Energy Informatics
05 Networks for Smart Grids

Christian Schindelhauer
Technical Faculty
Computer-Networks and Telematics
University of Freiburg
What is Smart Grid?
RFC 6272

- **Smart grid**
  - electricity network utilizing digital technology
  - delivers electricity from suppliers to consumers
  - using two-way digital communications
  - control appliances at consumers' homes

- **Features**
  - saves energy, reduces costs, increases reliability, transparency.
  - net metering system
  - smart meters, integrates renewable energy

- **Communication**
  - between system users, operators, automatic devices
  - monitoring, tracks electricity flows
European Smart Grid Programs

- CEN/CENELEC/ETSI Smart Grids Joint WG
  - A common initiative http://www.smartgrids.eu
  - European technology platform for the electricity networks of the future

- IEC Global Standards for the Smart Grid
  - Strategic Group 3 – working on Smart Grid since April ’09
  - Cooperation with NIST
  - Identified relevant IEC standards for Smart Grid
  - http://smartgridstandardsmap.com
OSGP: supported by:

- CoNe
- Freiburg
- VATTENFALL
- Fortum
- LINZ AG
- STRÖM
- netbeheer
- nederland
- energie in beweging
- ENERGI MIDT
- NRGi
- CIAC
- MITSUBISHI ELECTRIC
- aSAY Energy
- VIKO
- GÖRLITZ
- IBM
- Conlog
- ZIRODE MANAGEMENT SERVICES
- FERRANTI Computer Systems
- GIZA SYSTEMS
- rms
- TELVENT
- ModemTec
- ORACLE
- DIEHL
- EVB ENERGIE
- EnergieGrupe
OSGP

Goal
- Globally-applicable standards for Information and Communications Technologies
- Based on Echelon specifications for Data Concentrator – Smart meter communications
- Layered protocol stack
- Common data model for utilities
- High-performance and reliability
- Mandatory security and privacy

Standardized by ETSI
- European Telecoms Standards Institute (ETSI)
- EU-recognized standards with CEN, ETCSI, CENELEC
OSGP Powerline communication

- Lower cost investment
- Lower operating cost
  - Communication cost (daily on-going communication)
- Reliability, performance
  - Proven, up to 99.8% ->99.94%-100%
  - Daily, including Load profiles
- Technical information
  - Phase, Grid
  - Outage detection
  - Grid Topology
- LV Transformer centric approach
  - Be able to run applications within a LV area
    (the next generation DC: Edge Control Node)
Smart Metering Standards Activities

- EU: many standards
- M/441 standardization mandate
  - CEN, CENELEC and ETSI
- European OPEN meter project
  - 7th Framework Programme, finished 2012
  - http://openmeter.com/
- DLMS/COSEM: IEC 62056 / EN 13757
  - projects in Netherlands, France,
Layered OSI protocol stack
ETSI Group spec GS OSG 001
  - Application layer Protocol
  - Media independent
ISO/EN14908.1 Control Networking
  - Layers 2 to 6
ETSI Technical spec TS 103 908
  - High performance power line communication media
  - Support many smart grid device types
Designed for additional media
Supported and maintained by ESNA
Events allow devices to report information asynchronously

- Alerts/alarms (e.g., tamper)
- Conditions/thresholds being met (e.g., under voltage)
- Exceptions detected (e.g., phase loss)
- Self-check errors (e.g., low battery detected)
- State or status change (e.g., season change)

- 96 events (50 basic, 46 extended)
- OSGP provides a standard way for devices to send extended events
ETSI OSG 001

- Models devices as a collection of data, methods and events
  - bandwidth efficient, enabling high performance on bandwidth constrained media
  - Includes core meshing services for reliable, scalable operation
  - Built-in, mandatory security and privacy for every data exchange
  - allows commissioning, automated device discovery, automatic topology management

- Deployed in over 3.5 million smart grid devices
ISO/IEC 14908.1 (LonTalk)

- Optimized, multi-application control network protocol stack
  - reliable delivery, multi-cast messaging
  - Low overhead, low bandwidth

- Probably insecure:
  - Philipp Jovanovic and Samuel Neves.
    Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol 2015
    https://eprint.iacr.org/2015/428 - The Cryptology ePrint Archive
Any OSGB device can be a repeater
Repeating up to 16 hops
Automatic repeater selection
ETSI TS 103 908

- Based on ISO/IEC 14908.3 2006 with adaptations for A-band operation, per EN 50065-1
- High-performance narrow band power line channel for control networking in the smart grid
  - Binary Phase Shift Keyed (BPSK) modulated carrier
  - 3.24 kbps raw channel data rate
  - Deployed in over 35 million smart meters and grid devices
One of the major steps in favor of building the momentum around using IP end to end in the last mile of smart-grid networks was to demonstrate that IP could be light enough to be used on constrained devices with limited resources in terms of energy, memory, and processing power. Thus, FANs were seen as single-application, stub networks with end nodes (such as meters not running IP) that could be reached through IP through protocol-translation gateways, with each gateway being tied to a dedicated service and/or solution’s vendor.

The past two decades, with the transition of protocols such as Systems Network Architecture (SNA) (through data-link switching [DLSw]), Appletalk, DECnet, Internetwork Packet Exchange (IPX), and X.25, showed us that such gateways were viable options only during transition periods with smaller, single-application networks. But proprietary protocol and translation gateways suffer from well-known severe issues, such as high capital expenditures (CapEx) and operating expenses (OpEx) [SNA–IP], along with significant technical limitations, including lack of end-to-end capabilities in terms of QoS, fast recovery consistency, single points of failure (unless implementing complex stateful failover mechanisms), limiting factors in terms of innovation (forcing to least common denominator), lack of scalability, vulnerability to security attacks, and more. Therefore, using IPv6 end to end (that is, IP running on each and every device in the network) will be, in many ways, a much superior approach for multiservice FANs as shown in Figure 2.

Figure 2. Multiservice Infrastructure for Last-Mile Smart-Grid Transformation

1 See RFC 3027 as an example of protocol complications with translation gateways.
IPv6 for Field Area Networks

<table>
<thead>
<tr>
<th>Open Standards Reference Model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Layer</strong></td>
</tr>
<tr>
<td>Web Services, EXI, SOAP, RestFul, HTTPS/CoAP</td>
</tr>
<tr>
<td>IEC 61968 CIM, ANSI C12.22, DLMS/COSEM,...</td>
</tr>
<tr>
<td>SCADA</td>
</tr>
<tr>
<td>IEC 61850, 60870</td>
</tr>
<tr>
<td>DNP3/IP, Modbus/TCP,...</td>
</tr>
<tr>
<td>DNS, NTP, IPfix/Netflow, SSH RADIUS, AAA, LDAP, SNMP,...</td>
</tr>
<tr>
<td>(RFC 6272 IP in Smart Grid)</td>
</tr>
</tbody>
</table>

5.1. Diversity of Physical and Data Link Layers

As mentioned, one main difference between energy distribution networks and ICT is the pace of change in technologies. Every three to five years, physical and data link layers evolve, offering greater bandwidth, enhanced robustness, longer reach, lower cost, etc. This evolution contributes to the success of the IP architecture, which supports smooth evolution and upgrades without reconsidering the whole architecture. Such evolutions on the time scale above are familiar to anyone observing the evolution of Ethernet, Wi-Fi, or cellular technologies, to name just a few technologies with very high visibility.

- Open Standards - At all levels to help ensuring interoperability and reducing technology risk for utilities
- Future proofing - Common application layer services over various wired and wireless communication technologies

IEEE PHY and MAC standards

- **IEEE 802.15.4**
  - low-power wireless PHY and MAC layers
  - for smart object networks
  - low power consumption
  - link speeds up to 250 kbps in 2.4GHz ISM frequency band

- **IEEE 802.15.4g Task Group, aka Smart Utility Networks (SUN) Task Group**
  - OFDM, multiple data rates, Multirate and multiregional offset quadrature phase-shift keying

- **IEEE 1901.2 Power Line Communication**
  - „no new-wire technology“ reuses electrical wire
  - Data rate up to 500 kbps
  - low-frequency (<500 kHz) PLC spectrum
6LoWPAN

- main focus of the 6LoWPAN WG
  - optimize the transmission of IPv6 packets over low-power and lossy networks such as IEEE 802.15.4 (WPAN)
  - Header compression
  - Fragmentation of IPv6 packets (max 127 bytes)
  - Duplicate address detection
IEEE 802.15.4

- Fundamental lower network layer for wireless personal area network
- Features
  - Realtime by guaranteed time slots
  - Beacon messages
  - Collision avoidance
    - CSMA/CA, random exponential back off
  - Frequency bands (868/915/2450 MHz)
    - 20-250 kbit/s
- Topologies
  - Star, Peer-to-Peer (point-to-point)
Problem of Wireless Media Access (MAC)

- Unknown number of participants
  - broadcast
  - many nodes simultaneously
  - only one channel available
  - asymmetric situations

- Collisions produce interference

- Media Access
  - Rules to participate in a network
MACA

- Phil Karn
  - MACA: A New Channel Access Method for Packet Radio
    1990

- Alternative names:
  - Carrier Sensing Multiple Access / Collision Avoidance (CSMA/CA)
  - Medium Access with Collision Avoidance (MACA)

- Aim
  - Solution of the Hidden and Exposed Terminal Problem

- Idea
  - Channel reservation before the communication
  - Minimization of collision cost
**RTS/CTS**

- Sender sends Request to Send (RTS) to B.
- Receivers answers with Clear to Send (CTS) to A
- Sender sends Data
Details for Sender

- A sends RTS
  - waits certain time for CTS
- If A receives CTS in time
  - A sends packet
  - otherwise A assumes a collision at B
    - doubles $Backoff$-counter
    - and chooses a random waiting time from \{1,...,$Backoff$\}
- After the waiting time A repeats from the beginning
Details for Receiver

- After B has received RTS
  - B sends CTS
  - B waits some time for the data packet
  - If the data packet arrives then the process is finished
    • Otherwise B is not blocked
Details for Third Parties

- C receives RTS of A
  - waits certain time for CTS of B
- If CTS does not occur
  - C is free for own communication
- If CTS of B has been received
  - then C waits long enough such that B can receive the data packet
- D receives CTS of B
- waits long enough such that B can receive the data packet
- E receives RTS of A and CTS of B
- waits long enough such that B can receive the data packet
Zigbee

- Designed by the Zigbee alliance
  - for low power consumption embedded systems
  - provides network security

- Device Types
  - Zigbee coordinator node
    • root of network tree, bridge to other networks
  - Full function device
    • router, may be coordinator
  - Reduced function device
    • cannot relay, cheaper

- Application
- API
- Security
  32/64/128 bit encryption
- Network
  Star/Mesh/Cluster-Tree
- MAC
- PHY
  868MHz/915MHz/2.4GHz
Energy Informatics
05 Networks for Smart Grids

Christian Schindelhauer
Technical Faculty
Computer-Networks and Telematics
University of Freiburg