Data-Link Layer and Management Protocols for IoT

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

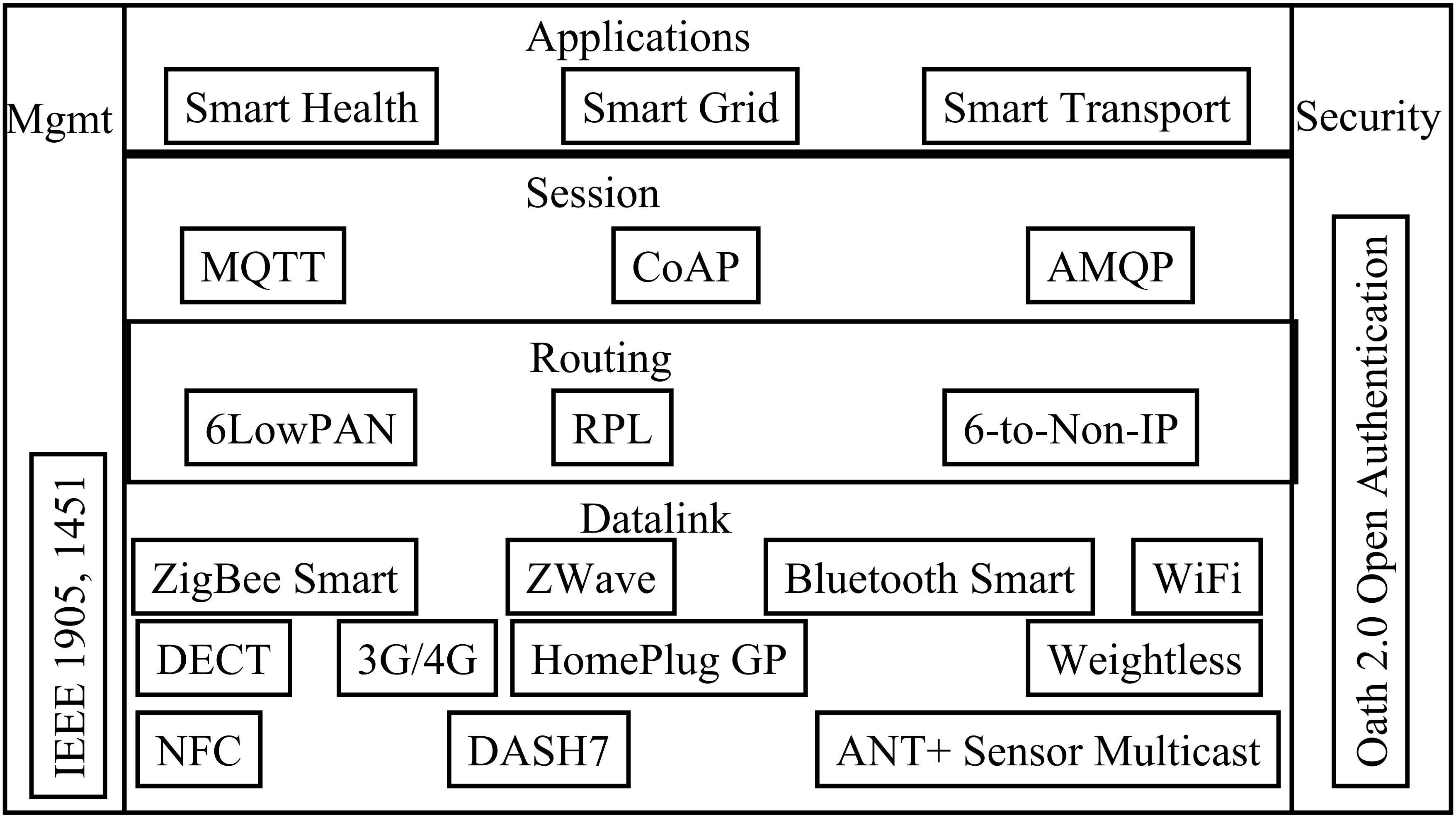
These slides and audio/video recordings of this class lecture are at:
http://www.cse.wustl.edu/~jain/cse570-15/

Overview

1. L2 Protocols for IoT
2. IEEE 1901 - Power Line Communication (PLC)
3. IEEE 1905.1 - Convergent Digital Home Network

Note: This is part 2 of a series of class lectures on IoT. Wireless datalink protocols are covered in CSE 574 Wireless Network Class. More protocols are covered in other parts of this series.

Recent Protocols for IoT



Mgmt

IEEE 1905, 1451

Applications

Smart Health

Smart Grid

Smart Transport

Session

MQTT

CoAP

AMQP

Routing

6LowPAN

RPL

6-to-Non-IP

Datalink

ZigBee Smart

ZWave

Bluetooth Smart

WiFi

DECT

3G/4G

HomePlug GP

Weightless

NFC

DASH7

ANT+ Sensor Multicast

Security

Oath 2.0 Open Authentication

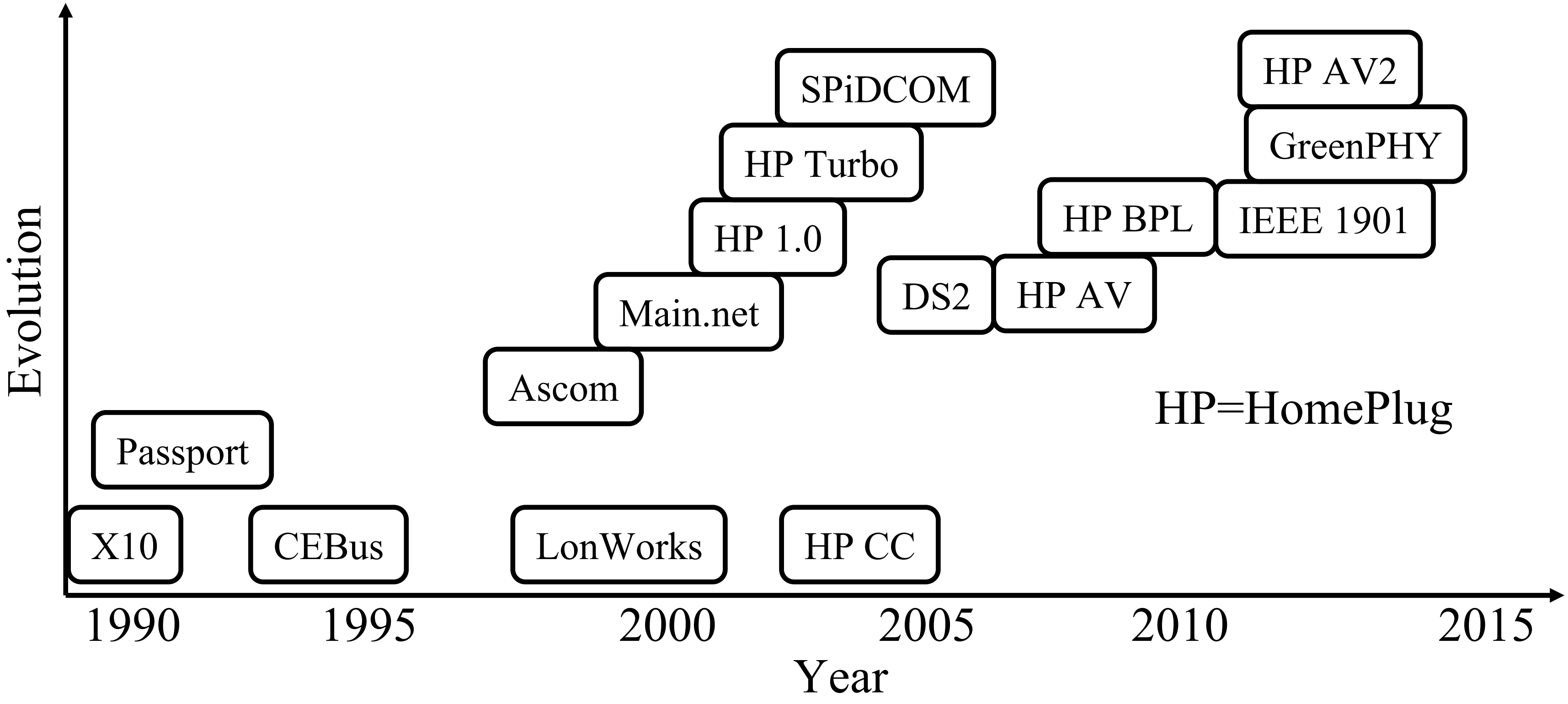
Ref: http://tools.ietf.org/html/draft-rizzo-6lo-6legacy-00, http://en.wikipedia.org/wiki/OAuth, http://en.wikipedia.org/wiki/ANT%2B http://en.wikipedia.org/wiki/Near_field_communication, http://en.wikipedia.org/wiki/Weightless_%28wireless_communications%29

L2 Protocols for IoT

1. ZigBee, Z-Wave, Bluetooth, WiFi, 3G/4G are wireless protocols. These are covered in CSE 574 Wireless Networks class.
2. In this lecture we cover Powerline Communications (PLC) and associated management protocols

Power Line Communication (PLC)

- Used in 1950 for remote ignition and lighting of street lights. 100 Hz and 1 kHz signals over electrical wires
- Two way systems using 3-148.5 kHz for reading electric meters, and home automation, alarms etc.



Ref: H. Chaouchi, "The Internet of Things: Connecting Objects," Wiley, Jun 2010, 288 pp., ISBN: 9781848211407 (Safari Book)

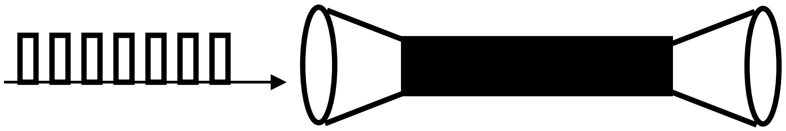
Broadband Over Power Lines (BPL)

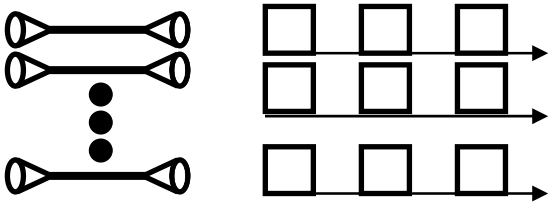
- High-speed internet connection using power lines (like DSL)
- IEEE 1901-2011 Broadband over Power Line standard
- Not cost competitive with optical fiber or DSL
  ⇒ Suitable for remote locations
- High-frequency signal cannot pass through transformers and so the signal has to be bypassed using a repeater
- In US 1 transformer per house ⇒ Very expensive
  In Europe: 1 transformer per 10-100 houses ⇒ More cost effective
- Radio frequency interference with existing wireless services is avoided using OFDM

Ref: http://en.wikipedia.org/wiki/Broadband_over_power_lines

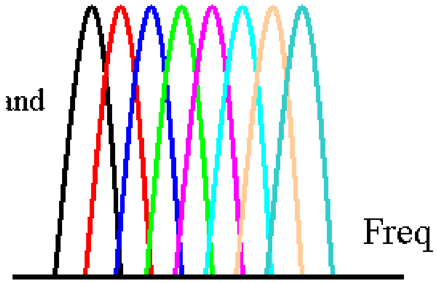
OFDM

- Orthogonal Frequency Division Multiplexing
- Ten 100 kHz channels are better than one 1 MHz Channel ⇒ Multi-carrier modulation





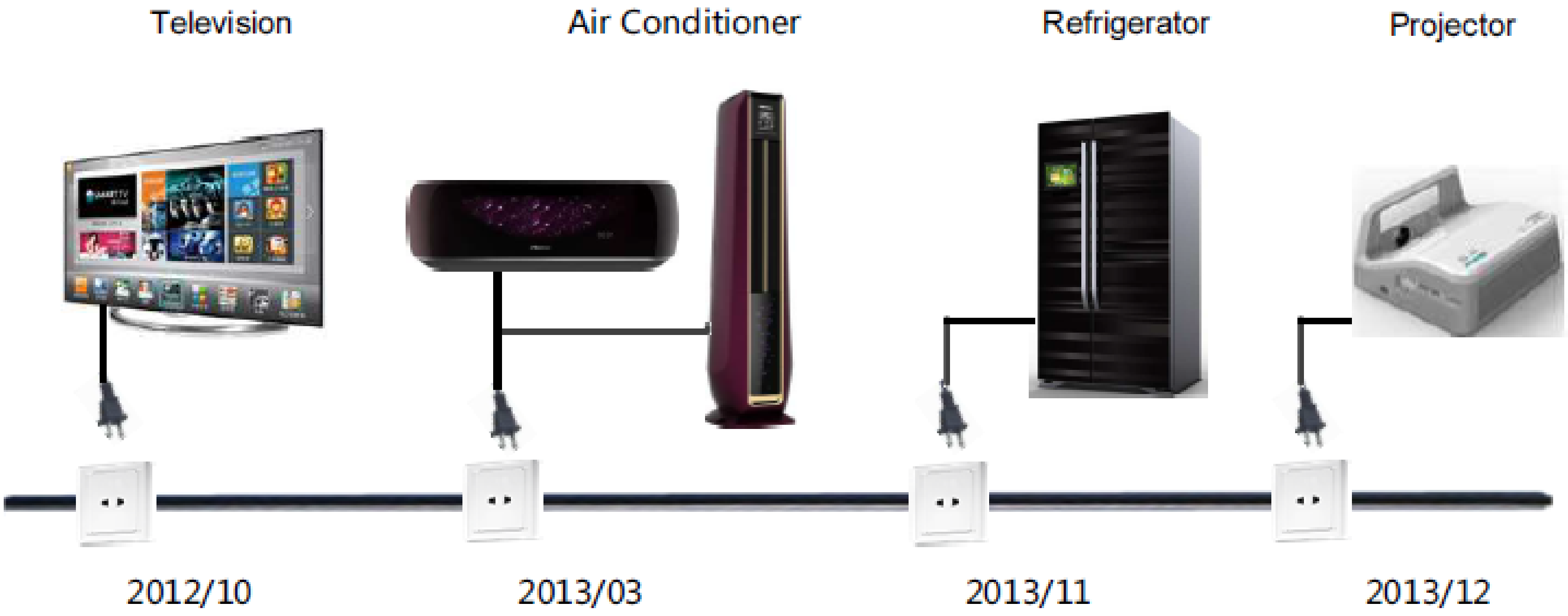
- Frequency band is divided into 256 or more sub-bands. Orthogonal ⇒ Peak of one at null of others
- Each carrier is modulated with a **BPSK** (2bps/Hz), **QPSK** (4 bps/Hz), **16-QAM** (8bps/Hz), **64-QAM** (16 bps/Hz) etc depending on the noise (Frequency selective fading)
- Used in 802.11a/g, 802.16, Digital Video Broadcast handheld (DVB-H)
- Easy to implement using FFT/IFFT



HomePlug

- HomePlug 1.0
- HomePlug AV
- HomePlug AV2
- HomePlug GP

Connected Home



Ref: HomePlug Alliance, "HomePlug Connected Home Summits 2013 Presentations," http://www.homeplug.org/tech/whitepapers/Connected_Home_Summits_2013.pdf

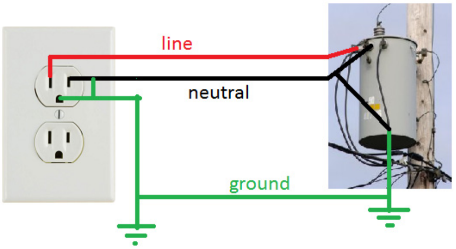
HomePlug AV

- ❑ Leading industry consortium for power line communications 90% of PLC devices use HomePlug
- ❑ 1.8 MHz to 30 MHz spectrum = 28 MHz ⇒ 20 to 200 Mbps
- ❑ Multipath distortion
- ❑ **Orthogonal Frequency Division Multiplexing (OFDM):** Using 1155 carriers at 24.414 kHz spacing of which 917 are used for signal. Rest as pilots.
- ❑ **Adaptive bit loading**: Each carrier is modulated based on the noise level and multipath at that frequency.
  2-bits/symbol to 10 bits/symbol.
- ❑ **Tone Maps**: Each receiver keeps a table of signal strengths from each of the other receivers ⇒ n-1 tone maps in a n-device system

Ref: HomePlug Alliance, "HomePlug AV White Paper," http://www.homeplug.org/tech/whitepapers/HPAV-White-Paper_050818.pdf

HomePlug AV (Cont)

- **Robust OFDM** (ROBO) mode for highly reliable transmission. The same information is transmitted on 2-5 subcarriers using a low-bit rate modulation



- Use only Line-neutral pair (ground is not used)
- Four channel access priorities
- MAC is similar to that of WiFi ⇒ **Carrier Sense Multiple Access (CSMA).**
- All devices part of the same trust domain form a "**AV Logical Network** (AVLN)."
- All members of the AVLN share a Network Membership Key 128-bit AES.
- Each AVLN has a **central coordinator (CCo)**

HomePlug AV (Cont)

- CCo transmits beacons containing schedule
- Long best effort transmissions declare their queues to CCo and use a pre-allocated **persistent shared CSMA** region
- Short best effort transmissions use **non-persistent CSMA** region.
- Real-time traffic uses periodic time division multiple access (TDMA) allocation in the **contention-free** period
- Before video transmission, the transmitter tests the channel for achievable throughput. Helps determine the required transmission interval per beacon period

Beacon Region	Persistent Shared CSMA Region	Non-Persistent Local CSMA	Non-Persistent Local CSMA	Persistent Allocation 1	Persistent Allocation n

HomePlug AV Security

- A station can participate in a AVLN if it has the **Network membership key (NMK)**.
  A station with multiple keys can participate in multiple AVLNs.
- All devices have a default NMK and so can form the network. Users should program the devices to use specific NMK.
- Once a devices has a NMK, it will be given the **network encryption key** which is used to encrypt the data.
- If there are multiple networks on the same wire,
  CCos coordinate their transmission schedules

HomePlug AV2

- Gigabit networking using home powerline wiring. Peak PHY rate of 1.256 Gbps. 600 Mbps net throughput.
- Can transmit multiple HD video streams
- Compatible with HomePlug AV devices on the same wires

1. **Additional Spectrum**: 2MHz-86MHz (84 MHz)
2. **Multiple-input Multiple-output (MIMO)**: transmissions using two wires with three-wire configuration (Line-Neutral, Line-Ground, Neutral-Ground)
3. **Beam forming**: Bit loading for each transmitter
4. **Lower overhead**: Shorter packet delimiter and delay acks.
5. **Efficient notching**: Of noisy carriers

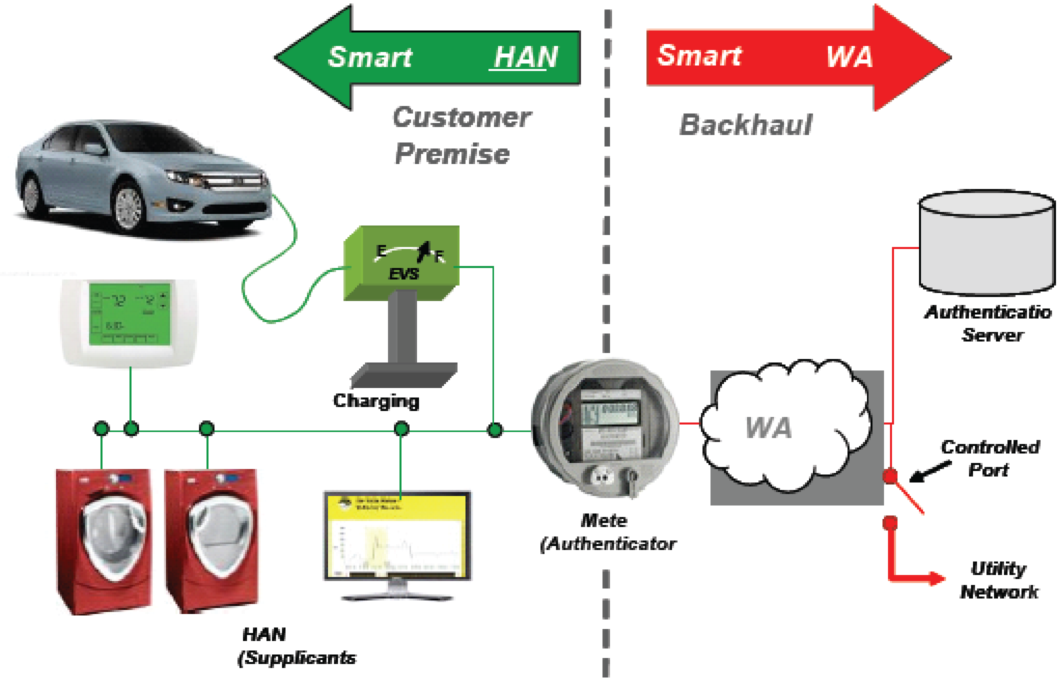
Ref: HomePlug Alliance, "HomePlug AV2 Technology," http://www.homeplug.org/tech/whitepapers/HomePlug_AV2_whitepaper_130909.pdf

HomePlug AV2 (Cont)

6. **Repeating**: Signal is demodulated and re-modulated at intermediate devices
7. **Better coding**: 12 bps/Hz and aggressive code rates (8/9)
8. **Power Control**: Manage transmission power to enhance coverage and throughput
9. **Power Save**: Stations can declare sleep periods. Other transmit only when the destination is awake.

HomePlug GreenPHY

- Designed for **home area network (HAN)** for monitoring and control of energy consuming/controlling devices including electric vehicle charging.
- Low cost. Low power. Low data rate version of HomePlug AV.



Ref: HomePlug Alliance, "HomePlug GreenPHY White Paper," http://www.homeplug.org/tech/whitepapers/HomePlug_Green_PHY_whitepaper_121003.pdf

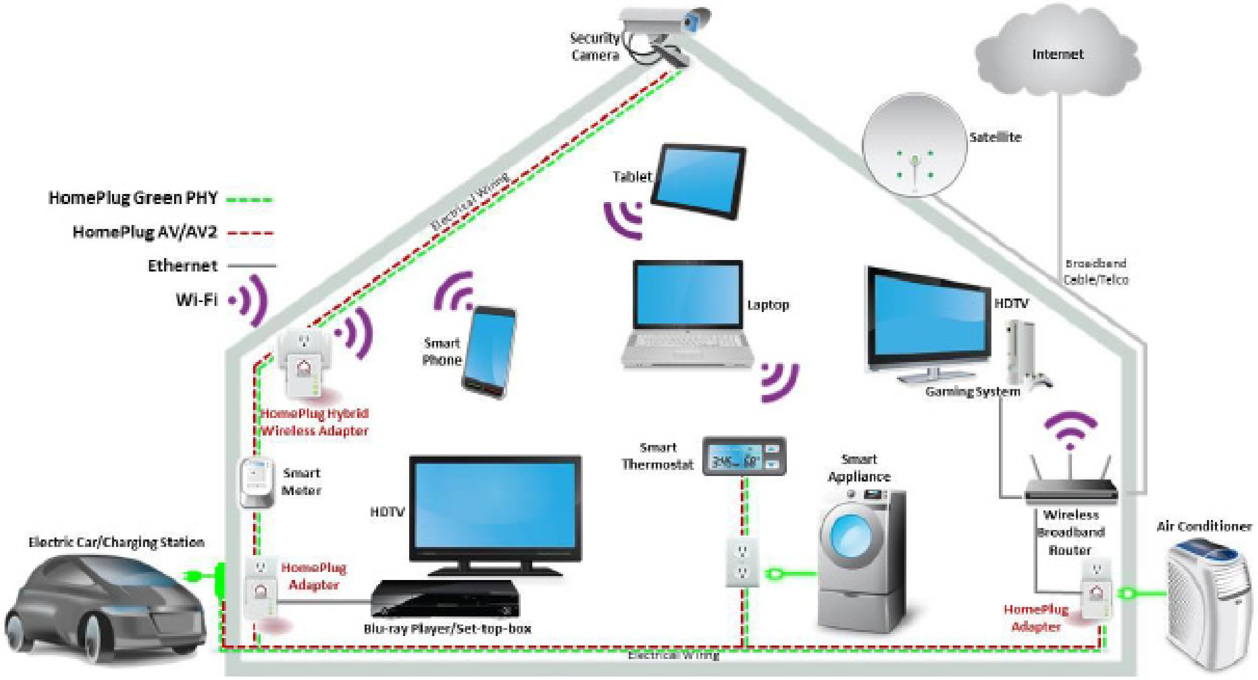
HomePlug GP (Cont)

- HomePlug GP is a profile of **IEEE 1901-2010** standard for Powerline Networks and is compatible with HomePlug AV and HomePlug AV2.
- 28 MHz ⇒ 256 kbps to 10 Mbps using only one modulation No tone maps.
- Use 75% less power than HomePlug AV.
  75% less bill of materials
- Devices coordinate their sleep cycle and may sleep for 2^n beacon intervals, n=1,..,10
- HomePlug GP 1.1 adds new power management and features for electric vehicles. Secure billing is possible at a public charging station.

Ref: HomePlug Alliance, “HomePlug GreenPHY Overview,” http://www.homeplug.org/tech/whitepapers/HomePlug_GreenPHY_Overview.pdf

Convergent Digital Home Network

- IEEE 1905.1-2013 Convergent Digital Home Network for Heterogeneous Technologies
- Combined use of WiFi, HomePlug, Ethernet, Multimedia over Coax (MoCA) in a home



Ref: http://en.wikipedia.org/wiki/IEEE_1905

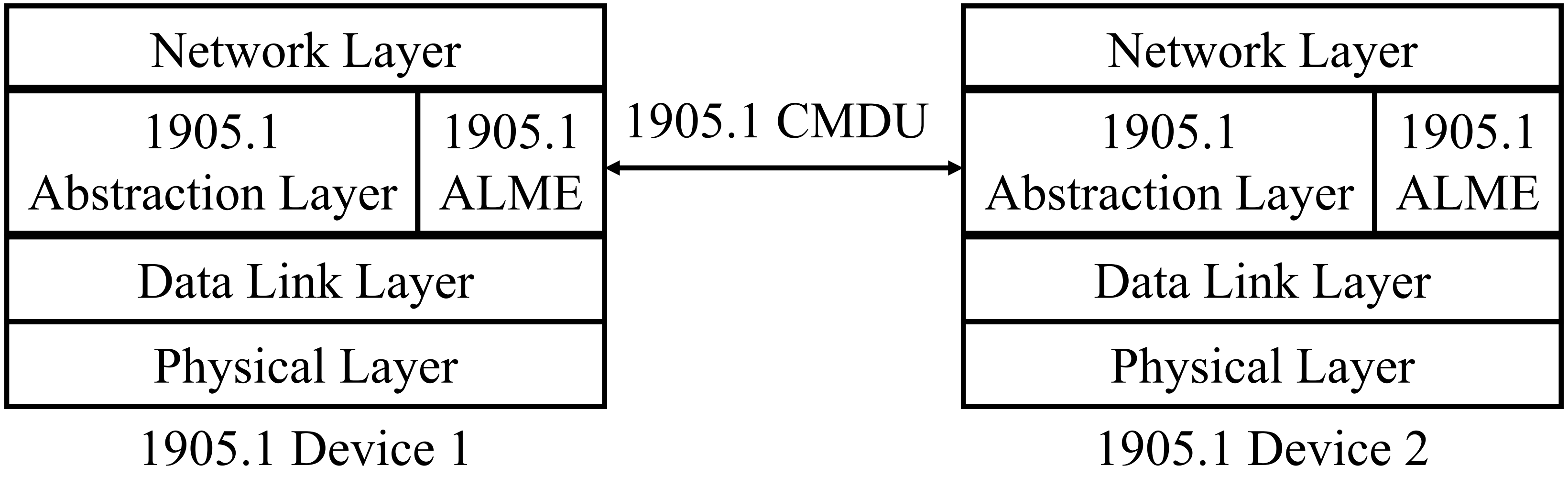
Convergent Digital Home (Cont)

- Entire home looks like a single network with automated provisioning, management, and operation
- Allows a device to aggregate throughput from multiple interfaces
- A link can be used fallback when another link fails
- An abstraction layer is used to exchange **Control Message Data Unit (CMDU)** among 1905.1 compliant devices
- No changes to underlying technologies is required.

<table>
<tr><td colspan="4">Network Layer</td></tr>
<tr><td colspan="4">1905.1 Abstraction Layer</td></tr>
<tr><td>802.3</td><td>802.11</td><td>PLC
1901</td><td>MoCA</td></tr>
</table>

IEEE 1905.1 Management

- 1905.1 compliant devices speak Abstraction Layer Management Entity (ALME) Protocol



IEEE 1905.1 Management (Cont)

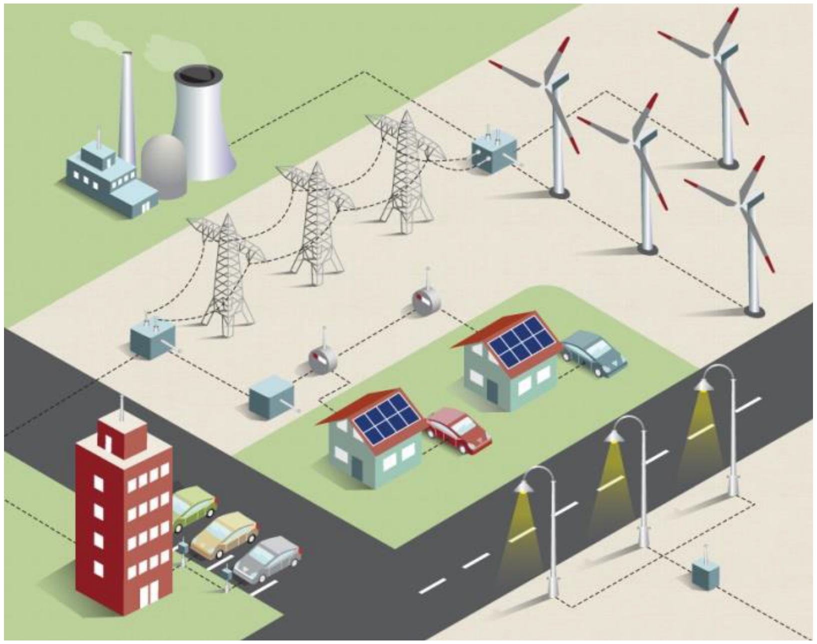
- ALME has messages for
  - Neighbor discovery,
  - Topology exchange,
  - Topology change notification,
  - Measured traffic statistics exchange,
  - Flow forwarding rules, and
  - Security associations
- HomePlug AV2 can be used as a backbone for Wi-Fi
- Existing IEEE 802.1 bridging protocols are used for loop prevention and forwarding

IEEE 1905.1 Security and Configuration

- Security Setup:
  - **Push Button**: Press buttons on new and existing devices The new device gets the keys from the existing device
  - User can configure **passphrase/key** in the new device
  - **NFC**: User touches the new device with a NFC equipped smart phone which is existing member of the network
- Auto configuration:
  - New Access Points (APs) can get configuration information from existing APs
- The certification program for IEEE 1905.1 is called "**nVoy**" Connects disparate networks = Network Diplomat = Network Envoy ⇒ nVoy
- Qualcomm Atheros products implementing IEEE 1905.1 are called **Hy-Fi** (for Hybrid Fidelity)

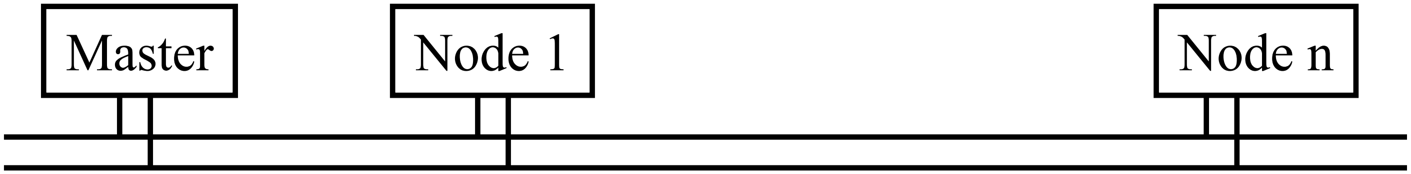
Netricity

- Long-range outside-the-home PLC for smart grid applications
- Certification for IEEE 1901.2 Low Frequency, Narrowband Powerline Communications Standard is called "Netricity"



Fieldbus

- Family of protocols for *short-range* real-time distributed industrial control systems standardized as IEC 61158
- Fieldbus connects programmable logic controllers to sensors, actuators, electric motors, console lights, switches, valves, and contractors
- Hundreds of nodes are connected to a single microcontroller using a *single* cable, e.g., 250 nodes on 13.2 km cable ⇒ High-level Datalink Control (HDLC)-like master-slave communication with polling



Ref: H. Zhou, "The Internet of Things in the Cloud: A middleware Perspective," CRC Press, 2013, 366pp., ISBN:9781439892992 (Safari Book)
Ref: http://en.wikipedia.org/wiki/Fieldbus

Fieldbus (Cont)

- Collection of 8 different *incompatible* “Types”
  1. Foundation Fieldbus H1
  2. ControlNet
  3. PROFIBUS
  4. P-NET
  5. FOUNDATION Fieldbus High Speed Ethernet
  6. SwiftNet
  7. WorldFIP
  8. Interbus
- Only PHY, Datalink, and application layer
  ⇒ No routing ⇒ Need Ethernet/IP from microcontroller

Industrial Ethernet

- Same as regular Ethernet but with rugged connectors and designed for extended temperature/humidity environment
- Full duplex links (no CSMA/CD)
- Optical fibers (electrical interference)
- Min frame size of 64 byte may be too big for some applications

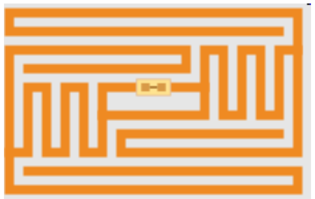
Ref: http://en.wikipedia.org/wiki/Industrial_Ethernet

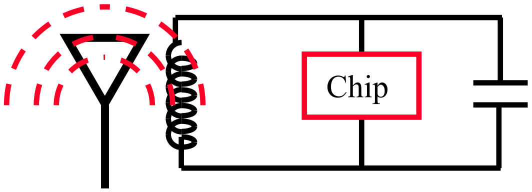
IEEE 1451

- Set of smart transducer interface for sensors and actuators
- Transducer electronic data sheets (TEDS) is a memory device that stores transducer id, calibration, correction data, and manufacturer information
- Allows access to transducer data regardless of wired or wireless connection
- XML based ⇒ Allows manufacturers to change the contents

Ref: http://en.wikipedia.org/wiki/IEEE_1451

Smart Cards





- Smart ⇒ With a processor
- Radio Frequency ID (RFID) is a subset
- Reader queries using RF, ID sends its ID using RF
- Used for retail loss prevention, toll collection, bus/rail passes, passports
- May have battery (active), no battery (passive), small battery (semi-passive)
- Get power from the reader by inductive or capacitive coupling
- Standards: ISO 14443 (Proximity ~10cm), ISO15693 (vicinity ~50cm), ECMA 340 (near field communication transceiver)
- More details in CSE 574 wireless networking course http://www.cse.wustl.edu/~jain/cse574-10/index.html

Smart Card Security Issues

1. Skimming: Read w/o knowledge of owner
2. Eavesdropping or sniffing: Man-in-the-middle
3. Data Tampering: Erasing or changing data
4. Spoofing: Mimic another source
5. Cloning: Making a copy of data
6. Malicious Code: Insertion of executable virus code
7. Denial of Service: Overwhelm the receiver's capacity
8. Killing: Disable
9. Jamming: Interfere with a strong signal
10. Shielding: Mechanically prevent reading

Ref: H. Zhou, "The Internet of Things in the Cloud: A middleware Perspective," CRC Press, 2013, 366pp., ISBN:9781439892992 (Safari Book)
Ref: http://en.wikipedia.org/wiki/Radio-frequency_identification#Security_concerns

Reading List

- HomePlug Alliance, "HomePlug AV White Paper," http://www.homeplug.org/tech/whitepapers/HPAV-White-Paper_050818.pdf
- HomePlug Alliance, "HomePlug AV2 Technology," http://www.homeplug.org/tech/whitepapers/HomePlug_AV2_whitepaper_130909.pdf
- HomePlug Alliance, "HomePlug Connected Home Summits 2013 Presentations," http://www.homeplug.org/tech/whitepapers/Connected_Home_Summits_2013.pdf
- HomePlug Alliance, "HomePlug GreenPHY Overview," http://www.homeplug.org/tech/whitepapers/HomePlug_GreenPHY_Overview.pdf
- HomePlug Alliance, "HomePlug GreenPHY White Paper," http://www.homeplug.org/tech/whitepapers/HomePlug_Green_PHY_whitepaper_121003.pdf
- J. Bradley, "The Internet of Everything: Creating Better Experiences in Unimaginable Ways," Nov 21, 2013, http://blogs.cisco.com/ioe/the-internet-of-everything-creating-better-experiences-in-unimaginable-ways/#more-131793

Wikipedia Links

- http://en.wikipedia.org/wiki/IEEE_1905
- http://en.wikipedia.org/wiki/IEEE_1901
- http://en.wikipedia.org/wiki/Broadband_over_power_lines
- http://en.wikipedia.org/wiki/Power_line_communication
- http://en.wikipedia.org/wiki/HomePlug
- http://en.wikipedia.org/wiki/Cyber-physical_system
- http://en.wikipedia.org/wiki/HomePlug_Powerline_Alliance
- http://en.wikipedia.org/wiki/MIMO
- http://en.wikipedia.org/wiki/SCADA
- http://en.wikipedia.org/wiki/Smart_grid
- http://en.wikipedia.org/wiki/G.hn
- http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing
- http://en.wikipedia.org/wiki/IEEE_Smart_Grid
- http://en.wikipedia.org/wiki/Fieldbus
- http://en.wikipedia.org/wiki/Industrial_Ethernet
- http://en.wikipedia.org/wiki/IEEE_1451

Wikipedial Links (Cont)

- http://en.wikipedia.org/wiki/List_of_broadband_over_power_line_deployments
- http://en.wikipedia.org/wiki/Qualcomm_Atheros
- http://en.wikipedia.org/wiki/G.9972
- http://en.wikipedia.org/wiki/Home_network
- http://en.wikipedia.org/wiki/SPiDCOM
- http://en.wikipedia.org/wiki/Smart_meter
- http://en.wikipedia.org/wiki/IEC_62196

References

- H. Chaouchi, "The Internet of Things: Connecting Objects," Wiley, Jun 2010, 288 pp., ISBN: 9781848211407 (Safari Book)
- H. Zhou, “The Internet of Things in the Cloud: A Middleware Perspective,” CRC Press, 2013, 365 pp., ISBN: 9781439892992 (Safari Book)
- NITRD, http://www.nitrd.gov/
- NITRD, “FY 2014 Supplement to the President’s Budget,” http://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=48
- “Gartner Identifies Top 10 Strategic Technologies,” http://www.cioinsight.com/it-news-trends/gartner-identifies-top-10-strategic-technologies.html
- Workshop on Future Directions in CPS Security, July 2009, http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf

Acronyms

6LowPAN	IPv6 over Low Power Wireless Personal Area Network
AES	Advanced Encryption
ALME	Abstraction Layer Management Entity
AMQP	Advanced Queueing Message Protocol
AP	Access Point
AV	Audio-Visual
AVLN	Audio-Visual Logical Network
BPL	Broadband Over Power Lines
BPSK	Binary Phase-Shift Keying
CCo	Central Coordinator
CD	Collision Detection
CEBus	Consumer Electronic Bus
CMDU	Control Message Data Unit
CoAP	Constrained Application Protocol
CP	Cyber Physical

Acronyms (Cont)

CPS	Cyber Physical Systems
CSIA	Cyber Security and Information Assurance
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DARPA	Defense Advance Research Project Agency
DCS	DIstributed Control Systems
DECT	Digital Enchanced Cordless Telephony
DOE	Department of Energy
DS2	Design of Systems on Silicon (name of a company)
DSL	Digital Subscriber Line
DVB-H	Digital Video Broadcast handheld
ECMA	European Computer Manufacturers Association
FFT	Fast Fourier Transform
GE	General Electric
GP	Green PHY
GreenPHY	Green Physical Layer

Acronyms (Cont)

HAN	Home Area Network
HCSS	High Confidence Software and Systems
HD	High Definition
HDLC	High-Level Datalink Control
HEC	High-End Computing
HP	HomePlug
HPAV	HomePlug Audio-Visual
ID	Identifier
IEC	International Electrotelecommunications Commission
IEEE	Institution of Electrical and Electronic Engineers
IFFT	Inverse Fast Fourier Transform
IM	Information Management
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol V6
ISO	International Standards Organization

Acronyms (Cont)

IT	Information Technology
kHz	Kilo Hertz
LonWorks	Local Operating Network
LSN	Large Scale Networking
MAC	Media Access Control
MHz	Mega Hertz
MIMO	Multiple-input Multiple-output
MoCA	Multimedia over Coax
MQ	Multi-Queue
MQTT	MQ Telemetry Transport
NASA	National Aeronautical and Space Administration
NFC	Near Field Communication
NIH	National Institute of Health
NITRD	Networking and Info Technology Res and Development
NMK	Network Membership Key
NSF	National Science Foundation

Acronyms (Cont)

OAuth	Open Standard for Authorization
OFDM	Orthogonal Frequency Division Multiplexing
ONR	Office of Naval Research
PHY	Physical Layer
PLC	Power Line Communication
PROFIBUS	Process Field Bus
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low Power and Lossy Networks
SCADA	Supervisory Control and Data Acquisition
SDP	Software Design and Productivity
SPiDCOM	Name of a company
TDMA	Time division multiple access
TEDS	Transducer electronic data sheets

Acronyms (Cont)

US	United States
WiFi	Wireless Fidelity
WorldFIP	Factory Instrumentation Protocol
XML	Extensible Markup Language