Chapter 10
IP Connected Low Power Wireless Personal Area Networks in the Future Internet

Rune Hylsberg Jacobsen
Aarhus School of Engineering, Denmark

Thomas Skjødeberg Toftegaard
Aarhus School of Engineering, Denmark

Jens Kristian Kjærgaard
Tieto, Denmark

ABSTRACT

The Internet of Things is a key concept of the Future Internet. The Internet of Things potentially interconnects billions of small devices in a large ubiquitous infrastructure based on the Internet Protocol (IP). Typically, these devices will be limited in computational capacity, memory, and available energy and will suffer a high data loss rate when integrated into a network infrastructure. This poses significant challenges in the network design. This chapter describes the assumptions, technologies, and challenges for transmitting IPv6 over low power wireless personal area networks (LoWPANs). The authors address the key mechanisms from network aspects down to device design aspects and discuss how technologies interplay to make real application deployment practical for the Internet of Things.

INTRODUCTION

The Future Internet extends the current Internet from the communication between humans to the communication between humans and the surrounding devices such as small sensors. The Future Internet will use the Internet Protocol (IP) as the foundation for communications. The IP protocols will serve as the common denominator from large systems to small devices by allowing interaction between networks build from different underlying transmission technologies – wired as well as wireless – and by reusing protocol layer implementations across different platforms. With IP as the unifying internetwork technology the number of communication translations reduces

DOI: 10.4018/978-1-4666-0203-8.ch010

from an *N*-*N* question to an *N*-1 question. There will still be a need for gateways in the Future Internet to cope with different network technologies and network characteristics, but by having IP as a common conceptual framework large economic savings will be provide in a global perspective.

Wireless sensor networks have evolved from the idea that small wireless devices distributed over large geographical areas can be used to collect information from the physical environment in many situations such as e.g. environmental and industrial monitoring. On the node-level, challenges result from the limited available resources. The handling of the unreliable networks and the large size of the networks becomes especially challenging when these sensors are interconnected.

Different wireless protocols have evolved for personal area networks and sensor networks as e.g. Z-wave, Bluetooth and Zigbee, and until recently the perception has been that a full-fledged IP stack was too large and complex to implement in small devices. However, based on the standardisation work in Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineer (IEEE) the foundation for realising IP in a small device domain has been made. Several research projects have shown that it is possible to realise sensor nodes with a fully functional IPv6 stack (Mazzer and Tourancheau, 2008).

In this chapter, we address the key concepts of low power wireless area personal network (LoWPAN) and demonstrate how efficient support for IPv6 over IEEE 802.15.4 links can be achieved. We explain the basis for IPv6 networking and we discuss how benefits of IP technology can be applied to limited, unreliable devices in the Future Internet. Throughout the chapter we discuss technologies and protocols in the context of sensor networks since these are the main applications of LoWPAN devices. Furthermore, we address the main building blocks for LoWPAN device designs, and we conclude the chapter by outlining future directions of work in the area.

BACKGROUND

During the past few years Future Internet has been on the research agenda on a European level (European X-ETP Group, 2010). Future Internet research has chosen a holistic perspective by taking into account all building blocks from users, services and applications down to the networks. Information and communication technology are becoming smarter, smaller and faster; and, at the same time, society is progressively becoming more densely connected. As a result, Internet supported services are entering a new phase of mass deployment which brings a large number of new opportunities; but also challenges in terms of scalability, capacity, throughput, mobility and security etc.

A main strategic challenge for the European Future Internet initiative is the concept of Internet of Things. At the network level, there is no global architecture for the Internet of Things, and there is still an ongoing debate on how much intelligence shall be distributed to the edge of the networks instead of a more centralised approach (Islam and Grégoire, 2010). Despite this ongoing debate several attempts to define the Internet of Things concept can be found in the literature. As an example Atzori, Iera, and Morabito (2010) describes Internet of Things as a world-wide network infrastructure of interconnected objects that are uniquely addressable and that communicate by using standard protocols.

To make the Internet of Things vision a reality, several key technologies must be developed and deployed. A number of leading radio device manufacturers have implemented wireless communication standards targeting a widespread use in embedded applications, such as control network, home automation and sensor networks. These applications generally require numerous low-cost nodes communicating over multiple hops to cover a larger geographical area. Furthermore, nodes must be able to operate unattended for