Short-range wireless communication technologies
Course T-110.5111 Fall 2014
Computer Networks II – Advanced Features

Mario Di Francesco

Department of Computer Science and Engineering, Aalto University

October 27, 2014
Summary of the last two weeks

Lecture 6

- IEEE 802.15.4 and ZigBee
  - network topologies and channel access methods
  - overview of higher-level features
- wireless sensor networks
  - taxonomy of energy conservation techniques
  - beyond sensors: smartphones and Internet-connected objects

Exam week

- (practical) work for the assignment
- preparation of the report
Learning outcomes

- Identify short-range wireless communication technologies used in real products
- List the most important technologies with specific reference to mobile devices
- Describe the physical and medium access layers of relevant technologies
- Compare the different options based on application-specific criteria
- Reflect upon communication technologies beyond radio signals
Short-range wireless technologies

Major features

- distance limited to a few meters or even less
- mostly for local network access and interconnection of personal devices
  - thus also called personal area networks
  - special case: body area networks
- usually (but not necessarily) based on radio signals

Several standards

- most of them using the unlicensed Industrial, Scientific and Medical (ISM) frequency bands
- availability depends on the actual country
- most of them available worldwide
Source: iFixit Nexus 7 Teardown
https://www.ifixit.com/Teardown/Nexus+7+Teardown/9623
Identifying technologies

- **product specifications**
  - Wi-Fi 802.11a/b/g/n
  - NFC (Android Beam)
  - Bluetooth 4.0

- **chipsets**
- **antennas**

**Example**

- **WiFi**
- **Near-Field Communication (NFC)**
- **Global Positioning System (GPS)**

*Source: iFixit Nexus 7 Teardown*
Most important technologies

WiFi

- already addressed in a previous lecture

Bluetooth

- different versions of the standard
  - “regular” Bluetooth or Bluetooth Classic (versions 2–3)
  - Bluetooth Low Energy (BLE) or Bluetooth Smart (version 4)

Near-Field Communication (NFC)

- a Radio Frequency Identification (RFID) technology
- also supports a (bi-directional) peer-to-peer mode
Origin of Bluetooth

Special interest group

- formed in 1998
- by Nokia, Ericsson, Intel, IBM and Toshiba
- as a cable replacement technology

Name

- nickname of Harold Blåtand Gormsen, King of Denmark (940–985 A.D.)

2.3.2 Bluetooth Technological Overview

The Bluetooth SIG was formed in May 1998 by the so-called promoter companies, consisting of Ericsson, IBM, Intel, Nokia, and Toshiba, and later on 3Com, Lucent, Microsoft, and Motorola. The SIG also contains associate members; participating entities pay membership fees and, in turn, can vote or propose modifications for the specifications to come. Adopter companies can join the SIG for free but can only access the oncoming specifications if these have reached a given evolutional level. The name Bluetooth supposedly comes from a Scandinavian history-enthusiast engineer involved in the early stages of developing and researching this short-range technology, and the name stuck; nobody being able to propose a better one. Bluetooth was the nickname for Harold Blåtand—"Bluetooth,"—King of Denmark (940–985 A.D.). Bluetooth conquered both Norway and Denmark, uniting the Danes and converting them to Christianity. One of the major goals of the Bluetooth standard is to unite the "communication worlds" of devices, computers, and peripherals and to convert "the wired" into wireless; thus, the analogy.

The Bluetooth specification defines functions for all the layers of the ISO-OSI 7-layer architecture; the protocol stack of Bluetooth is depicted in Figure 2.3. Bluetooth is designed so that a single chip can implement the bottom three layers with a serial (RS-232, USB, or similar) interface connecting the chip to the controller host through the so-called HCI (Host Controller Interface).

2.3.2.1 The RF Layer.

The physical or RF Layer (Radio Frequency) of Bluetooth is built on a synchronous fast-frequency-hopping paradigm with a symbol rate of 1 Mbps operating in the publicly available 2.4 GHz ISM band. In a normal operation mode, Bluetooth units will change the carrier frequency (hop) 1600 times a second over 79 different carrier frequencies separated 1 MHz apart, starting with 2.402 GHz. (Since the 2.4 GHz ISM band is not equally available in all countries, e.g., France and Spain, Bluetooth enables the operation on a reduced band with only 23 different carrier frequencies.) The modulation scheme employed is similar to that of GSM, that is, GFSK (Gaussian Frequency Shift Keying).

Bluetooth protocol stack

Baseband layer

- medium access and radio frequency control layer

Link manager

- piconet management
  - attachment (detachment) of slaves and low-power modes
  - setting the connection type (see slide 22)

- link configuration
  - quality of service negotiation
  - power-control parameters
  - accepted packet types (e.g., multislot packets)

- security
  - authentication through the pairing process
  - (symmetric) encryption
Logical link control and adaptation protocol layer (L2CAP)

- link control sublayer
  - protocol multiplexing
  - segmentation and reassembly
  - group management

Higher layers

- service discovery protocol (SDP)
- serial line emulation protocol (RFCOMM)

Profiles

- standardized services for Bluetooth links
  - headset, local area network, file transfer and synchronization
Physical layer

Radio channels
- 2.4 GHz ISM band
- 79 distinct channels with 1 MHz separation

Frequency hopping spread spectrum
- a certain channel is used for a short time
- channel are switched at 1,600 hops/s
- the hopping sequence is pseudo-random and unique for each network
- adaptive frequency hopping
  - devices keep track of the channel quality
  - channels with high interference are removed from the hopping sequence
Adaptive frequency hopping
Device roles and network types

Master
- establishes the hopping sequence
- decides when other devices communicate
- only one master for each network

Slave
- connects to the master
- up to 7 active slaves for each network

Piconet
- a master and all the slaves which are synchronized to its hopping sequence
- maximum 8 active devices (plus inactive ones)

Scatternet
- different overlapping piconets sharing at least one (bridge) device
Piconets and scatternets

A bridge is either a master or a slave in the piconets it belongs to.

Multiple access scheme

Contention-free token-based access
- the master decides which slave communicates in a slot
- polling scheme
  - actual details not specified by the standard
  - baseline: round robin scheduling

Time division duplexing
- slots are numbered according to the clock of the master and correspond to different frequency channels
- the duration of a slot is 625 µs
- the master uses even slots, slaves use odd slots
Time division duplexing

Multi-slot packet transmission

- slaves can use three or five consecutive slots for long messages
  - in this case the channel does not change until the master gets the token back

Frame structure

Different data rates

- **basic data rate** of 1 Mbps
- **enhanced data rates** of 2 and 3 Mbps
Establishing a Piconet

Device discovery
- inquiry process

Device pairing
- paging process

Parameter negotiation
- initiated by the link manager to set up the connection
Inquiry phase

Inquiry scan

- performed by the device willing to be discovered
- periodically listens for inquiry packets on a special inquiry hopping sequence of 32 frequencies

Inquiry

- sends an inquiry packet with a specific inquiry access code
- the code indicates who should respond
  - either generic or dedicated to certain type of devices

Inquiry response

- sends a response packet containing the responding device address after receiving inquiry message during the inquiry scan
- sends the corresponding inquiry hopping response sequence
Paging phase

Page

- master sends a page message to the (addressed) slave
- sends a special page hopping sequence of 32 frequencies
- master uses the clock information from slave to be paged

Page scan

- slave enters page scan state to receive page packets
- slave listens to packets addressed to its own address

Page response

- entered by the slave upon receiving a page message
- send back a page response containing its own address
- use frequencies from corresponding page response sequence
  - for each page hop there is a corresponding page response hop
Connection types

Synchronous connection oriented
- point-to-point symmetric link between master and a slave
- for delay-sensitive traffic (e.g., voice)
- reserved slots with maximum rate of 64 kbps

Asynchronous connectionless
- point-to-multipoint link between master and all slaves
- less priority than the synchronous connection oriented links
- reliable message delivery via automatic repeat request (ARQ)
Bluetooth low energy

History
■ project initiated by Nokia
■ WiBree (2006)
■ part of Bluetooth 4.0 (2009)

Features
■ very low-power and cheap
■ for a limited amount of data
■ two implementations
  – single mode for low-power devices (e.g., sensors)
  – dual mode for less constrained devices
BLE channels

40 channels with 2 MHz spacing

Source: Rolf Nilsson, “Shaping the Wireless Future with Low Energy Applications and Systems”
BLE features

Protocol stack

- **simpler**: only a few layers
  - L2CAP, link layer and physical layer
  - completely different medium access
- **less states**
  - Standby, Advertising, Scanning, Initiating, and Connection
- **low-power achieved through a low duty-cycle**
  - devices wake-up periodically for connection events and then sleep

Market availability

- besides devkits, recently appeared in off-the-shelf smartphones
  - iPhone 4S and 5, iPad 3rd gen, Samsung Galaxy S3
- the real (standard) sensor network communication technology
Conventional radios and tags

Radio transceiver

- transmitter and receiver hardware
  - powered by an external source, usually a battery
  - complex signal processing eventually through an external microcontroller

Radio tag

- a possibly battery-less means of identification
- radio version of a barcode
  - machine-readable description of an object

Image source: Example barcode from Wikimedia Commons
Enablers of battery-less communications

Electromagnetic backscatter (radiative coupling)
- similar to radar systems
  - transmitter sends electromagnetic waves
  - waves bounce back from an object
  - transmitter extracts information about the object based on the reflected signal
- up to a few meters range, mostly used in the 915 MHz band

Inductive coupling
- similar to a transformer but without a magnetic core
  - magnetic flux propagates through free-space
  - induces a current in the coil of the receiver
- less than one meter range, mostly used in the 13.56 kHz band
Electromagnetic backscatter

Load modulation

Note

- the modulating signal for the transistor has a low frequency
  - much lower than the carrier frequency
  - modulation circuitry in the tag is cost and power effective

Inductive coupling

Note

- similar scheme for load modulation

Image source: Gorferay Card Services Contactless Card
RFID roles and communication modes

**Initiator**
- tag reader or
tag reader/writer
- probes nearby tags and waits for a reply

**Target**
- tag
- replies back to the initiator once probed
- limited amount of memory
- usually less than 1 kB

**Passive**
- exchanges between a reader/writer and a battery-less tag
- purely based on backscatter/coupling

**Active**
- exchanges between a reader/writer and a battery-powered tag
- extends the communication range
RFID standards

ISO-11784
- frequency range between 129 and 139.4 kHz
- designed for animal tracking with suitable data fields

EM4100
- operating frequency of 125 kHz
- designed for proximity cards with only a unique identifier

ISO-14443
- operating frequency of 13.56 MHz
- designed for payment systems and smart cards
- different formats
  - MIFARE Ultralight and DESFire, ePassports, EMV contactless cards
  - ISO-14443A tags are compatible with NFC
Near field communication

Communication modes

- same as RFIDs (i.e., initiator and target)
- NFC device is usually more powerful than RFIDs and can also be programmed

Operating modes

- reader/writer as the corresponding RFID initiator
- card-emulation as the corresponding RFID tag
- peer-to-peer bi-directional data exchange

Physical layer

- inductive coupling, frequency range of 13.56 MHz
- radio specification according to the ISO-14443-2 standard
NFC protocol stack

Source: Tom Igoe, Don Coleman, and Brian Jepson, “Beginning NFC”, O’Reilly Media, First edition (January 2014) [Chapter 2 – NFC and RFID, p. 16]
NFC Data Exchange Format (NDEF)

Data exchange in NFC

- messages are composed of different NDEF records
- different record types for different purposes
  - applications should know what to do with them

Well-known NDEF record types

- **simple text** a string with metadata (e.g., language and encoding)
- **URIs** a uniform resource indicator
- **smart posters** may include a URI but also other data
- **signatures** trusted data originator
## NFC tag types

<table>
<thead>
<tr>
<th>#</th>
<th>Features</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>based on ISO-14443A, read-only or read/write, 96 B to 2 kB of memory, data rate of 106 kbps, no mechanism to prevent collision</td>
<td>Topaz, BCM20203</td>
</tr>
<tr>
<td>2</td>
<td>based on ISO-14443A and similar to Type 1, with additional anti-collision mechanisms</td>
<td>Mifare, Ultralight</td>
</tr>
<tr>
<td>3</td>
<td>based on ISO-18092 and JIS-X-6319-4 with no authentication and encryption, read-only or read/write, up to 1 MB per exchange, data rates of 212 and 424 kbps, anti-collision mechanisms</td>
<td>Sony FeliCa</td>
</tr>
<tr>
<td>4</td>
<td>based on ISO-14443A and similar to Type 1; 2, 4 or 8 kB of memory, up to 32 kB for exchange; data rates of 106, 212 and 424 kbps; anti-collision</td>
<td>NXP DESFire, SmartMX-JCOP</td>
</tr>
</tbody>
</table>
NFC peer-to-peer mode

Logical link control protocol (LLCP)
- compact data-link protocol based on IEEE 802.2
- two service types
  - connectionless with no reliability nor flow-control mechanisms
  - connection-oriented in-order and reliable delivery, flow-control
- link management, segmentation and reassembly, and protocol multiplexing

Simple NDEF exchange protocol (SNEP)
- request-and-response protocol based on LLCP
  - connection-oriented transport mode
- the Android implementation is called Android Beam
Card emulation mode

Basics
- **device acts as a tag, namely, as a contactless smart card**
  - it relies on an external reader/writer (initiator)
- **emulation of specific smart cards is implemented in software**

Security issues
- **smart cards contain sensitive or valuable information which should be adequately protected**
  - is your bank fine with your phone pretending to be a payment card?
- **secure element or secure access component**
  - custom hardware with some processing capabilities
  - performs some cryptographic functions
**Basic features**
- proprietary ultra-low power **wireless sensor network protocol**
- operating in the 2.4 GHz ISM band with a data rate of 1 Mbps
- supports peer-to-peer, star, tree and mesh topologies

**ANT channels**
- a master and a slave form a (synchronous, bi-directional) **channel**

---

**Image source:** “ANT Message Protocol and Usage” document
## ANT+

### Device profile
- Network rules for a specific **use-case**
  - bicycle power, speed and cadence, multi-sport speed and distance
  - muscle oxygen monitor, blood pressure, heart rate monitor
- **ANT+** is a **managed network** using device profiles
  - participating devices use a **network key**
  - obtaining a key requires to join the **ANT+ alliance** as a member

### Commercial adoption
- Mostly targeting **fitness and wellbeing**
  - Adidas miCoach, Suunto Ambit, Garmin GPS devices
- Many off-the-shelf smartphones have an **ANT transceiver**
  - Sony Xperia Z3, Samsung Galaxy S4/S5
Non-radio tags

Bi-dimensional barcodes
- leverage smartphone camera for visual data communication
- long range (if the code is big enough) but need line-of-sight

Quick-response (QR) codes
- widely used, different levels of robustness with error correction

Image source: Two-dimensional (2D) from Wikimedia Commons
Non-radio tags

Magnetic key

Acoustic codes

Acoustic communication

Audio-based networking

- smartphones have speakers and microphones
  - recent platforms have very low-power hardware
- audio can easily manipulated by software
  - encode data into the audio streams
  - either audible or not

Capacitive communications

Touch screen
- major input device in smartphones
- based on capacitive sensors

Can transfer data?
- apparently yes
- custom hardware
  - realizes high-frequency “screen tapping”
- very slow: up to 5 bps

Source: Tam Vu et al., “Distinguishing users with capacitive touch communication”, the 18th international conference on mobile computing and networking (Mobicom ’12), pp. 197–208, 2012
Summary and agenda

Today’s lecture

- short-range wireless communications
  - definition and overview
  - technologies for mobile devices
- Bluetooth Classic and Low Energy
- Near Field Communication (NFC)
  - backscattering and Radio Frequency Identification (RFID)
  - peer-to-peer and card emulation modes

Next lecture

- Monday, November 3, 2014
- topic: mobile (cellular) networks

First assignment deadline

- Friday, October 31, 2014 at 16:00 EET
Further study

Suggested activities

- study the additional reading material in Noppa
- find research articles related to the topics in the lecture
- write a simple Android application using Bluetooth and (or) NFC

Curriculum development

- Seminar on Internetworking (T-110.5191)
- Special Assignment in Networking and Security (T-110.6101)
- Applications and Services in Internet (T-110.5150)
- Mobile Cloud Computing (T-110.5121)