
Jing Zhang

College of Electronic Engineering Huaihai Institute of Technology, Lian yungang, China
JingZhang112@tom.com

Abstract. Wireless sensors networks (WSNs) consist of a number of sensor nodes connected through a wireless network that detect data and relay the detected data to the sink node using the multi-hop wireless transmission. Now, one of the most important issue is how to implement critical security tasks such as intrusion or tamper detection, and therefore must be protected. In this paper, we first analyse the security challenges in the wireless sensor network from the application layer, transport layer, network layer, data link layer and physical layer based on the system model. Then we give the security strategy which usually used in wireless sensor networks from the key management, security routing, security integration, intrusion detection and confidence model. This strategy can ensure the data confidentially implement, reliably generate, efficiently integrate and securely transmit.

Keywords: wireless sensor networks (WSNs), security strategy, key management, security routing, security integration, intrusion detection.

1 Introduction

A wireless sensors networks (WSNs) [1] consist of a number of sensor nodes connected through a wireless network that detect data and relay the detected data to the sink node using the multi-hop wireless transmission. The applications of a wireless sensor network can be used in monitoring disaster areas, monitoring patients, assisting disabled patients, helping the military, remote virtual measurement and so on.

Wireless sensor network as a task-based network is not only for data transmission, data, but also for data collection and integration, cooperative control etc. It is an important issue to ensure the data for confidentially implement, reliably generate, efficiently integrate and securely transmit. In order to ensure the confidentiality and security, WSNs need implement some basic security mechanisms: confidentiality, point to point message authentication, integrity, freshness, authentication broadcasting and security management.

In recent years, more and more people are engaged in wireless sensor network security technology. Eschenauer and Gligor [2] proposed a distributed sensor network key management scheme, which including three processes of key pre-distribution, shared key discovery and path key establishment. Chan etc [3] put forward a random
key pre-distribution scheme for a sensor network which have three security mechanisms: First is has q composite key management scheme; second, multi-path key to strengthen the program; third is random key distribution scheme. Jolly etc [4] put forward an energy-efficient key management protocol which based on the IBSK scheme. Perrig etc [5] proposed a sensor network security protocol SPINS, which consists of two parts: SNEP (secure network encryption protocol) by using the counter and the message authentication code to provide data confidentiality, authentication and freshness and so basic security mechanism, but it can not provide efficient broadcast authentication; uTESLA( (micro timed efficient streaming loss - tolerant authentication protocol) is an extended form of TESLA which can provide broadcast authentication. Ren [6] given a detection methods to ensure the safety of the MACL program, but this program is only the ability to resist passively. J. Deng etc [7] proposed a new secure routing protocol, namely, INSENS (Intrusion-tolerant routing in wireless sensor networks),which is able to tolerate attacks.

In this paper, we first analyse the security challenges in the wireless sensor network from the application layer, transport layer, network layer, data link layer and physical layer based on the system model. Then we give the security strategy which usually used in wireless sensor networks from the key management, security routing, security integration, intrusion detection and confidence model. This strategy can ensure the data confidentially implement, reliably generate, efficiently integrate and securely transmit.

2 System Model

A. Network Model

In this work, we consider the wireless sensor networks where all nodes in the network are homogenous and energy constrained. In order to convenient describe, we assume that the network is a two-tier structure rather than multi-level topology, namely, the entire wireless sensor network is divided into many clusters, each cluster has a cluster head and lots of member nodes. The communication of cluster members with cluster head, cluster heads with base station are the single-hop, the information which apperceived by menmber nodes directly send to the cluster head, then forwarded to the base station by cluster head. Base station can directly send commands and control information to all nodes which do not through the cluster head.

Cluster head implements periodic election, when a node to becomes cluster head, it not only shoulder the task of data fusion and forwarding, but also still able to perform cognitive tasks.

We assumed that all sensor nodes are the same and have the same initial energy, base station determines the selection of cluster head and has enough storage capacity, processing power and energy, and can store all nodes information.

B. Energy Model

We adopt a simplified power model of radio communication in document [8], namely, in order to send a k-bit packet information and the sending distance is d, the sending energy consumption is