Wireless Sensor Networks

M

Homero Toral-Cruz
University of Quintana Roo, Mexico

Faouzi Hidoussi
University Hadj Lakhdar of Batna, Algeria

Djallel Eddine Boubiche
University Hadj Lakhdar of Batna, Algeria

Azeddine Bilami
University Hadj Lakhdar of Batna, Algeria

Miroslav Voznak
VSB-Technical University of Ostrava, Czech Republic

Sergej Jakovlev
Klaipeda University, Lithuania

INTRODUCTION

Wireless sensors network have been recognized as one of the emerging technologies of the 21st century (Duan et al., 2006; Nassr et al., 2007). WSN consists of several sensor nodes that collect data in inaccessible areas and send them to the base station (BS) or sink after initial processing (Akyildiz et al., 2002-1).

The architecture of protocol stack used by the base station and sensor nodes (Akyildiz et al., 2002-2), integrates power and routing awareness (i.e., energy-aware routing), integrates data with networking protocols (i.e., data aggregation), communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes (i.e., task management plane). The sensor network protocol stack is much like the traditional protocol stack (Maraiya et al., 2011).

WSNs have various applications; examples include *military applications, environmental monitoring, medical application, home application, industrial* and *commercial application*.

WSNs are deployed in physical harsh and hostile environments where nodes are always exposed to physical security risks damages (Alrajeh et al., 2013). In WSNs, one of the most important constraints is the low power consumption requirement. Sensor nodes carry limited, generally irreplaceable, power sources. Therefore, they must have inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay (Akyildiz et al., 2002-1). In order to acquire energy efficiency, various hierarchical or cluster-based routing methods, originally proposed in wire networks, are well-known techniques with special advantages related to scalability and efficient communication.

In a hierarchical architecture, higher energy nodes can be used to process and send the information, while low-energy nodes can be used to perform the sensing in the proximity of the target. The creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency. The main aim of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication. Cluster formation is typically based on the energy reserve of sensors and sensor's proximity to the cluster head. Several cluster-based routing protocols are proposed in the literature such as LEACH (Heinzelman et al., 2002), TEEN (Lee et al., 2013), APTEEN (Manjeshwar and Agrawal, 2002), HEED (Younis and Fahmy, 2004), PEGASIS (Lindsey et al., 2002) and HEEP (Boubiche et al., 2011). Where LEACH is one of the first hierarchical routing approaches for sensors networks.

DOI: 10.4018/978-1-4666-5888-2.ch575

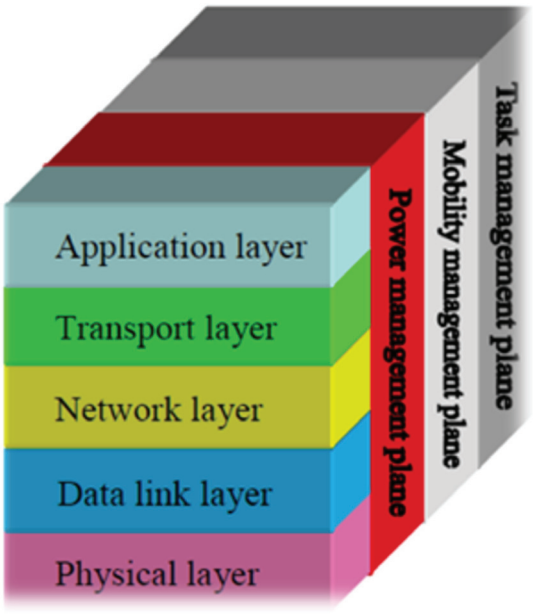
Additional to the energy constraint, most of WSNs are vulnerable to many types of security attacks due to open wireless medium, multi-hop decentralized communication, and deployment in hostile and physically nonprotected areas (Alrajeh et al., 2013). Based on (Karlof et al., 2003) research, we can classify routing attacks into six categories: *sink hole attack, black hole attack, selective forwarding, sybil attack, hello flood attack and misdirection.*

In addition to energy efficiency and security there still exist some other open research issues, such as: *integration of sensor networks and the Internet, WSNs in challenging environments WUSNs & UWSNs).*

BACKGROUND: ARCHITECTURE OF PROTOCOL STACK

The protocol stack is a combination of different layers and consists of the physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane and task management plane. Each layer has a set of protocols with different operations and integrated with other layers. The protocol stack used by the sink and sensor nodes is shown in Figure 1.

Figure 1. The WSN protocol stack



Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. The physical layer presents many open research issues that are largely unexplored, such as: modulation schemes, strategies to overcome signal propagation effects and hardware design (Kifayat et al., 2010).

Data Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, and medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network. The data link layer is combination of different protocols includes: medium access control (*MAC*) and *error control*.

Network Layer

The network layer is to provide Internetworking with external networks like other sensor networks, in one scenario, the sink nodes can be used as a gateway to other networks. The network layer in a WSN must be designed with the following considerations in mind: power efficiency, WSNs are data-centric networks WSNs have attribute-based addressing and sensor nodes are location aware.

Transport Layer

The transport layer comes into play when the system needs to communicate with the outside world. Transmitting data from sink to outside user is a problem because WSNs do not use global identification and attribute based naming is used for sending the data. Very little research has been done at the transport layer.

Application Layer

The Application layer contains the logic required for data acquisition and processing. A simple application might measure quantities such as temperature, humidity or luminosity in regular intervals and forward the data to a sink node. Other applications might also process measured data, serve data requests or send messages in