A Holistic Solution for Reliable Over-the-Air Software Updates in Large Industrial Plants

Florian Kauer, Florian Meyer, Volker Turau

June 13th, 2017
Motivation

- Industrial Wireless Networks
- Concentrated Solar Power Plants
  - 1,000 - 1,000,000 heliostats
  - Wired → Wireless Field Bus
    ⇒ Cost reduction
- Software maintenance required for
  - Network components
  - Third-party devices
Components

- Motor Controller
- Radio Transceiver
- Control Room
- Radio Gateway
Radio Transceiver

IEEE 802.15.4 Transceiver

RS-485 Bus to Motor

16 Mbytes Flash
How to realize reliable and efficient software updates in such large scale wireless networks?
**Requirements**

- Scalable to thousands of devices
- Suitable for a IEEE 802.15.4 network
  - Low data rate (250 kbit/s)
  - Small packets (< 127 Bytes)
  - Forwarding over multiple hops
- Sufficiently fast
  - Updating the whole plant over night
- Fail-safe
  - Maintain a working system if something goes wrong
Requirements

- Scalable to thousands of devices
- Suitable for a IEEE 802.15.4 network
  - Low data rate (250 kbit/s)
  - Small packets (< 127 Bytes)
  - Forwarding over multiple hops
- Sufficiently fast
  - Updating the whole plant over night
- Fail-safe
  - Maintain a working system if something goes wrong

Deluge

- Fast and efficient data dissemination for multi-hop networks
- Split large file into multiple pages
- Exchange page informations via Trickle algorithm
- Send pages via link-layer broadcasts
- Pages can be redirected before whole file was received
  \[\Rightarrow\] Spatial multiplexing

Coffee File System

- File system abstraction for resource-constraint devices

- Efficient usage of Flash storage
  - Problem: Overwriting data only possible by erasing whole sector
  - Solution: Micro Logs
    Write to empty memory first, write back occasionally

Interplay of Deluge and Coffee

\[ \text{:Node A} \quad \text{:Node B} \]

- Advertisement
- Advertisement
- Request
- Data
- Data
- Data

\[ D_{data} \uparrow \quad D_{write} \downarrow \]
Interplay of Deluge and Coffee

- $D_{data}$ too high
  $\Rightarrow$ Transmission takes too long

- $D_{data}$ too low
  $\Rightarrow$ Sometimes writing not finished
  $\Rightarrow$ Retransmissions required
  $\Rightarrow$ Transmission takes too long
Interplay of Deluge and Coffee

- $D_{data}$ too high
  $\Rightarrow$ Transmission takes too long
Interplay of Deluge and Coffee

- **Node A**
  - Advertisement
  - Request
  - Data
  - Data

- **Node B**
  - Data

- $D_{data}$ too high
  - $\Rightarrow$ Transmission takes too long

- $D_{data}$ too low
  - $\Rightarrow$ Sometimes writing not finished
  - $\Rightarrow$ Retransmissions required
  - $\Rightarrow$ Transmission takes too long
Interplay of Deluge and Coffee

- Repeated writes to file when new packets arrive
  - Micro Logs grow fast
  - Write-back can occur at any time and takes very long
  - Severe delays for data dissemination

- Proposed Solutions:
  - **Cache** larger chunks in RAM
  - **Optimize** the write back
  - Selective **direct** memory access
Comparison of Flash Access Techniques

Duration for a file of 20 kB [s]

- Naive
- Cache
- Optimized
- Optimized & Cache
- Direct
- Direct & Cache

Per-link duration $T_{pg}(i,j)$ for transmitting a single page. Recursively calculate duration for multiple hops and pages: $T_{mh_p,j} = T_{pg}(p_j,j) + \max(T_{mh_p,p_j},T_{mh_p-1,j},T_{mh_p-1,c_j},\ldots,T_{mh_p-1,c_j}|C_j|)$. 

Florian Kauer, Florian Meyer, Volker Turau A Holistic Solution for Reliable Over-the-Air Software Updates in Large Industrial Plants
Analytical Model

- Topology
- Channel Utilization

Per-link probabilities for a successful
- data transmission
- request transmission

Analytical Model

Topology

Channel Utilization

Per-link probabilities for a successful

\{ data transmission
\{ request transmission

Per-link duration $T_{pg}(i,j)$ for transmitting a single page

Analytical Model

- Topology
- Channel Utilization

Per-link probabilities for a successful data transmission and request transmission

Per-link duration $T_{pg}^{(i,j)}$ for transmitting a single page

Recursively calculate duration for multiple hops and pages

$$T_{mh}^{p,j} = T_{pg}^{(p_j,j)} + \max\left( T_{mh}^{p,p_j}, T_{mh}^{p-1,j}, T_{mh}^{p-1,c_j,1}, \ldots, T_{mh}^{p-1,c_j,|C_j|} \right)$$
Duration of Firmware Distribution

⇒ Analytical model matches simulation
⇒ Spatial multiplexing allows for fast firmware distribution
Components

- Motor Controller
- Radio Transceiver
- Control Room
- Radio Gateway
Procedure - 1. Phase

1. Switch to Maintenance Mode
2. Conversion
3. File Transmission
4. Verify
5. OK
Procedure - 2. Phase

Start Deluge
Deluge
Verify
Pending
Verify
OK
**Procedure - 3. Phase**

- **Control Room PC**: Start Update
- **Radio Gateway**: Update
- **Radio Transceiver**: Finished
- **Motor Controller**: Switch to Normal Mode
- **OK**: OK
Summary

- Software updates in large-scale industrial wireless networks
- Using Deluge and the Coffee File System
  - Interplay optimized
  - Delay largely reduced
- Analytical model developed
  - Shows good conformance to the simulation
  - Spatial multiplexing allows for fast firmware distribution
- Holistic approach tested with real-world components
A Holistic Solution for Reliable Over-the-Air Software Updates in Large Industrial Plants

Florian Kauer
Ph.D. Student

Phone +49 / (0)40 428 78 3746
e-Mail florian.kauer@tuhh.de

http://www.ti5.tu-harburg.de/staff/meier