Understanding the technology behind IEEE 802.11 based Wireless Local Area Networks

Instructors: Dr. S. Srikanth and Mr. K. Bhaskar

Schedule

- **Overview of 802.11 and course objectives (1 hour)**

  - History and evolution of 802.11
  - Typical 802.11 products and networks
  - Frequency bands of operation

- **Radio Frequency (RF) Fundamentals (1 hour)**

  - RF behavior and properties
  - Basics of wireless channels
  - Fading
  - Intersymbol Interference
  - Principles of antennas
  - Noise floor, Noise Figure, and SNR
  - RF math calculations
  - Link budgets and receiver sensitivity
  - RSSI concepts

- **Physical Layer of 802.11 networks (1 hour)**

  - Key challenges for the 802.11 PHY. layer
  - OFDM as a solution
  - Use of OFDM in 802.11
  - Parameters of the IEEE 802.11 a/b/g PHY. Layer
  - Evolution of the PHY layer to 802.11n

- **Medium Access Control in 802.11 (4 hours)**

  - Challenges for the 802.11 MAC
  - The Distributed Coordination Function (DCF)
  - Solving the hidden node problem
  - Infrastructure Vs Ad-hoc networks
  - The Point Coordination Function (PCF)
  - Network entry process; role of beacons
  - Concepts of SSID, BSSID, etc.
  - Virtual AP ideas
  - Performance of 802.11
  - Drawbacks of 802.11 MAC

- **Security in 802.11 networks (4 hours)**

  - Security Overview
    - Wired Scenario
    - Wireless Scenario
      - Benefits
      - Problems & Solutions
  - Confidentiality
    - Secret key cryptography
    - Stream Cipher - RC4 Cipher
    - Wired Equivalent Privacy (WEP)
      - WEP Working, WEP weakness
    - WiFi Protected Access (WPA1)
      - Evolution of WPA, TKIP details
      - Defeating attacks
    - Robust Secure Network (WPA2)
    - Differences between WPA1 & WPA2
    - CCMP
  - Integrity
    - WEP integrity, Attacks
    - TKIP Integrity
    - RSN Integrity
  - Authentication
    - WEP Authentication, Attacks
    - Dot1X Authentication Details
    - Public key Cryptography, Certs & PKI
    - EAP-TLS,TTLS,PEAP,LEAP,MD5
  - Scalability & Management
    - WEP Key Management
    - Dot1X Auto key Management
    - Pair wise key establishment
  - Wireless Intrusion
    - WIDP, Layered Approach
  - WiFi Protected Access (WPS)

- **QoS in 802.11 WLANs (1.5 hours)**

  - Drawbacks of basic 802.11 MAC with respect to QoS
  - Introduction to the IEEE 802.11e standard
  - The EDCF mode of operation
  - The HCF mode of operation
  - WMM certification

- **Overview of 802.11n (1 hour)**

  - Motivations and objectives
  - Physical layer enhancements; MIMO
  - MAC layer enhancements; Aggregation
  - Data rates
  - Backward compatibility with 802.11g