IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB11708

This chapter appears in the book, *Web and Information Security*
edited by Elena Ferrari and Bhavani Thuraisingham © 2006, Idea Group Inc.

Chapter XII

Framework for Secure Information Management in Critical Systems

Rajgopal Kannan, Louisiana State University, USA

S. Sitharama Iyengar, Louisiana State University, USA

A. Durresi, Louisiana State University, USA

Abstract

The techniques described in this chapter will develop an understanding of three critical areas in sensor network security, namely, data confidentiality, anonymity, and integrity along with associated security-performance tradeoffs. These results should contribute toward the design of a security framework for a common sensornet architecture and enable the flexible deployment and use of sensor networks for a large variety of applications, including homeland security.

Introduction

The IT revolution has led to the development of sophisticated information systems that play a crucial role in the national economy. These information systems are not stand-alone; rather, they are fully distributed with connectivity through a mix of heterogeneous networks, for example, sensor networks, wireless and cellular networks, mobile and distributed systems, along with the Internet. Figure 1 illustrates a typical information system consisting of wireless sensor networks for gathering data, which is then transmitted to data processing sites over a wired backbone.

The changing trends in information management, diverse user information needs, and the widespread use of the Internet coupled with significant advances in hacking technology has made it crucial to shield information systems by developing robust trust and security schemes. Our information systems are characterized by the vast amounts of data generated continuously by their components, especially the large and easily deployable networks of small autonomous devices, and transported toward processing and dissemination centers. This whole process is vulnerable to serious security threats at various levels. Consequently, a major technical challenge is to design security solutions for managing this data over such heterogeneous environments.

Current research efforts are focused on solving the problem of data security in large information systems in an ad hoc or patchy manner. Such efforts do not

Figure 1. Information security mechanisms