Helsinki University
of Technology

T-79.7001 Postgraduate Course in Theoretical Computer Science
T-79.5401 Special Course in Mobility Management: Ad hoc networks
(2 - 10 cr) P V

professor Hannu H. Kari

Laboratory for Theoretical Computer Science

Department of Computer Science and Engineering

Helsinki University of Technology (HUT), Espoo, Finland

email: Kari [at] tcs [dot] hut [dot] fi

Credits

- **Material based on**
  - **C. Siva Ram Murthy and B. S. Manoj: "Ad Hoc Wireless Networks: Architectures and Protocols**
  - **Teemu Vainio: The Applicability of Bluetooth in Ad Hoc Networks, Master's thesis 2003, Helsinki Univ. of Tech, CSE-department**

Errata

- **Time to form ad hoc network with BlueTooth:**
  - **Correct figures:**
    - **With two nodes:**
      - **Depending on the inquiry duration:**
        - **4s: about 20s to form a network**
        - **8s: about 33s**
        - **12s: about 40...50s**
    - **With three nodes:**
      - **Depending on the inquiry duration:**
        - **4s: about 60-80s to form a network**
        - **8s: about 110-120s**
        - **12s: about 120-160s**
        - **Maximum time to converge the network was 240 seconds**

Wireless networks

- **Address vs. location**
  - **Hierarchical routing of packets based on IP-addresses**
- **Error prone media**
  - **10 ^-4 bit error rate (wireless) vs. 10^-9 (wired)**
- **Dynamic topology**
  - **Connectivity restrictions**
- **Vague definition of ”boundaries”**
  - **Access control problems**

Helsinki University
of Technology

Wireless network eavesdropping

BlueTooth Sniper rifle: range 1500+ meters
WiFi Sniper rifle: range 10+ km
(http://www.tomsnetworking.com/2005/03/08/how_to_bluesniper_pt1)

Design goals

- **Operation simplicity**
- **Power-efficiency**
- **Licence-free vs. licenced bands**
- **Interference tolerance**
- **Global usability**
- **Security**
- **Safety requirements**
- **Quality of service requirements**
- **Compatibility with other technologies**

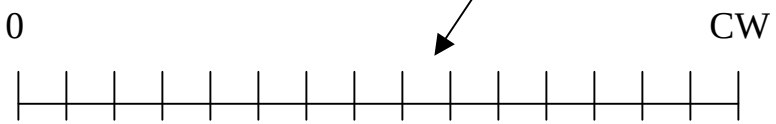
- **Infrastructure mode vs. ad hoc mode**
  - **Infrastructure mode**
    - **Association, reassociation, disassociation, distribution, integration**
    - **Authentication, deauthentication, privacy, data delivery**
    - **Basic service set (served by one access point, AP)**
    - **Extended service set (served by several APs)**
  - **Ad hoc mode**
    - **All nodes equal**
    - **No separate APs**
    - **Direct communication between mobile nodes is possible**

IEEE 802.11 MAC protocol

- **Carrier sensing in wired/wireless networks**
  - **Wired network:**
    - **e.g., CSMA/CD (Carrier Sense Multiple Access/Collision Detection)**
    - **Carrier (=transmission of other nodes) can be detected**
    - **Collisions can be detected**
  - **Wireless network:**
    - **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)**
    - **Carrier (=transmission of other nodes) can be detected**
    - **Collisions can't be detected**
      - **They should be avoided**

Helsinki University
of Technology

IEEE 802.11 MAC protocol: Contention Window/Back-off time

- **Contention Window (CW) for back-off timing**
  - **Window in which nodes may randomly access channel**
    - **E.g., IEEE 802.11a: CWmin = 15, CWmax=1023**
    - **Algorithm:**
      1. **CW= CWmin**
      2. **Transmission starts at random(0, CW)**
      3. **If collision, CW = min (CW*2, CWmax), goto 2**
    - 

    - **Adaptibility on the network load?**
      - **If node could know the number of active nodes, CW could be optimized**

Helsinki University
of Technology

IEEE 802.11 MAC protocol: CSMA/CA

- **Distributed Cordination Function (DCF)**
- **Inter-Frame Spacing (IFS)**
- **DIFS (DCF IFS)**
- **SIFS (Short IFS)**
  - **For high priority data transmission**
- **RTS (Ready to send)**
- **CTS (Clear to send)**
- **NAV (Network Allocation vector)**

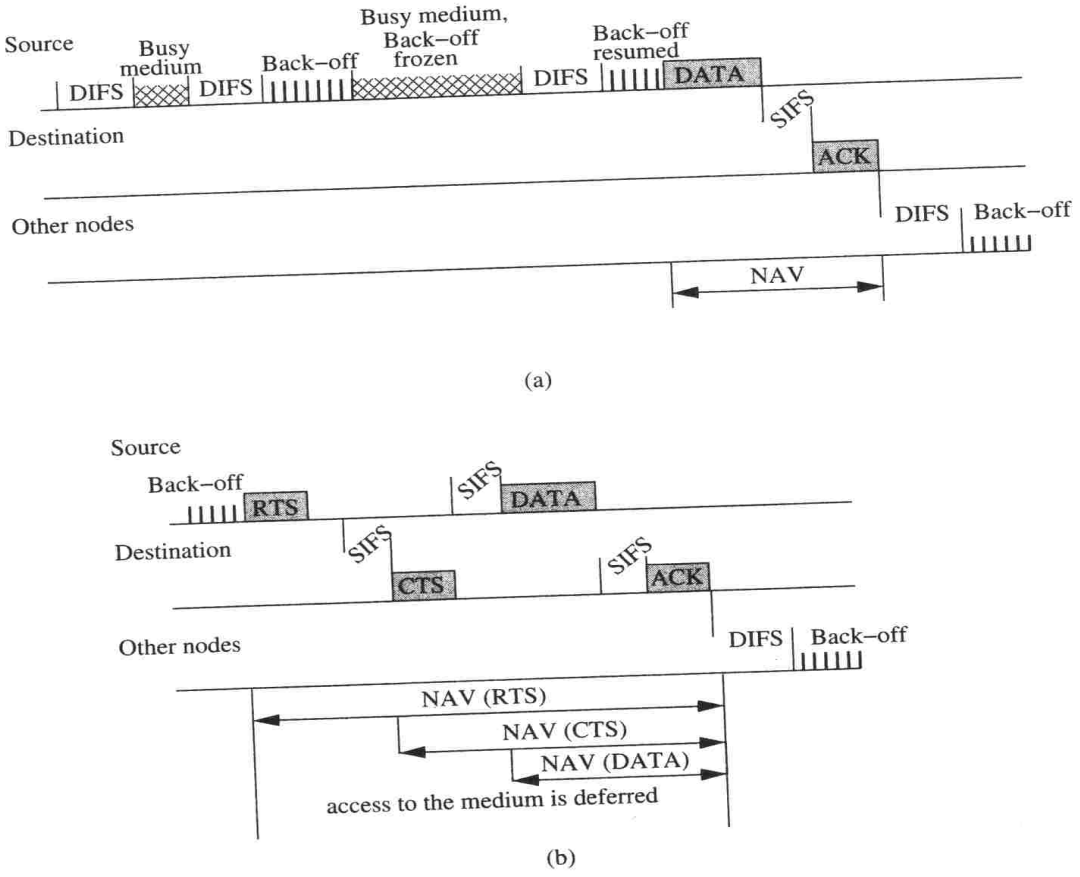
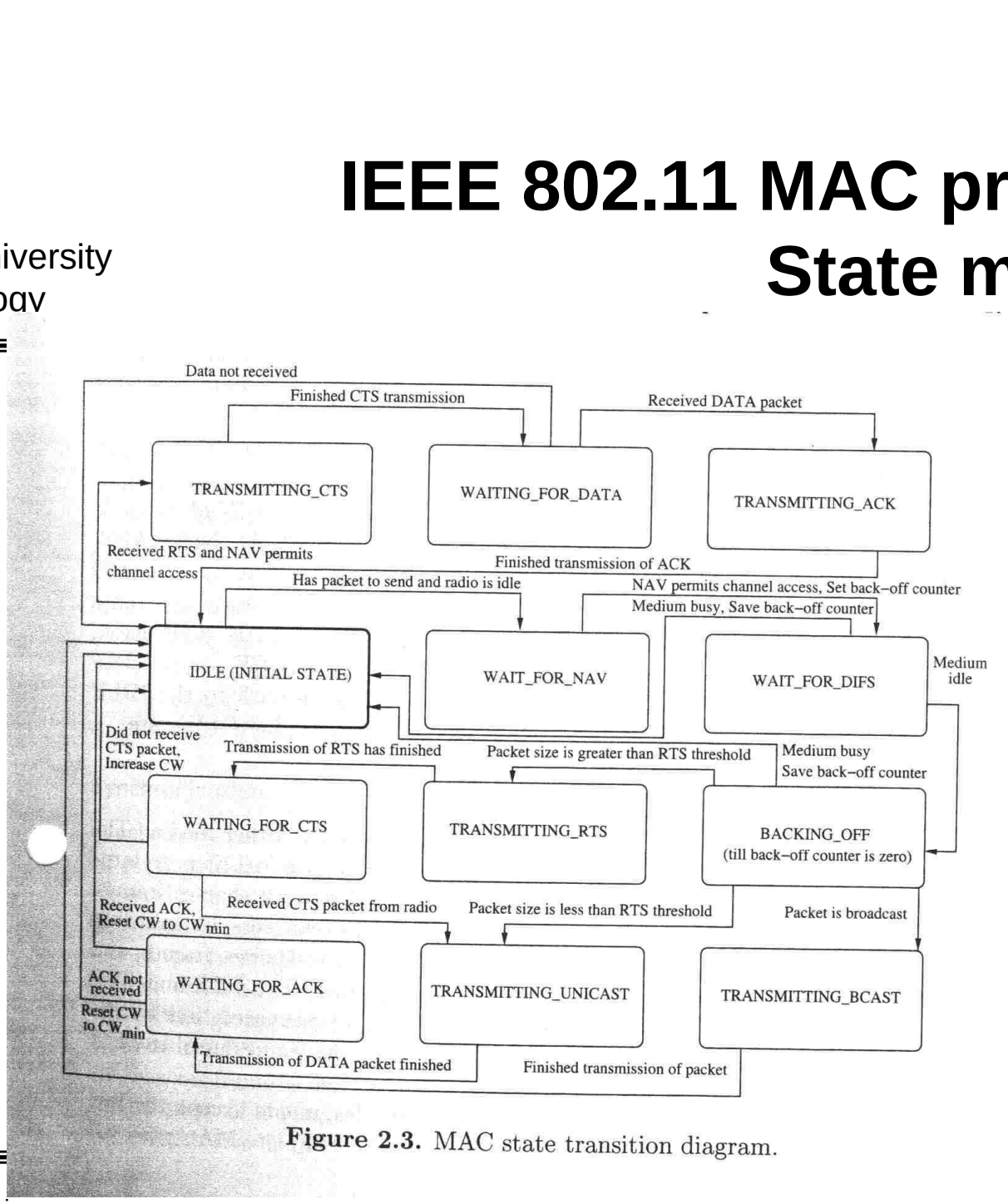


Figure 2.2. IEEE 802.11 DCF and RTS-CTS mechanism.

IEEE 802.11 MAC protocol:

Table 2.1. IEEE 802.11 parameters

Parameter	802.11 (FHSS)	802.11 (DSSS)	802.11 (IR)	802.11b	802.11a
t_{slot}	50 μsec	20 μsec	8 μsec	20 μsec	9 μsec
SIFS	28 μsec	10 μsec	10 μsec	10 μsec	16 μsec
PIFS	SIFS $+t_{slot}$				
DIFS	SIFS$+(2 \times t_{slot})$				
Operating Frequency	2.4 GHz	2.4 GHz	850-950 nm	2.4 GHz	5 GHz
Maximum Data Rate	2 Mbps	2 Mbps	2 Mbps	11 Mbps	54 Mbps
CWmin	15	31	63	31	15
CWmax	1,023	1,023	1,023	1,023	1,023



Helsinki University
of Technology

IEEE 802.11 MAC protocol: State machine

Figure 2.3. MAC state transition diagram.

Helsinki University
of Technology

IEEE 802.11 MAC protocol: Other functions

- **Point Coordination Function (PCF)**
  - **Used with AP-mode: To ensure maximum delays, minimum bandwidth, QoS**
    - **AP splits access time into ”super frames”, where higher priority nodes have better service**
- **Synchronization**
  - **Clock synchronization for power management, PCF, frequency hopping, ...**
  - **Beaconing can be used for synchronization**
- **Power Management**
  - **Sleep vs. active mode; Active vs. monitoring mode**
- **Roaming**
  - **Handing off a mobile node from one AP to another**
- **Encryption**

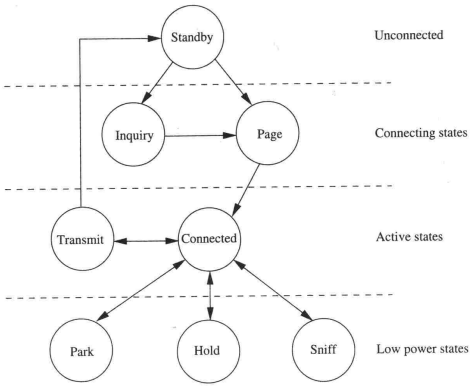
Helsinki University
of Technology

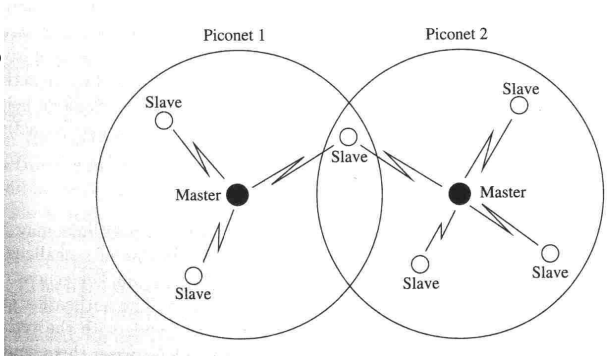
Other short range wireless standards

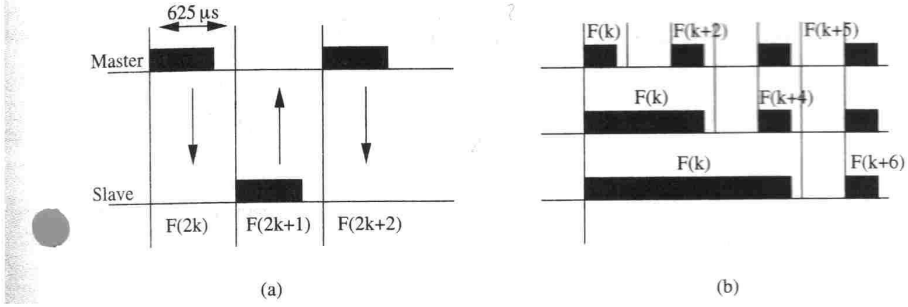
- **Telestandards:**
  - **HiperLAN/1 ... dead**
  - **HiperLAN/2 ... dead**

Other short range wireless standards: BlueTooth

- **BlueTooth ... in mobile phones**







Helsinki University
of Technology

Other short range wireless standards: Open standards

- **Open/”Internet”-standards**
  - **Home RF, IrDA, ...**
  - **ZigBee: < 1Mbps**
    - **Low power, low speed, low cost device**
    - **Three node types:**
      - **ZigBee coordinator: Form network (tree) structure**
      - **ZigBee router: Route data**
      - **ZigBee end node: Send/receive data**
  - **Wibree: Max 1Mbps**
  - **Wireless USB: 400 Mbps**

Questions

- **Benefits of RTS/CTS over PCF?**
- **Difference between Hand-over & Hand-off?**
- **Complexity of MAC protocol (state machine) and potential DoS attacks?**