

Efficient IoT Framework for Industrial Applications

Pablo Puñal Pereira

Industrial Electronics



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

Part I	1
CHAPTER 1 – INTRODUCTION	3
1.1 Problem formulation	4
1.2 Methodology	5
1.3 Thesis scope	6
1.4 Thesis outline	6
CHAPTER 2 – INTERNET OF THINGS	9
2.1 Historical (r)evolution	10
2.1.1 Software	10
2.1.2 Hardware	13
2.2 Wireless Sensor and Actuator Networks	14
2.3 Constrained Application Protocol	15
2.4 Service Oriented Architecture (SOA)	17
CHAPTER 3 – SECURITY	19
3.1 Secure communications	19
3.1.1 Standard end-to-end security mechanisms	21
3.1.2 Access control analysis	21
3.2 Access control	22
3.2.1 Standard solutions	22
3.2.2 Ticket-based access control	24
3.2.3 Alternatives under development	37
CHAPTER 4 – EFFICIENT INDUSTRIAL IOT FRAMEWORK	39
4.1 Network architecture	40
4.2 Services	42
4.2.1 Bootstrapping	42
4.2.2 Configuration	43
4.2.3 Device management	45
4.2.4 Authentication and authorization	45
4.3 Case studies	45
4.3.1 Mobile machinery monitoring	45
4.3.2 Smart rock bolts	45
4.4 Experiments and results	47
4.4.1 Test setup	47
4.4.2 Results	47

4.4.3 Summary	48
CHAPTER 5 – CONTRIBUTIONS	55
CHAPTER 6 – DISCUSSION	59
6.1 Conclusions	62
6.2 Future work	64
REFERENCES	65

Part II 71

PAPER A	73
1 Background and Related work	75
2 Architecture	77
3 Performed experiments	80
4 Results	82
5 Future work	86
6 Conclusion	87
7 Acknowledgment	88
PAPER B	93
1 Introduction	96
2 Background	99
3 EXI Processor Design and Implementation	106
4 EXI data binding	117
5 CoAP/EXI/XHTML Web page engine	118
6 Conclusions	121
2A Acknowledges	125
PAPER C	131
1 Introduction	133
2 Background and Related work	135
3 Framework	138
4 Authentication Process	140
5 Security Analysis	143
6 Experiments and results	144
7 Future work	146
8 Conclusion	146
9 Acknowledgment	147
PAPER D	149
1 Introduction	151
2 Background and Related Work	152
3 Problem Definition	154

4	Proposed Solution	156
5	Application Scenario	159
6	Implementation and Results	161
7	Conclusion	163
8	Future Work	164
9	Acknowledgment	164
PAPER E		167
1	Introduction	169
2	Related work	173
3	Proposed approach	173
4	Use cases and evaluation	178
5	Discussion	183
6	Conclusion	183
7	Future work	183
8	Acknowledgment	184
PAPER F		187
1	Introduction	189
2	Background and Related work	190
3	Network infrastructure	193
4	System Architecture	195
5	Results	197
6	Discussion	201
7	Future work	202
8	Conclusion	202
9	Acknowledgment	203
PAPER G		207
1	Introduction	209
2	Background and Related work	210
3	Proposed Industrial IoT framework	212
4	Test and Results	219
5	Discussion	224
6	Future work	225
7	Conclusions	225
8	Acknowledgment	226