Security and self-organizing mechanisms for the Internet of Things

Axel Moinet & Benoit Darties
Laboratory Le2i - CNRS UMR 6306
axel.moinet@u-bourgogne.fr

Abstract

The last ten years have seen the development of mobile technologies, from smartphones to everyday life connected devices and cloud computing. In this context, Wireless Sensor Networks (WSN) have emerged from specific industrial applications to everyone. These networks encounter routing and organization issues, especially in the context of the IoT, where needs and resources between devices are different. This paper introduce the experimentation testbed we are deploying to check routing and topology correctness of simulations and research work, using the 802.11s mesh network protocol as a base.

1. Overview, the "Future Internet"

Networking technologies have grown to many subdomains, from Cloud computing to Wireless Sensor Networks (WSN) and even social networks relying persons. The "Future Internet" is the main term to refer to all interconnections between these networks.

In these interconnections, the IoT is the branch which integrates WSNs to end user cloud-based applications. A middleware is used between the cloud and WSNs, providing the application with information about and interaction with the environment. It can be a particular environment, like a house or office, or a more global environment, as an entire country.

We focus our research on organization and routing inside WSNs, the root part of the IoT. Globally, network dimensioning is a recurrent problem in WSN, as node number and evolutivity of the network topology causes routing and network map construction issues.

2. Adaptable networking inside WSNs

Wireless Sensor Networks are build up by low power and low resources heterogenous devices. Since these devices have different purpose, they also have different material architecture and resources levels. Energy and computing resources are a main concern in this field, because sensors don't have a fixed power supply, making batteries the energy supplier for all device lifetime. Moreover, devices may be mobile, and they may become defective [2].

Mutable networks are one approach to these concerns. The main principle is to allow devices to spread in the network when they need. This way, each device energy saving and resource control policies will be able to manage connection time, to save power and/or computing time. This also resolves the mobility and defectivity issues, by making no node absolutely necessary in the network. Thus, the organization of devices inside the network must be evolutive, but still secure [2].

The most efficient way of building mutable networks is to use a mesh networking infrastructure, which provides connection with neighbouring nodes. Since some theoritical and simulation research work have already been made in this domain, we choose an experimental approach.

2.1. Testbed

We currently are deploying a testbed aimed at testing multi-hop communications in a network composed of heterogeneous nodes, in real conditions. The short-term objective is to have an experimentation platform, allowing us to exceed simulators limits. This will also help us to characterize security, energy and computing costs for different strategies and topologies, in real conditions. We choose 802.11s as the mesh protocol inside our network, because it as many advantages. First, it allows us to easily modify or implement our own routing protocol and strategies. Second, it provides standardized high-security connectivity mechanisms [1]. And it also has the advantage to be implemented in the Linux kernel since the IEEE ratified the standard.

Our testbed will be composed of four different devices with different architectures and resources: ARM Cortex-A8, ARM Cortex-A5, ARMv6 1176jzf-s and ARM Cortex-A7.

References

[1] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke. IEEE 802.11s: The WLAN Mesh Standard. *IEEE Wireless Communications*, 17(1):104–111, 2010. 1

[2] D. Kyriazis and T. Varvarigou. Smart, Autonomous and Reliable Internet of Things. *Procedia Computer Science*, 21:442–448, Jan. 2013. 1