Intelligent Energy Usage via M2M Communication

Short version

Rune Torbensen
rto@cfsi.dk

PhD, Aalborg University

Outline

PhD project work
  Home Automation
  Communication
  Cooperation
  Security

M2M Project Ideas

Conclusion

References
Outline

PhD project work
  Home Automation
  Communication
  Cooperation
  Security

M2M Project Ideas

Conclusion

References
Current Home Automation

Home automation has not become mainstream yet

Few complete smart house installations
  ▶ Building automation in the residence
  ▶ Installed by experts
  ▶ Predominantly wired and centralized (control)
  ▶ Components are expensive and variety is limited
  ▶ No dominating standard in foreseeable future

Subsystems are available
  ▶ Limited market share
  ▶ Islands of functionality
  ▶ Unable to interoperate with the outside
Future Home Automation

All electronic devices in the residence can cooperate as services

- Consumers may easily compose a system out of products
- Easy to install and use
- Remote access for smartphone

Many vendors, No lock-in

- Product-by-product purchasing
- Product variety
- Possibility to compete on price, quality and functionality

Distributed control scheme

- Many small controllers
- Ad hoc discovery of services
- Sensors reused for many controllers (applications)
Communication Challenges

*Based on taxonomy of protocols for home networks*

Communication methods
- Control wires are costly to install in existing houses
- Power line is immature and unreliable due to noise
- Low-power Short Range Wireless (SRW)

Focus on SRW technology
- Flexibility and refitting to existing buildings
- Well suited for battery powered devices
- Many useful but incompatible technologies
- Physical: bandwidth, frequencies, modulation, etc.
- Reliability problems due to wall penetration

Full home coverage
- Multi-hop routing are immature solutions
- Repeaters are impractical and often unsupported (disruptive)
Interoperable Home Automation Platform

An architecture to connect different networks into one heterogeneous network covering the whole residence

- Using IP as common protocol
- End-devices visible as IP devices
- Controllers on IP
- End-to-end communication
- Generic distributed communication infrastructure
- IP room bridges
- Expandable via adapter modules
Cooperation Challenge

Based on market actor and technology analysis

Many different applications, controllers, end-devices
  ▶ Number of applications growing over time (unbounded set)
  ▶ Incompatible service frameworks, message representation
Standard applications, profiles are predominant
  ▶ Considerable time and cost to introduce new ideas
  ▶ Standardization delay
  ▶ Alliance memberships and licensing costs
  ▶ Limit designs and innovations
A centralized, translator box is not a usable solution
  ▶ Hard to realize in a resource limited system
  ▶ Constitutes a gatekeeper
  ▶ Creates unwanted dependency between actors
  ▶ Inconsistent with concept of a generic infrastructure
Open Device Service Description Language

Enable cooperation between unfamiliar devices

End-devices in IHAP provide a service descriptor

Service description language:

- Description of any design
- Existing devices and profiles
- Legacy support allows bootstrapping the market
- New designs avoids standardization delay
- Supports fast-to-market and innovation in SME

Simple application protocols of home automation end-devices

- Get value or device state
- Send command with a parameter
- Listen for event
Security Challenges

Motivations for security in embedded systems
- Devices control the environment
- Capture and share personal data

Threats from wireless and Internet
- Disruption - system unable to send alarm
- Eavesdropping - undetectable passive data-mining
- Unauthorized access
- Opening of door locks and stealing personal data

Security must be user friendly
- Users often misunderstand difficult operations
- Misconfiguration can breach security
Secure Embedded Exchange Protocol (SEEP)

A secure end-to-end communication protocol

SEEP design philosophy:

- Internet-grade security level
- Optimized for resource-constrained embedded platforms
- Low overhead, short messages, minimal network traffic
- Simple and therefore formally verifiable

A formally verified alternative to SSL for embedded devices
Not required but fully compatible with IHAP
Outline

PhD project work
   Home Automation
   Communication
   Cooperation
   Security

M2M Project Ideas

Conclusion

References
M2M Project Ideas

Intelligent energy usage via M2M communication
- The motivation is energy usage optimization in buildings
- Reduce or move energy consumption

Development of new M2M communication technology
- Connecting systems both locally and remotely via the Internet
- Enable ad-hoc resource sharing and signal exchange
- Report energy usage and errors
- Security and privacy by design
Analysis and Requirements

Energy usage optimization strategies

- Avoiding or postponing energy consumption, store energy
- User involved or automated via M2M communication
- Systems log information and provide overview
- Smartphone interface, website access
- Control systems communicate with utility company server
- Great variety of subsystems by many different vendors

Technology requirements:

- Ad-hoc cooperation and resource sharing
- Retain autonomy of each system
- Heterogeneous network
- Internet access
- Secure communication
Outline

PhD project work
  Home Automation
  Communication
  Cooperation
  Security

M2M Project Ideas

Conclusion

References
Conclusion

M2M communication technology

- Energy usage optimization in smaller buildings
- Embedded devices instead of server, lowers overall system cost
- Connecting heterogeneous environments to the Internet
- Existing products can connect without supporting IP
- Low entry barrier, low development cost for new vendors
- Cooperation is flexible, autonomy is retained
- Data sharing with privacy precautions
- Internet grade secure communication
- Usability, short setup time for installer/owner
Outline

PhD project work
   Home Automation
   Communication
   Cooperation
   Security

M2M Project Ideas

Conclusion

References
References

Relevant published papers:

Future home automation systems


Classification of wireless protocols


Secure embedded communication