



# 3G Wireless Security - A Government Perspective

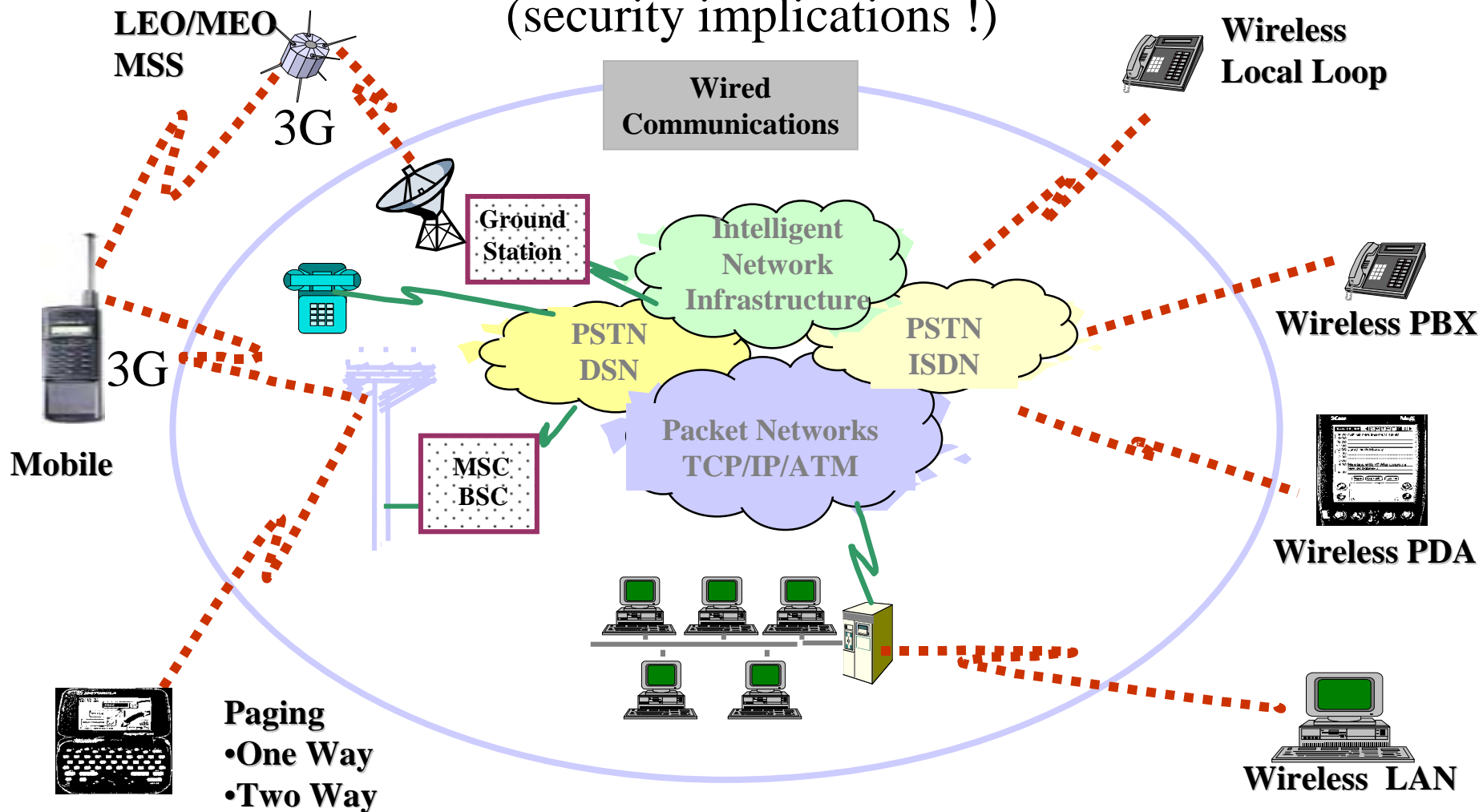
*Doug Rahikka*

National Security Agency

NSA-TRI23

djrahik@alpha.ncsc.mil

# Wireless = Extended Exposure of Wired (security implications !)



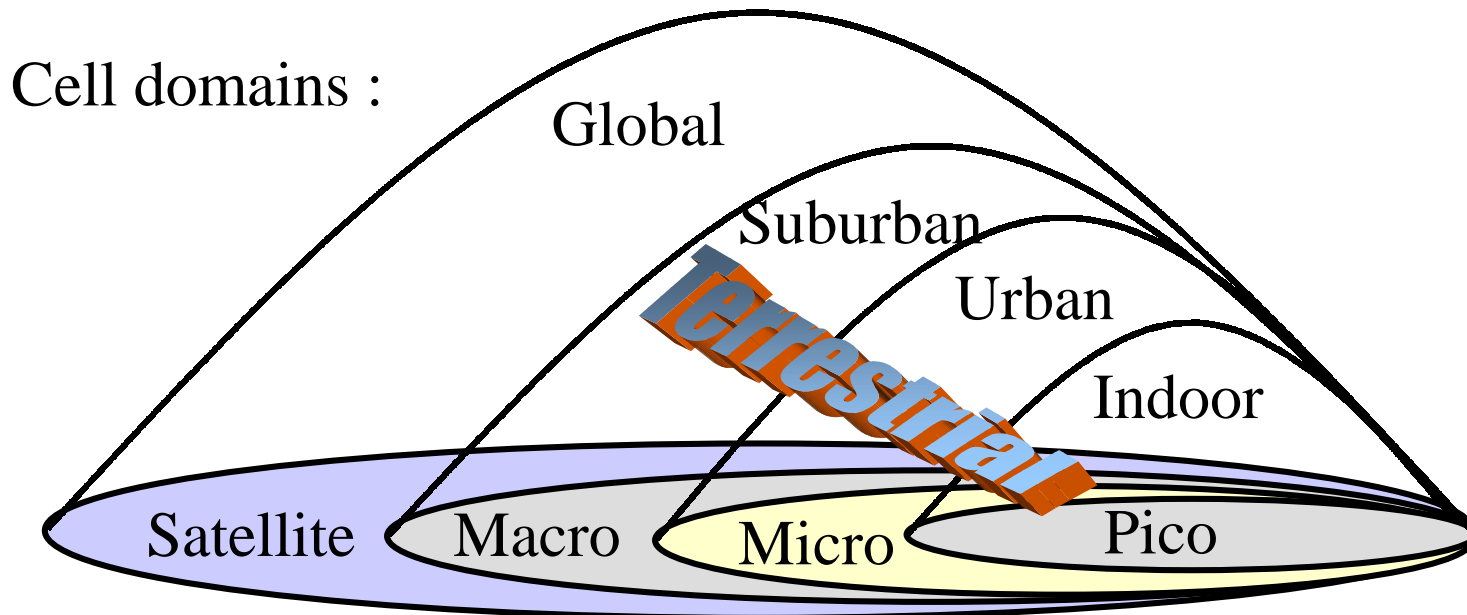
# Security Requirements

- *U.S. Government*
  - Good COTS AI security (for SBU Sensitive But Unclassified users)
  - End-to-End GOTS security
  - DUITs
    - Digital, Ubiquitous, Interoperable, Transparent, Secure
  - Confidentiality, Integrity, Availability, Authentication, Accountability (Nonrepudiation)
  - Multinetwork transport (FNBDT)
  - Voice then Data (STU3 paradigm)
  - Transparent low latency data
- *IMT-2000 ITU* (notes)
  - Bilateral authentication (e.g., User < > Base)
  - Joint ETSI/TIA authentication algorithm for global roaming (harmonizing IS41 w/ GSM)
  - Packet-by-Packet payload authentication (vs circuit-switched one time at call setup)
  - Network messaging security (e.g., keys and auth data)

# NIST Impacts

- Consensus building in TIA TR45 to adopt NIST *SHA-1 Secure Hash Algorithm* as preferred cryptographic primitive for 3G
  - Long history of proven robustness
- TIA TR45 AHAG considering using eventual NIST *AES Advanced Encryption Standard* algorithm for future 3G subscriber privacy applications
  - AES specifications included speed + power amenable to handheld wireless constraints !
  - NSA TRI22 did a paper on algorithm comparisons see <http://csrc.nist.gov/encryption/aes/round2/r2anlsys.htm#NSA>

# 3G IMT2000



Bit Rates :	144 kbps	High Speed Vehicular
	384 kbps	Pedestrian + Low Speed Vehicular
	2 Mbps	Pico/Indoor

(contrast with 2G rates ~10kbps to user, primarily voice)

# 3G Terrestrial Players

- CDMA-DS Direct Spread (3GPP)  
UTRA FDD or WCDMA
- CDMA-MC MultiCarrier (3GPP2)  
cdma2000
- CDMA TDD (3GPP+CWTS)  
UTRA TDD or TD-SCDMA
- TDMA Single Carrier (UWCC)  
UWC-136
- FDMA/TDMA (ETSI)  
DECT



(the tech-agnostic folk,  
per Fortune mag)

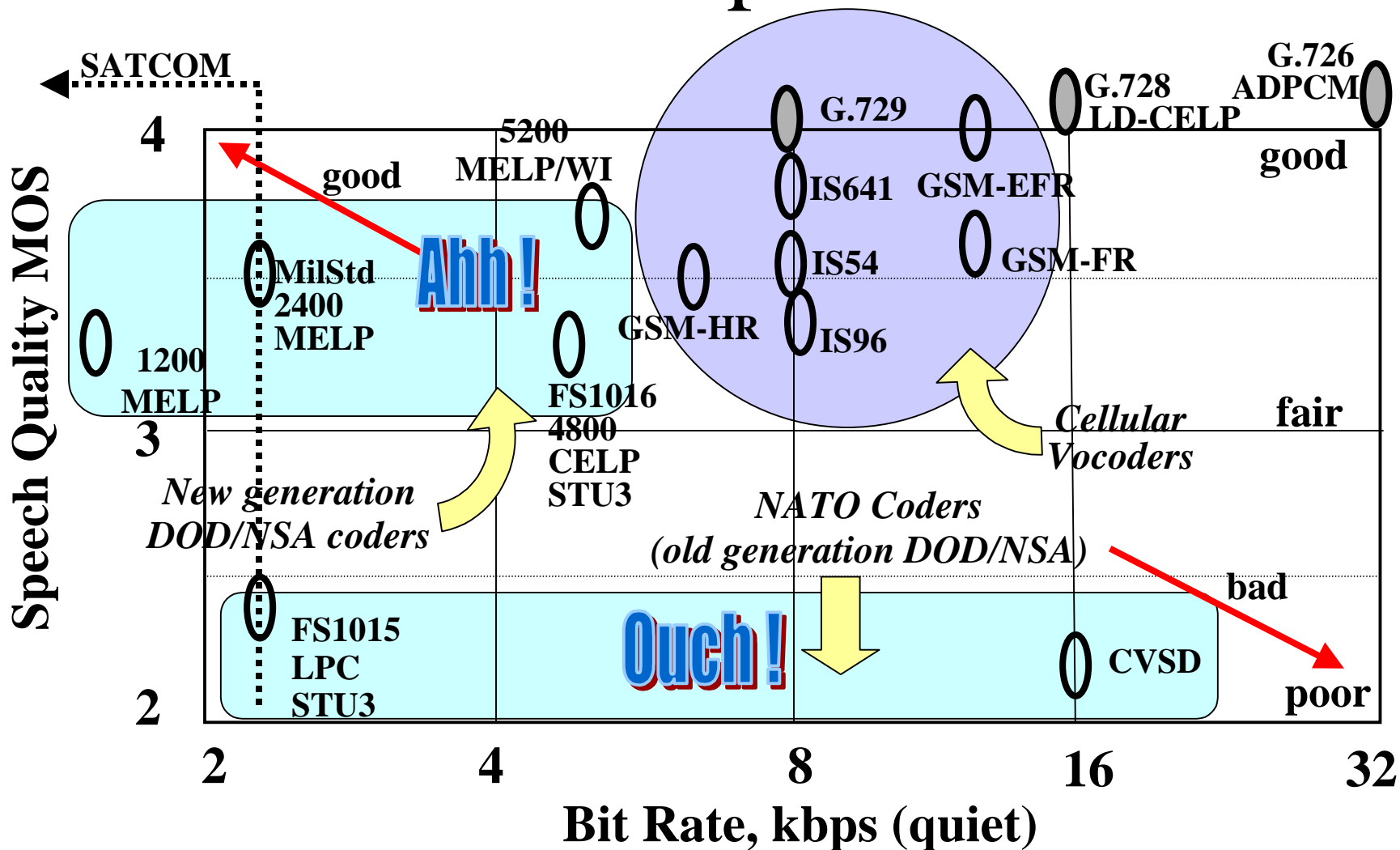
(spectrum efficiency  
advantages, per  
reaction to UK 3G  
spectrum auctions  
at VTC'00 Tokyo)

2G heritage : TDMA (IS136 + GSM)  
CDMA (IS95)

## What are all those bits for ?

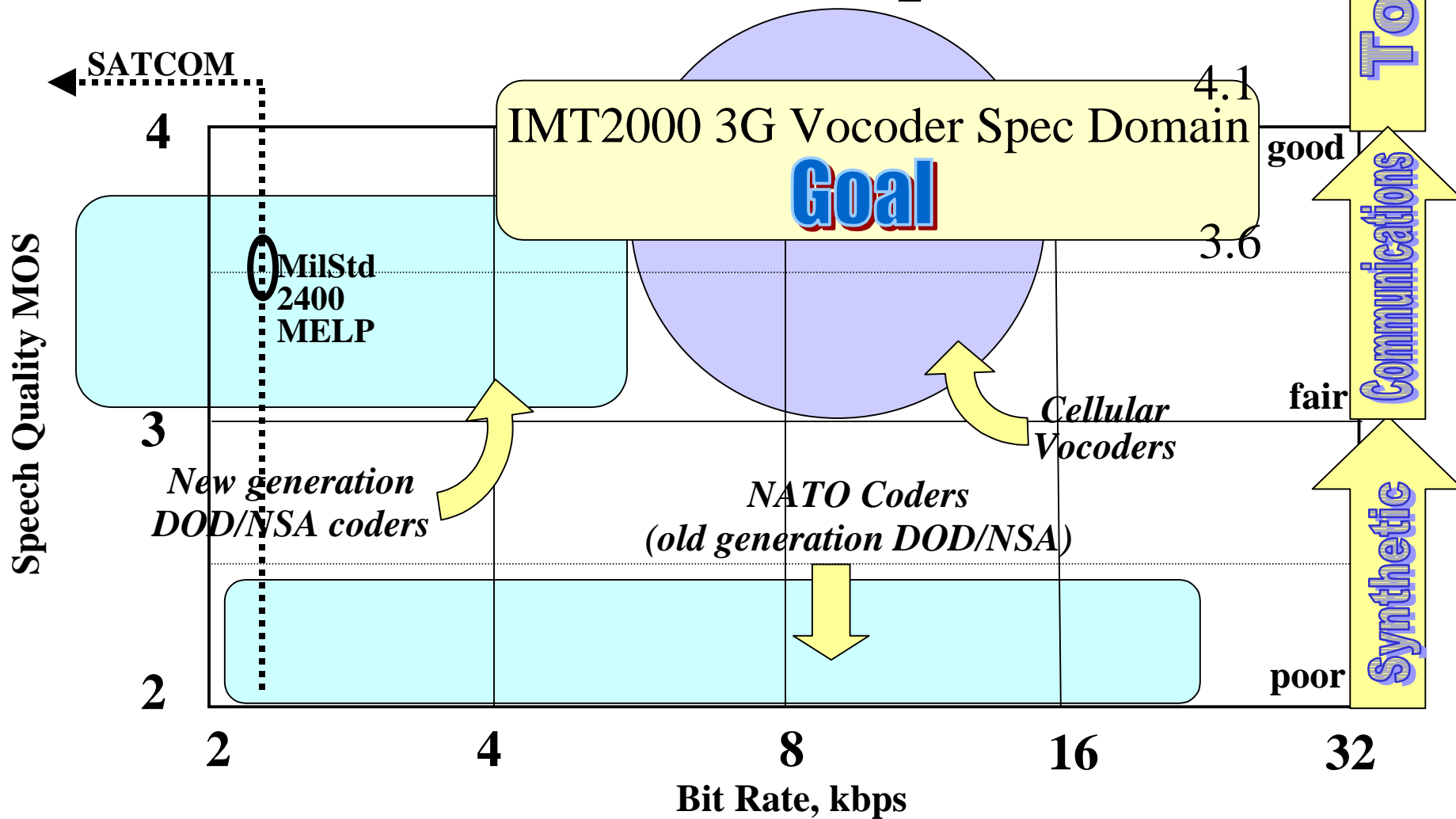
- 3G vocoders not much different than 2G in terms of bit rate !
- Higher bit rates for data, multimedia (voice + video), etc
- U.S. gov't secure interoperability based on foundation of :
  - MELP 2.4kbps vocoder (Mixed Excitation Linear Prediction) MilStd3005
    - NATO STANAG candidate (amongst FR, TU, US)
  - FNBDT signaling plan + crypto

# Vocoder Comparison Chart





# 3G Vocoder Specs



# MELP in 3G for Strat+Tact+Sat

- See <http://www.rta.nato.int/pubs/RTO-MP-026.htm> for MELP in tactical applications (NATO)
  - Papers by Collura (on Noise PreProcessing) and Rahikka (on Error Correction)
- When DoD adopts 3G for the battlefield, we want robust performance in acoustic noise (at microphone A/D) and jamming noise (at antenna A/D) !

# “Transitions”

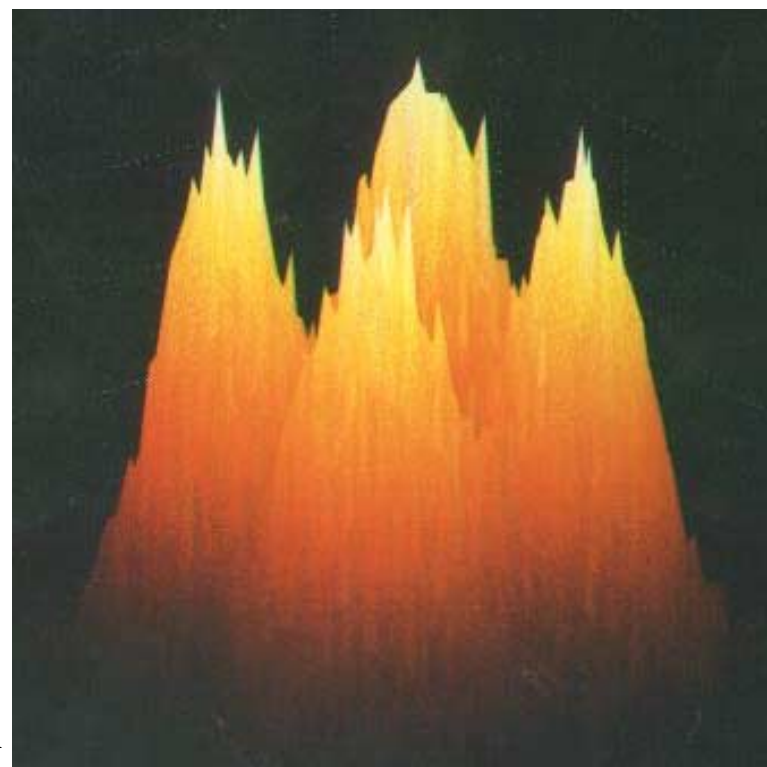
(or how to embrace change)

- Past and present is based on wireline STU3 (with LPC and CELP vocoders)
  - 500k users (including Tom Clancy characters)
  - Wireless 1G analog cellular version
  - Red gateways (Iridium etc)
- 2G/3G Future is based on FNBDT + MELP
  - ???k users (including STU6 in Tom Clancy’s “The Bear and the Dragon”)
  - Wireline STE Secure Terminal Equipment (on desktops)
- Attempt to bridge the eras with IWFs

# STU3 Interoperability ?

- STU3 2.4kbps modem through 2G ACELP/VSELP/QCELP vocoders at 7-10% BER
- STU3 won't work over 2G cellular
- Need for STU3 modem IWF in cell switches
- Failed business case !
- Use FNBDT signaling protocol !
- STU3 4.8kbps modem will operate over analog cellular 1G
- See MILCOM'97 and VTC'97
- Sadly, ~1/6 of 2G data bearer stds in TIA are STU3 IWF-related ! (case of standard adopted+never built)

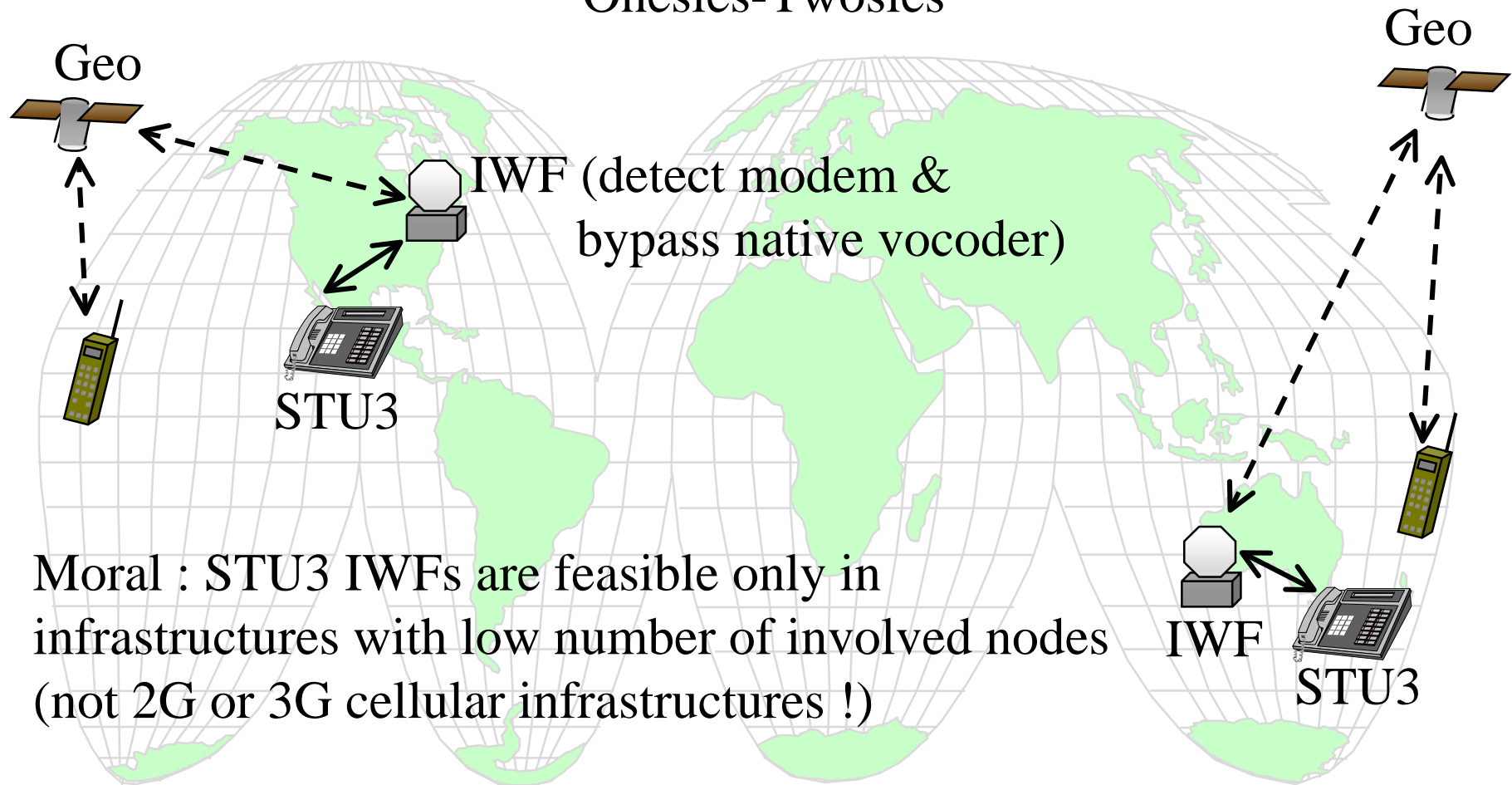
(~1M grains of sand in my Matlab sandbox)



(STU3 QAM Modem Demod)

# INMARSAT IWFs for STU3

“Onesies-Twosies”




Moral : STU3 IWFs are feasible only in infrastructures with low number of involved nodes (not 2G or 3G cellular infrastructures !)

# ‘Krechmer’s Etiquette’

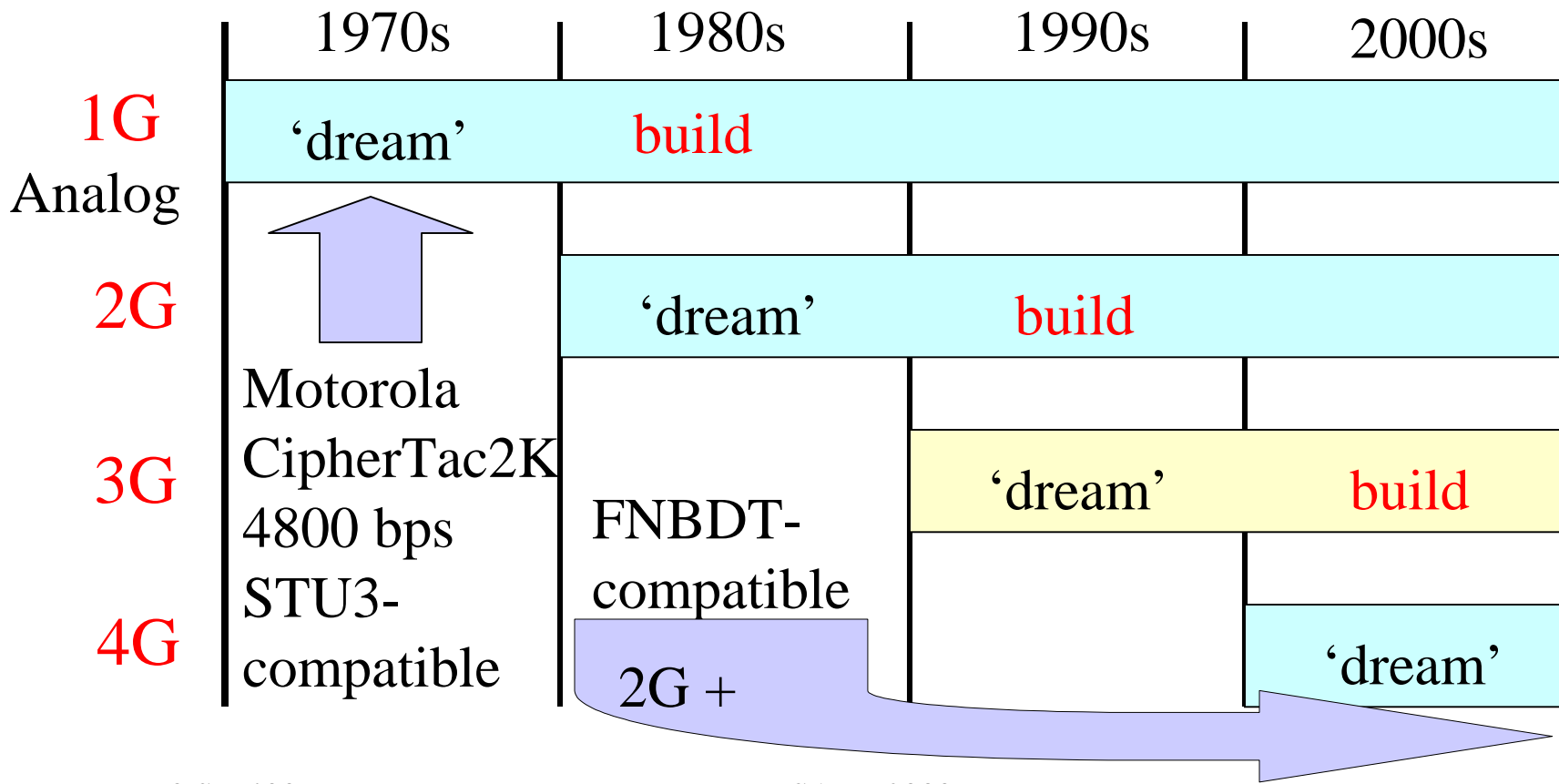
- See Ken Krechmer’s ISART’00 talk 9/8/00
  - Some modems have etiquette
  - Some modems have no etiquette

*and*

- Some modems are blatantly rude
  - e.g., STU3 modem (half-breed) 
    - at 2400 bps = V.26bis w/V.26ter Echo Canceling
    - at 4800 bps = V.32 w/Bell103 300bps capability msg  
(ID modem from go-secure tones up front)

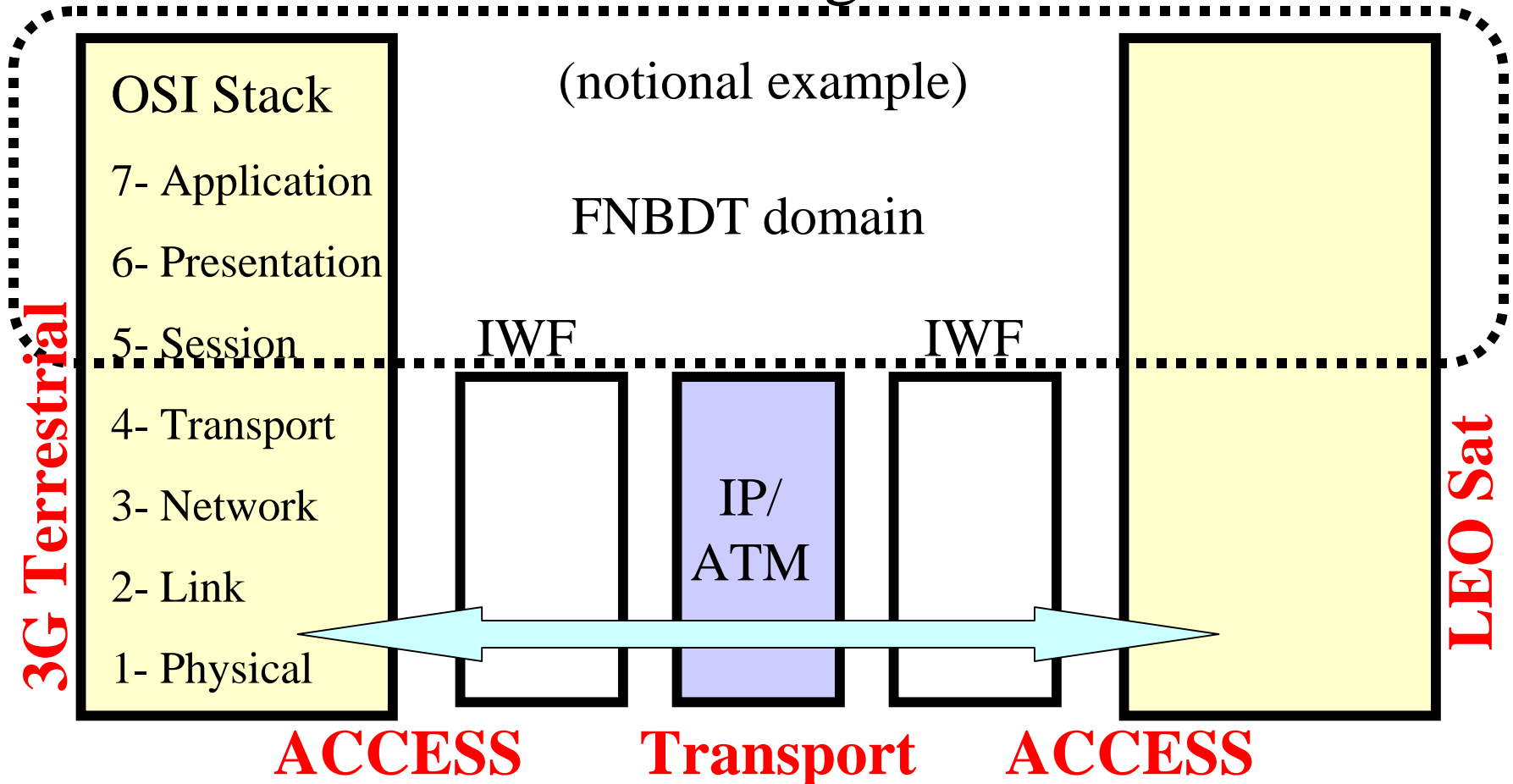
# Standards - 3G IMT2000

- Evolution



# FNBDT

- “Future Narrow Band Digital Terminal”

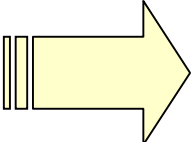


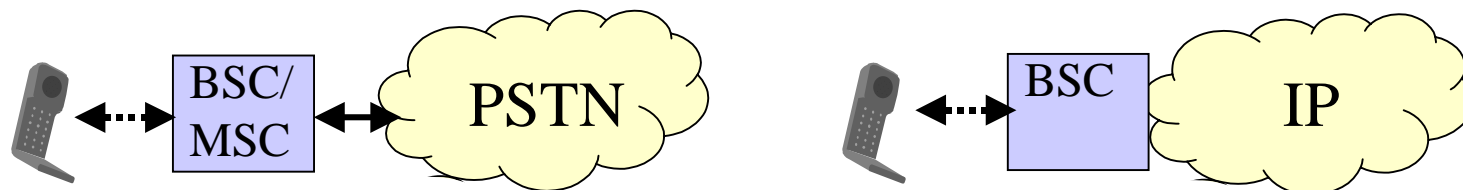


# What is FNBDT ?

- Above Transport layer
- Operates over most data/voice network configurations
- Least Common Denominator for end-to-end Interoperability
- Many media (wireless, satellite, IP, ATM, ISDN)
- Adapts to data rate
- Sync and Nonsync
- Negotiates security and application features
- Point-to-Point and Multipoint
- Realtime, Near Realtime, and NonRealtime Apps

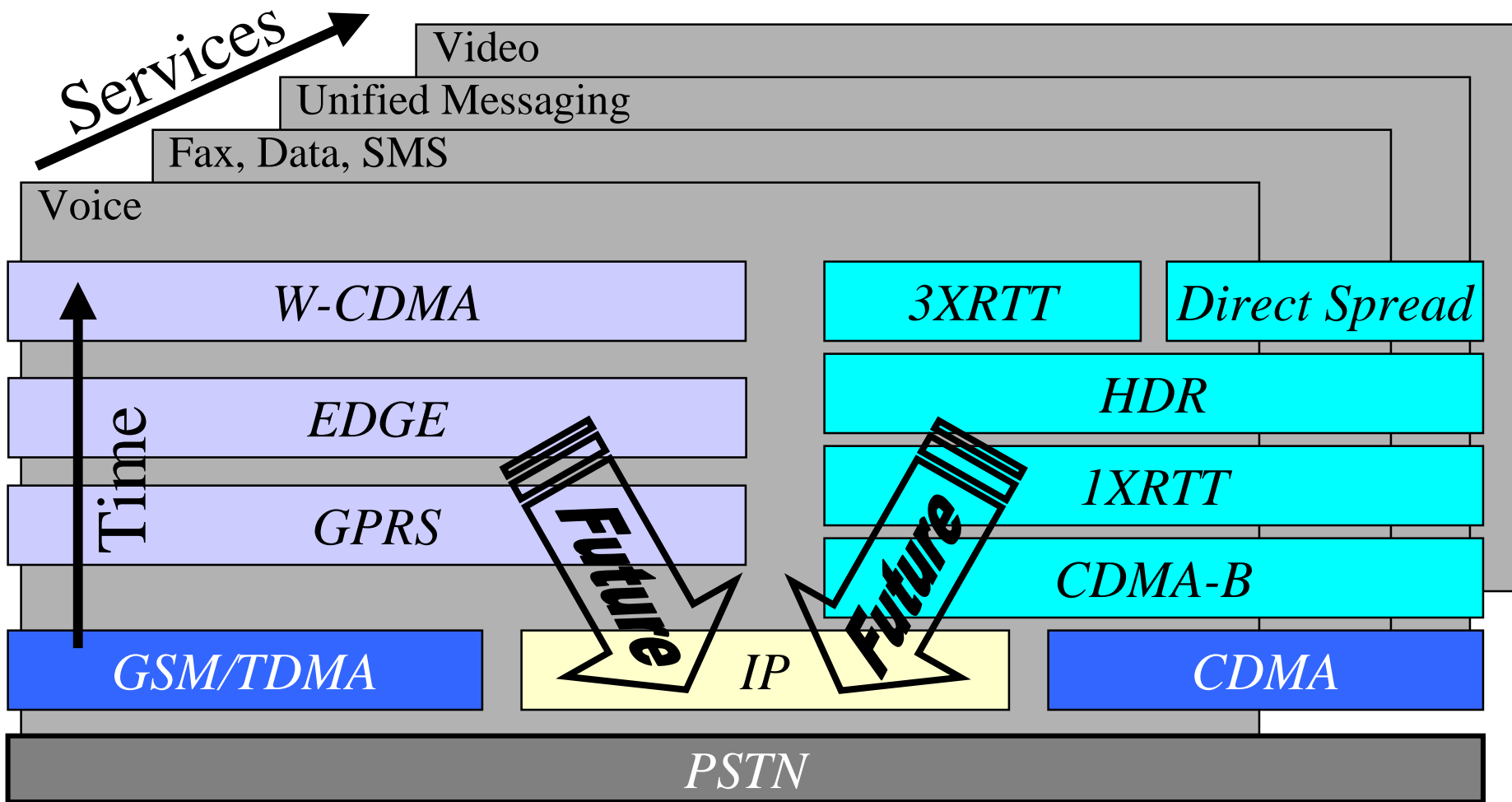
# Major Evolution

- 3G has radical architectural changes from 2G !
- Paradigm shift :  
Circuit-switched  Packet-switched
- Change from connection through BSC/MSC to direct links into the www IP cloud



(e.g., 2.5G GPRS Generalized Packet Radio Service)

# 3G Evolution to IP Core

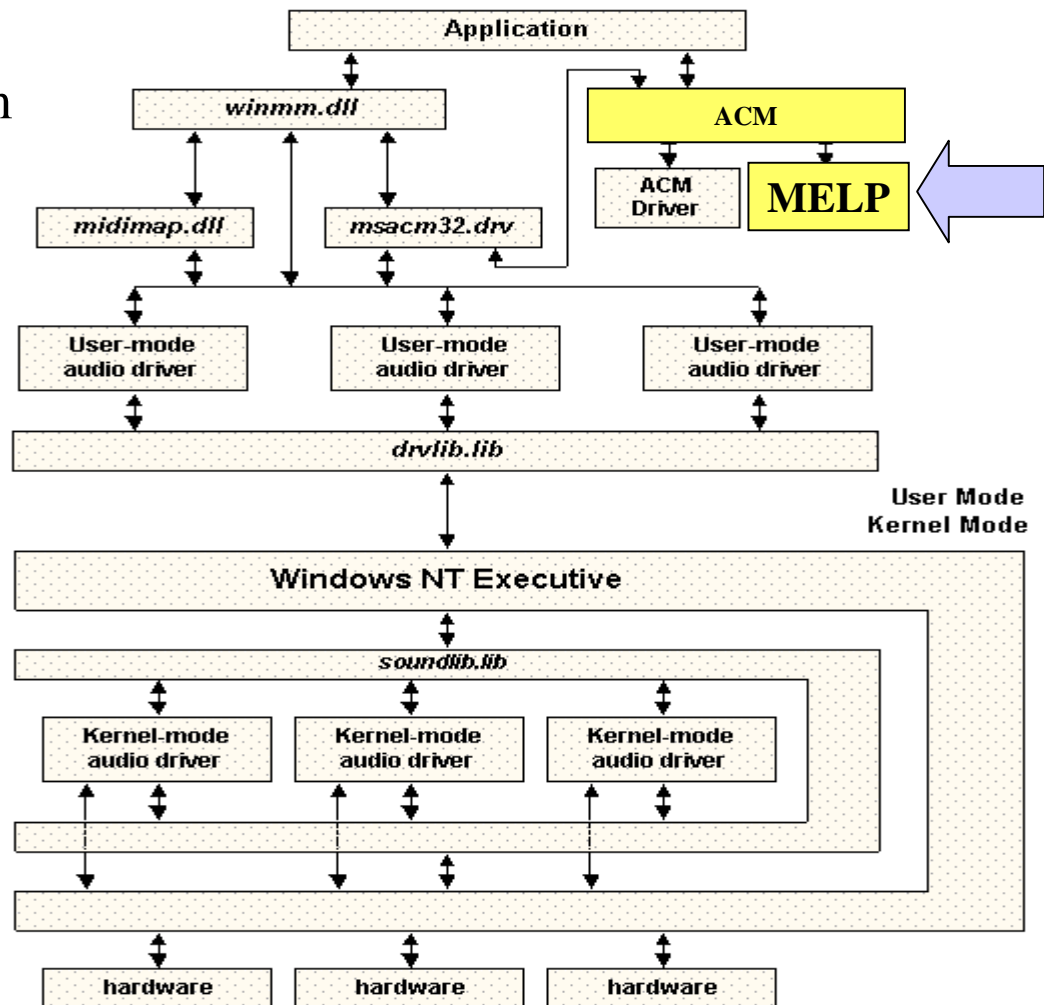


## Secure MELP VoIP on 3G

- NSA developing MELP VoIP solution with OSU Oklahoma State University (w/FNBDT)
- Looking to do trials of MELP VoIP on 2.5G GPRS as it is rolled out in U.S.
  - QOS issues
- Secure Multimedia potentialities :
  - MELP+video+crypto enabled laptop +GPRS handset transmitting to desktop PC in office
- Looking at installing MELP in NetMeeting
- H.323 ITU std on conferencing

# MELP Under Windows NT

- Layout of the audio subsystem of the Windows NT 4.0 OS
- Relationships between the various OS components, the ACM Audio Compression Manager, and the MELP CODEC
- The MELP CODEC is a user-mode ACM driver
- When installed under the ACM, a CODEC can be accessed by any application through a standard interface



# Spectrum Issues

- The *Catch-22* Rules - (spectrum is like sex)
  - “*you can’t have what you don’t use*”
  - “*you can’t use what you don’t have*”
  - “*you can’t have what you can’t afford*” (new one)
  - “*you can’t have enough*”
- [http://www.federaltimes.com/issues/loss\\_radio.html](http://www.federaltimes.com/issues/loss_radio.html)  
“Loss of Radio Spectrum Would Impair Security”  
(page 1 of 8/28/00 Federal Times)  
NTIA +DoD + etc looking at vacating 1755-1850 MHz
- How get spectrum for Fed users / tactical exercises ?

**Auctions**

## Spectrum Issues (continued)

- FWUF and CTIA addressed at June 2000 meeting in New Orleans (Federal Wireless User Forum)
- See Condello talk at  
<http://is2.antd.nist.gov/fwuf/june00slides/slindex.html>
- **4 Potential Solutions** (for Feds on licensed spectrum) :
  - Temporary Accounts
  - Extension of Service Area (Compatible Infrastructure - Fed Bases)
  - Federal Overlay, Underlay, or Extended Network (Fed Switch/Bases)
  - Federal Network in Unserved License Area
- Problematic with 2 ‘masters’, legal constraints, who is the ‘controlling authority’ ?, temporary situations/needs

## Conclusions

- 3G = exciting ! Security-enabling hooks req'd !
- Interoperability+Spectrum rolling 'Crisis'  
(Chinese compound word of 2 pictograms for  
*"danger"* and *"opportunity"*)
- Great new multimedia possibilities
  - Use will explode (with IP-centric higher data rates)
- Need for Gov't+Industry Partnership
- The standards are important
  - But please hold off on 4G until we have 3G issues resolved ! (Remember, the Gov't moves slowly - or at least not at 'Net Speed' !)



*Doug Rahikka*

National Security Agency

# Q & A

NSA-TRI23

[djrahik@alpha.ncsc.mil](mailto:djrahik@alpha.ncsc.mil)

