DOCTORAL THESIS

Efficient IoT Framework for Industrial Applications

Pablo Puñal Pereira

Industrial Electronics

LULEÅ
UNIVERSITY
OF TECHNOLOGY

Efficient IoT Framework for Industrial Applications

Pablo Puñal Pereira

EISLAB
Luleå University of Technology
Luleå, Sweden

Supervisors:

Jens Eliasson and Jerker Delsing

Printed by Luleå University of Technology, Graphic Production 2016

ISSN 1402-1544
ISBN 978-91-7583-665-2 (print)
ISBN 978-91-7583-666-9 (pdf)

Luleå 2016

www.ltu.se

To my family

Abstract

The use of low-power wireless sensors and actuators with networking support in industry has increased over the past decade. New generations of microcontrollers, new hardware for communication, and the use of standardized protocols such as the Internet Protocol have resulted in more possibilities for interoperability than ever before. This increasing interoperability allows sensors and actuator nodes to exchange information with large numbers of peers, which is beneficial for creating advanced, flexible and reusable systems.

The increase in interoperability has resulted in an increase in the number of possible attacks from malicious devices or users. For this reason, the use of encryption techniques to protect client and server communications has become mandatory. However, even with state-of-the-art encryption mechanisms, there is no protection that can control access to each particular service with fine-grained precision. The nodes within an industrial network of wireless sensors and actuators are resource-constrained embedded devices, and increasing interoperability therefore requires a higher level of computation capabilities. The nodes' intrinsic limitations of memory and processing exert an adverse effect on power consumption and communication delays, resulting in a shorter battery lifetime. Therefore, the standard computing solutions for Internet communications are not directly applicable, and new mechanisms to achieve security, scalability, dependability, interoperability and energy efficiency are needed.

Sensor and actuator networks can transmit sensed data, but they also offer access to the actuators. Such accesses, presumably provided via services, require an access protection scheme. For this reason, the use of access control mechanisms is mandatory. Access control assists in the creation of customized services and access policies. These access policies can isolate access permissions to devices with different roles, such as production and maintenance.

The main contribution of this thesis is a novel, efficient IoT framework for industrial applications, including design, implementation, and experimental validation. The framework includes features for communication protection, authentication, fine-grained access control, zero-configuration networking, and run-time reconfiguration. These technologies and their corresponding energy consumption data clearly demonstrate the feasibility of integrating a battery-operated IoT concept into a functional System of Systems. The provided data also pinpoint the most critical areas for improvement.

Contents