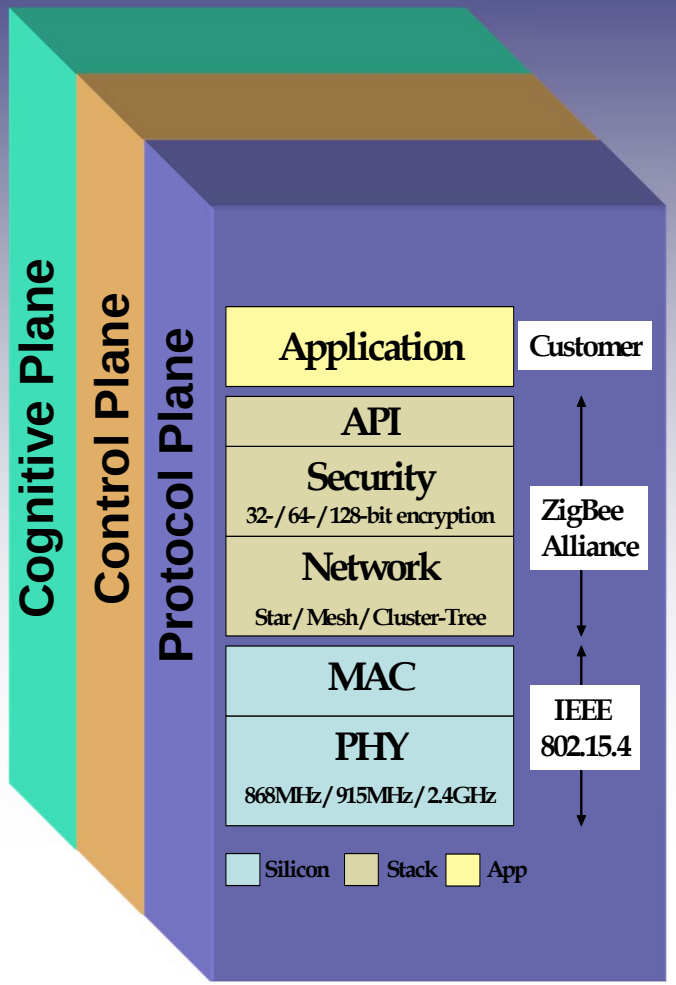
A TVWS ZigBee Prototype

James “Jody” Neel

james.neel@crtwireless.com

SDR 11

Nov 29-Dec 2, 2011



CRT
Cognitive Radio Technologies

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

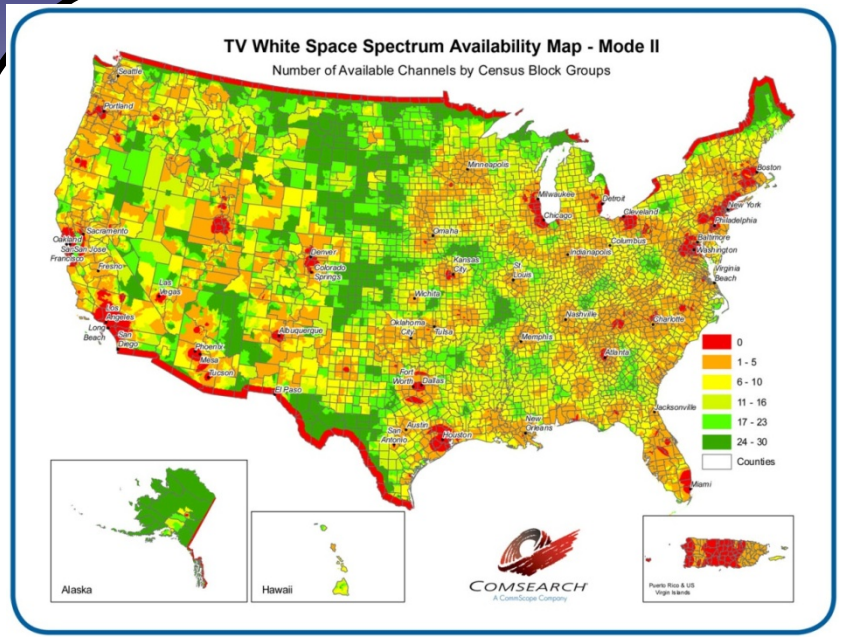
Presentation Material

- **Objective**: Design a ZigBee-based solution suitable for operation in the TV White Space without modifying PHY / MAC (802.15.4)
  - 802.15.4m PAR was approved this month
- Why ZigBee in the TV White Space (TVWS)?
- Design approaches for addressing issues posed by putting ZigBee in TVWS

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

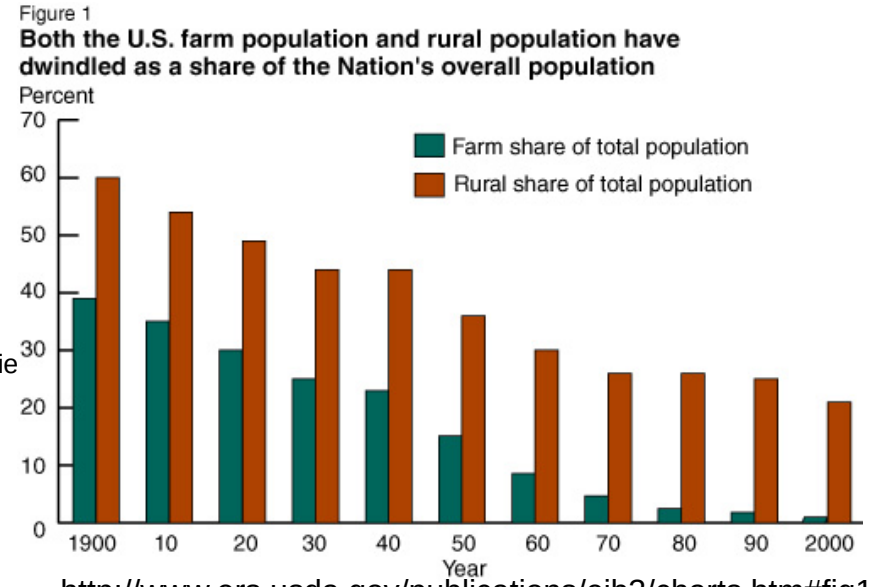
Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Trends and Motivating Insights



From M. Gibson, "TV White Space Geolocation Database Issues & Opportunitie
CommSearch, TVWS Workshop Sep 16, 2010

- Limited spectrum with large population presence
- Rural broadband demand is not that high



http://www.ers.usda.gov/publications/eib3/charts.htm#fig1

- Long history of automating agricultural applications
- Much greater range possible implied by Frijs

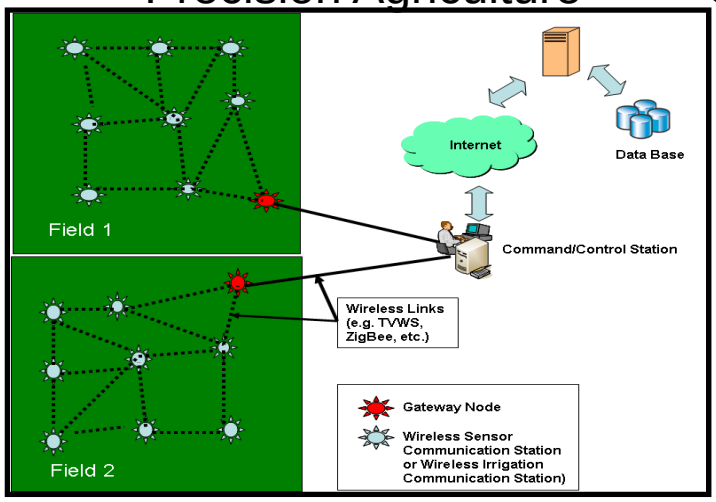
System	Free Space Range @ 2.4 GHz	Free Space Range @ 512 MHz
Minimal Zigbee	133 m	623 m
Zigbee with Advanced Transceiver[1]	923 m	4,300 m

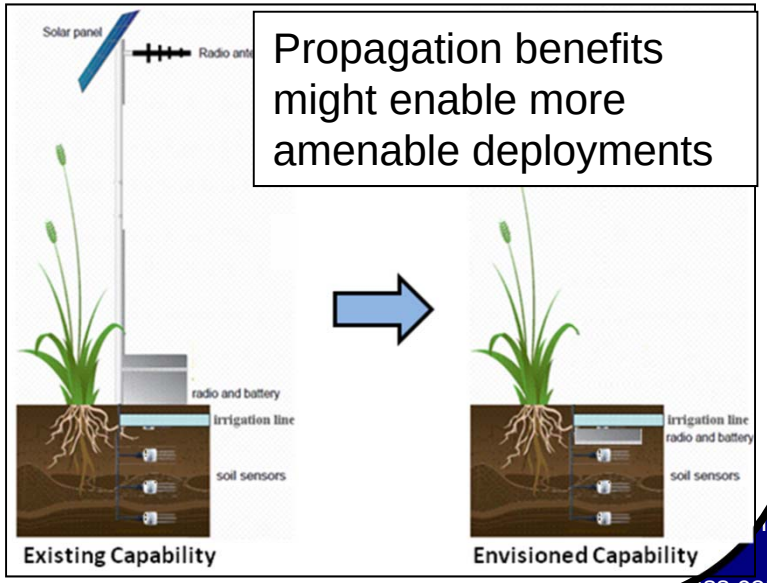
(100 mW)

TV White Space for Rural Sensor Applications

- Agricultural Applications
  - Soil Moisture, pH
  - Cattle Monitoring
  - Paddy field monitoring
  - Equipment tracking
  - Farm automation
- Environmental Applications
  - Water quality
    - Oil contamination
  - Weather Sensing Grid
  - Flood monitoring
  - Air quality
  - Forest health
    - Fires, disease
  - Seismic activity
  - Energy source management

Precision Agriculture

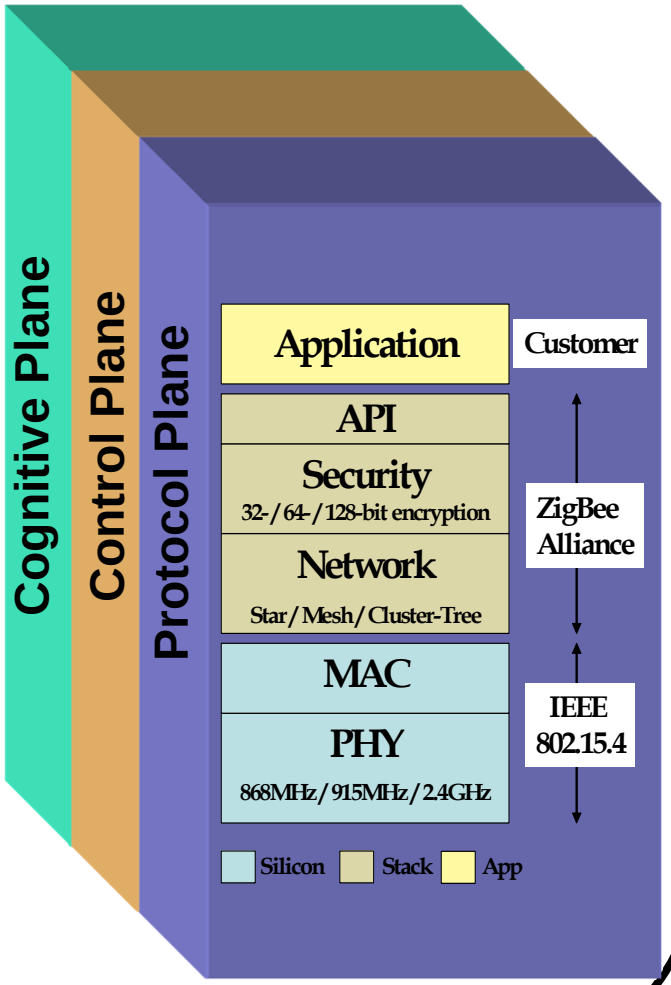




Propagation benefits might enable more amenable deployments

Why not modify 802.15.4?

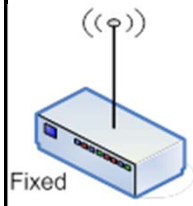
- Preserving existing chipsets and protocols:
  - Simplifies integration with existing applications
  - Reduces costs
  - Reduces time to market
    - Wanted to beat 802.15.4m
    - 802.15.4m PAR approved Nov 2011
      - IEEE 802.22-11/0136r1
- In theory, geo-location DSA does not require modifications to PHY or MAC if you can already control transmit frequency reasonably quickly
  - Not as true for sensing-based DSA or many other cognitive radio applications
  - A. Mody, "Making Current Military Radios Cognitive without Hardware or Firmware Modifications," *AIE CONFERENCE on Spectrum Management and Dynamic Spectrum Access for Government and Defense*, Sep 27-28, 2011.



147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502
Ph: (540) 230-6012
Email: info@crtwireless.com

TVWS Rules

- Geolocation + Database
  - Sensing kinda allowed
  - 9 Database providers
  - Regs (kinda) finalized Sep 23, 2010
    - FCC 10-174



Fixed TVBD
Geo-location +/- 50m
Geo-location capable or professional installer
Secure access to TVB Database with device Id
4W max power (EIRP)
TV channels useable: 2 (54-60Mhz), 5,6 (76-88Mhz), 7-13 (174-216Mhz) and 21-36, 38-51 (470-692 Mhz)
Max antenna height <30m and <76m for site

Mode II Personal Portable TVBD
Geo-location +/- 50m, check every 60 seconds
Secure access to TVB Database with device Id
100mW power, 40mW when adjacent to incumbent
TV channels useable: 21-36, 38-51 (470-692 Mhz)
Secure access to TVB Database with device Id

Mode I Personal Poratble TVBD
MUST obtain channels from Mode II or Fixed TVBD
100mW power, 40mW when adjacent to incumbent
TV channels useable: 21-36, 38-51 (470-692 Mhz)

Sensing Only TVBD
MUST sense for incumbents prior to channel use
50mW power
TV channels useable: 21-36, 38-51 (470-692 Mhz)

- Available Channels By Class

TV Channel	Frequency Band	Frequency (MHz)	Allowed Devices
2	VHF	54 – 60	Fixed
5 – 6	VHF	76 – 88	Fixed
7 – 13	VHF	174 – 216	Fixed
14 – 20	UHF	470 – 512	Fixed
21 – 35	UHF	512 – 602	Fixed & Portable
36	UHF	602 – 608	Portable
38	UHF	614 – 620	Portable
39 – 51	UHF	620 – 698	Fixed & Portable

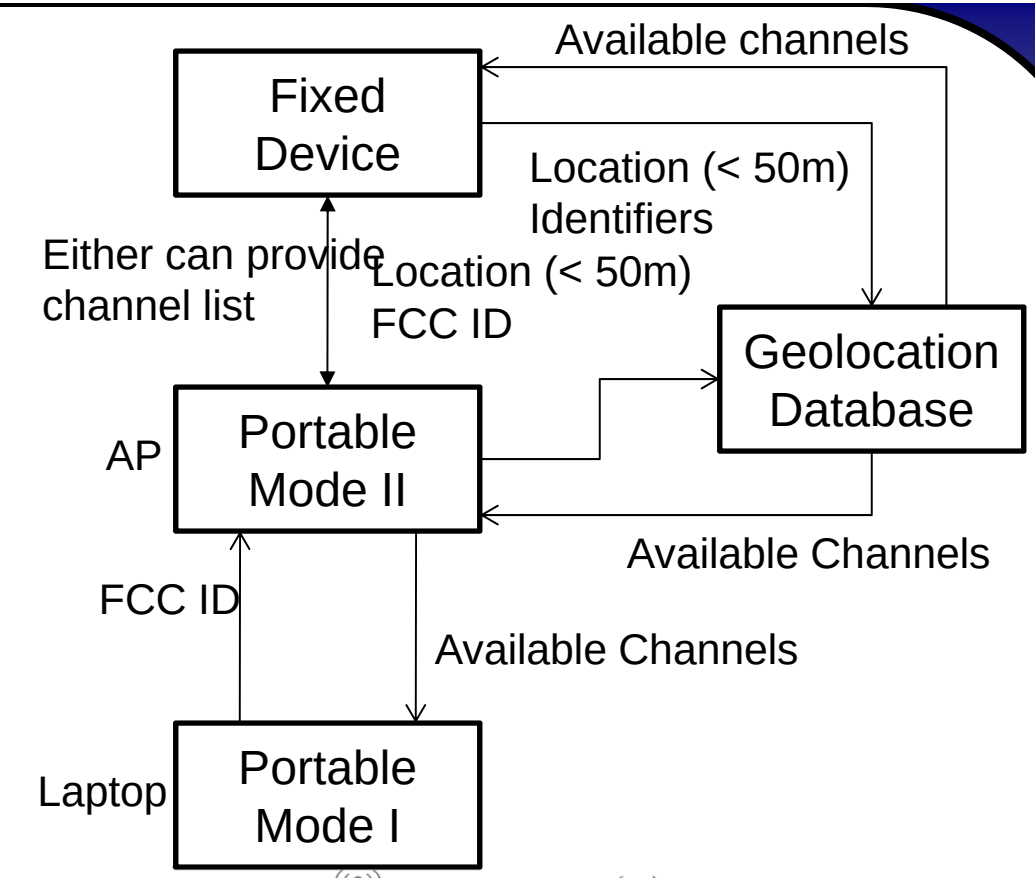
  - Above: no TVBD devices in 608-614 (adjacent to chan 37) in 13 metros (LMR conflict)
    - Channels 36,38 reserved for wireless mics

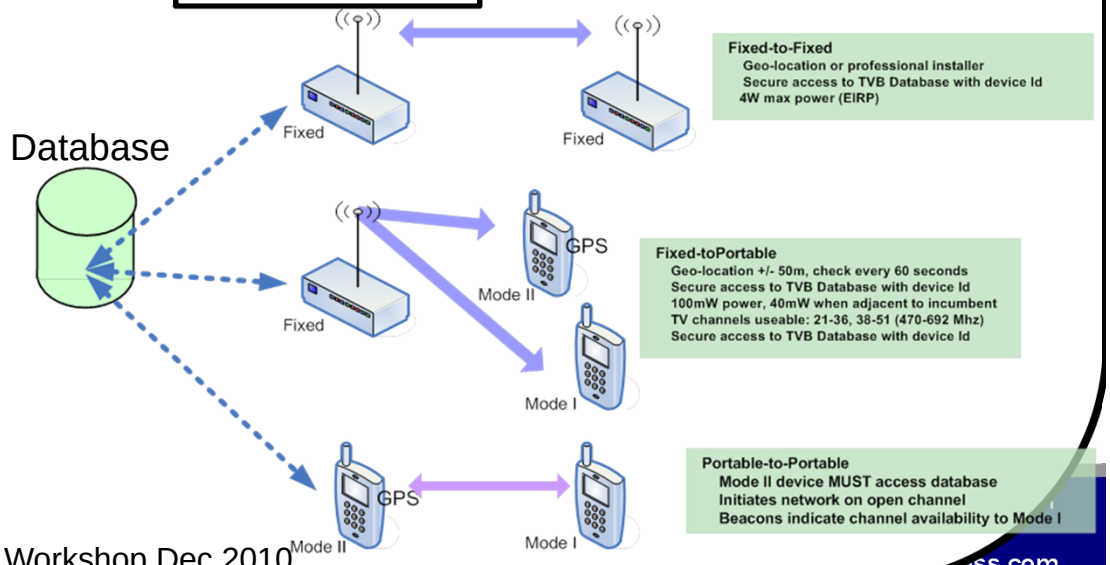
- Protected users:
  - TV (including low power), TV translators, TV boosters, licensed mics, registered mics for major events, PLMRS/CMRS, MVPD receive sites, radio astronomy

Diagram from: Marvell, WinnForum TVWS Workshop Dec 2010

More TVWS

- Fixed
  - HAAT restricted to 76 m, 30 m above ground
  - Not achievable in hilly terrain
- Less power when adjacent to incumbent + TPC
- Identifications to geolocation database
  - Fixed devices provide long list of identifying information. Stored in registration database (maintained with geolocation database)
  - Portables provide FCC ID
- Fixed / Mode II can pass along each others' information for channel availability
- Mode I must receive "enabling signal" every 60s
- Secure and authenticate channel lists

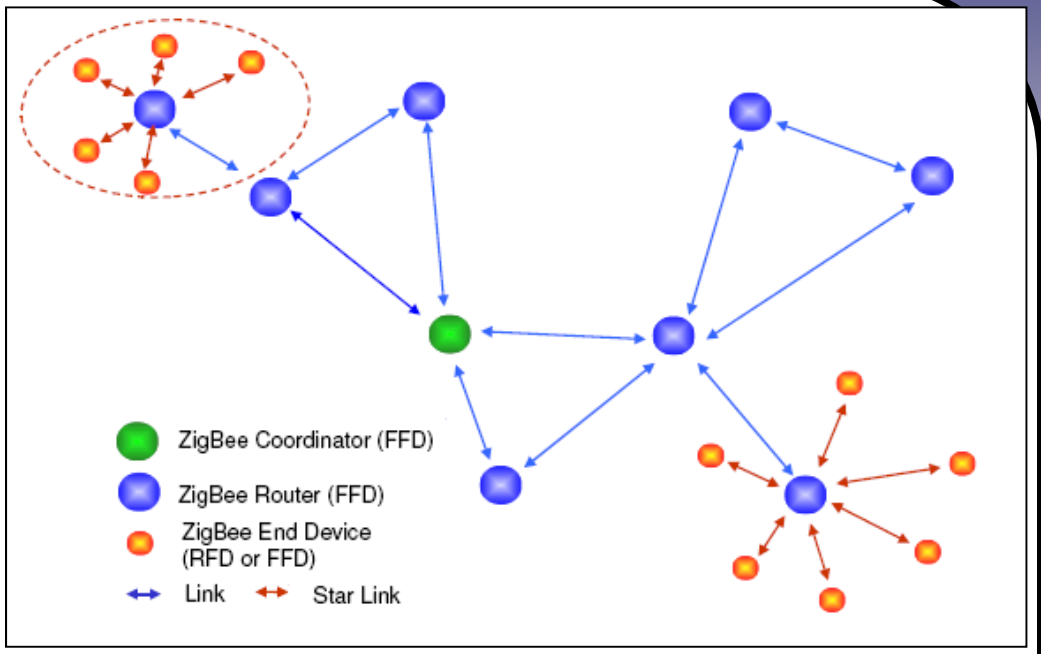




Power Diagram from: Marvell, WinnForum TVWS Workshop Dec 2010

High Level System Considerations

- Mode II devices implemented as 802.15.4 Full Function Devices (FFD)
  - Sends beacon frames
  - Offer network join services
  - Augment with GPS
- Mode I devices implemented as 802.15.4 Reduced Function Devices
  - Only interface with single FFD
- Network manager
  - Assumed co-located with coordinator (doesn't have to be)
  - Internet connection to database
  - FFD act as RFD until given channel assignment by NM
  - Send position initial



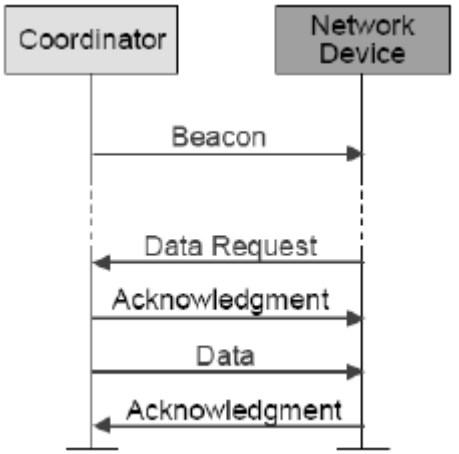
- Routing implemented in tree mode
  - Mesh mode does not implement beaconing

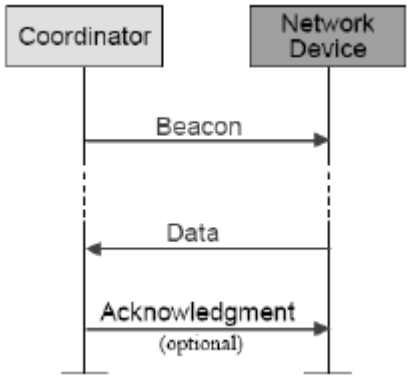
Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Communications

- Should operate in beacon-enabled mode
  - Mesh mode does not implement beaconing
  - Not strictly necessary, but non-beacon mode will greatly limit ability to sleep as active messaging every minute is required
- 60s enabling beacon
  - Superframe configured to satisfy 60 second interval
  - 802.15.4 allows 15 ms to 245 s
- Some performance issues in allowing FFD / Mode II devices to sleep as aggressively, but not unique to geo-location DSA



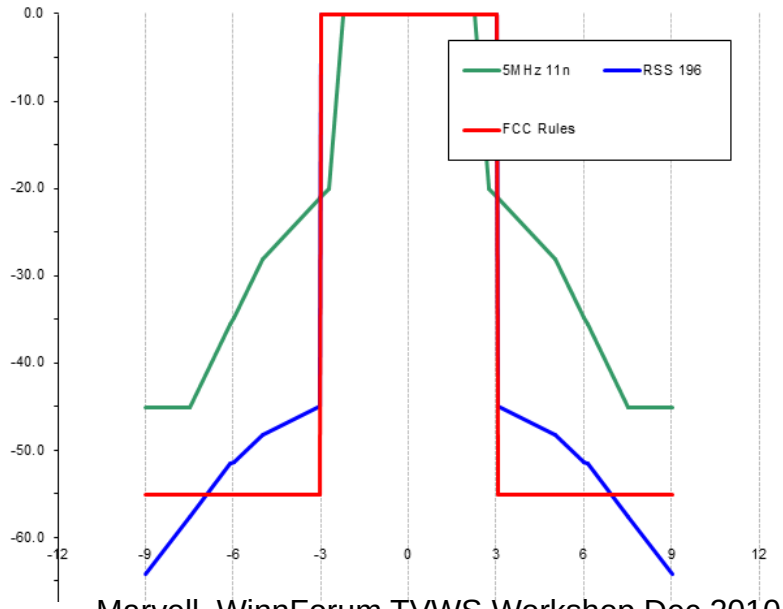


Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Channel Considerations

- 5 MHz BW < 6 MHz TV channel
  - 2.4 GHz PHY
  - Narrower version available but bad for PSD limits
- Network uses same channel
- Private ZigBee profiles used for custom channel restrictions
  - Remap channel #s in BSP
- Most chipsets have APIs for channel selection that can be leveraged
- 802.15.4 similarly has SAPs for configuring which channels to look at in a scan and transmit on
- Zigbee supports frequency agility
  - Network Manager can switch entire network over to a new frequency
  - Required in ZigBee Pro
  - Use when channel availability changes
- Coordinator uses 802.15.4 energy scan to select least congested channel (after getting list from database / other Mode II)
  - Has to consider available channels for all routers in network
  - Can get information from other devices
- More restrictive channel mask
  - More of a HW issue



Marvell, WinnForum TVWS Workshop Dec 2010

Network Formation and Rendezvous

- If Mode I
  - Use passive scan mode to find channel with appropriate beacons for association
  - MLME-SCAN primitive
  - Receive available channel list as part of DSA “application”
- If Mode II
  - If directly connected to internet
    - Report location (and other info) and get channels
    - Enter active scan to check for existing coordinator / network manager
      - Must prohibit active scan mode if channel list is not available
  - If not connected to Internet
    - Enter passive scan mode to find FFD that does have a connection
    - After connected, report type location and act as non-coordinator FFD
- If orphaned (e.g., channel switch while sleeping)
  - Mode I can’t directly use 802.15.4 orphan scan due to transmission of orphan notification commands
  - Mode II is not similarly limited if channel list is not out of date
- Mode I waking from sleep mode
  - Start passive scan on only previous channel
  - If fails go change scan channel list to previously received channel scan list
  - If that fails, scan over entire channel list

Other Considerations

- TPC already supported by 802.15.4
  - Step sizes of -25, -15, -10, -7, -5, -3, -1, 0 dBm
- TVWS requires encryption and authentication of channel info
  - All devices at least implement AES-CCM-64
  - MAC level authentication from CBC-MAC
  - Network and application layer authentication and from ZigBee
    - Application authentication more appropriate
- ZigBee has potential issue with regenerating PAN IDs when evacuating a channel and entering a channel with an existing PAN with the same ID
  - Not true for ZigBee Pro which enforces unique IDs even across different channels

Identifier	Security suite name	Security services				Subclause
		Access control	Data encryption	Frame integrity	Sequential freshness (optional)	
0 x 00	None					
0 x 01	AES-CTR	X	X		X	7.6.2
0 x 02	AES-CCM-128	X	X	X	X	7.6.3
0 x 03	AES-CCM-64	X	X	X	X	7.6.3
0 x 04	AES-CCM-32	X	X	X	X	7.6.3
0 x 05	AES-CBC-MAC-128	X		X		7.6.4
0 x 06	AES-CBC-MAC-64	X		X		7.6.4
0 x 07	AES-CBC-MAC-32	X		X		7.6.4

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502
Ph: (540) 230-6012
Email: info@crtwireless.com

Summary

- Geo-location DSA can be added onto many systems without amending existing protocols by exploiting existing APIs and configurations
  - Does not hold for many other CR apps
- Some compromises or limits may have to be made (e.g., why 802.15.4m)
  - Channel numbering solution not exactly elegant and would pose (surmountable) issues when integrated into a multi-band ZigBee solution
  - Existing mesh network and orphan procedures not well-suited
- ZigBee provides some key functions for DSA that 802.15.4 did not currently
  - Frequency agility to shift entire network
  - Support for App<->App authentication
  - Logical devices to help control
- Caveat – never put together the prototype, so probably overlooked something

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Extra Slides

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Relevant White Space Constraints

Rule	Requirements
15.707(a) 15.707(d) 15.711(b3)	**Operating channels** • Restricted to channels 21-36 and 38-51, and only on channels specified by Mode II device • To initiate contact with a fixed or Mode II device, a Mode I device may transmit on an available channel used by the fixed or Mode II TVBD or on a channel the fixed or Mode II TVBD indicates is available for use by a Mode I device on a signal seeking such contacts.
15.711 (b3)	**Enabling Signal** • When not in a sleep mode, receive a contact verification signal at least once every 60 seconds or contact Mode II / fixed device for updated list, else cease operation • Must recheck / re-establish contact if powered off on powering-on / waking • Mode I shall provide FCC identifier to Mode II / Fixed device
15.709(a2) 15.709(a3) 15.709(a5) 15.709(c1)	**Transmit power requirements** • In non-adjacent channel: ≤ 20 dBm EIRP, 2.2 dBm / 100 kHz PSD to antenna • In adjacent channel: ≤ 16 dBm EIRP, -1.8 dBm / 100 kHz PSD to antenna, adjacent channel emission ≤ 72.8 dB below the highest average power in the TV channel • Incorporate transmit power control for minimum power necessary for successful communication
15.709 (b1) 15.711 (c)	**Physical requirements:** • All antennas must be permanently attached • Be able to display a list of identified available channels and its operating channels.
15.711(f)	**Security requirements:** • Secure communications between Mode I and fixed / Mode II for providing lists of available channels against corruption or unauthorized modification of the data • Contact verification signals transmitted for Mode I devices are to be encoded with encryption to secure the identity of the transmitting device. Mode I devices using contact verification signals shall accept as valid for authorization only the signals of the device from which they obtained their list of available channels.

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Rule	Requirements
15.707(a) 15.707(d) 15.711(b3)	**Operating channels** • Restricted to channels 21-36 and 38-51, and only on channels specified by Database, other Mode II device, or Fixed device.
15.711(b2) 15.711(b3)	**Enabling via Geolocation and Database Access** • Mode II must determine its geographic coordinates to an accuracy of ±50 m • Re-establish its position after power-off or after sleeping and once every 60 seconds • Must have list of available channels from database prior to initial transmission, after each power-off and if it changes location by more than 100 m from last database access and once daily • Adjust their use of channels for 48 hour period following last database access • Cease operations if unable to re-establish contact with database by 11:59 PM of the day after last database access
15.711 (b3)	**Enabling Mode I** • Cannot provide Mode I device with list of channels until after Mode II device contacts the database, provides the database with the FCC ID of the Mode I device and receives verification that the FCC ID is valid for operation • If a Mode II device loses power and obtains a new channel list, it must signal all Mode I devices it is serving to acquire new channel list • Should provide a contact verification signal to associated Mode I devices or updated channel availability list every 60 seconds
15.709(a2) 15.709(a3) 15.709(a5) 15.709(c1)	**Transmit power requirements** • In non-adjacent channel: ≤ 20 dBm EIRP, 2.2 dBm / 100 kHz PSD to antenna • In adjacent channel: ≤ 16 dBm EIRP, -1.8 dBm / 100 kHz PSD to antenna, adjacent channel emission ≤ 72.8 dB below the highest average power in the TV channel • Incorporate transmit power control for minimum power necessary for successful communication
15.709 (b1) 15.711 (c)	**Physical requirements:** • All antennas must be permanently attached • Be able to display a list of identified available channels and its operating channels.
15.711(f)	**Security requirements:** • Secure communications between Mode I and fixed / Mode II for providing lists of available channels against corruption or unauthorized modification of the data • Contact verification signals transmitted for Mode I devices are to be encoded with encryption to secure the identity of the transmitting device. Mode I devices using contact verification signals shall accept as valid for authorization only the signals of the device from which they obtained their list of available channels.

Mode I Requirements

Enabling / Initialization

The enhanced Mode I node will add functions to realize the following:

- Detect and find the operating channels of a Mode II device so that an initial request for a channel list can be made and FCC ID can be provided
- Regularly listen for an enabling signal from the Mode II device
- Define a mechanism for re-starting this process when coming out of a sleep mode
- Ensuring that no transmissions occur when no enabling signals are received

Transmit power requirements / Operating Channels

The enhanced Mode I node will add functions to realize the following:

- Store an available channel list and associated maximum power levels for each channel
- Validate that specified channels do not fall outside of channels 21-36 and 38-51
- Transmit power control will leverage existing 802.15.4 capabilities

Mode II Requirements

Self-Enabling / Initialization / Database access

The enhanced Mode II node will add functions to realize the following:

- Determine its own location within 50 m
- Communicate over the Internet with a geolocation database to receive a list of available channels and adjacency information for the location
- Re-perform these actions each day and when power is lost or if the node's location differs by more than 100m from last database access

Enabling Signal for Mode II

The enhanced Mode II node will add the following functions to enable the Mode I devices:

- At least once every 60 seconds, broadcast an enabling signal that indicates the available channels for operation
- Receive and validate with the geolocation database, the validity of operation for each Mode I device it is enabling
- Re-send channel availability lists when the list received from the database changes
- Convey transmit power limits to Mode I device for available channels

Transmit power requirements / Operating Channels

The enhanced Mode II ZigBee node will add functions to realize the following:

- Store an available channel list and associated maximum power levels for each channel to Mo (use ?)
- Validate that specified channels do not fall outside of channels 21-36 and 38-51
- Transmit power control will leverage existing 802.15.4 capabilities

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502
Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

7.5.2.1 Scanning through channels

All devices shall be capable of performing passive and orphan scans across a specified list of channels. In addition, an FFD shall be able to perform ED and active scans. The next higher layer should submit a scan request containing a list of channels chosen only from the channels specified by *phyChannelsSupported.*

A device is instructed to begin a channel scan through the MLME-SCAN.request primitive. For the duration of the scan, the device shall suspend beacon transmissions, if applicable; and upon the conclusion of the scan, the device shall recommence beacon transmissions. The results of the scan shall be returned via the MLME-SCAN.confirm primitive.

7.5.2.1.4 Orphan channel scan

An orphan scan allows a device to attempt to relocate its coordinator following a loss of synchronization. During an orphan scan, the MAC sublayer shall discard all frames received over the PHY data service that are not coordinator realignment MAC command frames.

An orphan scan over a specified set of logical channels is requested using the MLME-SCAN.request primitive with the ScanType parameter set to indicate an orphan scan. For each logical channel, the device shall first switch to the channel, by setting *phyCurrentChannel* accordingly, and then send an orphan notification command (see 7.3.2.3). The device shall then enable its receiver for at most *aResponseWaitTime* symbols. If the device successfully receives a coordinator realignment command (see 7.3.2.5) within this time, the device shall disable its receiver.

If a coordinator receives the orphan notification command, it shall search its device list for the device sending the command. If the coordinator finds a record of the device, it shall send a coordinator realignment command to the orphaned device. The process of searching for the device and sending the coordinator realignment command shall occur within *aResponseWaitTime* symbols. The coordinator realignment command shall contain its current PAN identifier, *macPANId*, its current logical channel, and the short address of the orphaned device. If a coordinator finds no record of the device, it shall ignore the command and not send a coordinator realignment command.

The orphan scan shall terminate when the device receives a coordinator realignment command or the specified set of logical channels has been scanned.

7.5.2.1.3 Passive channel scan

A passive scan, like an active scan, allows a device to locate any coordinator transmitting beacon frames within its POS. The beacon request command, however, is not transmitted. This type of scan could be used by a device prior to association. During a passive scan, the MAC sublayer shall discard all frames received over the PHY data service that are not beacon frames.

Before commencing a passive scan, the MAC sublayer shall store the value of *macPANId* and then set it to 0 x ffff for the duration of the scan. This enables the receive filter to accept all beacons rather than just the beacons from its current PAN (see 7.5.6.2). On completion of the scan, the MAC sublayer shall restore the value of *macPANId* to the value stored before the scan began.

A passive scan over a specified set of logical channels is requested using the MLME-SCAN.request primitive with the ScanType parameter set to indicate a passive scan. For each logical channel, the device shall first switch to the channel, by setting *phyCurrentChannel* accordingly, and then enable its receiver for at most [*aBaseSuperframeDuration* * $(2^n + 1)$] symbols, where n is a value between 0 and 14. During this time, the device shall reject all nonbeacon frames and record the information contained in all unique beacons in a PAN descriptor structure (see Table 41 in 7.1.5.1.1). A device shall be able to store between one and an implementation- specified maximum number of PAN descriptors. A beacon frame shall be assumed to be unique if it contains both a PAN identifier and a source address that has not been seen before during the scan of the current channel.

If a beacon frame is received with the security enabled subfield set to 1, the device shall attempt to process the beacon frame for security, as described in 7.5.8. Any errors encountered during the secure processing of the beacon frame shall be ignored, and the beacon information shall be recorded in a PAN descriptor with the SecurityUse, ACLEntry, and SecurityFailure fields (see Table 41) set accordingly.

The passive scan on a particular channel shall terminate when the number of beacons found equals the implementation specified limit or the channel has been scanned for the full time, as specified in 7.5.2.1.3. If the latter condition has been satisfied, the channel shall be considered to have been scanned. Where possible, the scan shall be repeated on each channel. The entire scan shall terminate when the number of PAN descriptors stored equals the implementation-specified maximum or every channel in the set of available channels has been scanned.

Security Services Provider (SSP)

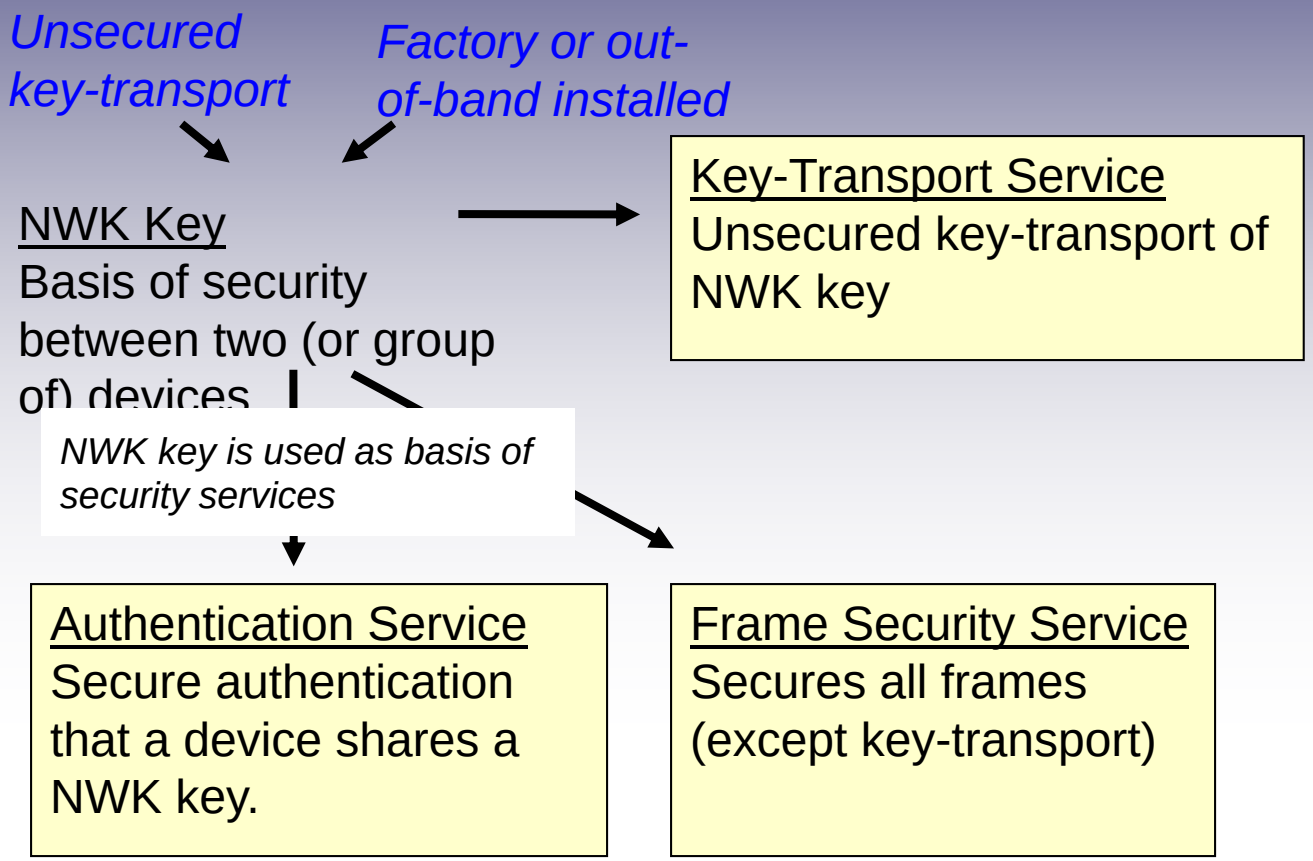
- **Security at each layer:**
  - Network (NWK) layer security for network command frames (route request, route reply, route error)
  - Application (APL) layer security for Application Support Sub-layer (APS) frames
- **Two Security Modes**
  - Standard Mode (ZigBee and PRO feature sets) – Two NWK keys, APL security via NWK key. Ability to switch NWK keys. Optional use of Application Link Keys for pairs of communicating devices at APL.
  - High Security Mode (PRO feature set only) – Two NWK keys, separate Link Keys for pairs of communicating devices at APL. Master Keys with the Trust Center for key transport and key establishment. Ability to switch NWK keys. Entity authentication between all pairs of communicating devices.
- **Security Implementation**
  - Trust Center –Creates and distributes the Network Keys. Manages switch from active to secondary Network Key (Standard and High Security Modes). Optionally supports Master Keys and Trust Center Link Key establishment and transport (Optional in Standard security mode and mandatory in High Security mode)

Security Services Provider (SSP)

- **Key Hierarchy**
  - Master Key (could be programmed in or provided *in the clear* from the Trust Center) – High Security mode only
  - Network Key (used for all NWK commands from any device and for APS messaging) – Standard and High Security modes
  - Link Keys (used for each pair of communicating devices) – Standard and High Security modes
- **Features in either Security Mode**
  - Authentication and Encryption
  - Freshness (frame counters)
  - Message Integrity

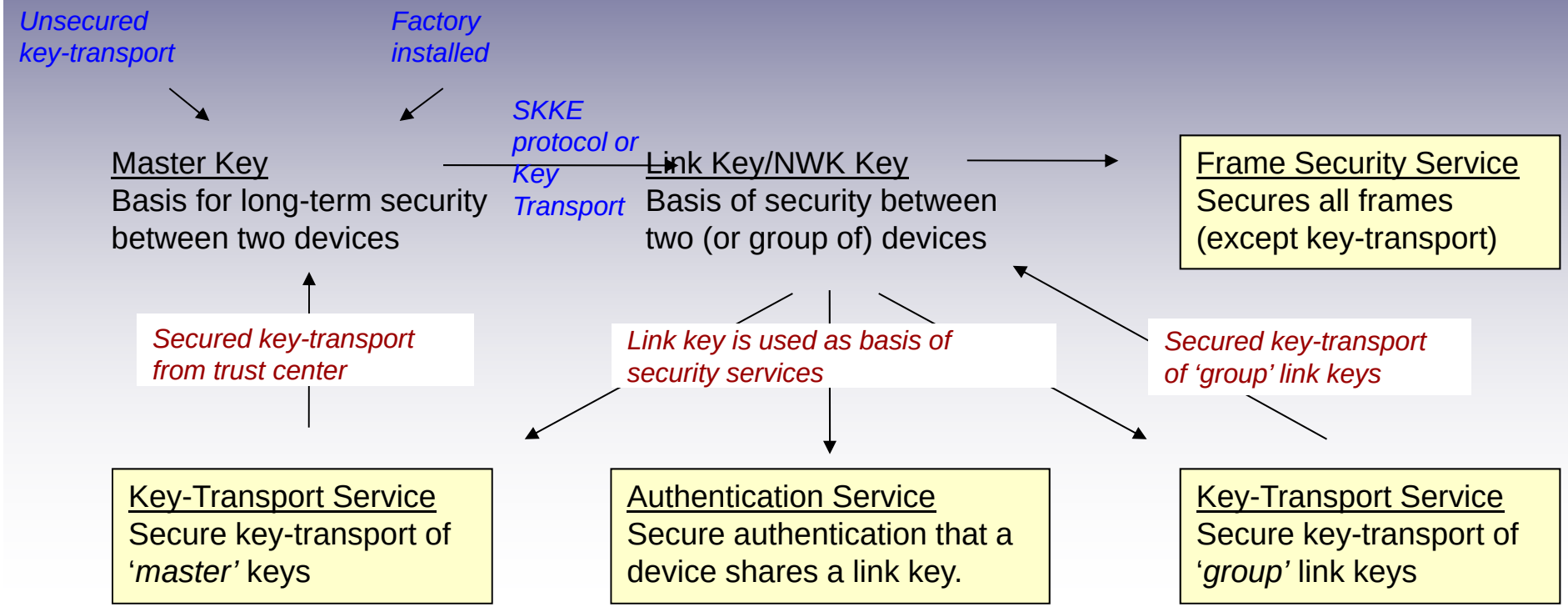
Slide from "ZigBee Technical Overview," *Wireless Japan*, 2008

Security Service in Standard Mode



Slide from "ZigBee Technical Overview," *Wireless Japan*, 2008

Security Service in High Security Mode



Slide from "ZigBee Technical Overview," *Wireless Japan*, 2008

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com