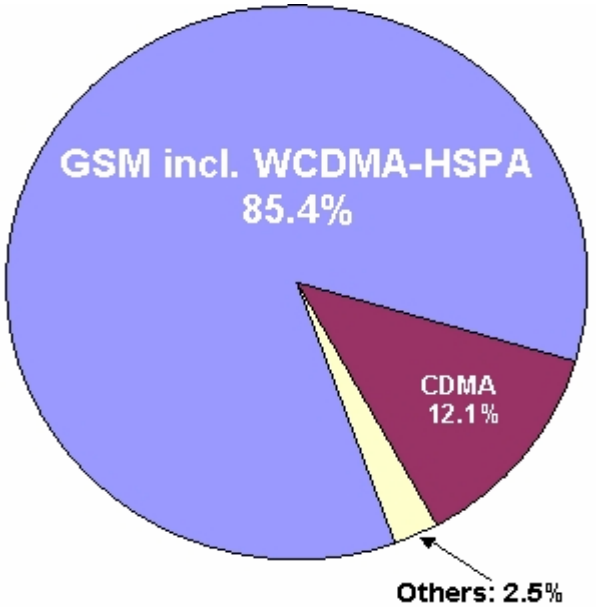
Global Cellular Market Data

- Currently over 2.3 billion cellular subscribers worldwide (INSTAT)
- By 2010 projected to be over 3.6 billion (over half the world - INSTAT)
- 3GPP (GSM/WCDMA) has most of the market (77% in 2005, 83% in 2006)
  - Most of that lead is in GSM
- 3GPP2 (cdma2000) got a massive jump on 3GPP
- However, WiMAX may soon outpace…



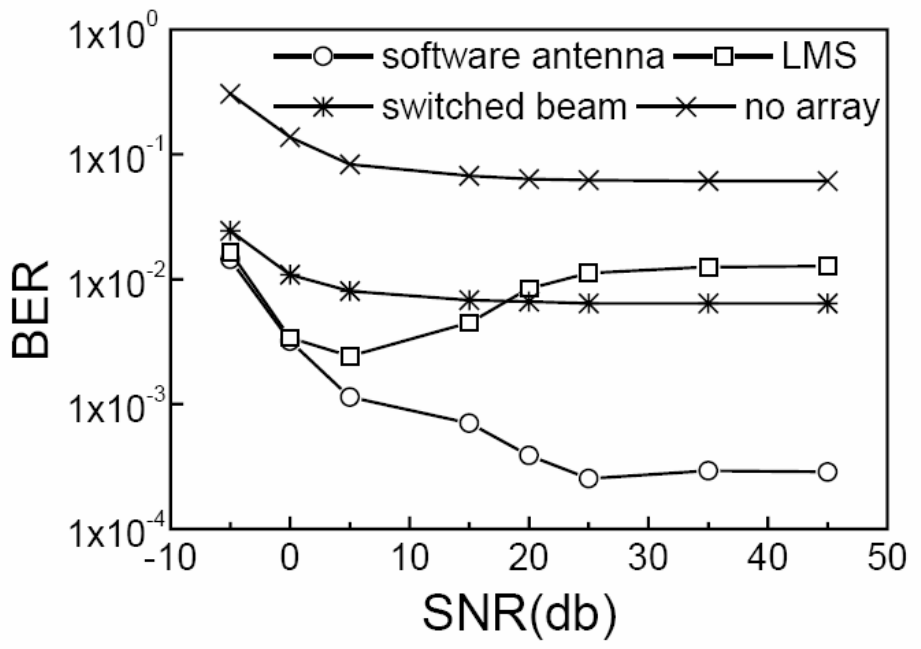
Others = AMPS, iDEN, NMT, PDC, TDMA

http://www.gsacom.com/news/statistics.php4

As of July 07
http://www.3gtoday.com/wps/portal/subscribers/

Role of Antenna Arrays in TD-SCDMA

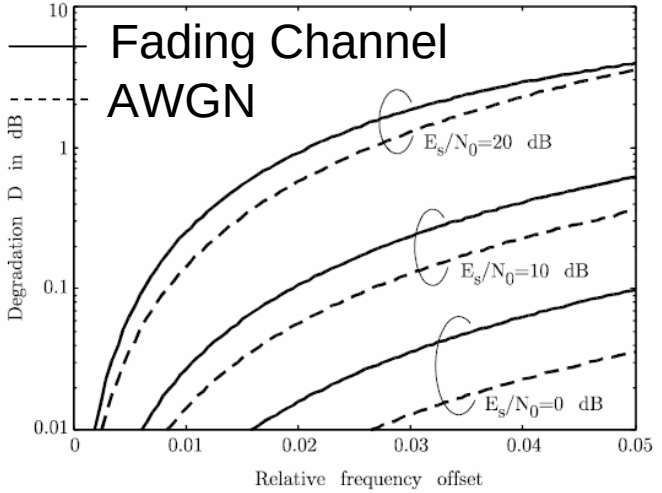
- Smart antennas are a commonly cited feature of TD-SCDMA
  - Shorter codes reported to be especially good for TD-SCDMA
- Standard might not even be feasible without smart antennas
- Brief study
  - 4 users
  - Average 2 chip timing error
  - Arrays
    - No array
    - Switched beam (9 beams)
    - LMS Smart Antenna
      - Unstable
    - Software radio technique that combines the two based on SINR

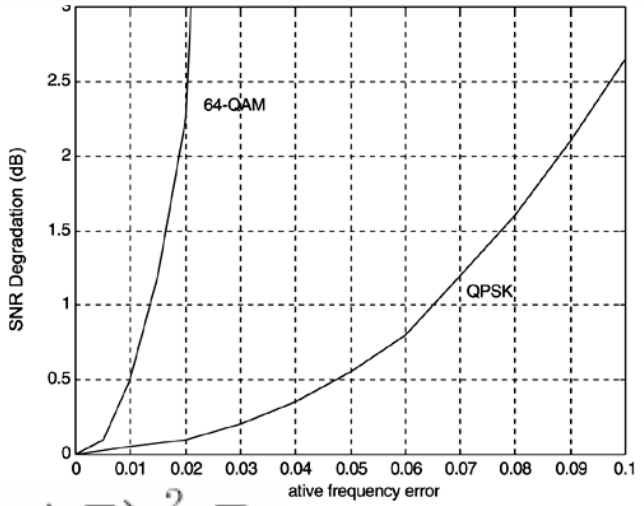


X. Ze-ming, "Software antenna using algorithm diversity in TD-SCDMA," Antennas and Propagation Society International Symposium 2006, pp. 2529 - 2532

Effects of Frequency Errors in OFDM

- Comments
  - Impact greater for higher SNR signals
  - Note 5% estimation error can lead to 5 dB effective degradation at 64-QAM like SNRs
  - Big frequency impact is why OFDM was originally for fixed deployments
- Techniques
  - Data aided
  - Non data aided
  - Cyclic prefix





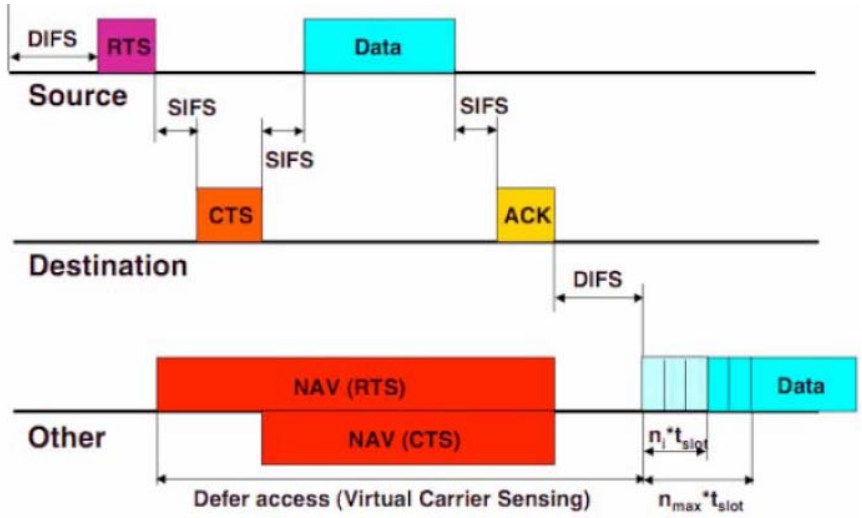
O. Edfors, M. Sandell, J. van de Beek D. Landström, F. Sjöberg, "An Introduction to Orthogonal Frequency Division Multiplexing," Sep 98, Available online: http://epubl.luth.se/avslutade/0347-0881/96-16/esb96rc.pdf

$$\Delta f = \frac{\Delta F}{W/N}$$

$$D\ (\mathrm{dB}) \approx \frac{10}{3\ln 10}(\pi \Delta f)^2 \frac{E_s}{N_0} = \frac{10}{3\ln 10}\left(\pi \frac{N \cdot \Delta F}{W}\right)^2 \frac{E_s}{N_0}$$

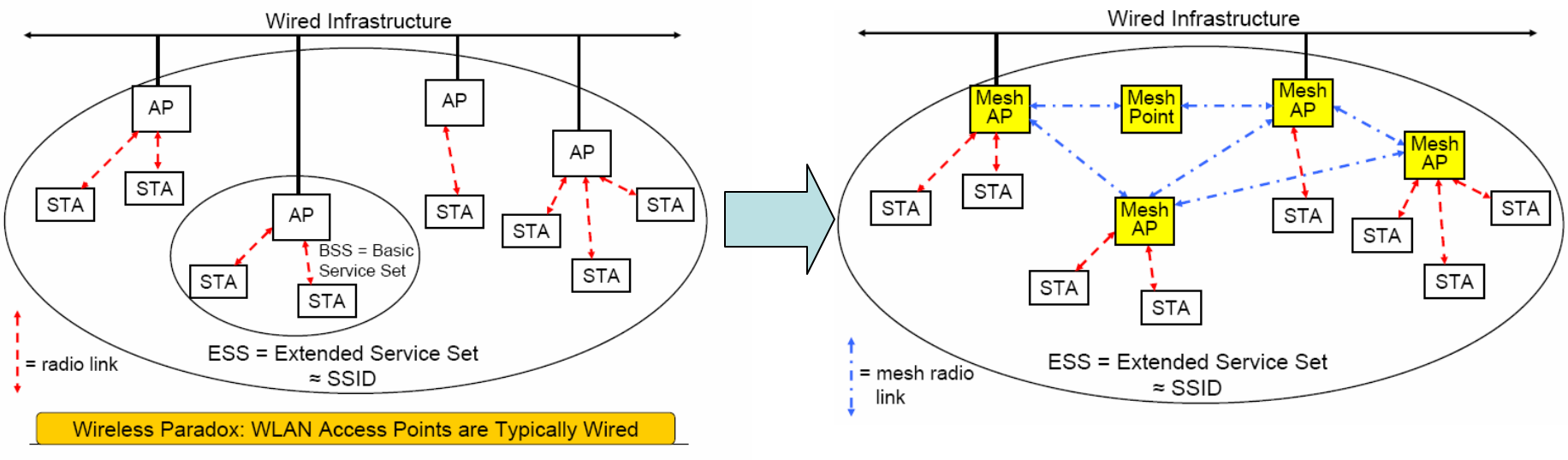
Distributed Coordination Function (DCF)

- Intended to combat “hidden nodes” in an uncoordinated network and generate fair access to channel
- Basic components:
  - –After waiting DIFS after last detected transmission, source sends Request to Send (RTS)
  - –Destination replies with Clear to Send (if OK)
  - –Data is then transferred and ACKed
  - –If an error occurs (e.g., collision), then station has to wait for DIFS + random backoff.
    - Random backoff grows with # of collisions



- Network allocation vector
  - – Acts as virtual carrier sense
  - – Duration given in RTS/CTS fields
- DIFS = DCF Interframe Space
- SIFS = Short Interframe Space

Conceptual Operation of 802.11s



http://ieee802.org/802_tutorials/nov06/802.11s_Tutorial_r5.pdf

- **WLAN Mesh** – An IEEE 802.11-based Wireless distribution service consisting of a set of two or more Mesh Points interconnected via IEEE 802.11 links and communicating via the WLAN Mesh Services.
- **Mesh Point** - A Mesh Services supporting device (bridge, access point)
- **Mesh AP** - Any Mesh Point that is also an Access Point.
- **Mesh Portal** - A boundary connection for the Mesh

802.16-2004 Security Vulnerabilities

- Replay Attack
  - Resend detected valid messages
  - Intention is to induce BS to send SS a reset message
- AP Spoof
  - Subscribers are authenticated, but not access point
- MAC Address Spoof
- RNG-RSP Denial of Service
  - Weaknesses in ranging (not encrypted, automatic acceptance of adaptations by SS)
- Auth Invalid Attack
  - "Auth Invalid" (possibly spoofed) puts subscriber in a vulnerable state
  - Followed with a "Permanent Auth Reject" message prevents all future communications until MAC reset

Nonetheless, Boom writes:

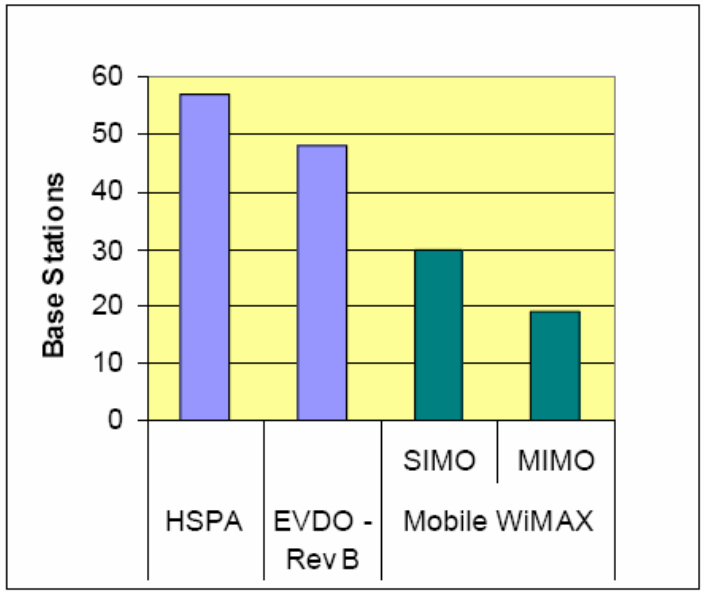
"*In the author's opinion, the standard is an excellent starting point for the basis of a military tactical network. Given that the above recommendations have been applied, there would remain changes required to create a military wireless network. Because of the unique military environment and requirement for very high availability, DoD should adopt an appropriately robust spread spectrum physical layer to improve conventional jamming resistance. Second, DoD should continue to use higher layer encryption to protect end-to-end transmissions*."

Based on D. Boom, "Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks," Thesis, Naval Post Graduate School, Sep 2004. Available online: http://www.ieee802.org/16/tge/contrib/C80216e-04_406.pdf

Cost Comparison: 3G vs WiMAX

- Fewer base stations to provide same capacity with Mobile WiMAX than HSPA or EVDO RevB
- Less cost tied up in IP royalties (~2-3% vs 10-15%)
- Lower spectrum costs
- http://www.wimaxforum.org/technology/faq/
  - The second generation of Subscriber Equipment is expected to be priced from $200 - $300 in 2008.
  - The third-generation CPEs will be integrated into laptops and other portable devices and are expected to initially cost approximately $100 and be available in 2nd half 2008.
- Note: the equation flips when coverage is more important than capacity

Mobile WiMAX: The Best Personal Broadband Experience! June 2006, Available at www.wimaxforum.org



- WiMAX Frequency = 2500 MHz
- HSPA, EVDO Frequency = 2000 MHz
- Occupied Spectrum = 10 MHz
- Frequency Reuse = (c,1,3)
- Coverage Area = 129 sq-km
- DL/UL Traffic Ratio = 2:1
- DL Data Density = 215 kbytes/sec/sq-km
- Monthly Capacity ~23 Gigabytes/sq-km