pressure sensor, etc.

DOI: 10.4018/978-1-5225-5736-4.ch002

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
In most of the applications, MEMS components are connected through infrastructure-less networks due to economic or geographical constraints. MEMS devices need to connect to each other through automatic configuration while providing the required services. This kind of set-up will result in a powerful network called Wireless Sensor Network (WSN). This network works in ‘ad-hoc’ mode that means various components of the network communicate with each other via radio links only without the use of any pre-existing infrastructure. All the devices forward the data to other devices. The ad-hoc mode allows these networks to set up anywhere, at any time with less cost. Ease of deployment of such network makes them suitable for various emergency applications like natural disaster prevention, enemy vigilance, forest fire detection, etc. In most of these applications, sensors are deployed in an unattended and trustless environment, which makes them vulnerable to various security attacks. Hence, efficient and secure data transmission becomes one of the most fundamental requirements for such kind of real-time WSNs.

**RELATED WORK AND MOTIVATION**

Limited and Irreplaceable batteries make energy conservation at sensor nodes as a crucial design issue for WSN. This becomes important as network lifetime mainly depends upon the energy consumption at sensor nodes. Clustering is a technique that can effectively reduce the energy consumption of sensor nodes and has been widely used in WSNs for data gathering and routing. A variety of clustering protocols have been proposed to address the energy efficiency problem in different network scenarios. Clustering protocols must be designed by appropriately selecting cluster heads to achieve load balancing and hence energy efficiency. LEACH (Low Energy Adaptive Clustering Hierarchy) and LEACH-C (Centralized LEACH) protocols (Heinzelmann, Chandraksan, & Balakrishnan, 2000; Heinzelmann, Chandraksan, & Balakrishnan, 2002) are widely known clustering protocols for two-tiered wireless sensor networks which minimize the energy consumption. LEACH-C is a kind of improved LEACH. This research work has expanded on the LEACH-C protocol to improve wireless sensor networks energy efficiency and security.

Although WSN shares lots of similarity with other traditional wireless networks so the basic security requirements like confidentiality, integrity, authentication, and availability (Carman, Krus, & Matt, 2000; Perrig, Stankovic, & Wagner, 2004) are same as of those networks. However, due to the limited resources, it is hard to apply the traditional security measures with WSNs. Various applications like military or healthcare, a WSN carries sensitive information that helps in making critical decisions. In these scenarios, any interruption in the flow of information may even lead to threats for human lives. So they require a high level of security. An increase in the level of security consumes more resources, this may badly affect the lifespan of the network. Hence, WSN requires high security with minimum usage of resources to ensure the secure data transfer.

There are some existing security protocols based on LEACH, such as SLEACH (Perrig et.al., 2001, Ferreira et. al., 2005), GS-LEACH (Banerjee, Jacobson, Lahiri, 2007), SecLEACH (Oliveira et. al., 2007), LS-LEACH (Alshowkan, Elleithy, & Alhassan, 2013) and SSLEACH (Kumar & Umanakeswari, 2016). Most of these protocols use the symmetric key encryption for security and increase the storage cost as well as the cost of communication. Which in turn decreases the lifespan of the resource constraint WSN. A secure WSN routing based on secure data aggregation technique was also proposed (Rahayu, Lee, & Lee, 2015) but the energy consumption of this protocol is higher than the other existing protocols.

The proposed protocol incorporates efficient encryption and MAC (Message Authentication Techniques) schemes to increase the overall lifetime of the WSN.
21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product’s webpage: www.igi-global.com/chapter/secure-and-energy-efficient-routing-for-cluster-based-wireless-sensor-networks/203779?camid=4v1


Related Content

Handling the Dataflow in Business Process Models
www.igi-global.com/chapter/handling-the-dataflow-in-business-process-models/198255?camid=4v1a

A Proactive Defense Strategy to Enhance Situational Awareness in Computer Network Security
www.igi-global.com/chapter/proactive-defense-strategy-enhance-situational/62375?camid=4v1a

The Future of National and International Security on the Internet
www.igi-global.com/chapter/the-future-of-national-and-international-security-on-the-internet/114375?camid=4v1a

Privacy and Security in the Age of Electronic Customer Relationship Management
www.igi-global.com/article/privacy-security-age-electronic-customer/2457?camid=4v1a