18-759: Wireless Networks
Lecture 18: PAN

Dina Papagiannaki & Peter Steenkiste
Departments of Computer Science and Electrical and Computer Engineering
Spring Semester 2009
http://www.cs.cmu.edu/~prs/wireless09/

Outline

- 802 protocol overview
- Bluetooth
- Personal Area Networks – 802.15
  - Applications and positioning
  - Bluetooth
  - High speed WPAN
  - Zigbee

IEEE 802.15:
Personal Area Networks

- Target deployment environment: communication of personal devices working together
  - Short-range
  - Low Power
  - Low Cost
  - Small numbers of devices
- Four standards:
  - IEEE 802.15.1 – “Bluetooth”
  - IEEE 802.15.2 – Interoperability (e.g. Wi-Fi)
  - IEEE 802.15.3 – High data rate WPAN (WiMedia) – 15.3a (UWB)
  - IEEE 802.15.4 – Low data rate WPAN (ZigBee)

Some Common Themes

- Master/slave notion
  - Or simple node versus coordinator
- Use of “piconets”
  - Small groups of devices managed by a master or coordinator
- Support for QoS
  - Want to support voice and other media
- But many small variants in how functionality is supported

Bluetooth

- Think USB, not Ethernet
  - Cable replacement technology
- Created by Ericsson
- PAN - Personal Area Network
  - Up to 1 Mbps connections
  - 1600 hops per second FHSS
  - Includes synchronous, asynchronous, voice connections
  - Piconet routing
- Small, low-power, short-range, cheap, versatile radios
- Used as Internet connection, phone, or headset
- Master/slave configuration and scheduling

IEEE 802.15.1 – Positioning

Wireless Positioning

Bluetooth

Cellular

Wireless LAN

Personal Space: Office, Room, Bedroom, Pocket, Car
Short Range/Low Power
Voice and Data
Low cost, Small form factor, Many Co-located Nets
Universal Bridge
Bluetooth “Profiles”

- Profile specifications describe the use of BT in support of various applications
  - Includes which parts of the core specification are mandatory, optional or not applicable

- Data and voice access points
  - Real-time voice and data transmissions

- Cable replacement
  - Eliminates need for numerous cable attachments for connection

IEEE 802.15.1

- Adopted the Bluetooth MAC and PHY specifications
- IEEE 802.15.1 and Bluetooth are almost identical regarding physical layer, baseband, link manager, logical link control and adaptation protocol, and host control interface
- Range of up to 30 feet, uses FHSS
- Data transfer rates of up to 1 Mbps
  - Up to 3 Mbps for version 2
- Not designed to carry heavy traffic loads

Piconets are Basis for Topology

- Master with up to 7 active slaves
  - Slaves only communicate with master
  - Slaves must wait for permission from master
- Master picks radio parameters
  - Channel, hopping sequence, timing, ...
- Scatternets can be used to build larger networks
  - A slave in one piconet can also be part of another piconet
  - Either as a master or as a slave
  - If master, it can link the piconets

Wireless Network Configurations

- Master with up to 7 active slaves
  - Slaves only communicate with master
  - Slaves must wait for permission from master
- Master picks radio parameters
  - Channel, hopping sequence, timing, ...
- Scatternets can be used to build larger networks
  - A slave in one piconet can also be part of another piconet
  - Either as a master or as a slave
  - If master, it can link the piconets

Bluetooth Standards

- Core specifications: defines various layers of Bluetooth protocol architecture
  - Radio - air interface, tx/power, modulation, FH
  - Baseband - power control, addressing, timing, connections...
  - Link manager protocol (LMP) - link setup & mgmt, incl. authentication, encryption, ...
  - Logical link control and adaptation protocol (L2CAP) - adapts upper layer to baseband
  - Service discovery protocol (SDP) – device info, services and characteristics.

Applications Protocols

- Cable replacement protocol
  - RFCOMM (ala EIA-232 aka RS-232)
- Telephony control protocol
  - Telephony control specification
- Adopted protocols
  - PPP (IP datagrams over point-to-point links)
  - TCP/UDP/IP
  - OBEX (Object Exchange protocol by IrDA)
  - WAE/WAP
Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets
- Total bandwidth divided into 79 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
  » Remember that all communication is with the master

Sharing the Channel

- Bluetooth devices use time division duplex (TDD)
- Access technique is TDMA
- FH-TDD-TDMA

Physical Links between Master and Slave

- Synchronous connection oriented (SCO)
  » Allocates fixed bandwidth between point-to-point connection of master and slave
  » Master maintains link using reserved slots
  » Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  » Point-to-multipoint link between master and all slaves
  » Only single ACL link can exist

Bluetooth Packet Fields

- Access code – used for timing synchronization, offset compensation, paging, and inquiry
  » Channel access code (CAC) – identifies a piconet
  » Device access code (DAC) – used for paging and subsequent responses
  » Inquiry access code (IAC) – used for inquiry purposes
- Header – used to identify packet type and carry protocol control information
  » Packet type, slave address, flow control, ARQ, HEC, seqn
- Payload – data and payload header, if present
  » Channel information, L2CAP information

ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits

Channel Control

- States of operation of a piconet during link establishment and maintenance
- Major states
  » Standby – default state
  » Connection – device connected
- Inquiry: master identifies nearby slaves
- Paging: establishing a connection between a master and a slave
Inquiry Procedure

- Potential master identifies devices in range that wish to participate
  - Transmits ID packet with inquiry access code (IAC)
  - Occurs in Inquiry state
  - On 32 wake-up carriers (out of 79)
- Device receives inquiry
  - Enters Inquiry Response state
  - Returns FHS packet with address and timing information
  - Moves to page scan state

Page Procedure

- Master uses device address to calculate a page frequency-hopping sequence
- Master pages with ID packet and device access code (DAC) of specific slave
- Slave responds with DAC ID packet
- Master responds with its FHS packet
- Slave confirms receipt with DAC ID
- Slaves move to Connection state

Logical Link Control and Adaptation Protocol - L2CAP

- Provides a link-layer protocol between entities with a number of services
- Relies on lower layer for flow and error control
- Makes use of ACL links, does not support SCO links
- Provides two alternative services to upper-layer protocols
  - Connectionless service
  - Connection-mode service

L2CAP Logical Channels

- Connectionless
  - Supports connectionless service
  - Each channel is unidirectional
  - Used from master to multiple slaves
- Connection-oriented
  - Supports connection-oriented service
  - Each channel is bidirectional with QoS on each direction
- Signaling
  - Provides for exchange of signaling messages between L2CAP entities

Flow Specification Parameters

- Service type
- Token rate (bytes/second)
- Token bucket size (bytes)
- Peak bandwidth (bytes/second)
- Latency (microseconds)
- Delay variation (microseconds)
Outline

- 802 protocol overview
- Bluetooth
- Personal Area Networks – 802.15
  - Applications and positioning
  - Bluetooth
  - High speed WPAN
- Zigbee

IEEE 802.15.3

- High data rate WPAN
- Higher bandwidths than currently supported with 802.15.1
  - 100 Mbps within 10 meter
  - 400 Mbps within 5 meter
  - Typical rates are in 10s of Mbps
- Data, High quality TV, Home cinema

IEEE 802.15.3 - Features

- Dynamic topology
  - Mobile devices often join and leave the piconet
  - Short connection times
- High spatial capacity
- Multiple Power Management modes
- Secure Network
- Based on piconets
  - Data Devices (DEV) establish peer-to-peer communication
  - Includes also a Piconet Coordinator (PNC)

Network Topology

- Piconet (~10m range)
- Peer-to-peer communication between devices
- Piconet Coordinator (PNC) is responsible of piconet management
  - (beacons, timeslot reservation)
  - Possibly child piconets
  - Maximum of 243 devices in piconet
  - Piconet Identifier (PiconetID) is used for identifying the piconets

Dependent Piconets

- If there is no free channel, a device may create a dependent piconet
- If two piconets operate in the same channel, one is parent piconet and other is dependent piconet
- Parent piconet
  - Child piconet
    - PNC belongs as a device in the parent piconet
    - Extends the coverage area of the piconet
  - Neighbor piconet
    - Does not extend the coverage area
- Dependent piconets are
  - Autonomous
  - They have distinct PiconetIDs
  - They use a dedicated timeslot from the parent PNC called Channel Time Assignment (CTA) to share the time between piconets

Piconet Creation

- Device must make sure that there are no existing piconets using the same channel
  - Passive scanning is used to detect existing piconets
  - Device goes through all the channels supported by the physical layer
  - Device listens the beacon frames from PNCs
  - A device creating a piconet becomes PNC and has the following responsibility:
    - Selects the channel
    - Starts to transmit beacon frames

Joining a Piconet

- Piconets are discovered using passive scanning
- Device authenticates with PNC
- Device exchanges the capability information with PNC (PHY data rates supported, power management status, buffer space, capability to act as PNC etc.)
- Device sends association request to join the piconet
- PNC sends association response
- After joining to the piconet, the device information is broadcast with the beacon

PNC handover

- Changing PNC during the operation (PNC handover)
  - When active PNC leaves the network or runs out of battery, another device may take over PNC responsibilities
  - When new device joins the piconet
    - If the new device is more capable and the current security policies allow it, then the PNC has the option of handing over control of the piconet to the device that has just joined
  - PNC handover maintains all existing time allocations so that there is no interruption in the delivery of data in the piconet
  - PNC selects the best device among those that have the PNC Capable bit set

IEEE 802.15.3 - Frame Structure

- CAP
  - Allows contention via CSMA/CA
  - Command exchange between DEV and PNC
  - File transfers from DEV without request
- CTAP
  - Time slot allocation specified in the beacon
  - Reserved bandwidth for DEV
  - MCTA: command (PNC→DEV)
  - CTA: data (DEV→PNC)

Quality of Service

- IEEE 802.15.3 supports various traffic types with different QoS requirements
- Best-effort data without reservations (contention based)
- PNC allocates resources (slots) for devices
  - Devices make requests
  - Periodic slot reservation for synchronous data
    - Voice, video
  - Aperiodic reservation for asynchronous data
    - Allocates a certain time for sending packets
    - Bursty data transmission: file transfer etc.

IEEE 802.15.4 - Overview

- Low Rate WPAN (LR-WPAN)
- Simple and low cost
- Low power consumption
  - Years on lifetime using standard batteries
- Mostly in sensor networks
- Data rates: 20-250 kbps
- Operates at multiple frequencies
  - 868 MHz, 915 MHz, 2.4 GHz
- Blends elements from 802.15.3 and 802.11

802.15.4 applications

- Monitors sensors automation control
- TV, VCR, DVD/CD, Remote control
- Personal Health Care
- LOW DATA-RATE RADIO DEVICES
- Home Automation
- Security
- HVAC lighting closures
- Multimedia keyboard joystick
Zigbee/802.15.4 architecture

- ZigBee Alliance
  - 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
  - Defining upper layers of protocol stack: from network to application, including application profiles
  - First profiles published mid 2003
- IEEE 802.15.4 Working Group
  - Defining lower layers of protocol stack: MAC and PHY

IEEE 802.15.4 devices

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

802.15.4 devices

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

IEEE 802.15.4 - Star

Star Topology

PAN Coordinator

Master/Slave

- Full function device
- Reduced function device

IEEE 802.15.4 - Peer-to-Peer

Peer-Peer Topology

Point to point

Cluster tree

- Full function device

IEEE 802.15.4 - MAC

- One PAN coordinator & multiple RFDs/FFDs
  - Association/disassociation
- CSMA-CA channel access
  - Reliable delivery of data
- Optional superframe structure with beacons
  - GTS mechanism
- AES-128 security
- QoS – 3 traffic types
  - Periodic data: e.g. Sensor data
  - Intermittent data: generated once a while, e.g. light switch traffic
  - Repetitive low latency data: E.g. Mouse device traffic
Summary

- WiFi PAN?
  - Laptops with WiFi operating on two modes
    - WLAN
    - WiFi PAN with up to eight WiFi-enabled devices
  - Devices can communicate directly (WiFi-enabled TV with a WiFi-enabled mp3 player)