Low Power WAN Protocols for IoT: IEEE 802.11ah, LoRaWAN

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

Audio/Video recordings of this class lecture are available at:
http://www.cse.wustl.edu/~jain/cse574-16/

1. Low Power WANs
2. IEEE 802.11ah
3. LoRaWAN

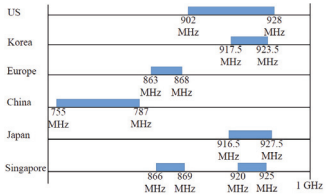
Note: This is the 5th lecture in series of class lectures on IoT. Bluetooth, Bluetooth Smart, IEEE 802.15.4, ZigBee were covered in the previous lectures.

Recent Protocols for IoT

Session	MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, IEC,…	**Security**	**Management**
Network	Encapsulation 6LowPAN, 6TiSCH, 6Lo, Thread…	IEEE 1888.3, TCG, Oath 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice, …	IEEE 1905, IEEE 1451, IEEE 1377, IEEE P1828, IEEE P1856
	Routing RPL, CORPL, CARP		
Datalink	**WiFi, 802.11ah, Bluetooth Low Energy,** Z-Wave, **ZigBee Smart, DECT/ULE, 3G/LTE**, NFC, **Weightless,** HomePlug GP, **802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN,** ISA100.11a, DigiMesh, WiMAX, …		

802.11ah Features

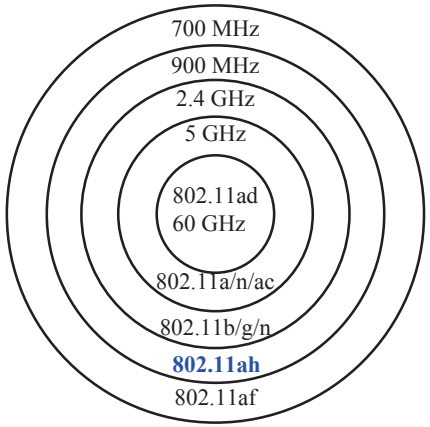
- *Aka "WiFi HaLow"* by WiFi Alliance.
- IEEE spec for Low-rate long-range IoT applications. Currently in 2nd Sponsor ballot (March 2016).
- **Spectrum**: Sub-Giga Hertz license-exempt spectrum. Not including TV white spaces (700 MHz for 802.11af).
  - 902-928 MHz (USA)
  - 863-868.6 MHz (Europe)
  - 916.5-927.5 MHz (Japan)
  - 755-587 MHz (China)
  - 917.5-923.5 MHz (Korea)



- **Sub-GHz frequency** ⇒ Longer range than 2.4 GHz, Less congested, better penetration
- Low bit rate for IoT, Short data transmissions, Power savings, Efficient MAC
- Goal: Support at least **4X devices** per AP than legacy 802.11

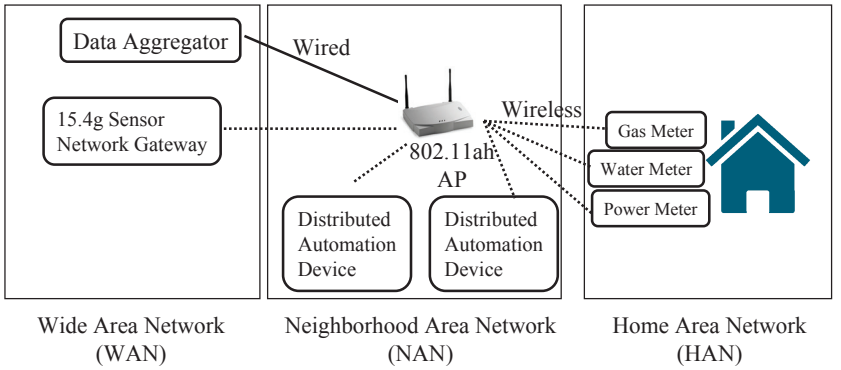
802.11 Standards: Ranges

- 150 kbps to 78 Mbps per spatial stream (up to 4 streams)



Ref: J. DeLisle, "What's the difference between 802.11af and 802.11ah," Microwave and RF, Oct 2015, http://mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah

Sample Application



Ref: H. Wei, "Self-Organizing Energy Efficient M2M Communications," http://cc.ee.ntu.edu.tw/~ykchen/1123-HWei.pdf

802.11ah PHY

1. 802.11ac PHY **down clocked** by 10X
   - 2/4/8/16 MHz channels in place of 20/40/80/160 MHz in ac
   - 20 MHz 11ac and 2 MHz 11ah both have 64 FFT size and 48 data subcarriers + 4 pilots ⇒ 1/10th inter-carrier spacing
     ⇒ 10X longer Symbols ⇒ Allows 10X delay spread
     ⇒ All times (SIFS, ACKs) are 10x longer
   - New 1 MHz PHY with 32 FFT and 24 data subcarriers
2. **Adjacent channel bonding**: 1MHz+1MHz = 2 MHz
3. All stations have to support 1MHz and 2MHz
4. Up to **4 spatial streams** (compared to 8 in 11ac)
5. 1 MHz also allows a new MCS 10 which is MCS0 with 2x repetition ⇒ Allows 9 times longer reach than 2.4GHz
6. **Beam forming** to create sectors

Ref: W. Sun, M. Choi, and S. Choi, "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz," River Journal, 2013, pp. 1-26, http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_115.pdf

802.11 MAC

- **Large number of devices** per Access Point (AP)
  - Hierarchical Association Identifier (AID)
- **Relays** are used to allow connectivity outside the coverage area. Limited to 2-hops.
- **Power Savings Enhancements**:
  - Allows stations to sleep and save energy.
  - AP negotiates a Target Wake Time (TWT) for individual stations
- **Speed frame exchange** allows stations to exchange a sequence of frames for a TXOP.

Ref: E. Khorov, et al., "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," Computer Communications, 2014, http://dx.doi.org/10.1016/j.comcom.2014.08.008

MAC Protocol Versions

- Protocol Version 0 (PV0) is same as that for b/a/g/n/ac
- Protocol version 1 (PV1) is optimized for IoT
  - Short headers
  - Null Data packets
  - Speed packet exchange
  - Improved channel access

Short MAC Header

- MAC Header shortened by 12-26 Bytes:
  - Removed: High throughput control, QoS, Duration field (No virtual carrier sensing)
  - Optional: 3rd address
  - 2-byte AID in place of some 6-byte addresses
  - Frame Control indicates what protocol version is being used
  - Sequence field indicates if 3rd /4th addresses are present

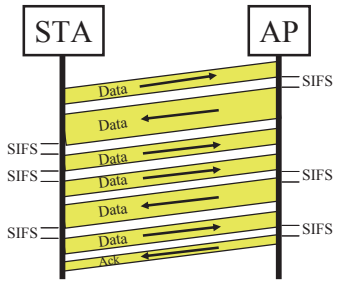
Legacy 802.11 36B	Frame Control 2B	Duration/ ID 2B	Addr 1 6B	Addr 2 6B	Addr 3 6B	Seq. Control 2B	Addr 4 6B	QoS Control 2B	HT Control 4B
802.11ah Downlink 10-24B	Frame Control 2B	AID 2B	BSS ID 6B	Seq. Control 0 or 2B	Addr 3 0 or 6B	Addr 4 0 or 6B			
802.11ah Uplink 10-24B	Frame Control 2B	BSS ID 6B	AID 2B	Seq. Control 0 or 2B	Addr 3 0 or 6B	Addr 4 0 or 6B			

Null Data Packet (NDP)

- Removed: MAC header, Frame check sequence and preamble from the ACK frame ⇒ **Only PHY bits**.
- ACK frame identified by Modulation (MCS) type
- **Block ACK** is also NDP with another MCS
- Clear to Send (CTS) is another NDP with a new MCS

Speed Frame Exchange

- Also called "**Bi Directional Transmit** (BDT)"
- Initiator sends a frame with response indicator set to "long response"
  - Receiver can send data instead of ACK within a SIFS
  - Frames are sent until there are no more frames



Types of Stations

- **High-Traffic**: Listens to Traffic Indication Map (TIM) in beacons and transmit accordingly within a restricted access window ⇒ *TIM Stations*
- **Periodic Low-Traffic**: Negotiate a transmission time allocated in a periodic restricted access windows. Do not listen to beacons ⇒ *Non-TIM Stations*
- **Very Low-Traffic**: Send a poll to AP and get a transmission opportunity in response ⇒ *Unscheduled Stations*

Channel Access for TIM

- Each station knows what segments they belong to.
- Stations wake up every "*DTIM*" interval and find out which beacon they should listen to. The beacon has detailed map indicating which station has pending traffic and when stations can contend for access
- If the map indicates, AP has buffered packets for a station, the station uses DCF (distributed coordination function) to send a PS-poll to get the packet
- If a station has a packet to send, it listens to the map and uses DCF to send RTS
- Small number of stations per slot reduces chances of collisions
- Under low load, it becomes TDMA

Response Indication Deferral (RID)

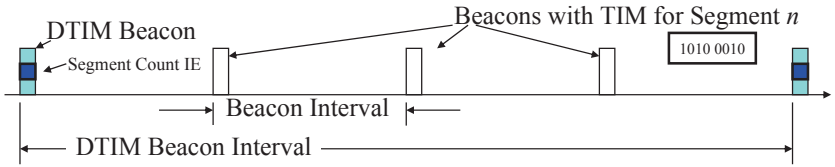
- New virtual carrier sense mechanism replacing NAV (Network Allocation Vector)
- Can not use NAV since there is no duration field
- RID is also a time count down mechanism similar to NAV
- RID is set after reception of PHY header
  NAV is set after reception of complete frame
- RID is set based on the 2-bit response indication field in the PHY header
  - Normal Response: RID ← SIFS + Ack or Block Ack time
  - NDP Response: RID ← SIFS + NDP Frame time
  - No Response (Broadcast frames): RID ← 0
  - Long Response: RID ← SIFS + Longest transmission time (Used with Speed Frame Exchange)

Power Enhancements

- Page Segmentation
- Restricted Access Window
- Target Wake Time

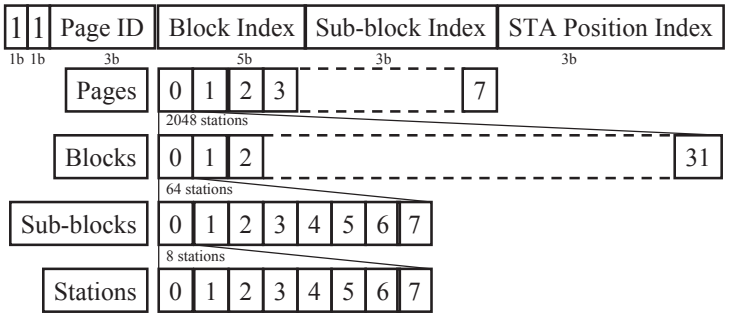
Page Segmentation

- Announcing all buffered frames in each beacon
  ⇒ 8096 bits would be wasted per beacon interval
- AP segments the TIM stations in segments and announces only one segment at a time.
- Every Delivery TIM (DTIM) interval, AP announces which segments have pending data and downlink, uplink periods.



Association Identifier

- 802.11 b/g/n/ac use 11-bit identifier ⇒ 2007 stations
  - 2000+ bits required in "Traffic Indication Map (TIM)"
- 802.11ah uses 16-bit identifier ⇒ 8X stations
  - 8 pages of ~2^{11} stations each. Actually 2007 stations.
    Currently only page 0 is allowed. Page 1-7 are reserved.
    First 2 bits should be 11 to distinguish AID from duration and others.



Restricted Access Window (RAW)

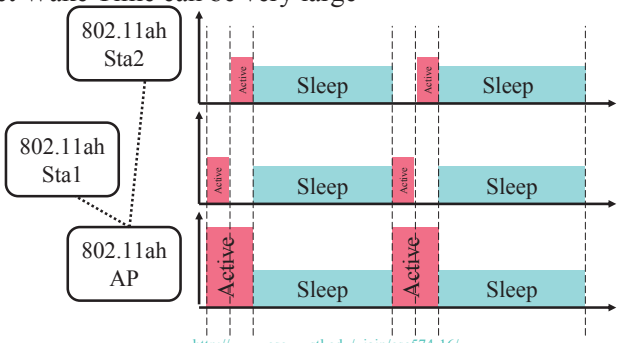
- Allows a set of slot to be restricted to a group of stations
  ⇒ Reduces contention
- A TIM station can be allocated slots during restricted access window (RAW) to transmit/receive packets
- RAW is a part of "Contention Free Period"
- Access may granted for transmission, reception, polling, etc for one or a group of stations
- A raw schedule is transmitted at the beginning of raw interval
- A station can tell AP that it has a frame to transmit using a Uplink Data Indication (UDI) bit
- Dividing stations into groups and dividing time into slots for each group increases the efficiency under heavy load.
  - At 100% load: RAW gives close to 100%.
    Regular EDCF gives 0%.

Other RAWs

- **Periodic RAW**: Period and duration of PRAW are announced by AP
- **Sounding RAW**: used for sector sounding
- **AP Power Management RAW**: use by AP to announce the time when it will be sleeping
- **Non-TIM RAW**: Protects transmission of non-TIM stations
- **Triggering Frame RAW**: Used to allow stations to send PS-poll frames indicating their need to transmit

Target Wake Time (TWT)

- Association request and responses include Target-Wake-Time, Minimum-Wake-Duration, and Wake Interval mantissa.
- AP sends a "Null Data Packet (NDP)" to a station at its target wake up time containing buffering status. A station can then send a PS-poll and get its frames.
- Target Wake Time can be very large



Authentication

- New mechanisms to allow authentication of a large number of stations
- **Centralized Authentication**:
  - AP announces a threshold in the beacon.
  - Each station draws a random number between 0 and 1022
  - Station attempts authentication only if # is less than the threshold.
- **Distributed Authentication**:
  - Truncated Binary Exponential Backoff
  - Each station draws a random slot #
  - Extends the range if unsuccessful

Group Sectorization

- AP can divide the space in sectors
  Each station is told which sector it belongs to.
- Beacon announces which sectors can transmit in this sector interval
- Some sector intervals may be for omni-directional transmissions
  Some may be for only some sectors
- Allows spatial reuse and increase throughput

802.11ah: Summary

1. 802.11ah runs at 900 MHz band ⇒ Longer distance
2. 802.11ah is 802.11ac down by 10x.
   It uses OFDM with 1/2/4/8/16 MHz channels.
   Longer symbols ⇒ Longer multi-path
3. MAC is more efficient by eliminating reducing header, aggregating acks, null data packets, speed frame exchanges
4. Saves energy by allowing stations and AP to sleep longer using Target Wakeup Time, Restricted Access Window

Other LPWANs

Low Power Wide Area Networks (LPWANs)

- **LoRaWAN**, https://www.lora-alliance.org
- SIGFOX, http://www.sigfox.com/
- Weightless-N (Narrowband), http://www.weightless.org/
- Weightless-P (High Performance), http://www.weightless.org/
- NWAVE, http://www.nwave.io/nwave-network/
- OnRamp Wireless, http://www.onrampwireless.com/
- PLATANUS, http://www.m2comm-semi.com/our-protocol/#
- Telensa, http://www.telensa.com/unb-wireless/
- M-Bus by Amber Wireless, https://www.amber-wireless.com/en/products/wireless-m-bus.html
- M2M Spectrum, http://m2mspectrum.com

Ref: C. Pham, "Long-Range Technology Overview," Dec 2015, http://web.univ-pau.fr/~cpham/LORA/WAZIUP-LoRa-overview.pdf

LoRaWAN

- Long Range Wide Area Network.
- Originally developed by Cyclos in France.
  Acquired by Semtech corporation, which formed **LoRa Alliance**.
  Now 160+ members.
- V1.0 spec dated January 2015. Released to public July 2015.
- Rapid Adoption: Products already available on Amazon.


Transceiver

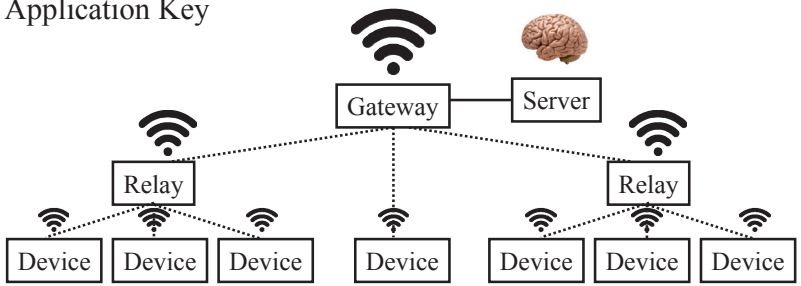

Arduino
Radio Shield

Connectivity Kit for
Arduino, Waspmote,
Raspberry Pi

Ref: https://www.lora-alliance.org/What-Is-LoRa/Technology

Key Features

- **Bidirectional** communication
  ⇒ Allows firmware/software updates of end devices
- **Low Rate**: 0.3 kbps to 22 kbps in Europe, 0.9 kbps in US
- **Star of Stars Topology**: Gateways are transparent bridges. Server is the brain. Simple devices. Relays are optional.
- **Secure**: EUI128 Device Key, EUI64 Network Key, EUI64 Application Key



Ref: https://www.lora-alliance.org/What-Is-LoRa/Technology

Classes of Devices

- **Class A**: Uplink transmission followed by 2 short downlink
  Schedule determined by the end point ⇒ Simple devices.
  - Pure Aloha ⇒ 18.4% =1/2e efficiency under heavy load.
  - Gateways listen to multiple transmissions on multiple channels
  - All gateways listen to all transmissions ⇒ Antenna Diversity.
  - Server selects one gateway for downlink/ack to device ⇒ Mobility
- **Class B**: Class A + extra receive window at scheduled time following the beacon from Gateway
  - All gateways transmit beacons every 2^n seconds (n=0..7)
  - All gateways are synchronized using GPS
  - Device is told receive slot
- **Class C**: Can receive anytime (unless transmitting).
  Generally on AC power

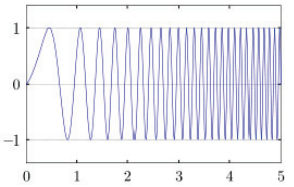
Frequency

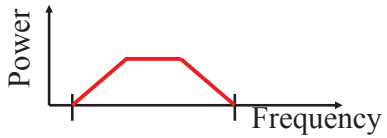
- Uses ISM license-exempt band:
  - 915 MHz MHz in US. Power limit. No duty cycle limit.
  - 868 MHz in Europe. 1% and 10% duty cycle limit
  - 433 MHz in Asia
- Same techniques can be used in 2.4GHz or 5.8 GHz
- Currently suitable for public (single) deployment in an area
  - All gateways report to the same server
  - A device can talk to any gateway
  - All devices use the same frequency

Ref: http://www.link-labs.com/what-is-lora/
http://www.radio-electronics.com/info/wireless/lora/lorawan-network-architecture.php

Chirp Spread Spectrum

- **Chirp**: A signal with continuously increasing (or decreasing) frequency (Whale sound)
- **Chirp Spread Spectrum**: signal is frequency modulated with frequency increasing (or decreasing) from min to max (or max to min) ⇒ power is *spread* over the entire spectrum

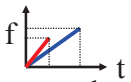




Ref: Z. Ianelli, "Introduction to Chirp Spread Spectrum (CSS) Technology," IEEE 802 Tutorial,
http://www.ieee802.org/802_tutorials/03-November/15-03-0460-00-0040-IEEE-802-CSS-Tutorial-part1.ppt

LoRa Modulation

- Designed to achieve high sensitivity using a cheap crystal
- Allows low power transmissions over long distances
- A form of Chirp spread spectrum.
- Data is encoded using the frequency increase/decrease rate ⇒ Data rate and link condition determines the frequency bandwidth required

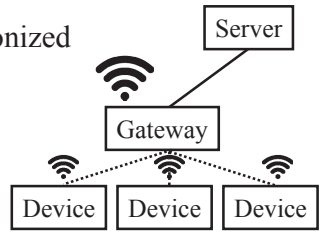


- Multiple parallel transmissions with different data rates on the same frequency
- Can receive signals **19.5 dB below** noise floor with forward error correction (FEC)
- Power level is determined adaptively based on data rate and link condition. Fast communication is used to save battery.

Ref: "LoRA Physical Layer and RF Interface," Radio-Electronics,
http://www.radio-electronics.com/info/wireless/lora/rf-interface-physical-layer.php

LoRaWAN MAC

- LoRaWAN: MAC function over LoRa PHY
- Server manages the network and runs MAC
  - Assigns each device is a frequency, spreading code, data rate
  - Eliminates duplicate receptions
  - Schedules acknowledgements
  - Adapts data rates
- All gateways of a network are synchronized
- Data rate is determined by distance and message duration
- Server determines the data rate using an adaptive data rate (ADR) scheme



LoRaWAN: Summary

1. LoRaWAN is the new MAC standardized by LoRa Alliance
2. LoRa modulation is a variation of chirp spread spectrum where the rate of frequency increase/decrease is modulated by symbol
   ⇒ Increases its resistance to noise
   ⇒ Allows multiple parallel transmissions in one frequency
3. Centralized management and media access control using a "server"
4. Devices broadcast to all gateways. The best gateway replies back.

Summary

1. Dozens of protocols for low-power WAN
2. LoRaWAN has already been implemented and is a leading candidate
3. IEEE 802.11ah is a new standard. To be productized.

Lab 1

A. Download InSSIDer v3.1.2.1 from:

- http://www.techspot.com/downloads/5936-inssider.html or
- http://www.filecroco.com/download-inssider

- Measure the signal levels of various WiFi networks
- Submit a screen capture

B. Download Wireshark from:

- https://www.wireshark.org/#download

- Run a trace packets on your wireless network
- Submit a screen capture

Reading List

- E. Khorov, et al., "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," Computer Communications, 2014, http://www.freepaperdownload.us/1752/Article5078210.htm
- W. Sun, M. Choi, and S. Choi, "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz," River Journal, 2013, pp. 1-26, http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_115.pdf
- http://www.link-labs.com/what-is-lora/
- "LoRA Physical Layer and RF Interface," Radio-Electronics, http://www.radio-electronics.com/info/wireless/lora/rf-interface-physical-layer.php
- https://www.lora-alliance.org/What-Is-LoRa/Technology

References

- C. Pham, "Long-Range Technology Overview," Dec 2015, http://web.univ-pau.fr/~cpham/LORA/WAZIUP-LoRa-overview.pdf
- GreenPeak, http://www.greenpeak.com/Company/Opinions/CeesLinksColumn36.pdf
- H. Wei, "Self-Organizing Energy Efficient M2M Communications," http://cc.ee.ntu.edu.tw/~ykchen/1123-HWei.pdf
- http://www.radio-electronics.com/info/wireless/lora/lorawan-network-architecture.php
- J. DeLisle, "What's the difference between 802.11af and 802.11ah," Microwave and RF, Oct 2015, http://mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah
- Z. Ianelli, "Introduction to Chirp Spread Spectrum (CSS) Technology," IEEE 802 Tutorial, http://www.ieee802.org/802_tutorials/03-November/15-03-0460-00-0040-IEEE-802-CSS-Tutorial-part1.ppt

Wikipedia Links

- https://en.wikipedia.org/wiki/Chirp_spread_spectrum
- https://en.wikipedia.org/wiki/Delivery_traffic_indication_message
- https://en.wikipedia.org/wiki/IEEE_802.11ah
- https://en.wikipedia.org/wiki/IEEE_802.1ah-2008
- https://en.wikipedia.org/wiki/LPWAN
- https://en.wikipedia.org/wiki/Traffic_indication_map

Wikipedia Links (Optional)

- https://en.wikipedia.org/wiki/6LoWPAN
- https://en.wikipedia.org/wiki/Comparison_of_wireless_data_standards
- https://en.wikipedia.org/wiki/DASH7
- https://en.wikipedia.org/wiki/Distributed_coordination_function
- https://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS
- https://en.wikipedia.org/wiki/NarrowBand_IOT
- https://en.wikipedia.org/wiki/Network_allocation_vector
- https://en.wikipedia.org/wiki/On-Ramp_Wireless
- https://en.wikipedia.org/wiki/Short_Interframe_Space
- https://en.wikipedia.org/wiki/Sigfox
- https://en.wikipedia.org/wiki/Weightless_(wireless_communications)

Acronyms

6Lo	IPv6 over Networks of Resource Constrained Nodes
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
6TiSCH	IPv6 over Time Slotted Channel Hopping Mode of IEEE 802.15.4e
AC	Alternating Current
ACK	Acknowledgement
ADR	adaptive data rate
AID	Association Identifier
AMQP	Advanced Message Queuing Protocol
ANT	A proprietary open access multicast wireless sensor network
ANT+	Interoperability Function added to ANT
AP	Access Point
BDT	Directional Transmit
BSS	Basic Service Set
CARP	Channel-Aware Routing Protocol
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environment

Acronyms (Cont)

- CORPL Cognitive RPL
- CSS Chirp Spread Spectrum
- CTS Clear to Send
- DASH-7 Named after last two characters in ISO 18000-7
- dB DeciBel
- DCF Distributed coordination function
- DDS Data Distribution Service
- DECT Digital Enhanced Cordless Telephone
- DECT/ULE Digital Enhanced Cordless Telephone with Ultra Low Energy
- DTIM Delivery Traffic Indication Map
- DTLS Datagram Transport Layer Security
- EDCF Enhanced Distributed Coordination Function
- EDSA Embedded Device Security Assurance
- EUI Extended Unique Identifier
- FEC Forward error correction
- FFT Fast Fourier Transform

Acronyms (Cont)

- GHz Giga Hertz
- GP Green PHY
- GPS Global Positioning System
- HAN Home Area Network
- ID Identifier
- IEC International Engineering Council
- IEEE Institution of Electrical and Electronic Engineers
- IoT Internet of Things
- ISA International Society of Automation
- ISM Instrumentation Scientific and Medical
- LoRa Long Range
- LoRaWAN Long Range Wide Area Network
- LowPAN Low Power Personal Area Network
- LPWANs Low Power Wide Area Network
- LTE-A Long-Term Evolution Advanced
- LTE Long-Term Evolution

Acronyms (Cont)

- MAC Media Access Control
- MCS Modulation and Coding Scheme
- MHz Mega Hertz
- MQTT Message Queue Telemetry Transport
- NAN Neighborhood Area Network
- NAV Network Allocation Vector
- NDP Null Data Packet
- NFC Near Field Communication
- NWAVE Name of a company
- OFDM Orthogonal Frequency Division Multiplexing
- PHY Physical Layer
- PLATANUS Name of a company
- PRAW Periodic Random Access Window
- PS Power Save
- PV0 Protocol Version 0
- PV1 Protocol Version 1

Acronyms (Cont)

- QoS Quality of Service
- RAW Restricted Access Window
- RF Radio Frequency
- RID Response Indication Deferral
- RPL Routing Protocol for Low Power and Lossy Networks
- RTS Request to Send
- SASL Simple Authentication and Security Layer
- SIFS Short Inter-frame Spacing
- SIGFOX Name of a company
- SMACK Simple Mandatory Access Control Kernel for Linux
- STA Station
- TCG Trusted Computing Group
- TDMA Time Division Multiple Access
- TIM Traffic Indication Map
- TV Television
- TWT Target Wake Time

Acronyms (Cont)

- TXOP Transmission Opportunity
- UDI Uplink Data Indication
- ULE Ultra Low Energy
- US United States
- WAN Wide Area Network
- WiFi Wireless Fidelity
- WiMAX Worldwide Interoperability of Microwave Access
- WLAN Wireless Local Area Networks

Scan This to Get These Slides

Related Modules

Internet of Things,
http://www.cse.wustl.edu/~jain/cse574-16/j_10iot.htm

Introduction to Vehicular Wireless Networks,
http://www.cse.wustl.edu/~jain/cse574-16/j_08vwn.htm

Introduction to 5G,
http://www.cse.wustl.edu/~jain/cse574-16/j_195g.htm

Wireless Protocols for IoT Part III: ZigBee,
http://www.cse.wustl.edu/~jain/cse574-16/j_13zgb.htm

Audio/Video Recordings and Podcasts of Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw