

Chapter 4

An Efficient Channel– Aware Aloha–Like OFDMA–Based Wireless Communication Protocol for IoT Communications in Wireless Sensor Networks

Elias Yaacoub
Arab Open University, Lebanon

ABSTRACT

Wireless sensor networks consisting of several sensors deployed in a given area, under an internet of things (IoT) paradigm, are considered. Sensor nodes may or may not be close enough to communicate with each other in order to perform collaborative transmissions. A communication protocol based on random access and orthogonal frequency division multiple access (OFDMA) is proposed in order to allow the sensors to operate autonomously by transmitting their measured data to a central processing system, where it is processed and analyzed. Whenever it has data to transmit, each sensor independently accesses a time-frequency slot in a probabilistic manner to avoid collisions. A controlling entity, e.g., a central base station (BS) covering a certain sensor deployment area receives the sensor transmissions and provides synchronization information by periodically transmitting a pilot signal over the available OFDMA subcarriers. Sensors use this signal for channel quality estimation. Results show that this approach performs well in terms of transmission data rates and collision probability.

1. INTRODUCTION

The Internet of Things (IoT) is expected to be a key enabler for smart cities, where sensor and actuator devices will be ubiquitous and will monitor every aspect of our lives (Ejaz et al., 2017). With the billions of devices expected to be deployed under the IoT paradigm, next generation cellular networks are

DOI: 10.4018/978-1-5225-2845-6.ch004

expected to face enormous challenges (Chen, 2012). In fact, they need to be able to support this large number of devices through the use of machine-to-machine (M2M) communications. The quality of service (QoS) requirements of IoT devices are expected to be varying and different, depending on the purpose for which each device was designed. Thus, these devices will affect the network in different ways since they will have different behaviors. For certain devices, the network will need to be accessed in a frequent and periodic manner for the sake of transmitting small amounts of measurement data. This would be the case in advanced metering infrastructure (AMI) where smart meters deployed in a smart grid setup would be sending their data (Yaacoub & Kadri, 2015). In other scenarios, it could be possible for devices to temporarily store their measured data and then transmit the stored data in bulk later on. A typical example would be the case of sensor networks deployed for monitoring the environment (Lloret et al., 2015). Indeed, the IoT will significantly consist of wireless sensor networks (WSNs) comprising a number of sensor nodes (SNs) that capture certain information and then transmit it wirelessly over the network (Mainetti et al., 2011). WSNs have a broad spectrum of applications. They can be used in intelligent transportation systems for road safety purposes, in military applications for border control and surveillance, and in environmental applications for the sake of air pollution monitoring, detection of water pollution, smart agriculture, etc. (Vieira et al., 2003).

An SN is, in most cases, an autonomous device that comprises: a sensing unit to measure the required data, a processing unit to process and (temporarily) store the measured information, a communication unit to transmit the data over the network, and a power unit to provide power for the device. Generally, the most important limiting factor for the operation of an SN is power consumption, since it is expected to operate for extended periods in areas where power infrastructure could be absent. Consequently, SNs should have the capability to perform their intended tasks with very low power consumption. Certain SNs can be powered by batteries that benefit from energy harvesting from the environment and thus, for example, can use solar power to replenish their energy, which allows them to operate autonomously for a longer time. Energy saving can also occur via the wireless communication unit. In fact, short range ad-hoc communication between SNs in a WSN via multihop communications can prove to be more energy efficient than a single hop long distance transmission to a base station (BS) or access point (AP) (Vieira et al., 2003).

In this Chapter, a wireless communication protocol for WSNs is presented and analyzed. It is an extension of the protocol presented in (Yaacoub et al., 2011) in order to apply it in various WSN scenarios. The presented protocol deals with the communication between SNs and APs or BSs. It is however applicable to scenarios where multihop communications take place in WSNs. In such scenarios, SNs communicate with each other over multihop links using a pre-defined communication protocol, and the SN at the last hop communicates with the BS by relaying the aggregated multihop data using the approach discussed in this Chapter. The presented protocol enables SNs to communicate efficiently with an AP by operating autonomously in different parts of the cell area covered by the BS or AP. It is a channel aware extension of slotted reservation Aloha to orthogonal frequency division multiple access (OFDMA) systems.

The chapter is organized as follows. Section 2 presents the relevant background/literature review. The proposed approach is presented in Section 3. Simulation results are presented and analyzed in Section 4. Finally, in Section 5, conclusions are drawn and future research challenges are outlined.

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/an-efficient-channel-aware-aloha-like-ofdma-based-wireless-communication-protocol-for-iot-communications-in-wireless-sensor-networks/186902

Related Content

Security Evaluation of Service-Oriented Systems Using the SiSOA Method

Christian Jung, Manuel Rudolph and Reinhard Schwarz (2011). *International Journal of Secure Software Engineering* (pp. 19-33).

www.irma-international.org/article/security-evaluation-service-oriented-systems/61151

Characteristics of Analysis Methods for the Impression Evaluation Method by Space

Shunsuke Akai, Teruhisa Hochin and Hiroki Nomiya (2016). *International Journal of Software Innovation* (pp. 65-77).

www.irma-international.org/article/characteristics-of-analysis-methods-for-the-impression-evaluation-method-by-space/157280

Empowering Microfinance Processes through Hybrid Cloud Based Services

Tagelsir Mohamed Gasmelseid (2015). *International Journal of Systems and Service-Oriented Engineering* (pp. 1-17).

www.irma-international.org/article/empowering-microfinance-processes-through-hybrid-cloud-based-services/134431

Liveness, Deadlock-Freeness, and Siphons

Kamel Barkaoui (2013). *Embedded Computing Systems: Applications, Optimization, and Advanced Design* (pp. 65-78).

www.irma-international.org/chapter/liveness-deadlock-freeness-siphons/76950

Covert End User Development: A Study of Success

Elaine H. Ferneley (2009). *Software Applications: Concepts, Methodologies, Tools, and Applications* (pp. 736-742).

www.irma-international.org/chapter/covert-end-user-development/29419