A Certificate-Based Secure Communication Protocol For Wireless Sensor Networks

A thesis submitted to The University of Manchester for the degree of Master of Science in the Faculty of Engineering and Physical Sciences

2007

Jian Song

School of Computer Science
Abstract

Wireless sensor network (WSN) is a new generation of wireless network, which uses numerous tiny sensors to sense, gather and process information from monitored objects in surveillance areas. Because of predominant characteristic of WSNs, they are widely used in fields of national defence, agriculture, manufacturing, construction, and home.

However, limited capacity of sensor devices brings latent threats of security and insecure factors for WSNs. Therefore, how to protect WSNs from attacks and how to improve security for WSNs are key issues currently in this area. This project is aimed at finding resource-aware self-adaptive security provisioning schemes for a home-care wireless sensor network, and designs and implements improved security architecture from existing schemes.

Security in WSNs is required for four features which are confidentiality, integrity, availability and authentication. This project proposes a new application layer – Certificate-Based Secure Communication (CBSC) protocol. The CBSC protocol is modified from a SPKI/SDSI security protocol, and it provides remote distribution of security mechanisms, fast re-authentication and secure communications for wireless sensor networks.