ZigBee/IEEE 802.15.4

Steven Myers

Electrical and Computer Engineering
University of Wisconsin Madison

Outline of Talk

- Introduction
  - Evolution of LR-WPAN Standard
  - Zigbee and IEEE 802.15.4
  - Zigbee vs. Bluetooth
- IEEE 802.15.4 WPAN
  - 2 types of WPAN devices
  - Network Topologies
  - Architecture
- IEEE 802.15.4 PHY Layer
- IEEE 802.15.4 MAC Layer
- Experimental Evaluation of 802.15.4 Transmission Power Control and Interference Minimization
- Video Surveillance demo

Evolution of WPAN

- Wired telephony network → Cellular Network
  - Need for mobility
  - Cost of laying new wires
- Cellular Network → WLAN
  - IEEE 802.11
  - Long range (100m), Data throughput of 2-11Mbps
- WLAN → WPAN
  - Even smaller wireless coverage area
  - Low-cost, low power, short range, and small size

IEEE 802.15.4 (ZigBee)

- IEEE 802.15.4
  - Specifies the PHY and MAC layers
  - Low data rate
  - Low power
- ZigBee Alliance
  - Joined with IEEE to specify entire protocol stack
  - Targeted towards automation, sensor networks, and remote control applications
  - Provides for upper layer services
    - security services, data networking, compliance testing, marketing, and advanced engineering for the evolution of the standard

ZigBee vs. Bluetooth

- ZigBee
  - Smaller packets over large network
  - Data rate 250 kbps @2.4 GHz
  - Allows up to 254 nodes
  - Simplified protocol stack
  - Used in time critical applications (15msec wake up time)
  - Mostly Static networks with many, infrequently used devices
  - Home automation, toys, remote controls, etc.
- Bluetooth
  - Larger packets over small network
  - Data rate is 1Mbps @2.4 GHz
  - Allows up to 8 nodes in piconet setup
  - More complex protocol stack
  - Not so time critical (3sec wake up time)
  - Ad-hoc networks
  - File transfer
  - Screen graphics, pictures, hands-free audio, Mobile phones, headsets, PDAs, etc.

Components of WPAN

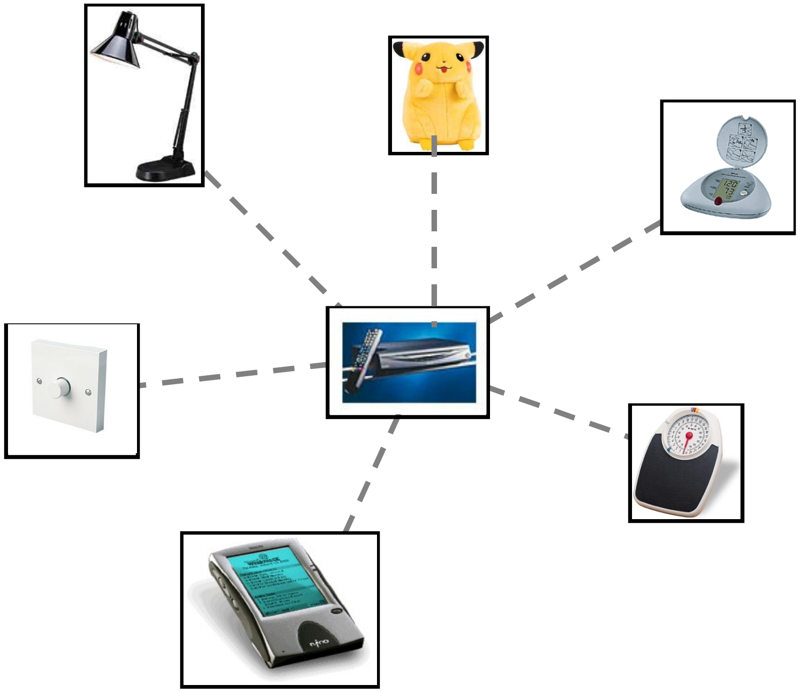
- Full function device (FFD)
  - Any topology
  - PAN coordinator capable
  - Talks to any other device
  - Implements complete protocol set
- Reduced function device (RFD)
  - Limited to certain topologies
  - Cannot become a PAN coordinator
  - Talks only to a network coordinator
  - Very simple implementation
  - Reduced protocol set

IEEE 802.15.4 Definitions

- Network Device:
  - An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.
- Coordinator:
  - An FFD with network device functionality that provides coordination and other services to the network.
- PAN Coordinator:
  - A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

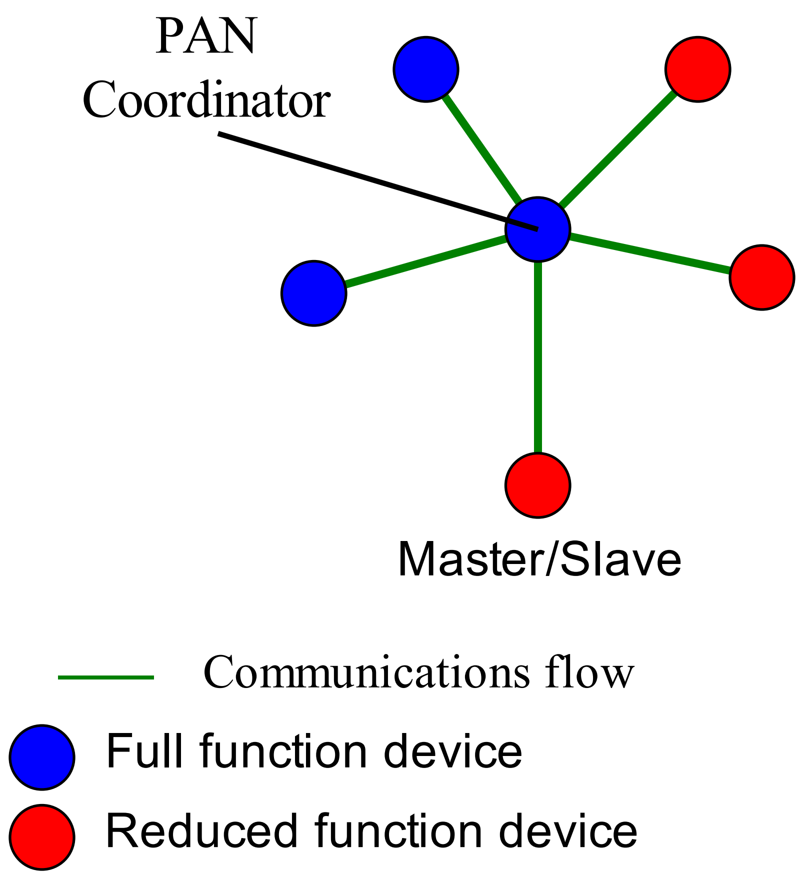
Network Topologies

- ZigBee supports 3 types of network topologies
  - Star topology
  - Peer-to peer topology
  - Cluster tree topology



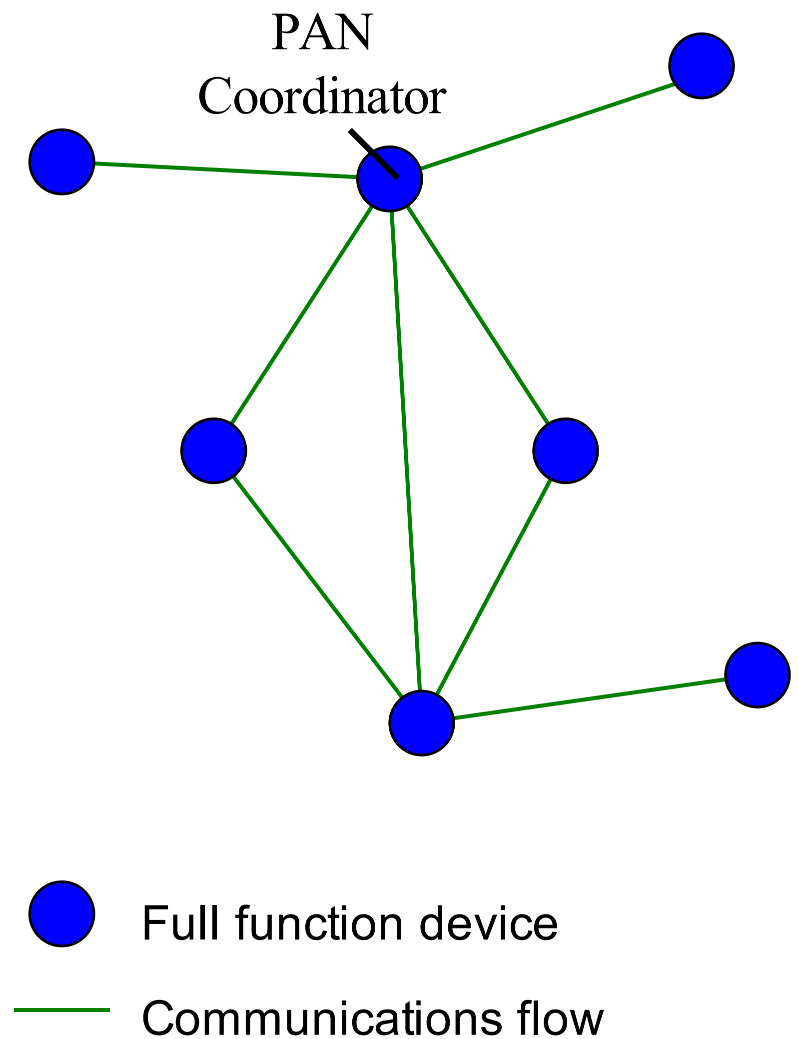
Star Topology

- Communication is done through the PAN coordinator
- PAN usually mains powered
- Devices battery powered
- Applications include:
  - Home automation
  - PC peripherals



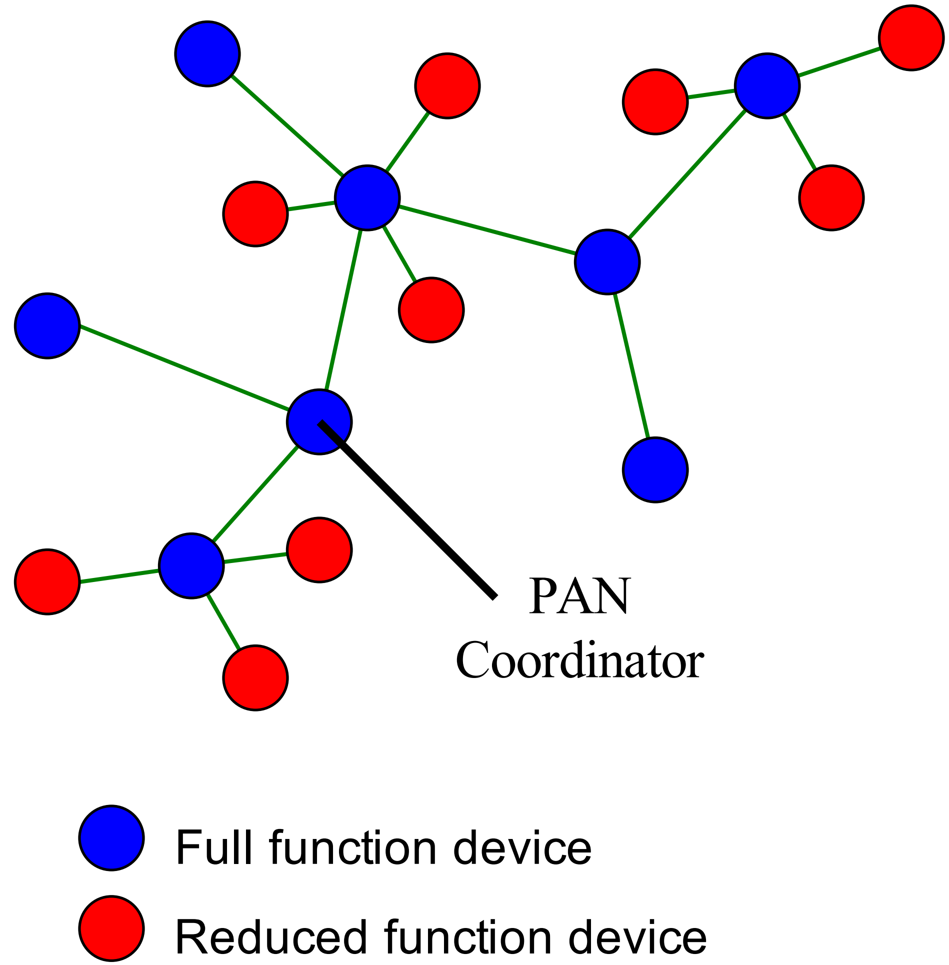
Peer-to-peer Topology

- Any device can communicate with any other device
  - Ad hoc
  - Self-organizing
- Allows for multiple hops to route messages
- Applications include:
  - Industrial control and monitoring
  - Wireless sensor networks
  - Inventory tracking

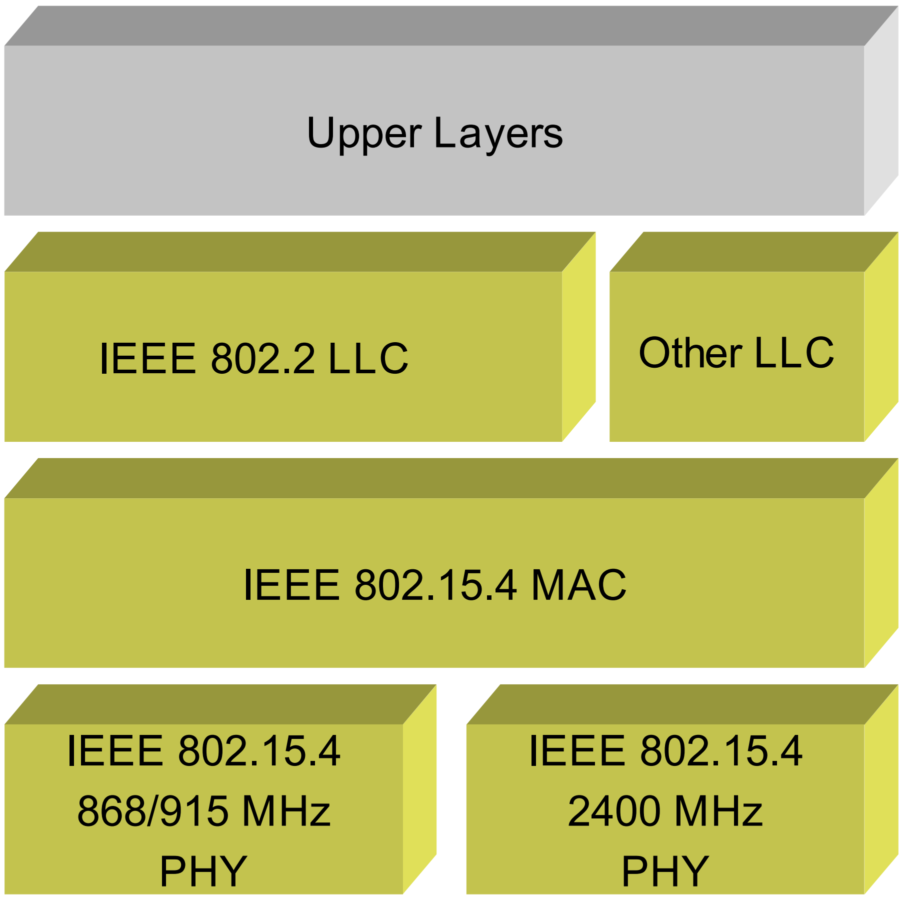


Cluster tree Topology

- Special case of peer-to peer
- PAN coordinator establishes itself as cluster head (CLH)
- Tree formed around PAN coordinator
- Advantage
  - Increased coverage area
- Disadvantage
  - Increased message latency



802.15.4 Architecture



THE UNIVERSITY of WISCONSIN MADISON

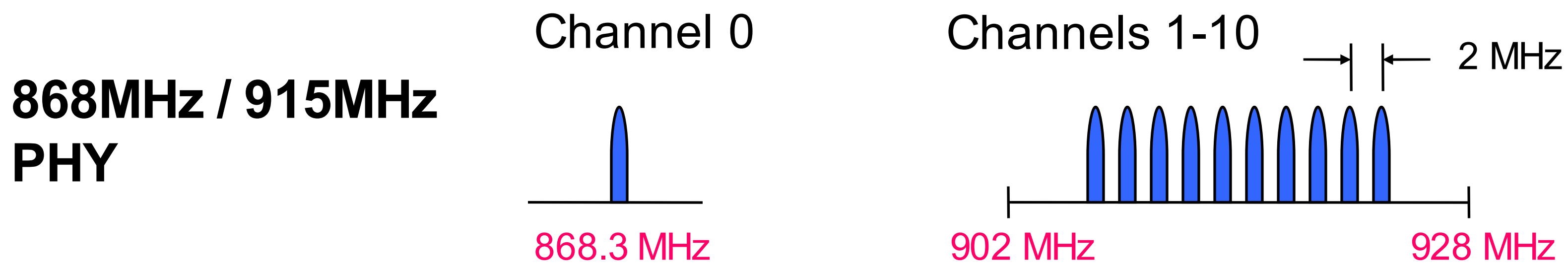
802.15.4
PHY LAYER

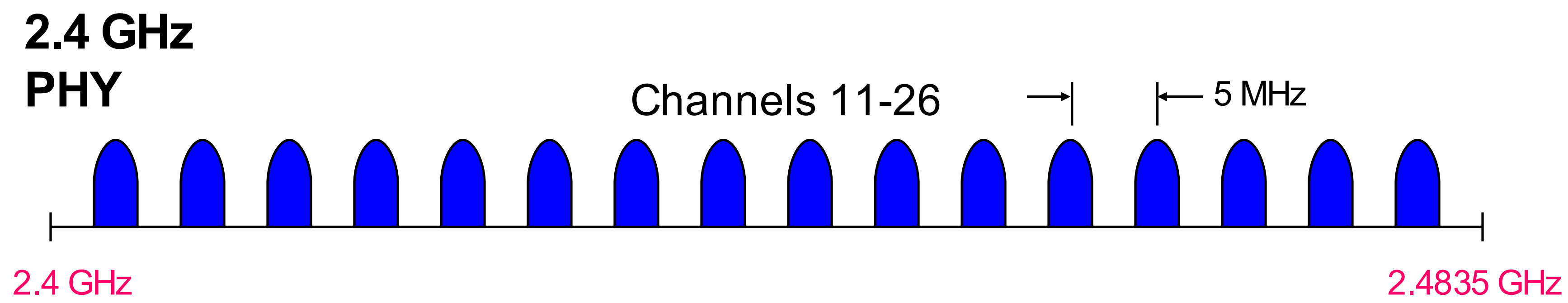
802.15.4 PHY Layer

- The standard offers two options based on the frequency band.
- Both based on direct sequence spread spectrum (DSSS).

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Operating Frequency Bands





THE UNIVERSITY of WISCONSIN MADISON

802.15.4 PHY Layer

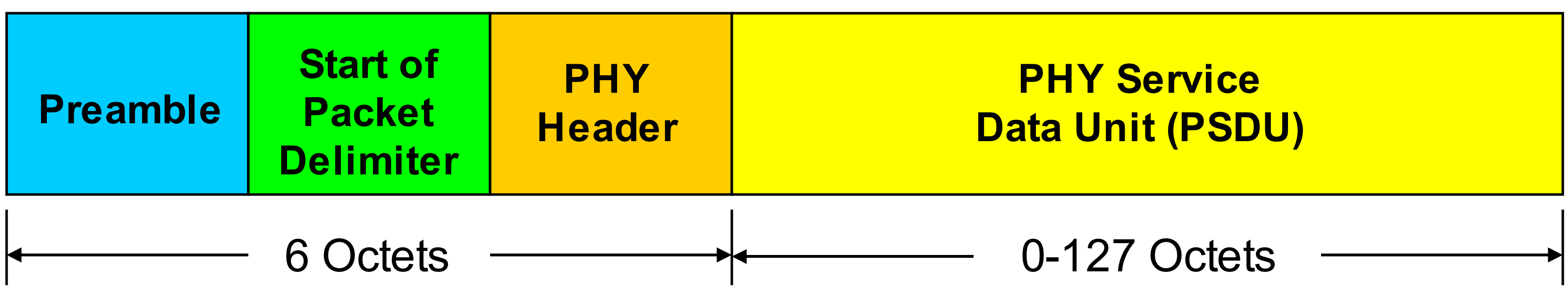
- Provides two services to physical layer management entity (PLME)
  - PHY data service
    - exchange data packets between MAC and PHY
  - PHY management service interface
    - Clear channel assessment (CCA)
      - 3 methods: Energy above threshold, Carrier sense only, or Carrier sense w/ energy above threshold
    - Energy detection (ED)
      - Used by network layer (channel selection)
    - Link Quality Indication (LQI)
      - Used by higher layers
      - Uses ED and/or SNR estimate

802.15.4 PHY Layer

Packet Structure

PHY Packet Fields

- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field



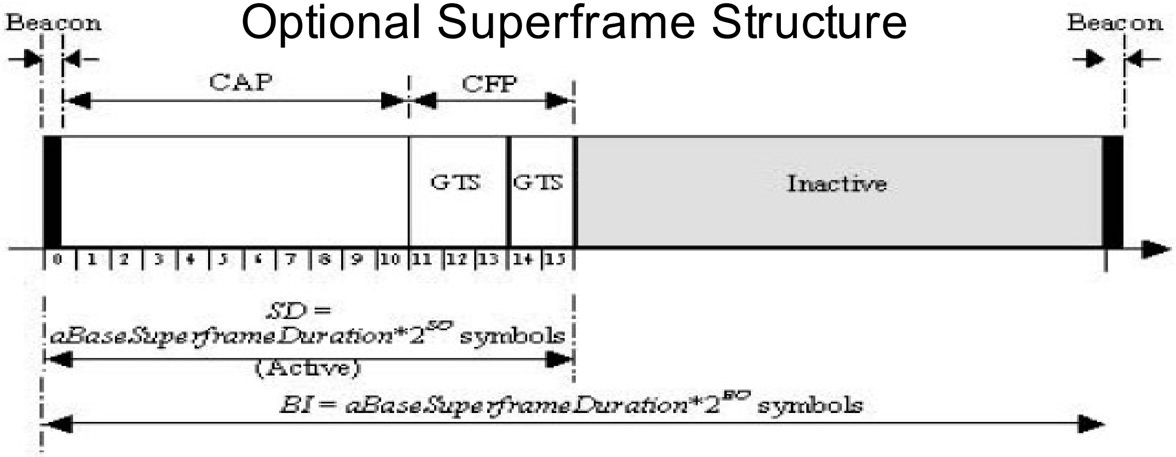
802.15.4
MAC LAYER

802.15.4 MAC Layer

- Provides two services to the MAC sublayer management entity (MLME)
  - MAC data service
    - Enables transmission and reception of MAC protocol data units (MPDU) across PHY data service
  - MAC management service
    - Beacon management
    - Channel access
    - GTS management
    - Frame validation
    - ACK frame delivery
    - Association and disassociation

802.15.4 MAC Layer

Optional Superframe Structure



Beacon – sent by PAN coordinator in the first slot of the superframe

Contention Access Period (CAP)

- Communication using slotted CSMA-CA

Contention Free Period (CFP)

- Guaranteed time slots (GTS) given by coordinator (no CSMA)

Beacon Order (BO)

- Describes the interval at which the coordinator shall transmit its beacon frames
- if BO = 15, superframe is ignored

Superframe Order (S0)

- Describes the length of the active portion of the superframe
- if SO = 15, superframe should not remain active after the beacon

THE UNIVERSITY of WISCONSIN MADISON

CSMA-CA Algorithm

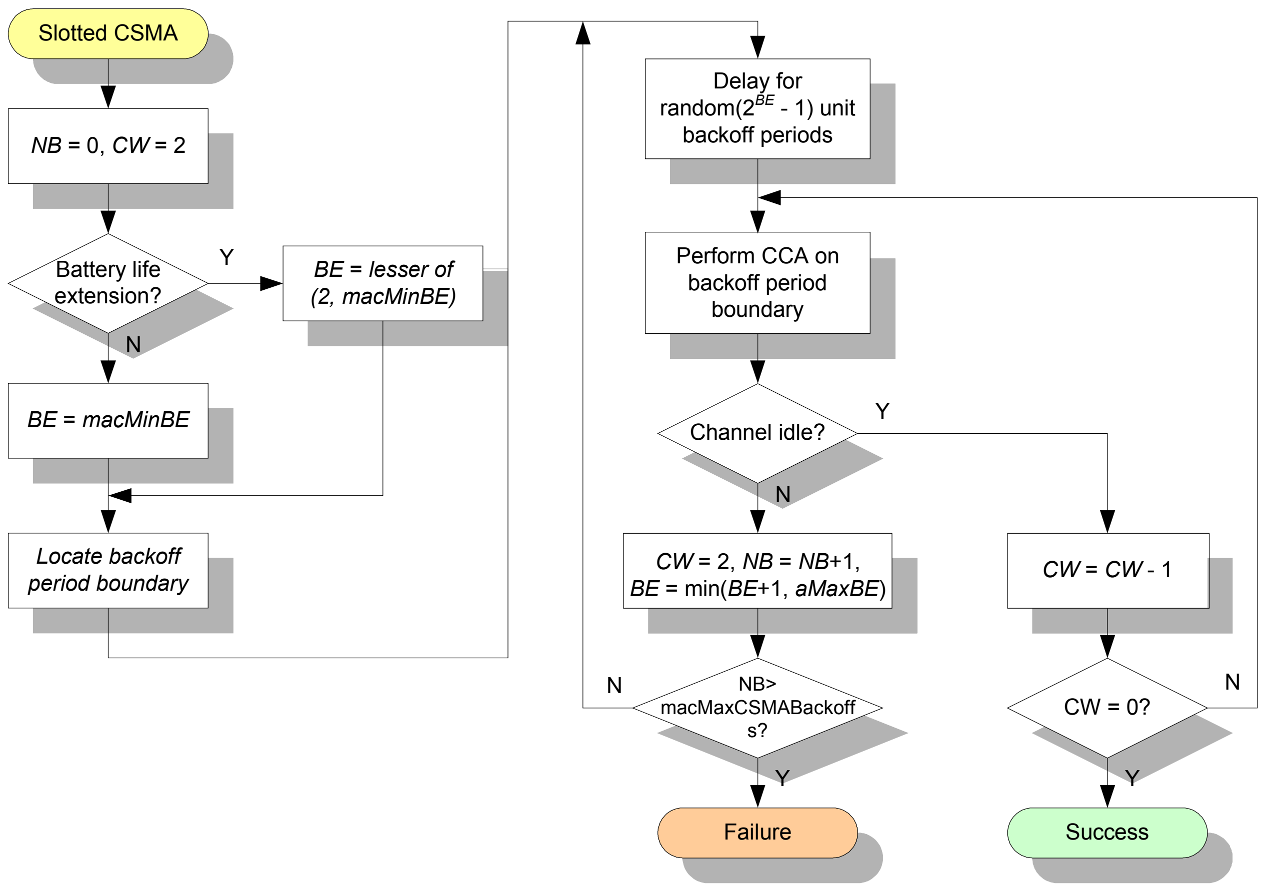
- Slotted CSMA-CA
  - Used in superframe structure
  - Backoff periods are aligned with superframe slot boundaries of PAN coordinator
  - Used in CAP, must locate boundary of the next backoff period to transmit data
- Un-slotted CSMA-CA
  - Non beacon enabled network
  - Backoff periods are not synchronized btw devices

CSMA-CA Algorithm

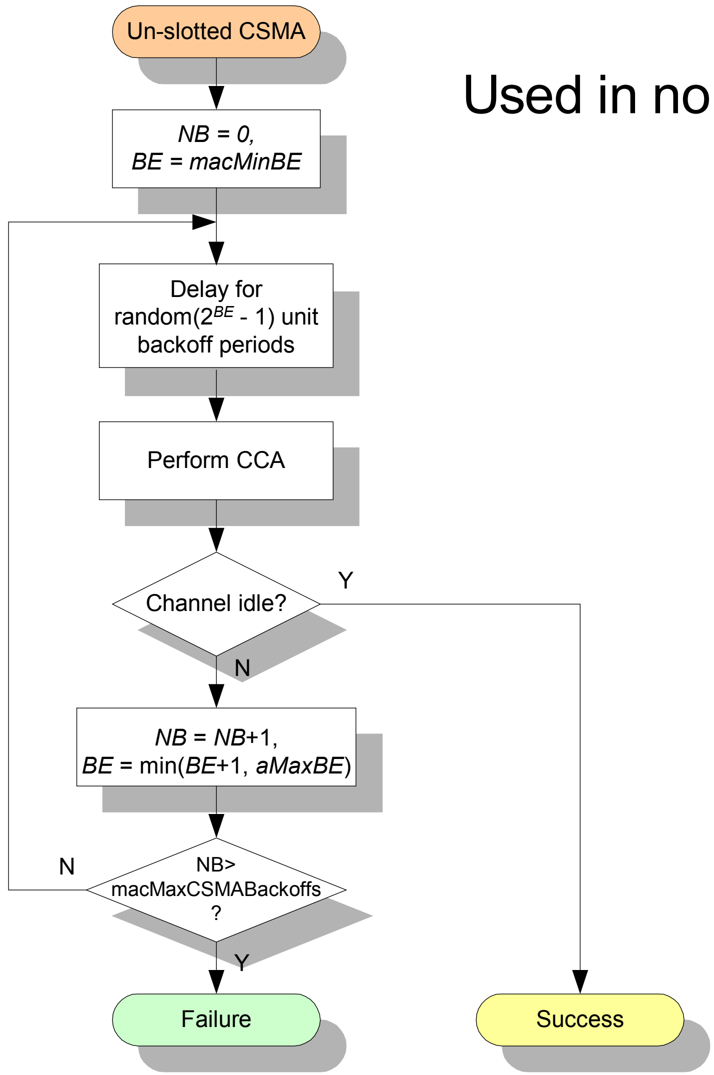
- Each device has three variables:
  - NB is the number of times the CSMA-CA was required to backoff while attempting a current transmission.
  - CW is the contention window length, which defines the number of backoff periods that needs to be clear of activity before a transmission can start.
  - BE is the backoff exponent, which is related to how many backoff periods a device shall wait before attempting to assess the channel.

Slotted CSMA Procedure

Used in beacon enabled networks.



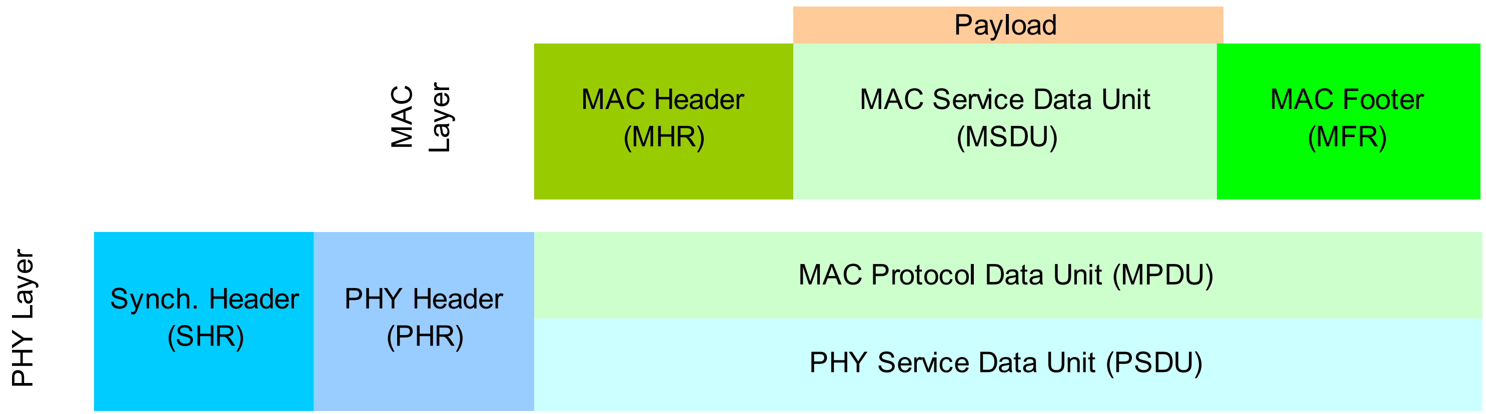
Unslotted CSMA Procedure



Used in non-beacon networks.

802.15.4 MAC Layer

General Frame Structure



4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

THE UNIVERSITY of WISCONSIN MADISON

References

- IEEE 802.15.4-2003 standard.
- Tutorial .ppt "IEEE 802.15.4 Tutorial" by Jose Gutierrez, Eaton Corporation, Jan. 2003.
- Tutorial .ppt "IEEE 802.15.4 MAC Overview" by Marco Naeve, Eaton Corporation, May 2004.
- Tutorial .ppt "802.15.4 and ZigBee" by Kevin Klues, Washington University in St. Louis.

THE UNIVERSITY of WISCONSIN MADISON

Experimental Investigation of IEEE 802.15.4 Transmission Power Control and Interference Minimization

Submitted to IEEE INFOCOM 2007

Steven Myers 1, Suman Banerjee 2, Seapahn Megerian 1, and Miodrag Potkonjak 3

smmyers@wisc.edu, suman@cs.wisc.edu, megerian@ece.wisc.edu, miodrag@cs.ucla.edu
1 Electrical and Computer Engineering Department, University of Wisconsin Madison
2 Computer Science Department, University of Wisconsin Madison
3 Computer Science Department, University of California Los Angeles

Research Motivation

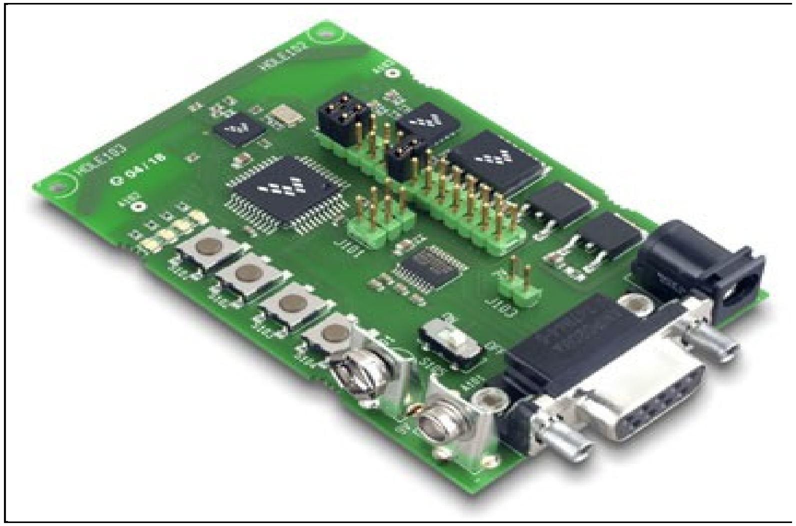
- Communication interference can severely reduce the performance of wireless networks.
- Simple models such as circular communication and interference “range” model don’t work for every wireless node package.
- Sensor networks are becoming very popular with industry.
- Studying the interference characteristics of actual hardware nodes is a fundamental research problem.

Research Goals

- In depth experimental study of the interplay between interference and transmission power using 802.15.4 physical layer hardware.
- Investigate the impact between interference and the relative positions and orientations of the wireless nodes.
- Development of experimental models of interference, transmission power, and achievable reliable communication ranges.
- Using these models in higher level algorithms.

Freescale Hardware Details

- Sensor Application Reference Design (SARD)
- MC13192 2.4 GHz RF transceiver
- MC9S08GT60 low-voltage, low-power 8-bit MCU
- Dipole antenna
- 3-axis accelerometers (-x,-y,-z)
- Interface RS-232 port



13192DSK board

SARD 13192 Radio

- Runs complete 802.15.4 PHY layer
- Operates in 2.4 GHz band
- Has 16 selectable channels
- Power supply range of 2 – 3.4 Volts
- Transmit powers from –27dBm to 4 dBm
- Theoretical throughput of 250 kbps
- Receive sensitivity of <-92 dBm @ 1% PER.
- Supports 3 power saving modes.

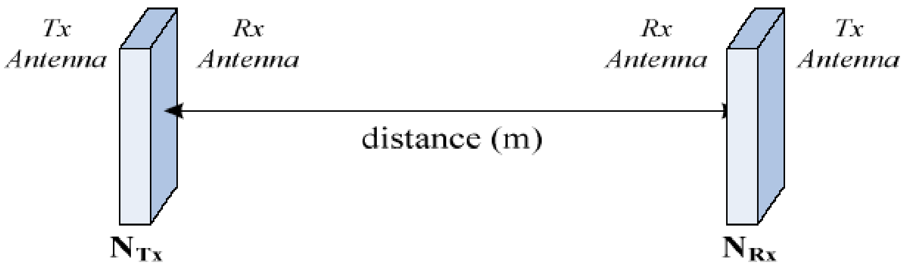
PA Power Adjust Reg 12[7:0] (Hex)	Typical Differential Power at Output Contact (dBm)	Typical PA Current (mA)
00	-27.6	1.7
04	-20.6	2.5
08	-17.7	3.8
0C	-16.3	6
1C	-15.7	6.1
2C	-15.2	6.1
3C	-14.6	6.1
4C – **PWR 4**	-8.9	6.9
5C	-8.2	7
6C	-7.5	7.1
7C	-7.1	7.2
8C – **PWR 8**	-1.6	9.3
9C	-1.1	9.6
AC	-0.7	9.9
BC – **PWR 11**	-0.3	10.2
CC	1.3	12.2
DC	1.9	13.6
EC	2.5	16.3
FC	2.6	16.6
FD	3.2	16.8
FE	3.7	16.9
FF – **PWR 15**	4.1	17

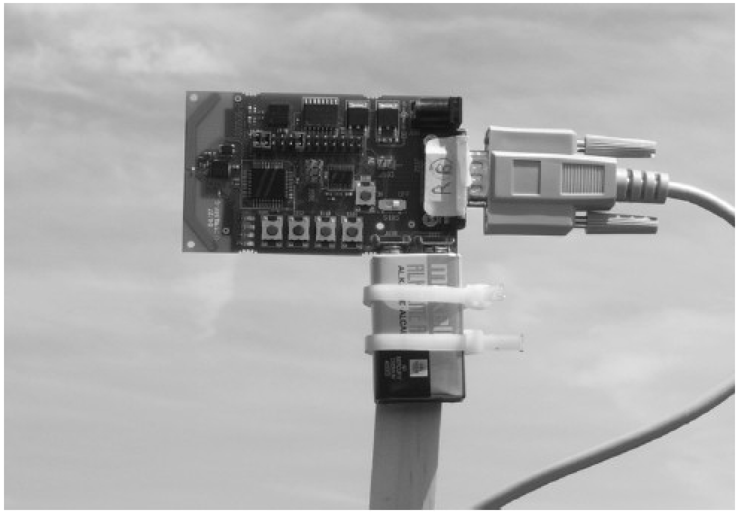
Freescale Development Flow

- Metrowerks Codewarrior 3.0 for HC08
  - Software debugger emulates CPU only
  - Supports on-chip debugging
- Programmed in C and assembly
  - Software floating point emulation available
  - Standard libraries supported
    - malloc, free, strlen, etc.
  - In line assembly used for “special” functionality
  - Interrupt driven coding style

Range Experimental Setup

- Placed NRx in a fixed location connected to a PC through RS-232.
- NTx moved at different distances (LOS) from NRx.
- Varied transmit power at NTx as well as packet size.
- Sent 256 packets at each power level tested.
- Experiments were done both indoor and outdoor.
- Varied heights and orientations of the board.
- Measured packet loss at NRx.





Range Results

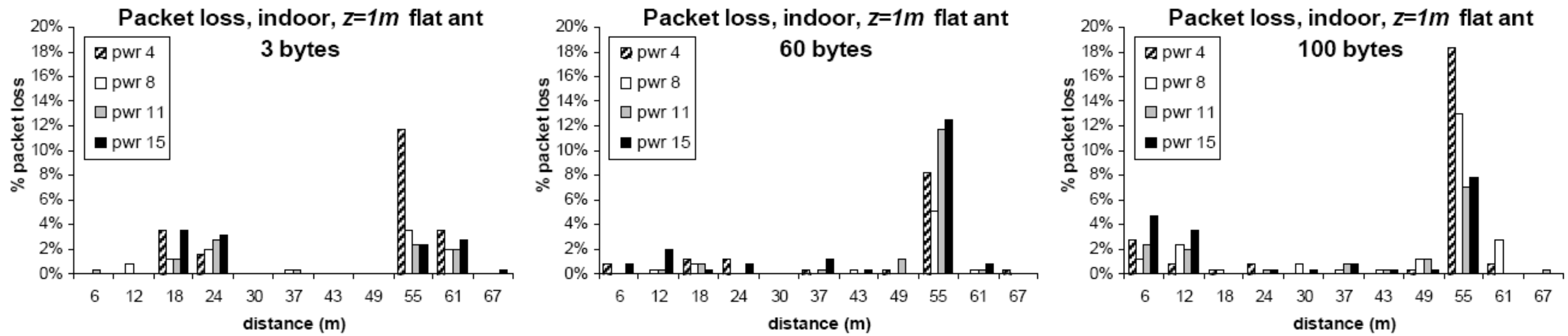


Figure 5. Indoor range test, 1m node height, flat antenna orientation, three packet sizes.

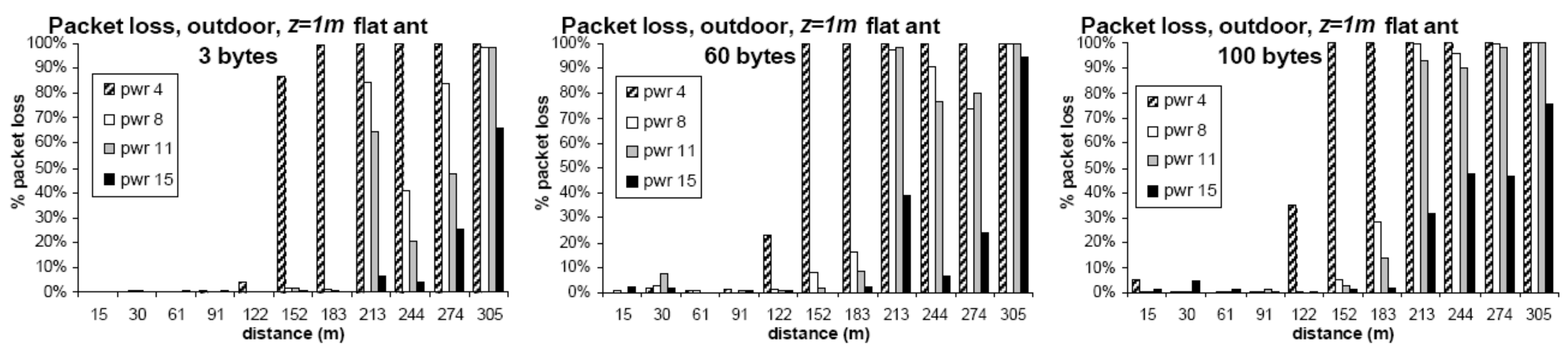


Figure 6. Outdoor range test, 1m node height, flat antenna orientation, three packet sizes.

THE UNIVERSITY of WISCONSIN MADISON

Range Results

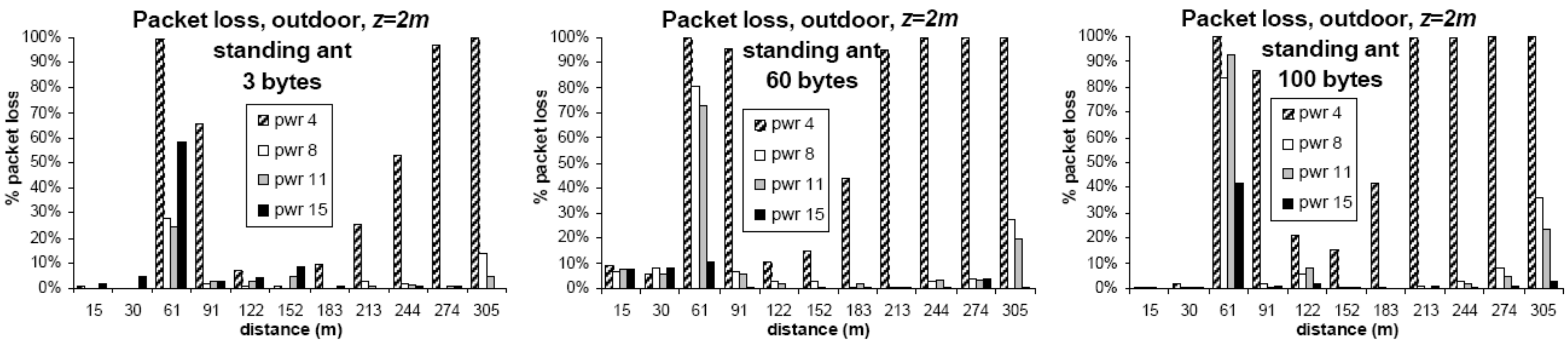


Figure 7. Outdoor range test, 2m node height, standing antenna orientation, three packet sizes.

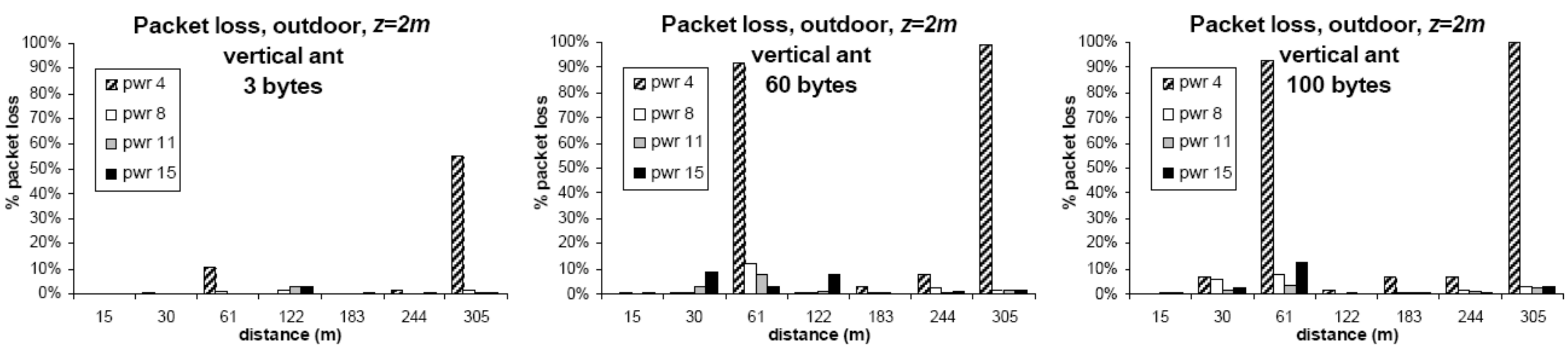


Figure 8. Outdoor range test, 2m node height, vertical antenna orientation, three packet sizes.

Interference Experimental Setup

- NRx and NTx fixed at 6m in LOS.
- Nint placed at different locations based on the Rx/Tx link. (LOS of NRx)
- All nodes place only 15 cm from the ground.
- NTx sent 1024 packets at various packet sizes with fixed transmit power.
- Nint send 100 byte continuous packets with fixed transmit power.
- Varied orientation of interferer.
- Measured packet loss at NRx.

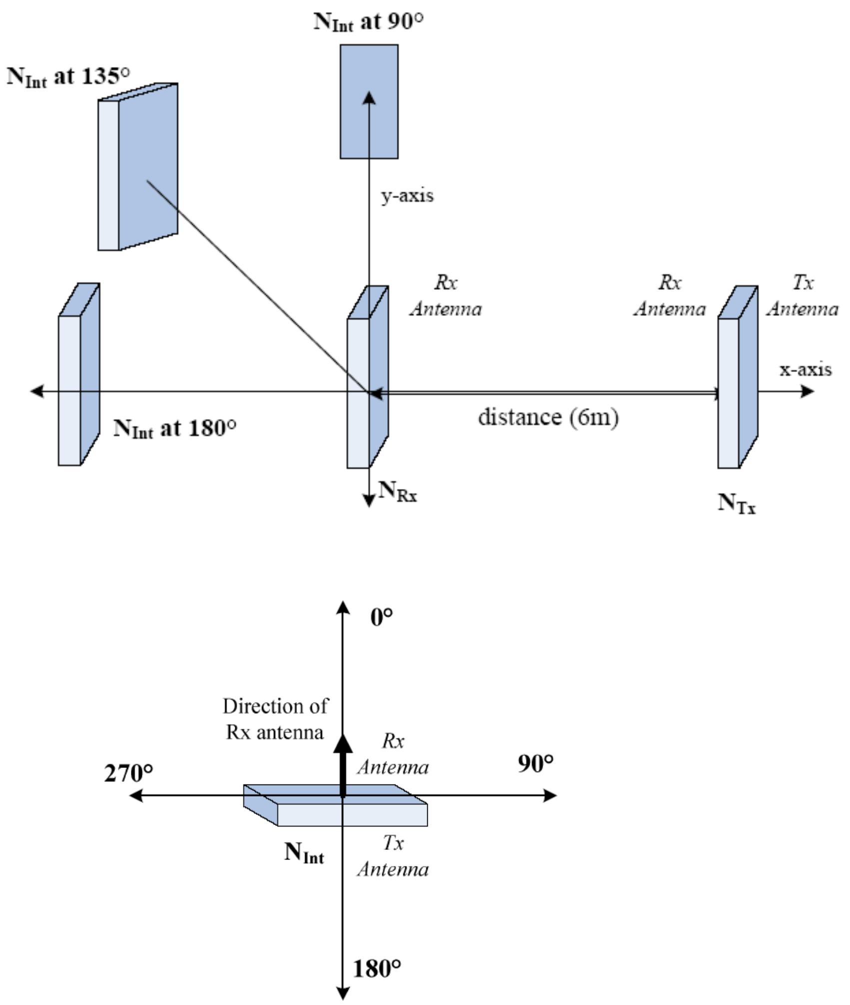


Figure 16. Orientations of the interferer N_{int}.

Interference Results

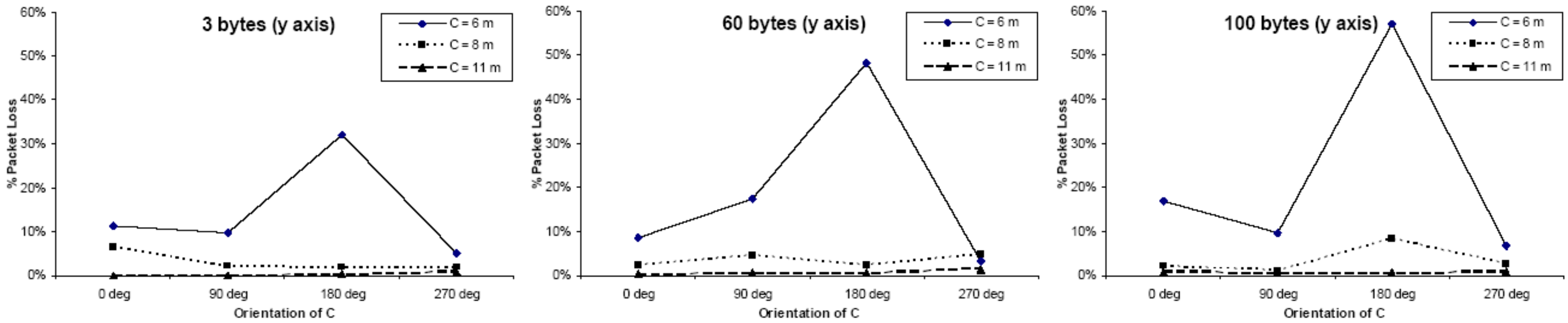


Figure 14. Effects of the positions and orientation of the interfering node on throughput at positions along the y axis.

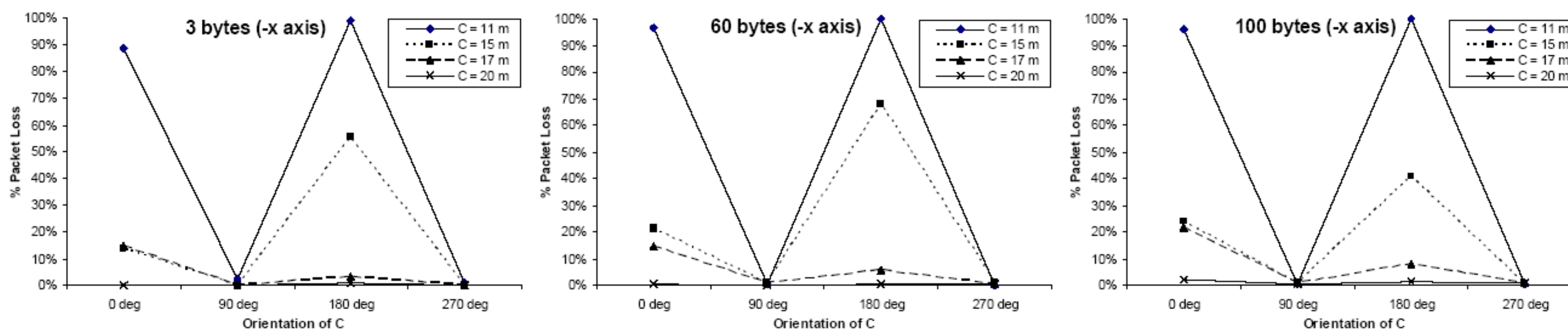


Figure 15. Effects of the orientation of the interfering node on throughput at positions along the –x axis.

THE UNIVERSITY of WISCONSIN MADISON

Future Work

- Now that we have range and interference models we need to find a way to use them.
  - Come up with scheduling algorithms to effectively schedule transmissions based on this link to node interference model
- Per packet channel switching to reduce interference.
- Also working on power minimization optimizations within different states of the radio and MCU. (ECE 751)

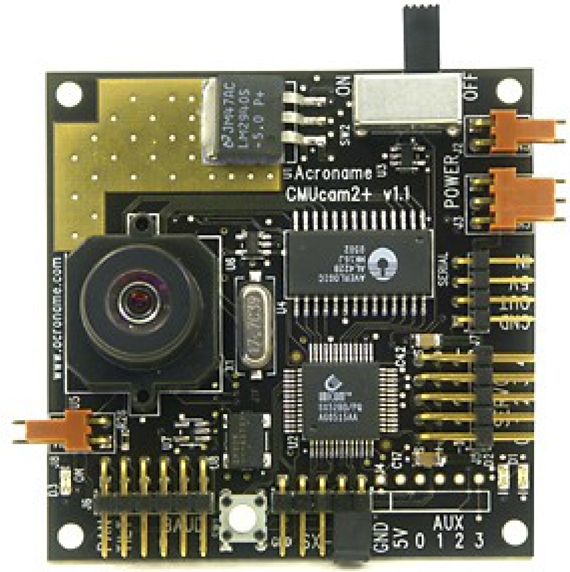
Video Surveillance demo

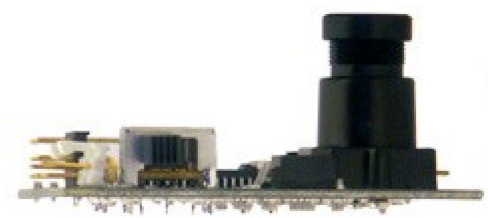
- Funded by the Defense Advanced Research Projects Agency (DARPA)
  - **ELASTIC project**: Expendable Local Area Sensors in a Tactically Interconnected Cluster
    - Cheap ad hoc sensors to be deployed rapidly
      - Ballistic deployment
      - Disaster areas
      - Military surveillance
    - Images and video desired
    - Other sensors
    - Location awareness and target tracking
    - A number of challenging research issues

Video Surveillance

- CMUCam2+
  - Commercially available (~$169)
  - SX52 microcontroller
  - 0V6620 Omnivision CMOS imager
  - Track user-defined colors at up to 50 FPS
  - Track motion using frame differencing at 26 FPS
  - Find the centroid of any tracked data
  - Gather mean color and variance information
  - Gather a 28 bin histogram of each color channel
  - Arbitrary image windowing
  - Dump a raw image (single or multiple channels)
  - Up to 160 X 255 resolution
  - Supports multiple baudrates (RS232 interface)
  - Control 5 servo outputs

  - 6-12V at ~200mA current requirement
    - Consumes a lot of power if not power managed.





Prototype Demo