Power Line Communications

Acknowledgement: Based on the slides
by Dr. Richard Newman in CIS 6930
at the University of Florida.

Outline

- What is PLC?
- PLC challenges
- Broadband Over Power Lines
- Channels
- Forward Error Correction
- HomePlug AV PHY
- HomePlug AV MAC
- IEEE P1901

What is PLC?

- PLC = power line communication
  - Uses existing power distribution wires
- PLC has been in use for many decades
  - Utility company use at very low data rates for control purposes
- Very challenging communication environment
  - High attenuation, low power
  - Multipath fading, noise
- Recent advances in processing power enable high-speed communication

Uses of PLC

- Control
  - Utility company use – plant control, AMR
  - Vehicular systems – trucks, planes, …
  - Smart home – security, HVAC, lighting/power, etc.
  - Industrial remote control
- In-home Networks
  - Power lines become “Ethernet”
  - Multimedia distribution – audio, video, VoIP
- Access Networks
  - Solves “last 100 meters” problem
  - Necessarily shared

Visions

- Imagine networking your PCs, laptops, printers, cable/DSL modem, etc. by simply plugging them into power outlets
- Imagine repositioning your wireless AP for improved reception by simply moving a device the size of a deck of cards to a different outlet
- Imagine streaming HDTV from DVD/PVR/set-top box to any display without adding new wires
- Imagine moving your telephone to any location by changing where it is plugged in

Visions (con't)

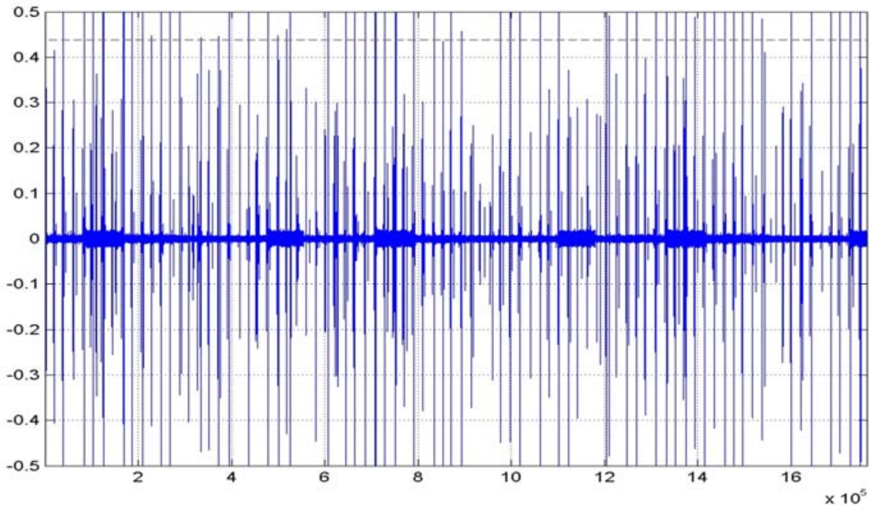
- Those can all be done today!
- Future: smart home/smart grid
  - Every electrical appliance could have PLC capability
  - Allow real-time monitoring and control
  - Enable new interactions between devices

PLC Challenges

PLC Challenges

- Low power (!) signals
  - Government regulations specify maximum emission levels
  - Must not interfere with existing uses
- High Attenuation
- Frequency-selective Fading
- Interference
- Impulse Noise
- Hidden Nodes

Hair Dryer Noise on Power Line

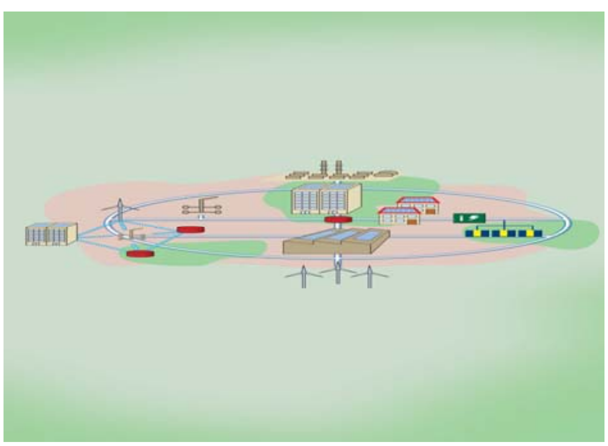


Broadband Over Power Lines

Narrowband PLC

- Smaller bandwidth, usually lower frequency
- Inexpensive
- Lower data rate
- Long used for control applications
- Standards
  - CEBus
  - LONworks
  - PLC4Trucks

Narrowband PLC - Utilities



- Distribution Automation
  - Intelligent grid
  - Asset control & monitoring
  - Load mgmt
- AMR
- Telesurveillance

In-home Broadband PLC

- Advances in processing, algorithms allows higher data rates
- ca. 2000 HomePlug 1.1
  - Up to 14 Mbps raw rate, 8 Mbps after coding
  - Up to 6 Mbps TCP/IP throughput
- ca. 2005 Panasonic proprietary – video xfer
- ca. 2006 HomePlug AV
  - Up to 200 Mbps raw, 150 Mbps after coding

In-home Broadband PLC

- Standardization efforts
  - HomePlug Powerline Alliance (HPA)
  - IEEE p1901
  - ITU-T G.hn
- Support
  - FCC ruling ca. 2006
  - NIST citation
- Issues from neighboring PLC networks

Access Broadband PLC

- Longer impulse response times mean lower efficiency (Cyclic Prefix in OFDM)
- Longer, straight wires mean higher emissions, interference
- Similar techniques as used in in-home PLC PHY still work, after modifications
- Access PLC network is shared

Access Broadband PLC (con't)

- Standardization efforts
  - UPA
  - IEEE p1901
  - OPERA
- Uncertainty
  - EMC rules vary or are not established in many countries
  - Opposition from amateur radio operators
  - FCC, CISPR

Broadband Over Power Lines

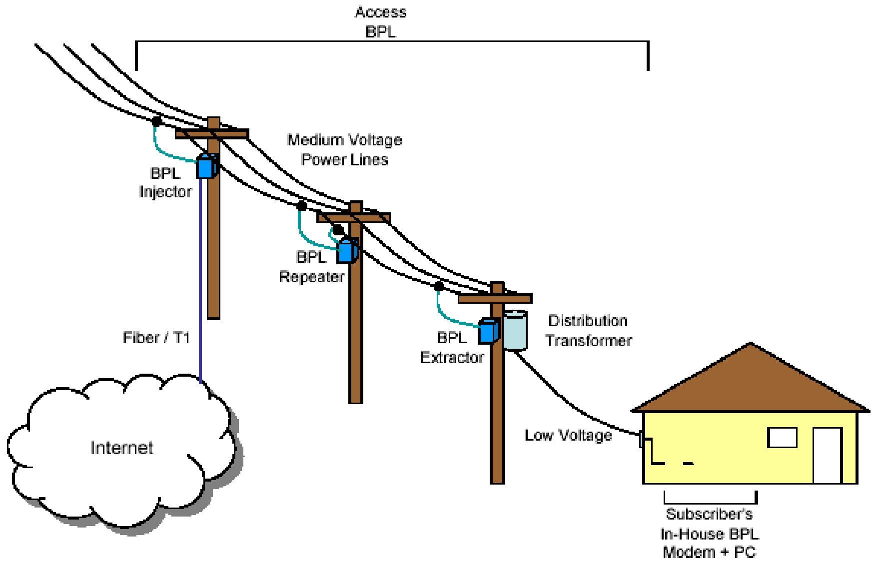


Figure 2-1: Basic BPL System

NTIA Report 04-413, Potential Interference From Broadband Over Power Line (BPL) Systems To Federal Government Radiocommunications AT 1.7 - 80 MHz, Phase 1 Study - U.S. DEPARTMENT OF COMMERCE, National Telecommunications and Information Administration

Broadband Over Power Lines

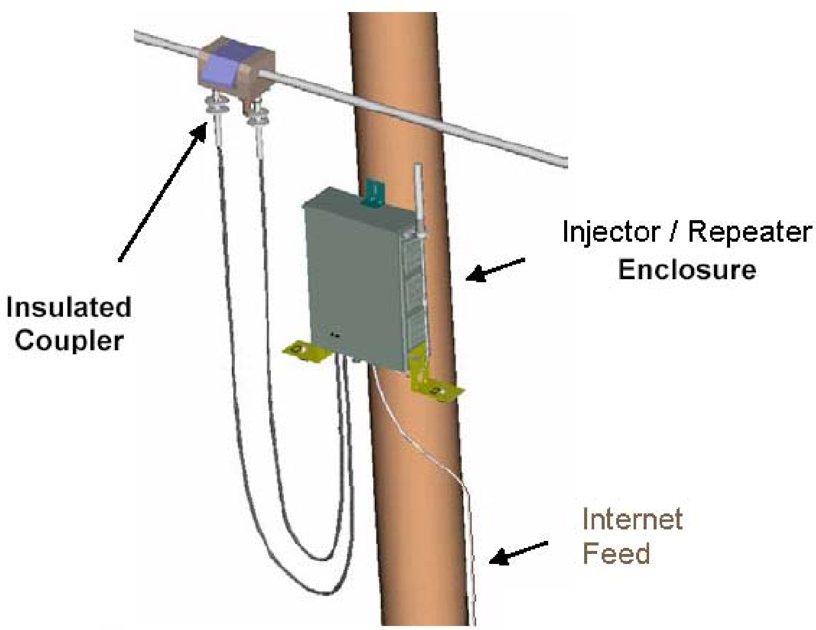
BPL and HF – A Primer © ARRL 2004

Broadband Over Power Lines

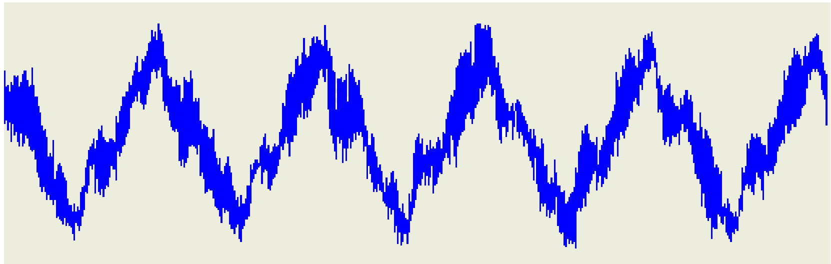
BPL and HF – A Primer © ARRL 2004

Broadband Over Power Lines

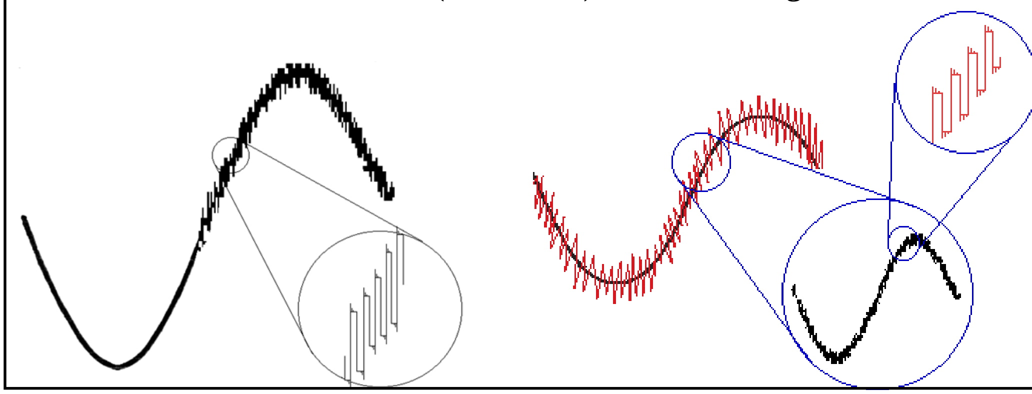
BPL Injector / Repeater



Broadband Over Power Lines



60 Hz AC with 1.4 MHz **AM** above,
with **PCM** below left (as in DSL), and below right for BPL



Coexistence

- In-home and access broadband PLC operate in same band
- Disaster if PLC technologies sabotage each other
- Standardization efforts
  - CENELEC
  - IEEE p1901
  - OPERA

Channels

Bands

- Low frequency: 0-1KHz
  - Utility use for control
- Medium frequency: 1 Khz- 1 MHz
  - Residential and commercial control, radio
- High frequency: 1 MHz – 100 MHz
  - Broadband – IH and AC
- Ultra-high frequency: > 100 MHz

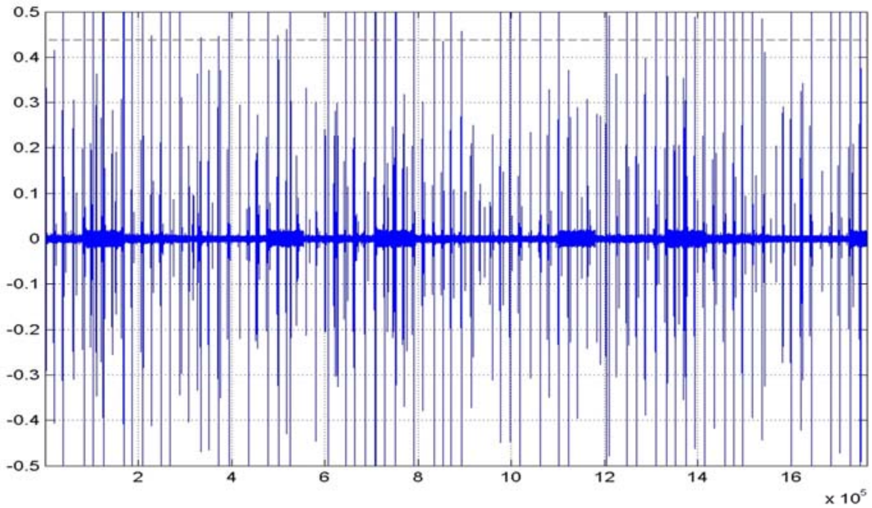
Frequency Dependent Fading

- Multiple reflection points in medium
  - Wire gauge changes
  - Sharp turns in wiring
  - Junction box connections
- Causes frequency dependent fading
- Longer impulse response => ISI
- Load changes affect channel
- Every path is unique (even in each direction)

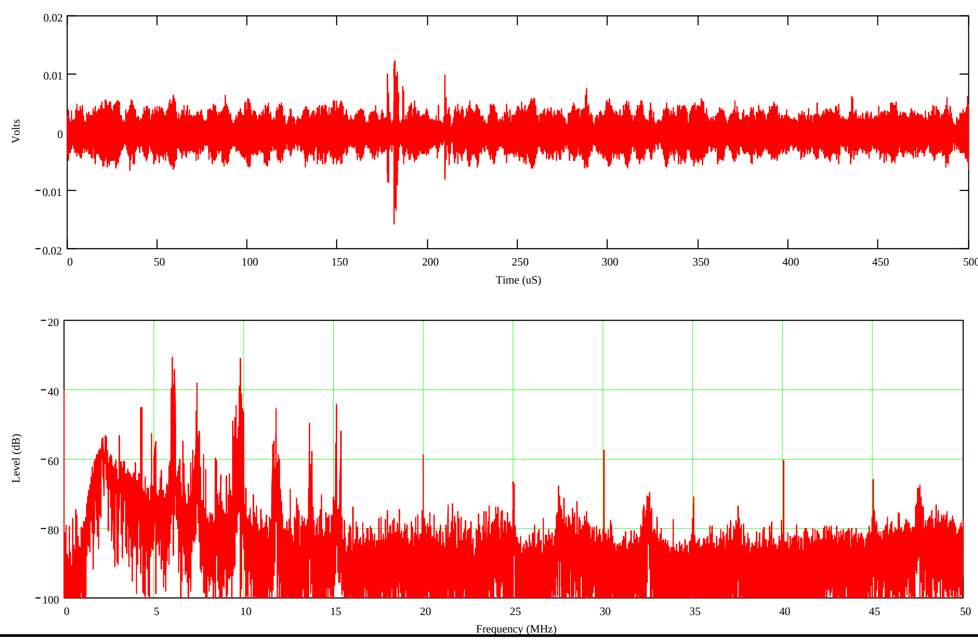
Noise Sources

- Brush motors
  - Hair dryer, drill, mixer, blender, etc.
  - Usually intermittent
- Periodic impulses
  - Switching power supply, halogen lamp, etc.
  - Severe noise power
- Random impulse noise
  - Light dimmer switch, power system “glitches”
- Radio interference
  - Amateur radio transmitters

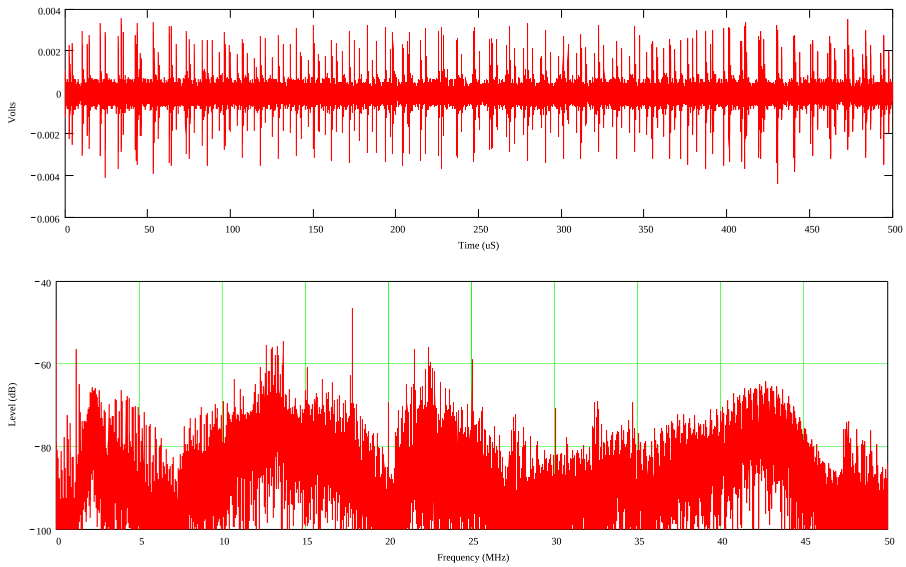
Hair Dryer Noise on Power Line



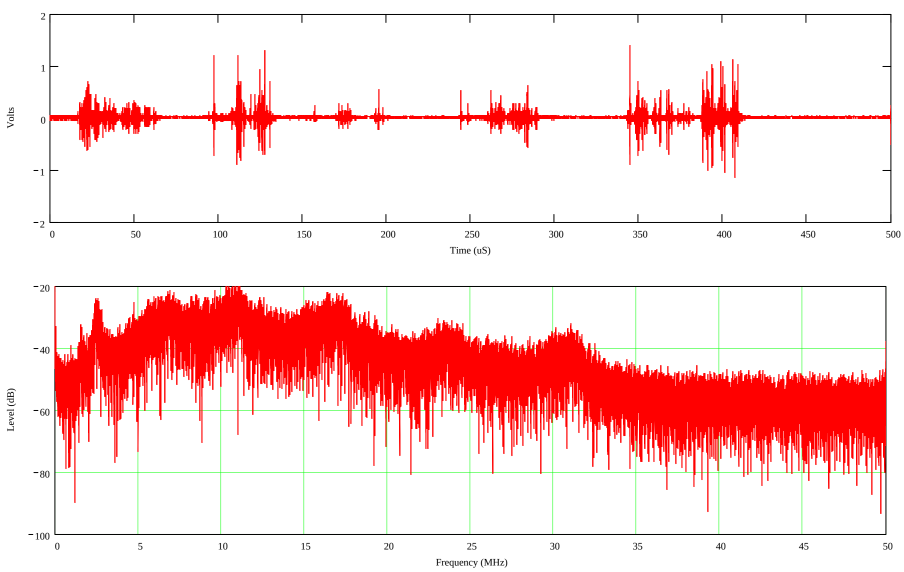
Drill Noise on Power Line



Periodic Impulse Noise



Random Impulse Noise



Forward Error Correction

Error Handling

- Forward Error Correction
  - Copy codes
  - Block codes
  - Convolutional codes
  - Scrambling
  - Concatenated codes
  - Turbo-codes
  - Low Density Parity Check (LDPC)
- Backward Error Correction (BEC)

Error Correction Strategies

- Forward Error Correction
  - Include sufficient redundancy in transmitted units that errors can be corrected
  - Simplifies sender protocol – used in PHY
- Backward Error Correction
  - Include sufficient redundancy in transmitted units that errors can be detected
  - Retransmit damaged units
  - More efficient – used in MAC and above
- Limitations
  - Hamming Distance of code limits capabilities
  - Always possible to “fool” receiver

General ECC Considerations

- Systematic vs. non-systematic
  - Systematic = data bits appear in coded stream
  - Non-systematic = no data bits identifiable
- Hamming Distance
  - H(x,y) = number of bits where x and y differ
  - Code C = {x1, x2, ..., xN} set of valid codewords
  - d = H(C) = min{H(x,y) | x and y are distinct codewords in C}
  - Maximum detection ability = d-1
  - Maximum correction ability = (d-1)/2

Forward Error Correction

- Block vs. continuous
- Block = set number of information symbols encoded into set number of code symbols
  - Internal fragmentation
  - Need for delimitation
- Continuous = stream of information symbols encoded into stream of code symbols
  - Memory/constraint length – must “fill the pipeline”
- Linearity
  - Sum of two code words is a code word
- Concatenation
  - Combine two codes (inner and outer) to increase correction capabilities

Forward Error Correction

- Efficiency = code rate
- Rate = k/n for (n,k) code
  - k = “information bits”
  - n = total bits
  - t = n-k = redundant bits
- With continuous codes, need to account for “tail” - the number of bits in the memory

Block Codes

- Copy codes
- LRC
- Hamming codes
- Reed-Solomon
- LDPC

Block Codes

- Copy Codes
  - Simplest code
  - Copy data bits r times to encode
  - Use received copies to “vote” for input value
  - Can survive a burst error if scrambled
- LRC – Longitudinal Redundancy Check
  - Information bits arranged in p-1 by q-1 matrix
  - Each row has parity bit at the end
  - Each column has parity bit at the bottom
  - n = pq, k = (p-1)(q-1), r = p+q-1
  - Detects single bit errors

LRC Example

1 0 1 1 0 1 1 0 1 0 1 1 = information bits

```
1 0 1 1 _          1 0 1 1 1
0 1 1 0 _    ->    0 1 1 0 0
1 0 1 1 _          1 0 1 1 1
_ _ _ _ _          0 1 1 0 0 <- LRC
                           ^ VRC
```

1 0 1 1 1 0 1 1 0 0 1 0 1 1 1 0 1 1 0 0 = code word

LRC Example

1 0 1 1 1 0 1 1 0 0 1 0 1 1 1 0 1 1 0 0 = sent

0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 = error

1 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 0 = received

```
1 0 1 1 1
0 1 0 0 0 X
1 0 1 1 1
0 1 1 0 0
    X
```

errors in LRC and VRC locate bit error

Hamming Codes

- Hamming Codes
  - “perfect” 1-bit error correction
  - $n = 2^t - 1$ bits per code word
  - t parity bits, remainder systematic information bits
  - Parity bit i is in position 2^i (i=0,1,2,…,t-1)
  - Parity bit i checks even parity of bits in positions with i-th bit of location non-zero
    - For example, i=2, it will check positions ?1??, which include 0100, 0101, 0110, 0111, 1100, 1101, 1110, 1111 (4, 5, 6, 7, 12, 13, 14, 15)

Hamming Code Example

t = 4, length n = 16-1 = 15 bits, k = 11

information bits = 10110110101

```
f  e d c b a 9 8 7 6 5 4 3 2 1     bit positions
1 0 1 1 0 1 1 _ 0 1 0 _ 1 _ _      info bits in pos n
---------------->1                 parity bit 3
---------           ------->0      parity bit 2
-----    -----    -----    -->0    parity bit 1
--   --  --   --  --   --   -- >0  parity bit 0
1 0 1 1 0 1 1 1 0 1 0 0 1 0 0      code word
```

Hamming Code Example

f e d c b a 9 8 7 6 5 4 3 2 1	bit positions
1 0 1 1 0 1 1 1 0 1 0 0 1 0 0	code word
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0	error
1 0 1 1 0 0 1 1 0 1 0 0 1 0 0	received word
---------------->0	parity bit 3 X
--------- ------->0	parity bit 2
----- ----- ----- -->1	parity bit 1 X
-- -- -- -- -- -- -- >0	parity bit 0

- Syndrome = 1010 = a = location of error
  - Bit error => invert received bit to correct it

Reed-Solomon Codes

- A special kind of BCH code (Bose, Chaudhuri, Hocquenghem ca. 1960)
- Based on oversampled polynomial
- Redundant samples allow optimal polynomial to be recovered if most samples are good
- Handles small bursts
- Popular
  - DVDs, CDs, Blu-Ray, DSL, WiMax, DVB, ATSC, Raid-6

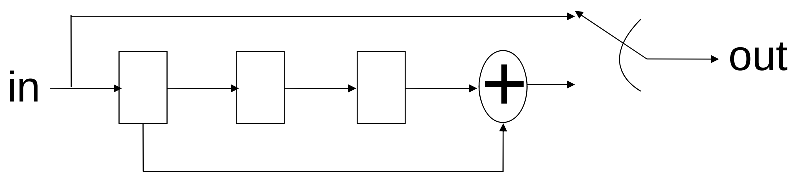
Low Density Parity Check Codes

- Linear code
- Capacity approaching code
  - Can get near to Shannon limit in symmetric, memoryless channel
- Uses iterative belief propagation
- Defined by sparse parity check matrix
- Used in DVB-S2 digital TV, ITU-T G.hn, 10GBase-T

Convolutional Codes

- May be systematic or not
- Shift register for information bits
- Each output bit has one or more taps into shift register
- Tapped values are XORed to produce output
- Outputs are sent round robin
- May “puncture” output to increase coding rate
- May “scramble” input to spread errors out

Convolutional Codes



1 0 0 1 1 0 1 -> = info bits

1 **0** 0 **0** 1 1 1 0 1 0 1 1 0 1 0 0 1 1 -> = output

----

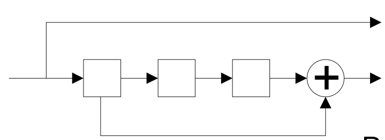
tail

Initialize shift register with 0's,
then shift in one bit at a time,
then read one bit from each output

Convolutional Codes

data = 1011001 tail = *00*

$G(x)=x^2+1$



Input				Parity
	0	0	0	
1	1	0	0	1
0	0	1	0	0
1	1	0	1	0
1	1	1	0	1
0	0	1	1	1
0	0	0	1	1
1	1	0	0	1
0	*0*	1	0	0
0	*0*	*0*	1	1

Output

1
1
0
0
1
0
1
1
0
1
0
1
1
1
0
0
0
1

Some Puncturing Matrix

Code Rate	Puncturing Matrix
1/2	1 1
2/3	1 0 1 1
3/4	1 0 1 1 1 0
5/6	1 0 1 0 1 1 1 0 1 0
7/8	1 0 0 0 1 0 1 1 1 1 1 0 1 0

Decoding Convolutional Codes

- Maximum Likelihood Decoding
- Viterbi Algorithm
  - "Trellis" decoding
  - Dynamic programming
  - Number of states = 2^m, m=constraint length
  - State = contents of shift regisiter
  - Cost = HD for transition based on received bits

http://www.cambridge.org/resources/0521882672/7934_kaeslin_dynpro_new.pdf

Scrambling

- Convolutional codes correct well when errors are sparse
- Tend to have problems with burst errors
  - Scramble bits after encoding, before decoding
  - Concatenated codes – allow errors/resynch
- Scrambling
  - Shuffle order of bits on the way out/in
  - Interleaver depth = memory required to shuffle
  - E.g., fill block in row order, read out column order

Turbo Codes

- Essentially concatenating two convolutional codes (may be the same code)
- One code operates on straight input
- Other code operates on delayed and interleaved input
- Decoding involves iteration between the two codes
- Can approach Shannon Limit
- Patents held by French Telecom

Backward Error Correction (BEC)

- Received data cannot be corrected
- Include checksum/redundancy check to detect errors
- Retransmit frames that have errors
- How does sender know which to resend?
  - ACK – OK, don't resend
  - NAK – Received damaged frame
  - No response – time out and resend
- ACKs
  - Cumulative vs. individual vs. SACK

Acknowledgements

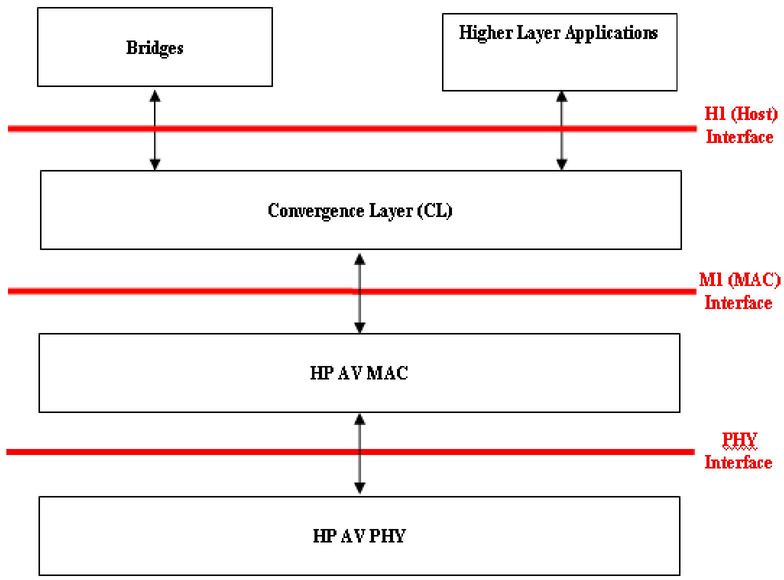
- ACK types
  - Individual ACK – just the SN indicated
  - Cumulative ACK – indicates next expected unit
    - Beneficial when ACKs are lost - redundancy
  - SACK – indicates multiple good/back units
- Sequence Number (SN) per unit
  - Units may be frames, bytes, cells, etc.
  - SNs eventually wrap around
  - Need to avoid confusion – send/receive window
  - Larger SN = more framing overhead

HomePlug AV PHY

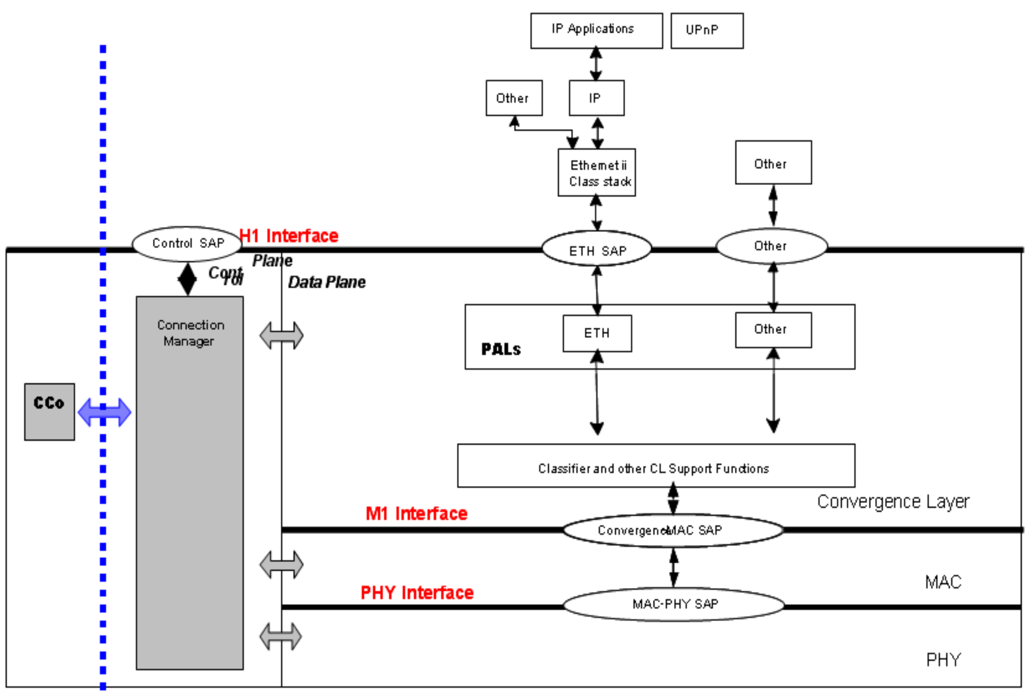
What is HomePlug AV?

- Broadband PLC for home networking
- Open industry standard
  - 6+ manufacturers
- Developed 2003-2007 by Homeplug Powerline Alliance (HPA)
  - Consortium of chip designers, OEMs, PLC users
  - Products shipped in 2006
- Second ethernet class PLC, most widely available
  - 150 Mbps coded PHY data rate
  - 0ver 40 million units shipped
- Comprises
  - PHY – modulation, coupling, FEC, etc.
  - MAC – medium access, ARQ, etc.
  - Bridging – to other PLC networks or to 803.3/11/etc.

Reference Model



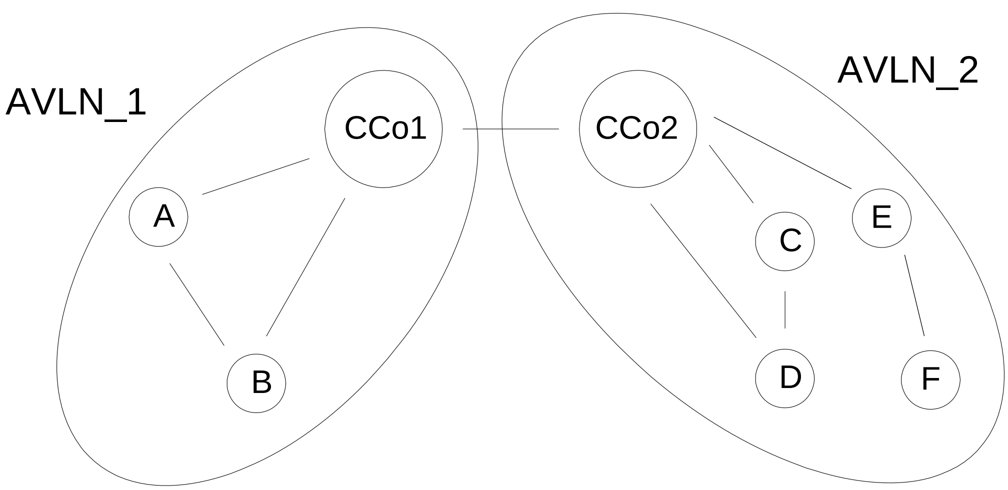
Protocol Layer Architecture



HPAV Networks

- Physical Network (PhyNet)
  - Relative to a station (STA)
  - All other STAs able to communicate with the reference STA
- Logical Network (AVLN)
  - Has a Central Coordinator (CCo) STA
  - Set of STAs with same
    - Network ID (NID) and
    - Network Membership Key (NMK) (usually)

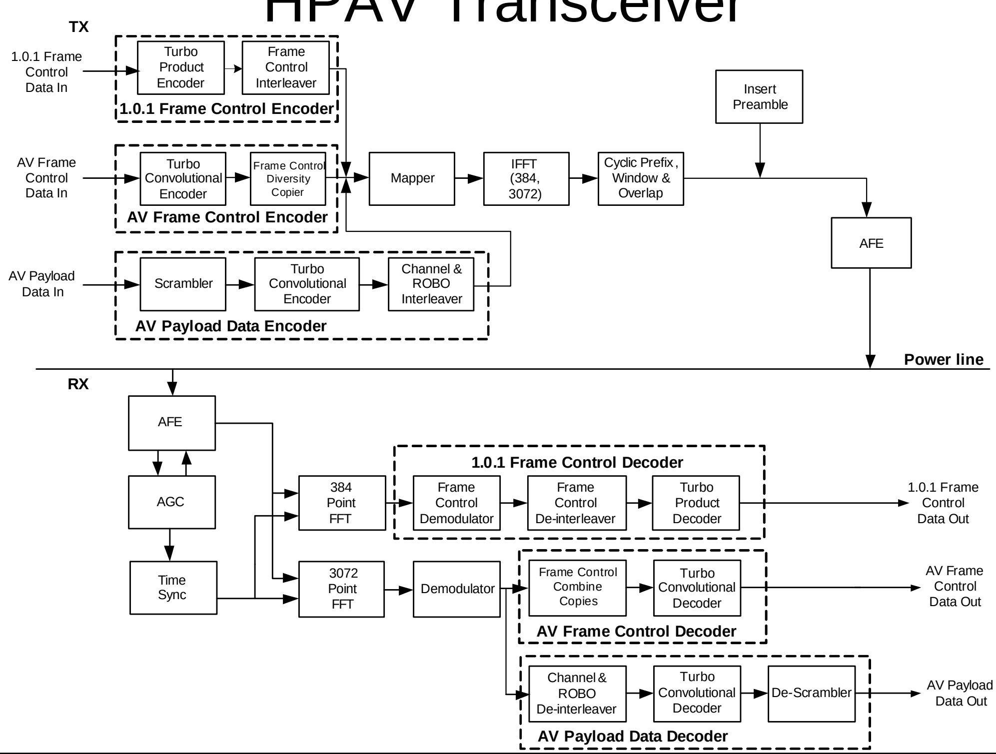
AV Logical Networks



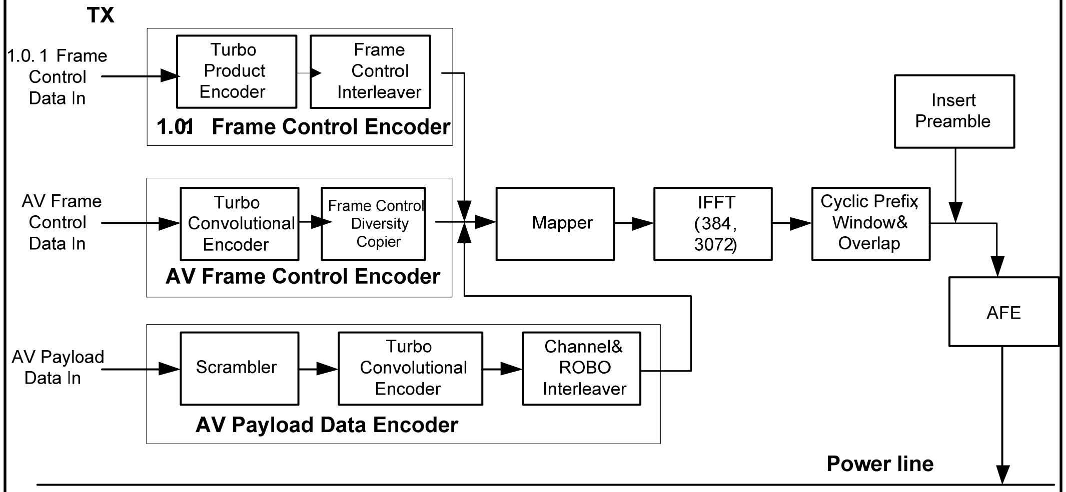
HPAV PHY

- Windowed OFDM – 917 carriers 1.8 – 30 MHz
- Turbo Convolution Codes, copy codes
- 200 Mbps channel rate/150 Mbps information rate

HPAV Transceiver

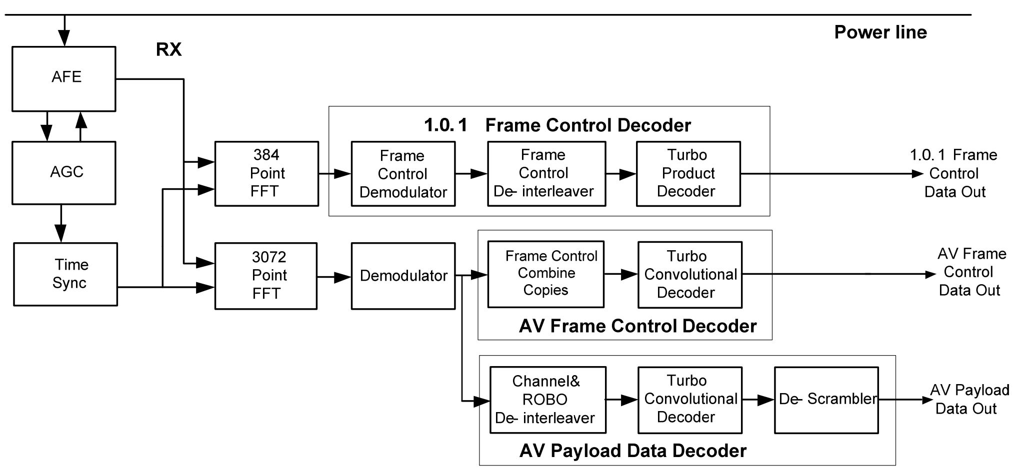


HPAV Transmitter



- Data paths for HP1.0.1 FC, AV FC, and payload
- Turbo convolutional encoders for AV paths
- Architecture similar to HP 1.0.1 transmitter

HPAV Receiver



- 384 point FFT for HP1.0.1 FC
- 3072 point FFT for AV FC and payload
- Turbo convolutional decoders for AV paths

HomePlug AV MAC

HPAV Challenges

- Backward compatibility with HP1.0
  - Delivered base of over 10 million chips
  - Return customers likely
- Take advantage of high speed PHY
  - Fixed time overheads for delimiters/VCS
  - MSDUs typically less than 1500 octets
- Provide QoS for video/audio/gaming/etc.
  - Latency and jitter control
  - Bandwidth “guarantees”
- Deal with PHY challenges
  - Channels change – can degrade, cause loss
  - Impulse noise may destroy 1-2 symbols per impulse
  - Hidden nodes, neighbor networks

HPAV Challenges (2)

- Minimize overhead
  - Aim at 80% MAC efficiency for streams
  - Low efficiency expected with low data rate streams
- User-friendly security
  - Must be understandable
  - Must be convenient
  - Must be secure
- Stations may leave unexpectedly
  - Consumer electronic devices
  - Not dedicated to AVLN like AP is to WLAN

HPAV Solution Approaches

- Backward compatibility with HP1.0
- Take advantage of high speed PHY
  - Maximize PHY Body length for efficiency
- Provide QoS for video/audio/gaming/etc.
  - Timestamp MSDUs with QoS needs
  - Move on if MSDU can’t be delivered on time
  - Admission control for new QoS streams
  - Scheduled access

HPAV Solution Approaches (2)

- Deal with PHY challenges
  - Maintain view of channel rates
  - Maintain view of stream backlogs
  - Allow partial reception of MPDU
  - RTS/CTS for hidden nodes
  - Redundancy for scheduling information
  - Neighbor network coordination
- User-friendly security
  - Network password entry
  - Device password entry

HPAV Solution Approaches (3)

- Minimize overhead
  - Aggregation of MSDUs, management messages
  - Minimize use of delimiters
  - Small addresses – 8-bit Terminal Equipment IDs (TEIs)
  - Allow for contention-free access
  - Integrated encryption/IV derivation
- Stations may leave unexpectedly
  - Employ soft state
  - Use negotiation for determining coordinator
  - Allow for handover/recovery of responsibilities

HPAV Solutions

- Backward compatibility with HP1.0
- Central Coordinator
  - Allows admission control/scheduled access
  - Must be able to move CCo/recover from loss of CCo
  - Maintains authoritative network time base
- Central Beacon
  - Provides common information
  - Provides synchronization for access
  - Advertises network time base (NTB) for QoS
  - Includes persistence for redundancy
  - Synchronized to line cycle
- Proxy Coordinator
  - Repeats Central Beacon for hidden nodes

HPAV Solutions (2)

- Contention-Free Periods
  - Managed by call admission through CCo
  - Regions reserved for specific streams
  - Reservations persist in same part of line cycle
  - QoS stream creation negotiated by all parties
  - Global link identifiers for efficient reference
  - Expand/squeeze as needs/channels change
- Two-level Segmentation/Reassembly
  - Aggregate MSDUs into MAC Frame stream
  - Segment MF Stream for encryption/transmission
  - Make segments unit of reliable delivery inside MAC
  - CRC per segment
  - Selective Acknowledgements for multiple segments

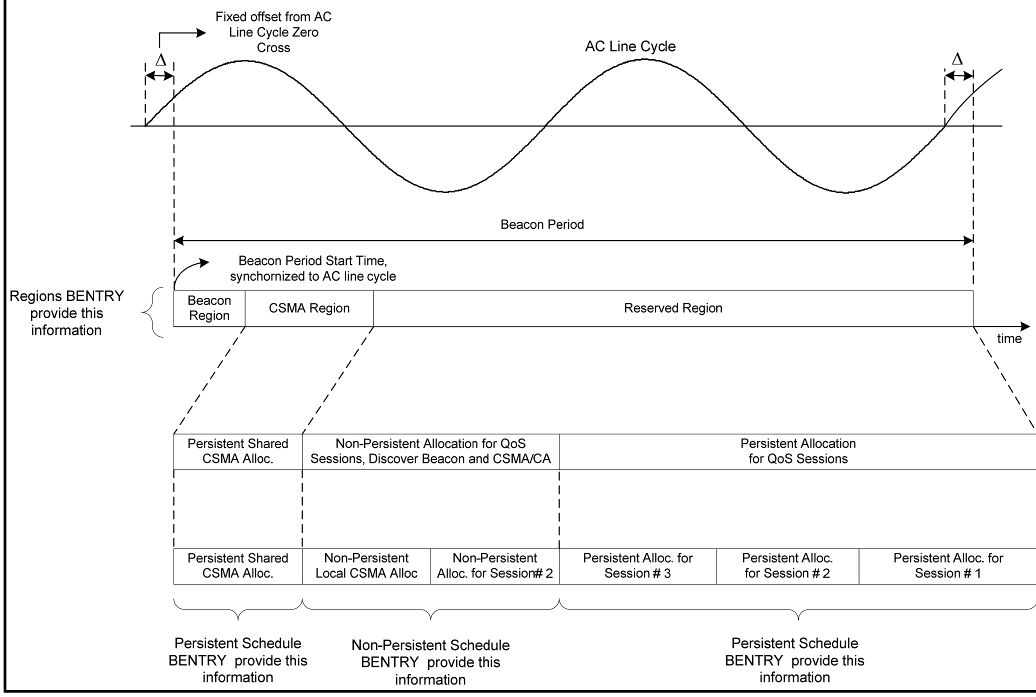
HPAV Solutions (3)

- MPDU bursting to save on ACKs
  - Acknowledge all segments in multiple MPDUs in SACK
  - MPDU number to know when to send SACK
  - MPDU count to know burst duration
- AV Logical Networks based on cryptography
  - Key hierarchy
  - NMK needed to join logical network
  - NEK used for data encryption
  - Integrated segmentation/encryption
  - IV derived from MPDU and segment information
  - Push-button inherently insecure at time of join
  - Two security levels
  - Password parameter definition

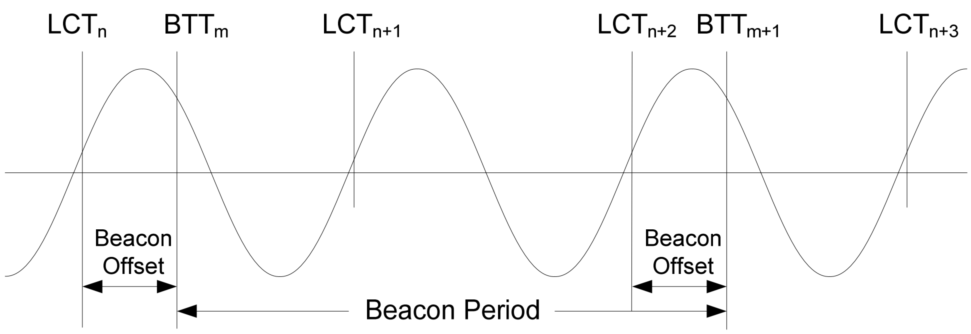
HPAV General Operation

- Each AVLN has a CCo
  - CCo is determined dynamically
  - CCo give general information in beacon
  - CCo admits new STAs
- STAs join AVLN by requesting NEK
  - STA must have Network Membership Key (NMK) to get Network Encryption Key (NEK)
  - Unauthenticated STAs can do very little
  - STA gets NEK from CCo
- Time divided into Beacon Periods (BPs)
  - Access information based on BP

HPAV Beacon Periods



HPAV Beacon Timing



- Line Cycle Crossing Time (LCT)
  - PHY detection and digital phase lock loop (DPLL)
- Beacon Offset
  - Use to keep network time base (NTB)
  - Advertise future beacon transmit times

HPAV Beacon

- Beacon Payload holds 136 octets

- Beacon sent periodically (once per BP)
  - Sent by Central Controller (CCo)
  - Provides reference Network Time Base (NTB)
  - Indicates offsets for future Beacons
- Three Beacon types
  - Central Beacon – issued by CCo
    - Provides scheduling information
  - Proxy Beacon – copy of central beacon repeated by Proxy Coordinator (PCo) when hidden nodes
  - Discovery Beacon – sent for network discovery

Beacon Scheduling Info

- Non-Persistent Scheduling Information
  - Can change from one Beacon Period to the next
  - Extra allocations to backlogged QoS streams
  - Extra CSMA region
  - Discover beacons
- Persistent Scheduling Information
  - Remains constant for advertised number of BPs
  - Allows access even when Beacon is lost
  - Persistence information included in Beacon
  - Persistent CSMA allocations – for CSMA access
  - Persistent TDMA allocations – contention-free
  - May include preview schedule when changing

Beacon Schedule Persistence

		1	2	3	4	5	6	7	8	9	10	11	12	...
Schedule A	PSCD	0	0	0	0	0								
	CSCD	3	3	2	1	0								
Schedule B	PSCD			3	2	1	0	0	0					
	CSCD			2	2	2	2	1	0					
Schedule C	PSCD						3	2	1	0	0	0	0	0
	CSCD						1	1	1	1	1	1	1	...
Current Schedule		*A*	*A*	*A*	*A*	*A*	*B*	*B*	*B*	*C*	*C*	*C*	*C*	*C*
Beacon Period #		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**...**

- CSCD – current schedule countdown
  - Minimum # BPs for which this schedule is valid
- PSCD – preview schedule countdown
  - # BPs in which this schedule will take effect

HPAV MAC Frames

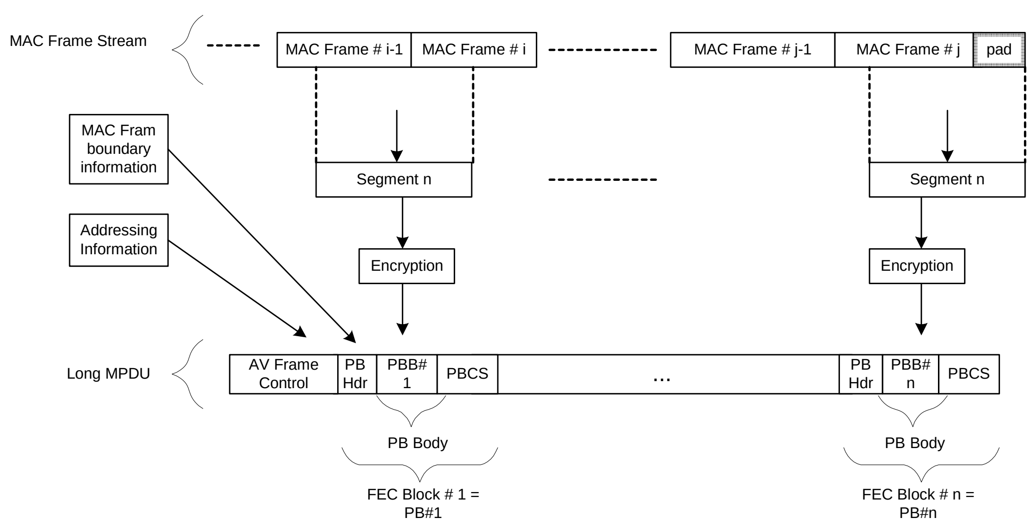
2 Octets	4 Octets	Variable number of Octets	4 Octets
MAC Frame Header	ATS/Confounder (Optional)	MSDU Payload or Management Message	ICV

- Delimit messages
  - Aggregation for efficient transmission at high speeds
  - Needed for disaggregation
- Provide timing information (Arrival TimeStamp)
  - Needed for jitter control, delivery guarantees
- Check correct reassembly, decryption
  - Integrity Check Value (ICV)

MAC Frame Fields

- MF Header
  - MF Type (2 bits)
    - Bit pad to end of segment
    - MSDU without ATS
    - MSDU with ATS
    - Management Message with confounder
  - MF Length (14 bits)
- ATS/Confounder (0 or 32 bits)
  - Arrival timestamp for AV streams
  - Random confounder for Management Messages
- Body
  - MSDU from higher layer or Management Message
- Integrity Check Value (32 bit CRC)
- Total overhead = 6-10 octets

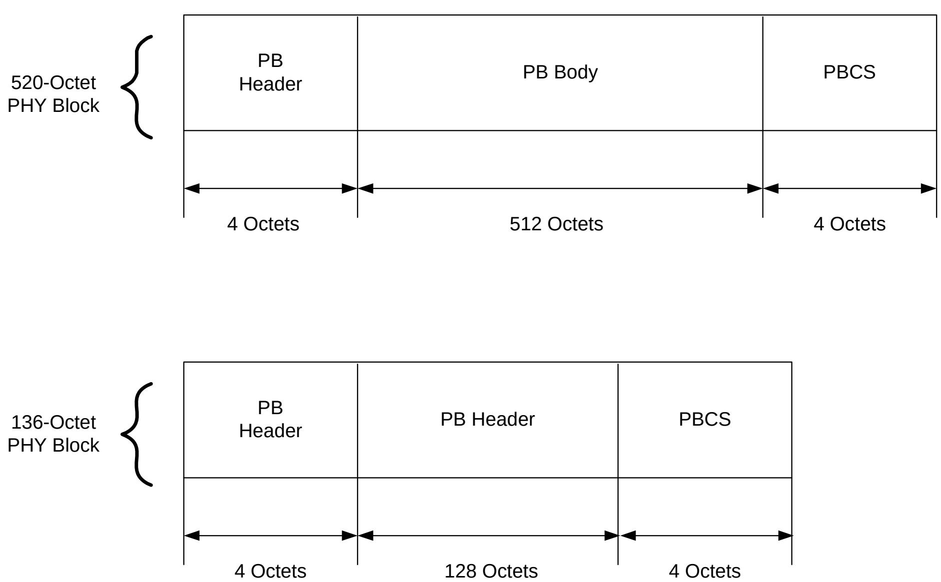
HPAV Segmentation



HPAV PHY Block Structure

- PBs are mapped by PHY to FEC Blocks
  - FEC succeeds or fails
- PBs are basic unit of delivery by MAC internally
  - PB is ACKed or retransmitted using SR-ARQ
  - SACK specifies ACK/NAK
- PH Header (PBH) – 4 octets
  - Info for reassembly, disaggregation, recovery
- PB Body (PBB)
  - 512 octets or 128 octets long – not interpreted here
- PB Check Sequence (PBCS)
  - CRC-32 – not encrypted – for checking PB reception
  - PB discarded and NAKed if incorrect

HPAV PHY Block Structure



HPAV PHY Block Header

- Segment Sequence Number (SSN)
  - 16 bits – segment # in MAC Frame stream
    - Init to 0, increment on each new segment sent
    - Discard duplicates
- MAC Frame Boundary Offset (MFBO)
  - 9 bits to indicate first octet of first MF in PB Body
  - Resynch if a segment is never received
- Flags

HPAV Reassembly

- MPDU Header
  - Provides STEI, DTEI, LID
  - These identify reassembly stream
- Segment Sequence Number (SSN)
  - Used to place segment in PBB into buffer position
  - Recreate MAC Frame Stream
- MAC Frame Boundary Offset + MFB Flag
  - If segment(s) never received, these allow next intact MAC frame to be found
- MAC Frame Header
  - Type and Length fields used to find next MAC Frame
  - Also used to locate MAC Frame Body
  - ATS (if present) determines when to deliver MSDU

Central Coordinator (CCo)

- Issues central beacon
- Associates new stations
  - Issues TEI with lease, announces to AVLN
- Authenticates new stations
  - Verifies possession of NMK, issues NEK
  - Rotates NEK
- Performs admission control
  - Determines resource needs and availability
  - Issues Global LID
  - Performs scheduling
- May perform handover
  - Transfer CCo functions to another STA
- Performs neighbor network coordination

CCo Behavior

- Perform CCo Duties
  - As long as there are other STAs in AVLN
- If all other STAs leave AVLN
  - Remain CCo for at least Discovery period
  - If no STA joins and another AVLN is present, become Unassociated STA
  - Else become Unassociated CCo
- If STA in AVLN should become CCo
  - Other STA is User-appointed and this one is not
  - Other STA is more capable or better positioned
  - Execute handover procedure
  - Become STA in AVLN

AVLNs

- Have a CCo
  - CCo issues central beacon, acts as coordinator
  - May have Proxy Coordinator(s) also
- Share same Network ID (NID)
  - NID normally derived from NMK
  - Should uniquely identify AVLN
  - Remains constant regardless of CCo
- Share same Security Level
  - NMK associated with SL
  - SL must be the same throughout AVLN
- Share same NEK
  - CCo provides NEK during authentication using NMK
  - NEK used to encrypt traffic in AVLN

Authentication

- Process Steps
  - Association is obtaining a valid TEI (Terminal Equipment Identifier)
  - Authorization is obtaining a valid NMK
  - Authentication is obtaining a valid NEK
- Obtaining a valid NEK
  - STA must have NMK first
  - STA requests NEK from CCo using NMK, provide nonce
  - If CCo decrypts, NMK is valid; provide NEK and nonce using NMK, else CCo indicates failure
- Updating NEK
  - NEK rotated at least once per hour
  - CCo requests nonce (NEK encrypted); STA responds with nonce (NEK encrypted)
  - CCo sends set key msg with nonce encrypted with NMK and old NEK; STA acknowledges using same keys

Selecting a CCo

- User Selection always has precedence
  - Allow user to control their network
  - User must enter CCo's MAC address
- Autoselection Criteria
  - CCo capability is most important
  - Number of other STAs in STA's physical network is next
  - Number of neighbor AVLNs seen is next
- Handover procedure to pass info to new CCo
  - Also inform STAs in AVLN of new CCo
  - NID remains the same
- Implementations must ensure handovers do not occur frequently

HPAV Security

- Purposes
  - Control access to the AVLN
  - Maintain confidentiality and integrity of messages
- Mechanisms
  - AES-128 in CBC mode
  - CRC-32 Integrity Check Value
  - SHA-256 Hash function
  - Nonces
  - Channel adaptation
- Usability
  - Network Password (NPW)
  - Device Password (DPW)
  - Push-button mechanism

HPAV Conclusions

- Comprehensive Protocol
  - Supports all traffic types
  - Supports jitter control, bandwidth, delay, etc.
- Complicated!
  - Variety of roles and modes
  - Large number of Management Messages
- Coexistence
  - Detects and coexists with HP1.0/1.0.1
  - Can coordinate with neighbor AVLNs
- User-friendly
  - A primary goal
  - Intuitive and easy security setup

IEEE P1901

- Two physical layers
  - Windowed OFDM modulation (HomePlug AV)
    - FFT OFDM
    - FEC based on Convolutional turbo code (CTC)
  - Wavelet OFDM modulation (Panasonic HD-PLC)
    - Wavelet modulation
    - A mandatory FEC based on concatenated Reed-Solomon (RS)
    - An option to use Low-Density Parity-Check (LDPC)
- In-Home System vs Access System