Mobile Networking (MobNet) Communication Networks III

Winter 2018/2019

Chapter 04: Wireless Local Area Networks

Module 01: Introduction to IEEE 802.11

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Dr. Gek Hong Sim
allyson.sim@seemoo.de

Outline & Learning Objectives

Chapter 04, Module 01

(1) IEEE 802 Families

(2) IEEE 802.11 Basics

(3) IEEE 802.11 Architecture

(4) Power Management

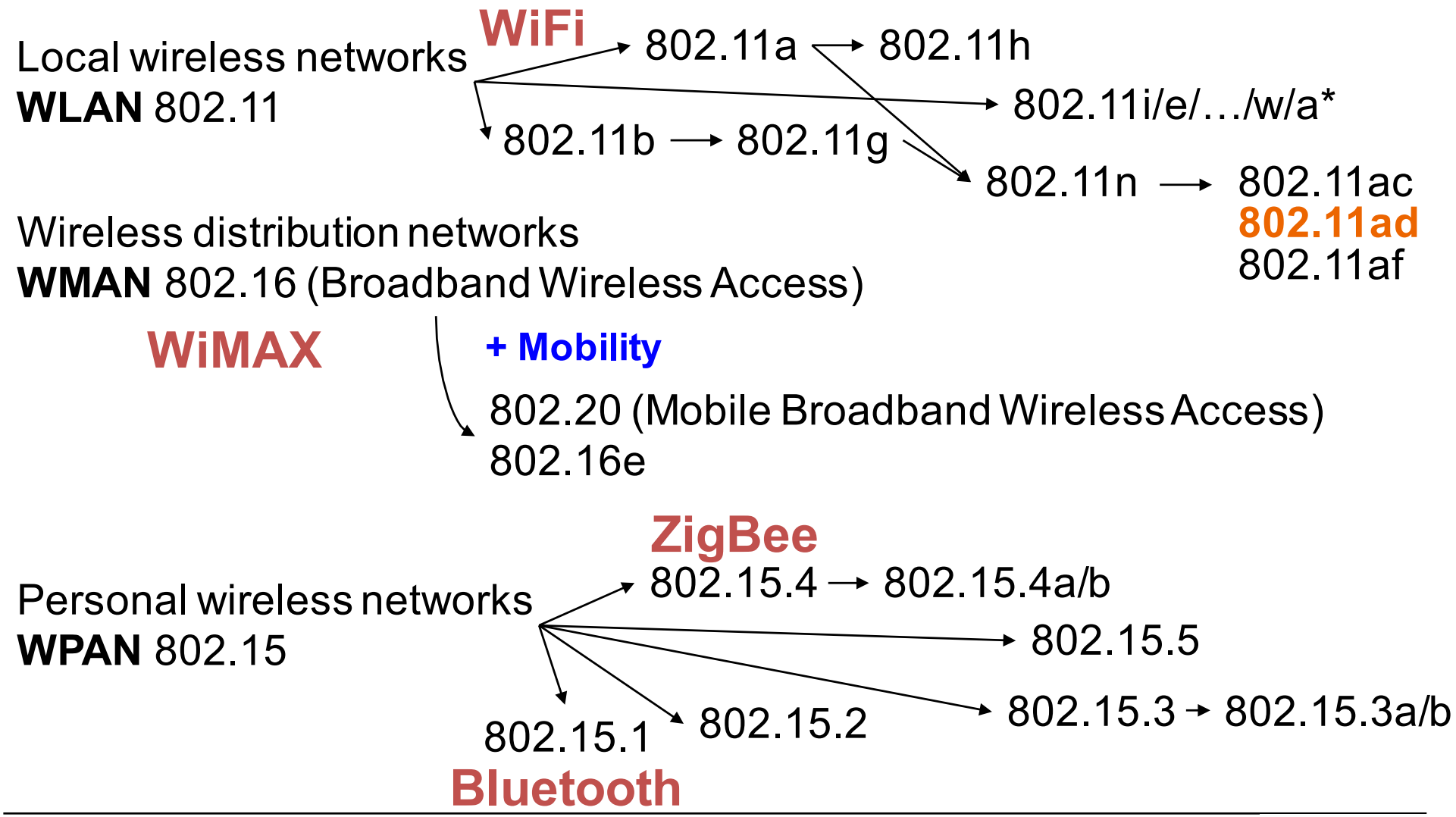
Be able to explain the basic principles underlying and motivating the IEEE 802.11 standard for Wireless Local Area Networks (WLAN)

- Characteristics and predictions for wireless LANs
- Discuss the standardization process of IEEE with respect to the 802.11 (and 802.x) family of standards
- An overview of PHY characteristics in 802.11

Chapter 04, Module 01

(1) IEEE 802 Families
(2) IEEE 802.11 Basics
(3) IEEE 802.11 Architecture
(4) Power Management

IEEE Wireless Communication Standard Families



IEEE 802.11 vs. WiFi

- **IEEE 802.11** is a standard
- **WiFi** focuses on the Wireless Fidelity
- **Fidelity** = Compatibility between wireless equipment from different manufacturers
- **WiFi Alliance** is a non-profit organization that does the compatibility testing (WiFi.org)
- 802.11 has many options and it is possible for two equipment based on 802.11 to be incompatible.
- All equipment with "WiFi" logo have selected options such that they will interoperate.

Chapter 04, Module 01

(1) IEEE 802 Families
(2) IEEE 802.11 Basics
(3) IEEE 802.11 Architecture
(4) Power Management

IEEE 802.11 Features

- Original IEEE 802.11-1997 was at 1 and 2 Mbps.
  Newer versions at 11 Mbps, 54 Mbps, 108 Mbps,..., 6Gbps
- All versions use "License-exempt" spectrum
- Need ways to share spectrum among **multiple users** and
- multiple LANs ➔ *Spread Spectrum* (CDMA)
- Three Phys:
  - Direct Sequence spread spectrum (**DSSS**) using ISM band
  - Frequency Hopping spread spectrum (**FHSS**) using ISM band
  - Diffused Infrared (850-900 nm) bands
- Supports multiple priorities
- Supports time-critical and data traffic
- Power management allows a node to doze off
  - Low power consumption

IEEE 802.11 Physical Layers

- Issued in several stages
- First version in 1997: IEEE 802.11
  - Includes MAC layer and three physical layer specifications
    - Two in 2.4-GHz band and one infrared
  - All operating at 1 and 2 Mbps
  - No longer used
- Two additional amendments in 1999:
  - IEEE 802.11a-1999: 5-GHz band, 54 Mbps/20 MHz,
    - OFDM
  - IEEE 802.11b-1999: 2.4 GHz band, 11 Mbps/22 MHz
- Fourth amendment:
  - IEEE 802.11g-2003 : 2.4 GHz band, 54 Mbps/20 MHz, OFDM

History of the 802.11 MAC

- Derived from Ethernet (CSMA/CD) philosophy
- Developed into present form 1990-1994
- Required much modification to fit wireless medium
  - CSMA/CA
- Widely regarded at the time as a kludge (hack)
  - Many attempts to do better than the perceived “kludge” of 802.11 CSMA/CA
  - HIPERLAN 1, HIPERLAN 2 (Wireless ATM)
    - Started with blank sheets of paper
    - But went in radically different directions
  - None able to overhaul 802.11, but solutions crept into IEEE standardization later

The market decided that 802.11 was the winner, INTEROPERABILTY and WORKING SYSTEMS being one of the key factors

ISM Bands

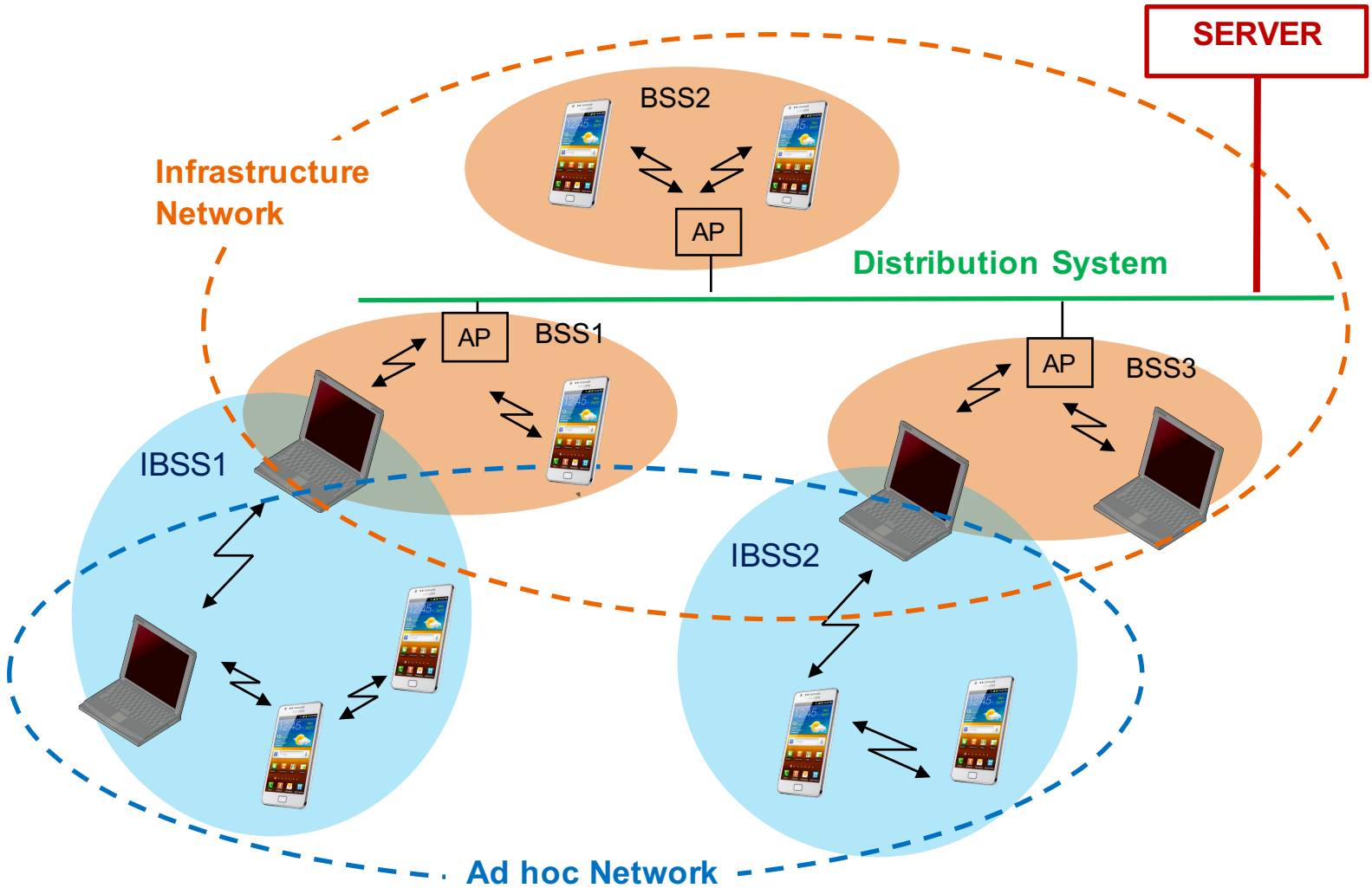
- Industrial, Scientific, and Medical bands. License-exempt

From	To	Bandwidth	Availability
6.765 MHz	6.795 MHz	30 kHz	
13.553 MHz	13.567 MHz	14 kHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	Europe, Africa, Middle east, Former Soviet Union
902.000 MHz	928.000 MHz	26 MHz	America, Greenland
2.400 GHz	**2.500 GHz**	**100 MHz**	**Worldwide**
5.725 GHz	**5.875 GHz**	**150 MHz**	**Worldwide**
24.000 GHz	24.250 GHz	250 MHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	
122.000 GHz	123.000 GHz	1 GHz	
244 GHz	246 GHz	2 GHz	

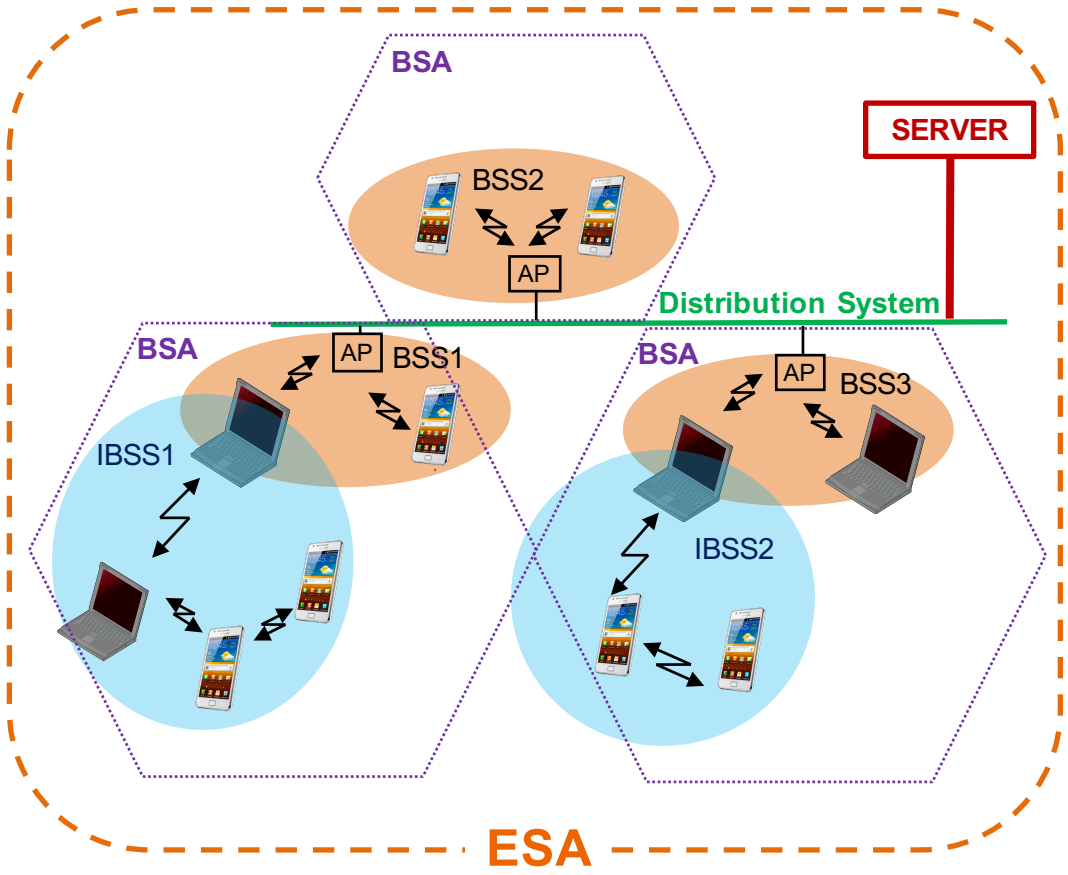
Chapter 04, Module 01

(1) IEEE 802 Families
(2) IEEE 802.11 Basics
(3) IEEE 802.11 Architecture
(4) Power Management

Comparison: Infrastructure vs. Ad-Hoc Networks



IEEE 802.11 Architecture

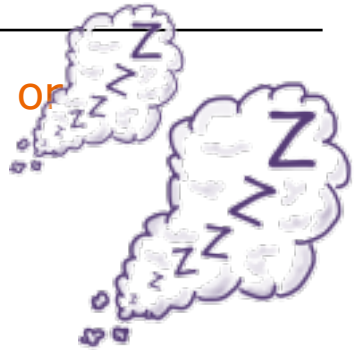


- **Basic Service Area (BSA):** A cell. Each BSA may have several access points (APs)
- **Basic Service Set (BSS):** Set of stations associated with one AP
- **Independent Basic Service Set (IBSS):** Set of computers in **ad-hoc mode**. May not be connected to wired backbone.
- **Distribution System (DS):** wired backbone
- **Extended Service Area (ESA):** Multiple BSAs interconnected via a distribution system
- **Extended Service Set (ESS)** = Set of stations in an ESA
- Ad-hoc networks coexist and interoperate with infrastructure-based networks

Chapter 04, Module 01

(1) IEEE 802 Families
(2) IEEE 802.11 Basics
(3) IEEE 802.11 Architecture
(4) Power Management

802.11 Power Management



- Station tells the base station its mode: **Power saving (PS)** or active
- Mode changed by power management bit in the frame control header.
- All packets destined to stations in PS mode are buffered
- AP broadcasts list of stations with buffered packets in its beacon frames: Traffic Indication Map (TIM)
- Subscriber Station (SS) sends a PS-Poll message to AP, which sends one frame.
- With 802.11e unscheduled Automatic Power Save Delivery (APSD): SS transmits a data or null frame with power saving bit set to 0. AP transmits all buffered frames for SS.
- With Scheduled APSD mode: AP will transmit at pre-negotiated time schedule. No need for polling.

Automatic Power Save Delivery (APSD)

- **Unscheduled APSD (U-APSD):**
  - AP announces waiting frames in the beacon
  - When stations wake-up they listen to beacon.
  - Send a polling frame to AP.
  - AP sends frames.
- **Scheduled APSD (S-APSD):**
  - Station tells AP its wakeup schedule
  - AP sends frame on schedule. No need for polling.
- **Hybrid APSD mode**: PS-poll for some. Scheduled for other categories

Acknowledgements & Additional Readings

SEEMOO SECURE MOBILE NETWORKING

- Some of the slides in this chapter have been adopted from
  - Duncan Kitchin @ Intel Corporation, Wireless Networking Group
  - Prof. Jochen Schiller @ FU Berlin, Prof. Schmitt @ U Kaiserslautern
  - Prof. Raj Jain @ Washington University in St. Louis

- Additional Readings
  - [Schiller2003] gives a an overview

  - Standards and web resources
    - http://grouper.ieee.org/groups/802/11/
      →IEEE 802.11 committee
    - http://standards.ieee.org/getieee802/
      →Download of selected specifications (see also download area on our course webpage)
    - http://www.wi-fi.org (Wi-Fi Alliance)
    - http://www.wifiplanet.com

Copyright Notice