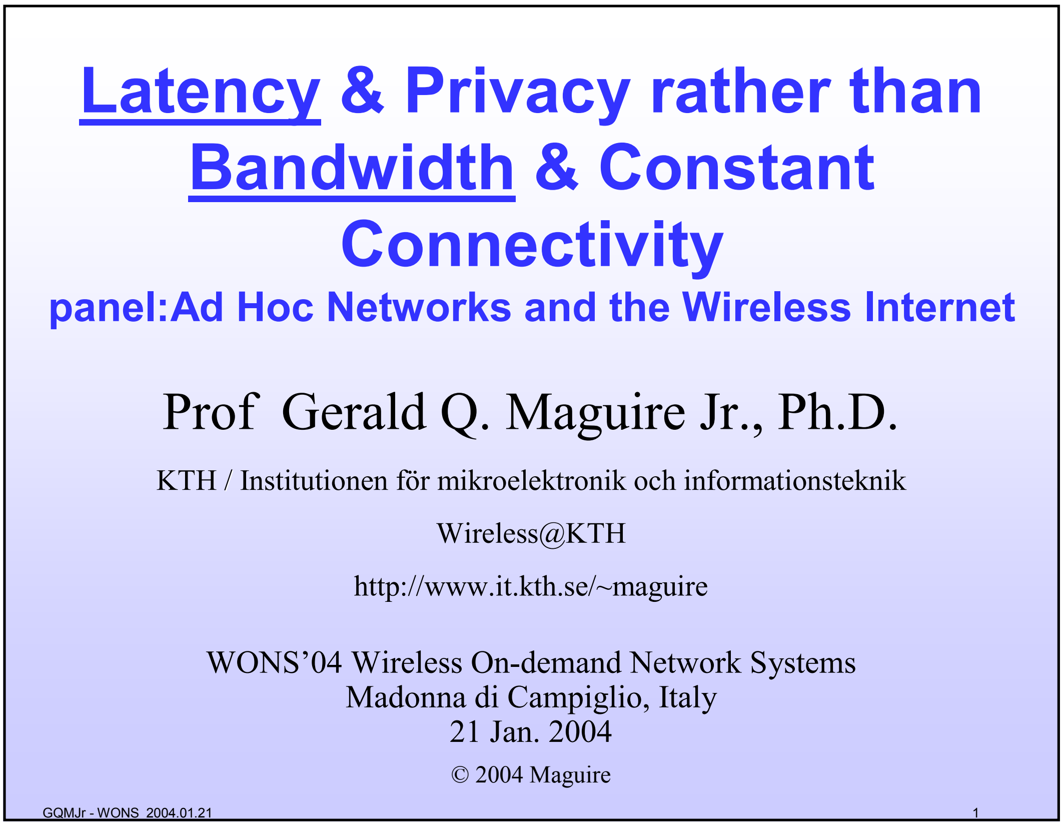


Latency & Privacy rather than Bandwidth & Constant Connectivity

panel:Ad Hoc Networks and the Wireless Internet

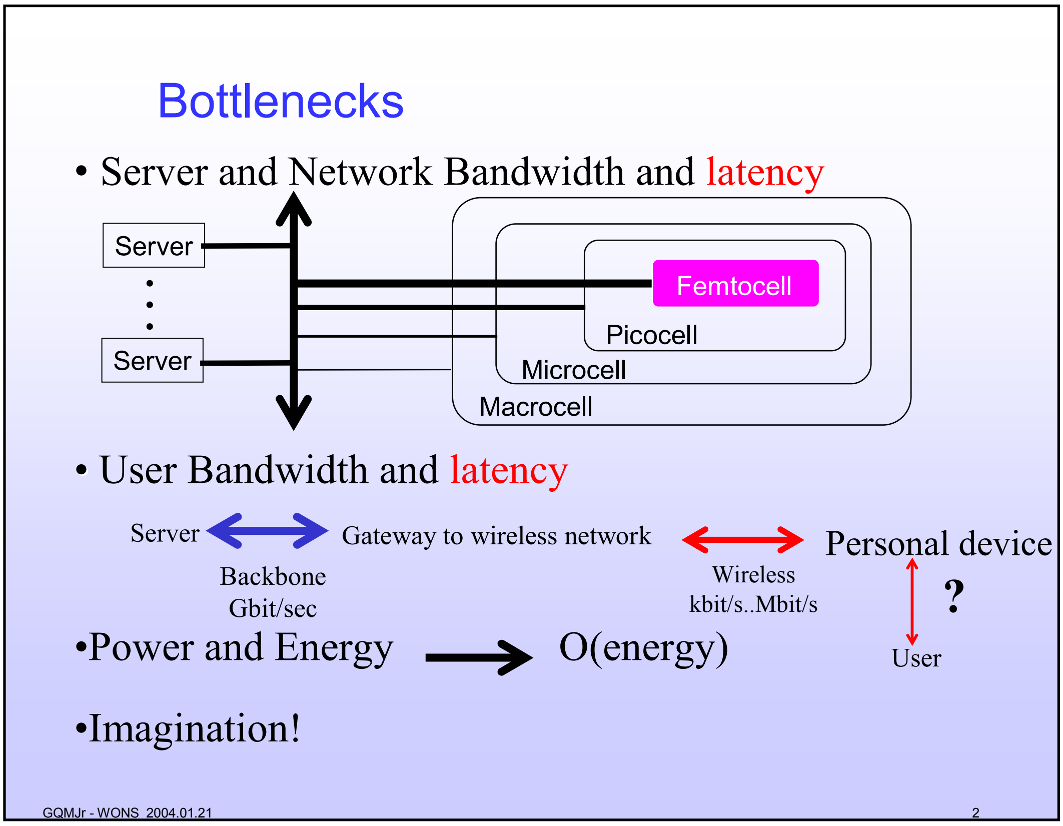
Prof Gerald Q. Maguire Jr., Ph.D.

KTH / Institutionen för mikroelektronik och informationsteknik

Wireless@KTH

http://www.it.kth.se/~maguire

WONS'04 Wireless On-demand Network Systems
Madonna di Campiglio, Italy
21 Jan. 2004



Bottlenecks

- Server and Network Bandwidth and latency

Server

Server

Femtocell

Picocell

Microcell

Macrocell

- User Bandwidth and latency

Server ↔ Gateway to wireless network ↔ Personal device

Backbone
Gbit/sec

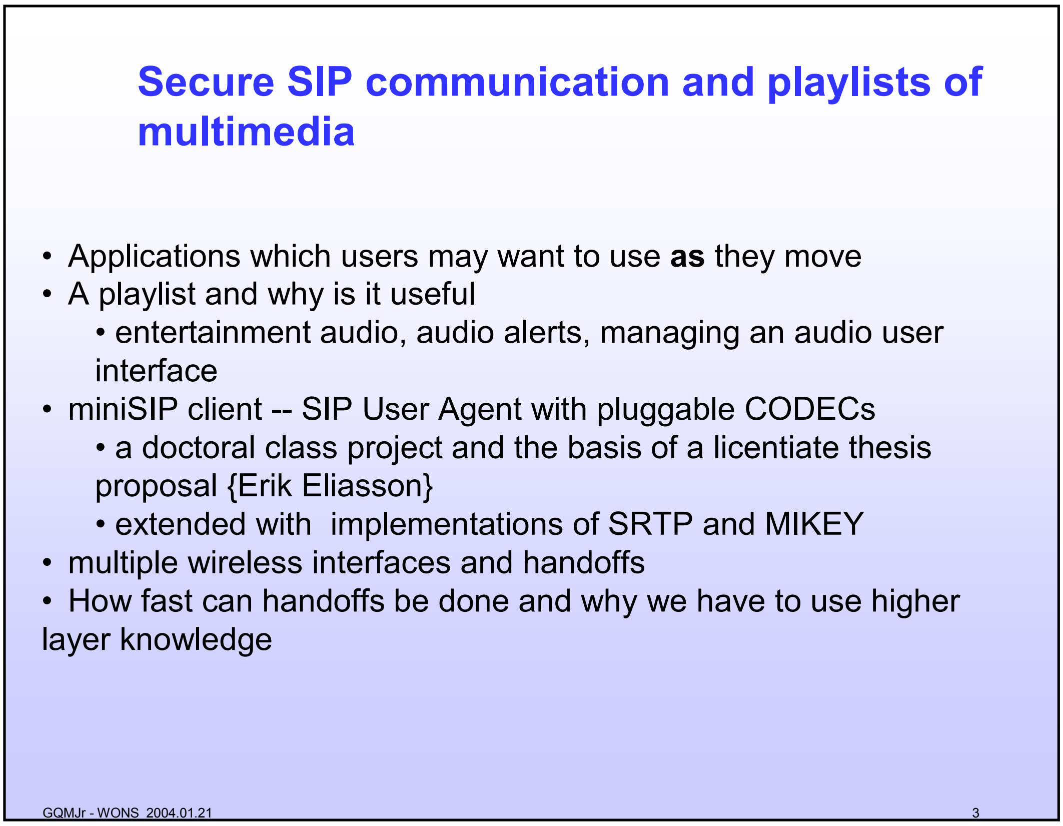
Wireless
kbit/s..Mbit/s

?

User

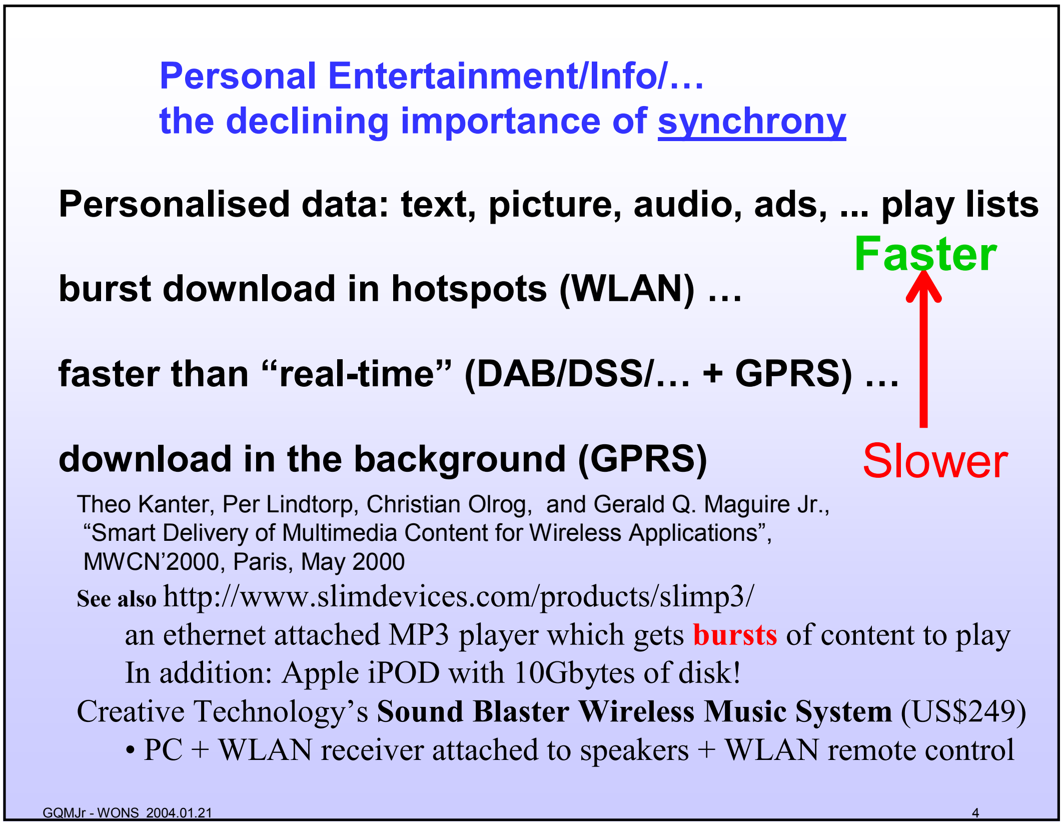
•Power and Energy → O(energy)

•Imagination!



Secure SIP communication and playlists of multimedia

- Applications which users may want to use **as** they move
- A playlist and why is it useful
  - entertainment audio, audio alerts, managing an audio user interface
- miniSIP client -- SIP User Agent with pluggable CODECs
  - a doctoral class project and the basis of a licentiate thesis proposal {Erik Eliasson}
  - extended with implementations of SRTP and MIKEY
- multiple wireless interfaces and handoffs
- How fast can handoffs be done and why we have to use higher layer knowledge



Personal Entertainment/Info/…
the declining importance of synchrony

Personalised data: text, picture, audio, ads, ... play lists

Faster

burst download in hotspots (WLAN) …

faster than “real-time” (DAB/DSS/… + GPRS) …

download in the background (GPRS)

Slower

Theo Kanter, Per Lindtorp, Christian Olrog, and Gerald Q. Maguire Jr., “Smart Delivery of Multimedia Content for Wireless Applications”, MWCN’2000, Paris, May 2000

See also http://www.slimdevices.com/products/slimp3/

an ethernet attached MP3 player which gets **bursts** of content to play

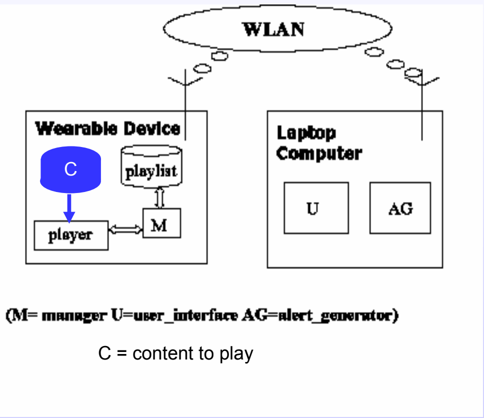
In addition: Apple iPOD with 10Gbytes of disk!

Creative Technology’s **Sound Blaster Wireless Music System** (US$249)

- PC + WLAN receiver attached to speakers + WLAN remote control

Playlists - the basis of commercial radio “programming”

- María José Parajón Domínguez, **Audio for Nomadic Users,** Master of Science Thesis, Royal Institute of Technology(KTH), December 2003**.**



```
struct song {
  char songfile[ ];     /* name of the file to play */
  char songname[ ];
  char artist[ ];
  char album[ ];
  int priority;          /* priority for playing a file */
  int recordingtype;  /* type of formatted audio
file */
  int songnumber;     /*order in the playlist*/
  float song_length;  /*length in seconds*/
  unsigned long songsize;    /*size in bytes */
  long samplerate;
  int audiotype;       /*type of  file: 1 song, 2 audio
alerts*/
  double time_to_play;
  struct song *next_song; struct song
*previous_song;
} list_entry;
```

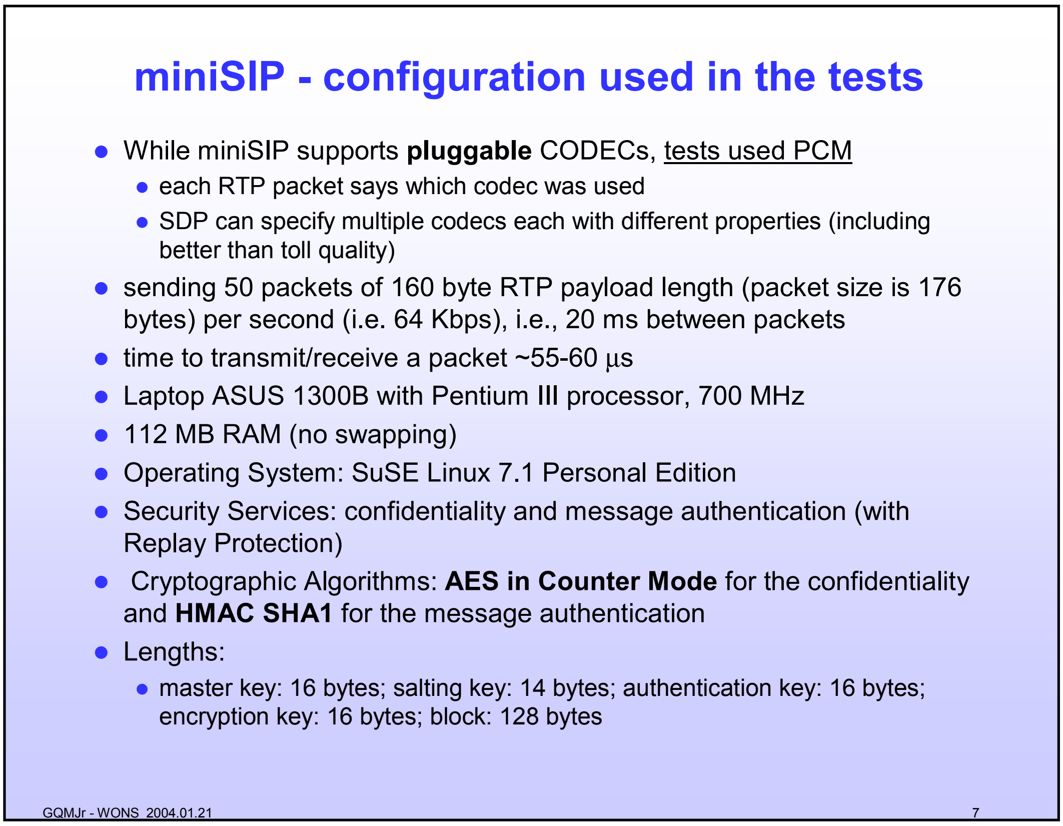
Operations: add/delete a song to/from the playlist, add a playlist, shuffle, …
Playlist Manager’s function is **scheduling**
Key features - content is **not** streamed, ∴ we can exploit local **caching** of content, prefetching, …

Personalized & Context Aware Audio

Photos courtesy of Choon Hai Wong

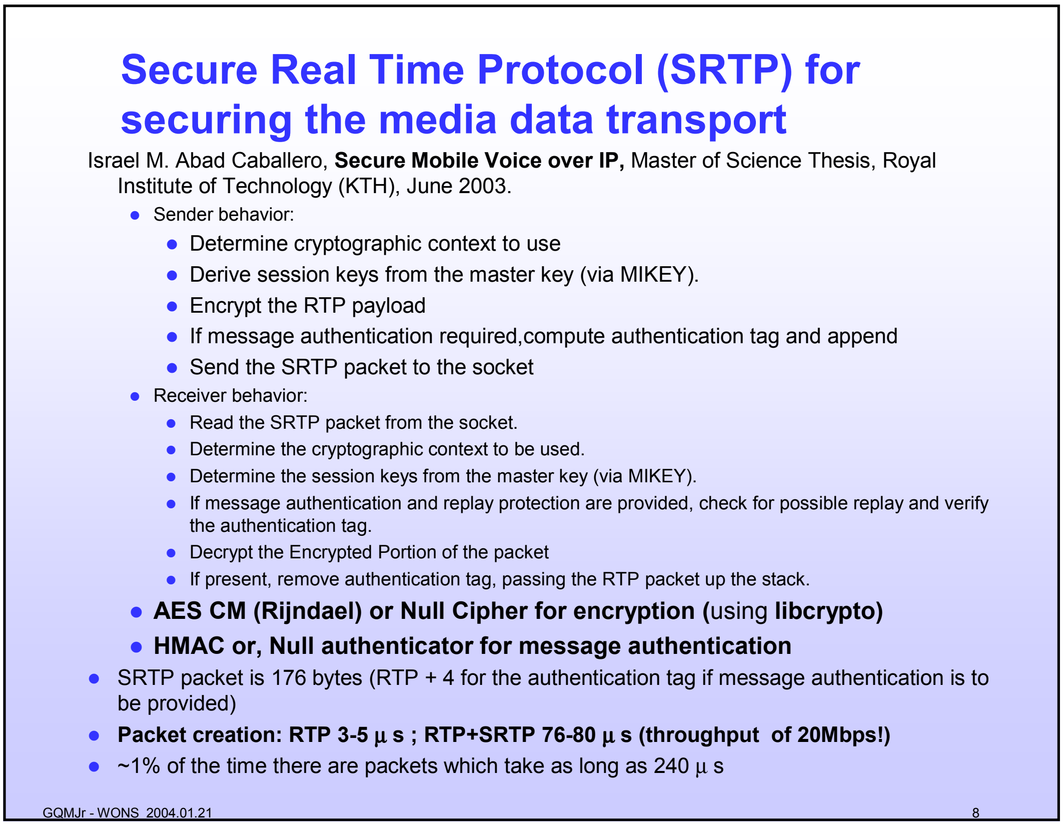
Mobile device equipped with
- WLAN +GPRS +IRDA
- Stereo audio in/out

- Audio play list + Play list manager
- text to speech (CMU’s flite)
- Mobile Presence + other context information
  - IR beacon(s)
  - IM systems: ICQ, Jabber, …
  - buddy status is much more annoying as audio than a window
- Separating/combining multiple activities
  - perhaps via *spatial audio*
  - good **scheduling**



miniSIP - configuration used in the tests

- While miniSIP supports **pluggable** CODECs, tests used PCM
  - each RTP packet says which codec was used
  - SDP can specify multiple codecs each with different properties (including better than toll quality)
- sending 50 packets of 160 byte RTP payload length (packet size is 176 bytes) per second (i.e. 64 Kbps), i.e., 20 ms between packets
- time to transmit/receive a packet ~55-60 µs
- Laptop ASUS 1300B with Pentium III processor, 700 MHz
- 112 MB RAM (no swapping)
- Operating System: SuSE Linux 7.1 Personal Edition
- Security Services: confidentiality and message authentication (with Replay Protection)
- Cryptographic Algorithms: **AES in Counter Mode** for the confidentiality and **HMAC SHA1** for the message authentication
- Lengths:
  - master key: 16 bytes; salting key: 14 bytes; authentication key: 16 bytes; encryption key: 16 bytes; block: 128 bytes

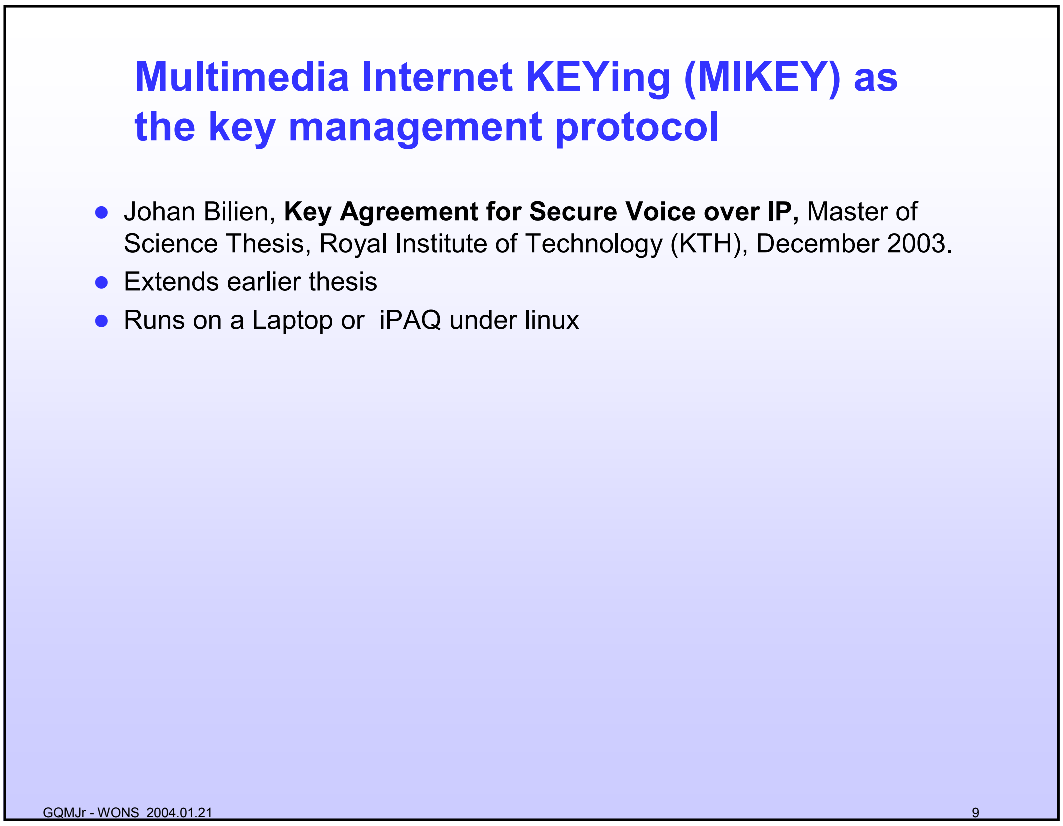


Secure Real Time Protocol (SRTP) for securing the media data transport

Israel M. Abad Caballero, **Secure Mobile Voice over IP,** Master of Science Thesis, Royal Institute of Technology (KTH), June 2003.

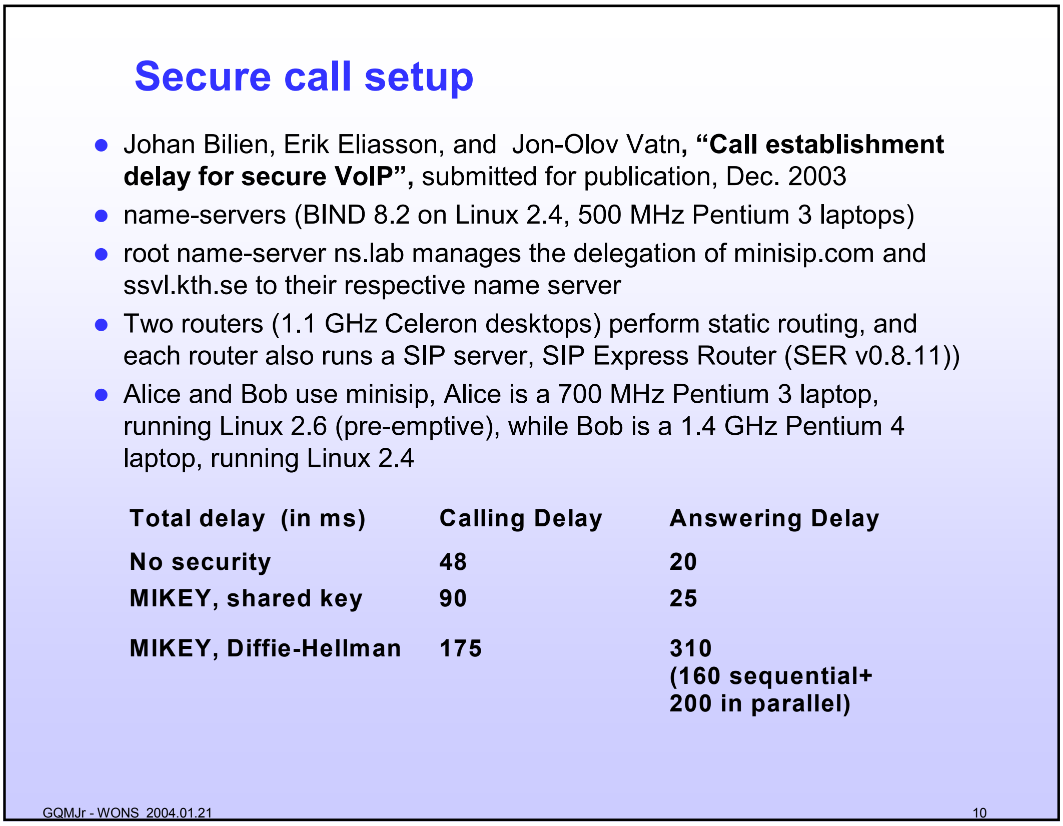
- Sender behavior:
  - Determine cryptographic context to use
  - Derive session keys from the master key (via MIKEY).
  - Encrypt the RTP payload
  - If message authentication required,compute authentication tag and append
  - Send the SRTP packet to the socket
- Receiver behavior:
  - Read the SRTP packet from the socket.
  - Determine the cryptographic context to be used.
  - Determine the session keys from the master key (via MIKEY).
  - If message authentication and replay protection are provided, check for possible replay and verify the authentication tag.
  - Decrypt the Encrypted Portion of the packet
  - If present, remove authentication tag, passing the RTP packet up the stack.
- **AES CM (Rijndael) or Null Cipher for encryption** (using **libcrypto)**
- **HMAC or, Null authenticator for message authentication**

- SRTP packet is 176 bytes (RTP + 4 for the authentication tag if message authentication is to be provided)
- **Packet creation: RTP 3-5 µ s ; RTP+SRTP 76-80 µ s (throughput of 20Mbps!)**
- ~1% of the time there are packets which take as long as 240 µ s



Multimedia Internet KEYing (MIKEY) as the key management protocol

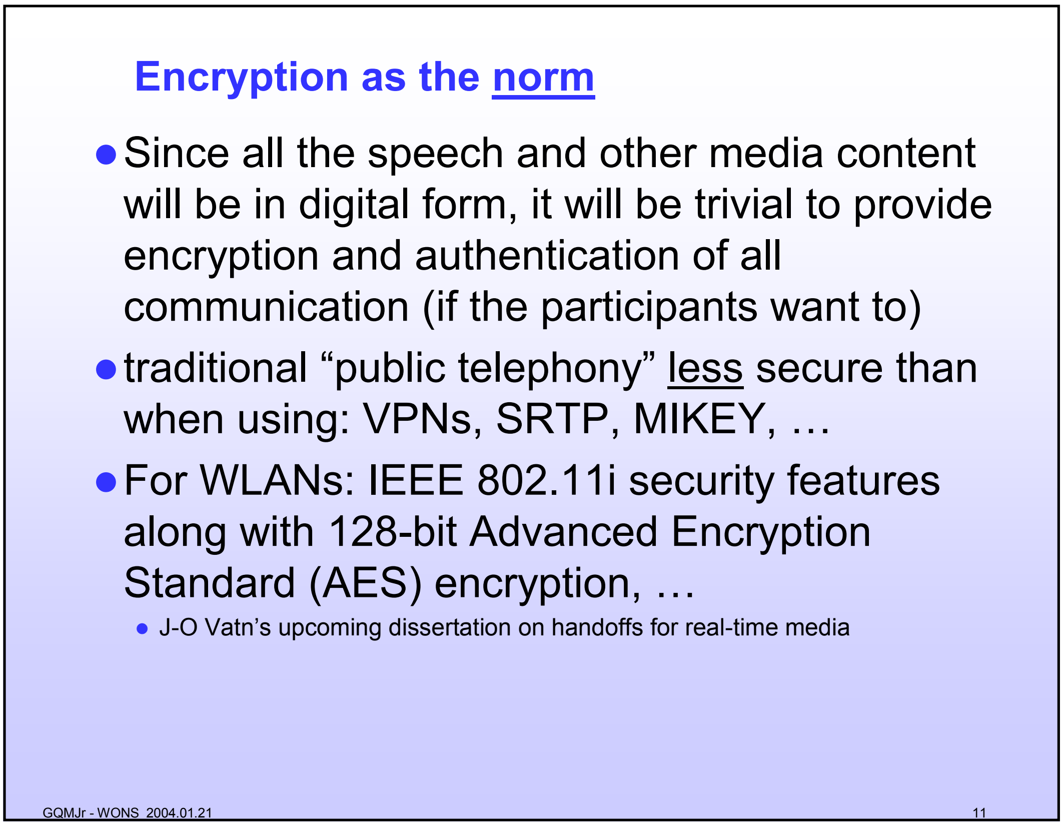
- Johan Bilien, **Key Agreement for Secure Voice over IP,** Master of Science Thesis, Royal Institute of Technology (KTH), December 2003.
- Extends earlier thesis
- Runs on a Laptop or iPAQ under linux



Secure call setup

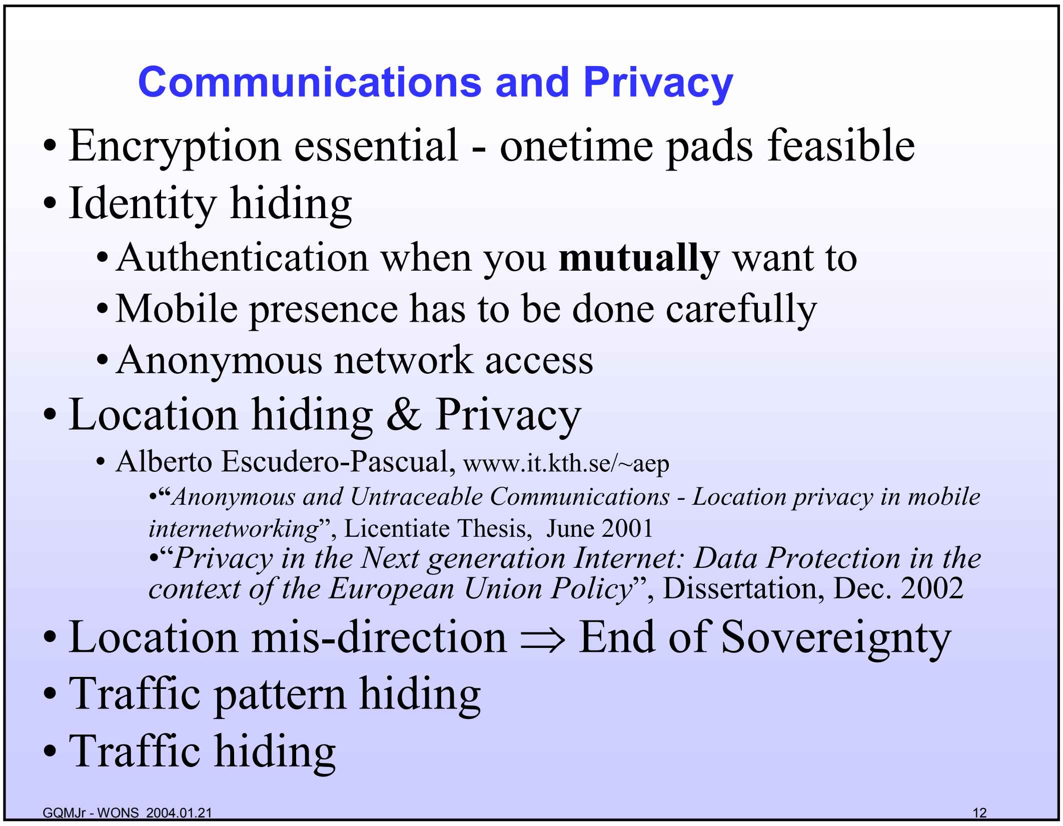
- Johan Bilien, Erik Eliasson, and Jon-Olov Vatn**, "Call establishment delay for secure VoIP",** submitted for publication, Dec. 2003
- name-servers (BIND 8.2 on Linux 2.4, 500 MHz Pentium 3 laptops)
- root name-server ns.lab manages the delegation of minisip.com and ssvl.kth.se to their respective name server
- Two routers (1.1 GHz Celeron desktops) perform static routing, and each router also runs a SIP server, SIP Express Router (SER v0.8.11))
- Alice and Bob use minisip, Alice is a 700 MHz Pentium 3 laptop, running Linux 2.6 (pre-emptive), while Bob is a 1.4 GHz Pentium 4 laptop, running Linux 2.4

Total delay (in ms)	Calling Delay	Answering Delay
No security	48	20
MIKEY, shared key	90	25
MIKEY, Diffie-Hellman	175	310 (160 sequential+ 200 in parallel)



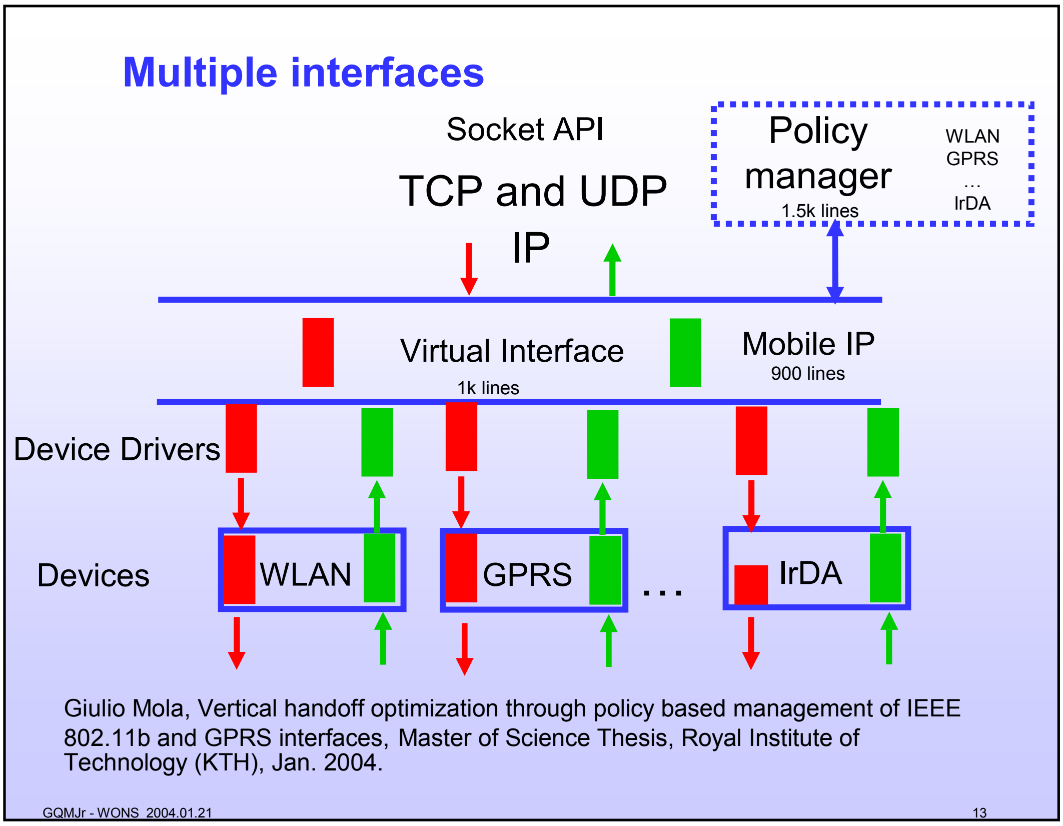
Encryption as the norm

- Since all the speech and other media content will be in digital form, it will be trivial to provide encryption and authentication of all communication (if the participants want to)
- traditional “public telephony” less secure than when using: VPNs, SRTP, MIKEY, …
- For WLANs: IEEE 802.11i security features along with 128-bit Advanced Encryption Standard (AES) encryption, …
  - J-O Vatn’s upcoming dissertation on handoffs for real-time media



Communications and Privacy

- Encryption essential - onetime pads feasible
- Identity hiding
  - Authentication when you **mutually** want to
  - Mobile presence has to be done carefully
  - Anonymous network access
- Location hiding & Privacy
  - Alberto Escudero-Pascual, www.it.kth.se/~aep
    - “*Anonymous and Untraceable Communications - Location privacy in mobile internetworking*”, Licentiate Thesis, June 2001
    - “*Privacy in the Next generation Internet: Data Protection in the context of the European Union Policy*”, Dissertation, Dec. 2002
- Location mis-direction ⇒ End of Sovereignty
- Traffic pattern hiding
- Traffic hiding



Multiple interfaces

Socket API

TCP and UDP

IP

Policy manager

1.5k lines

WLAN
GPRS
…
IrDA

Virtual Interface

1k lines

Mobile IP

900 lines

Device Drivers

Devices

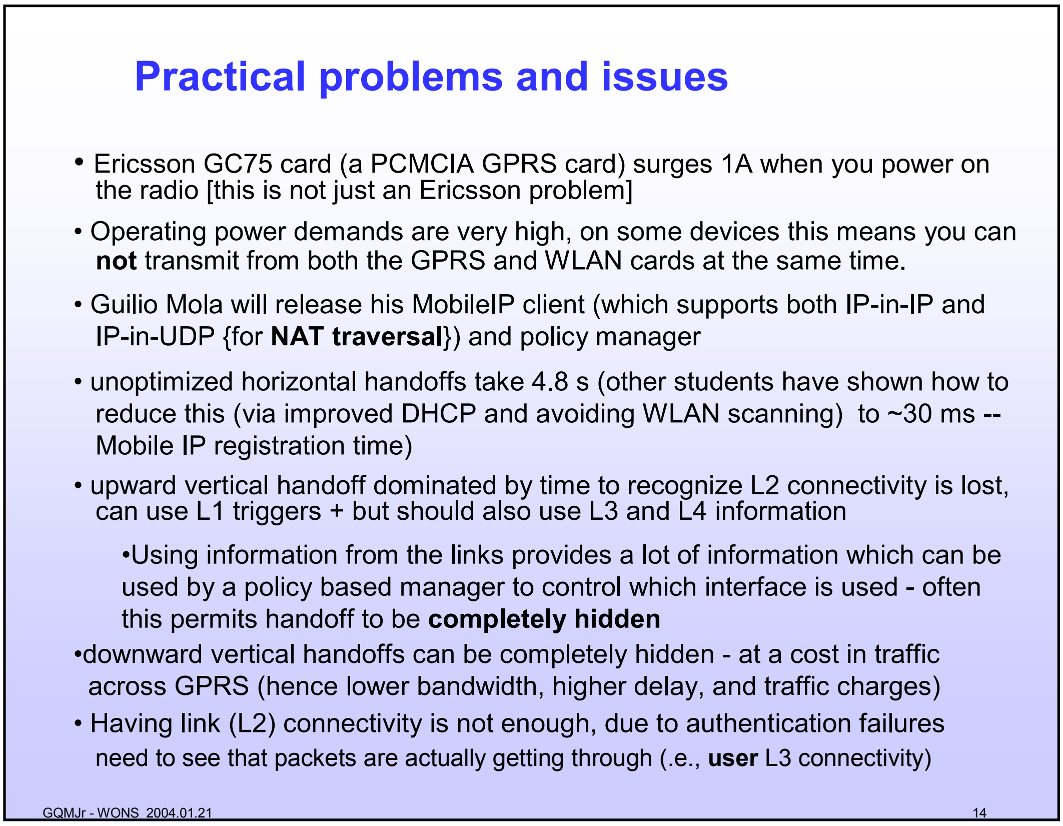
WLAN

GPRS

…

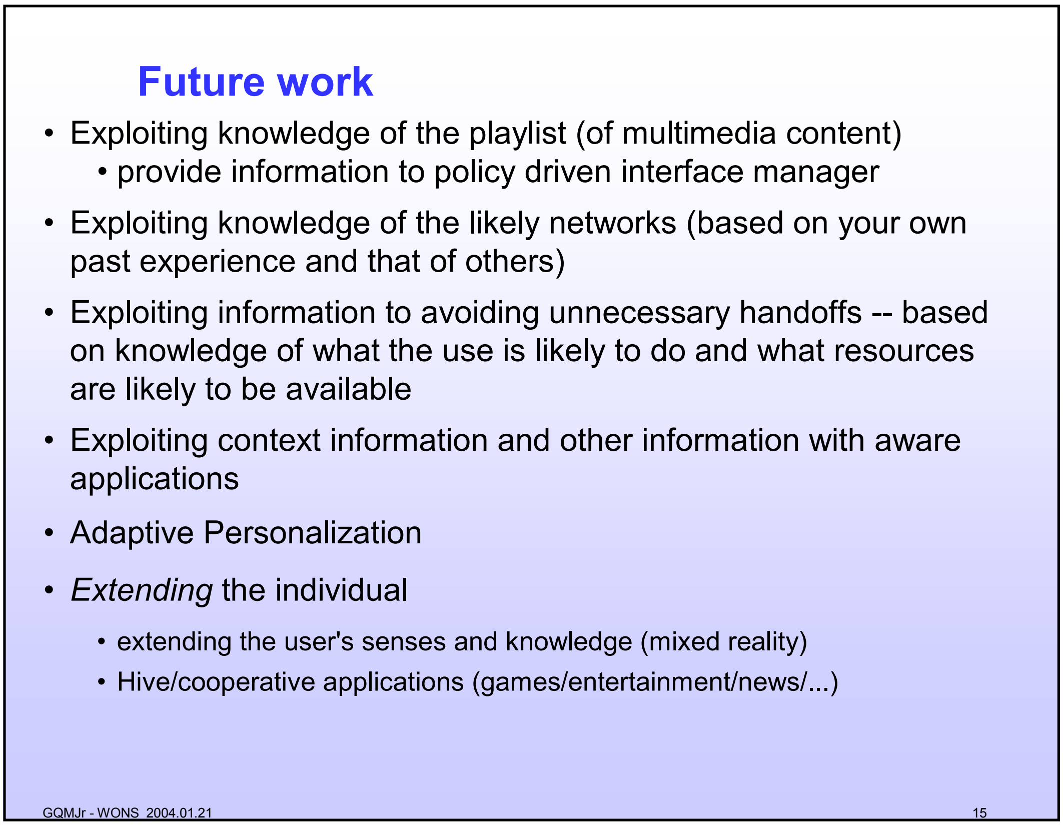
IrDA

Giulio Mola, Vertical handoff optimization through policy based management of IEEE 802.11b and GPRS interfaces, Master of Science Thesis, Royal Institute of Technology (KTH), Jan. 2004.



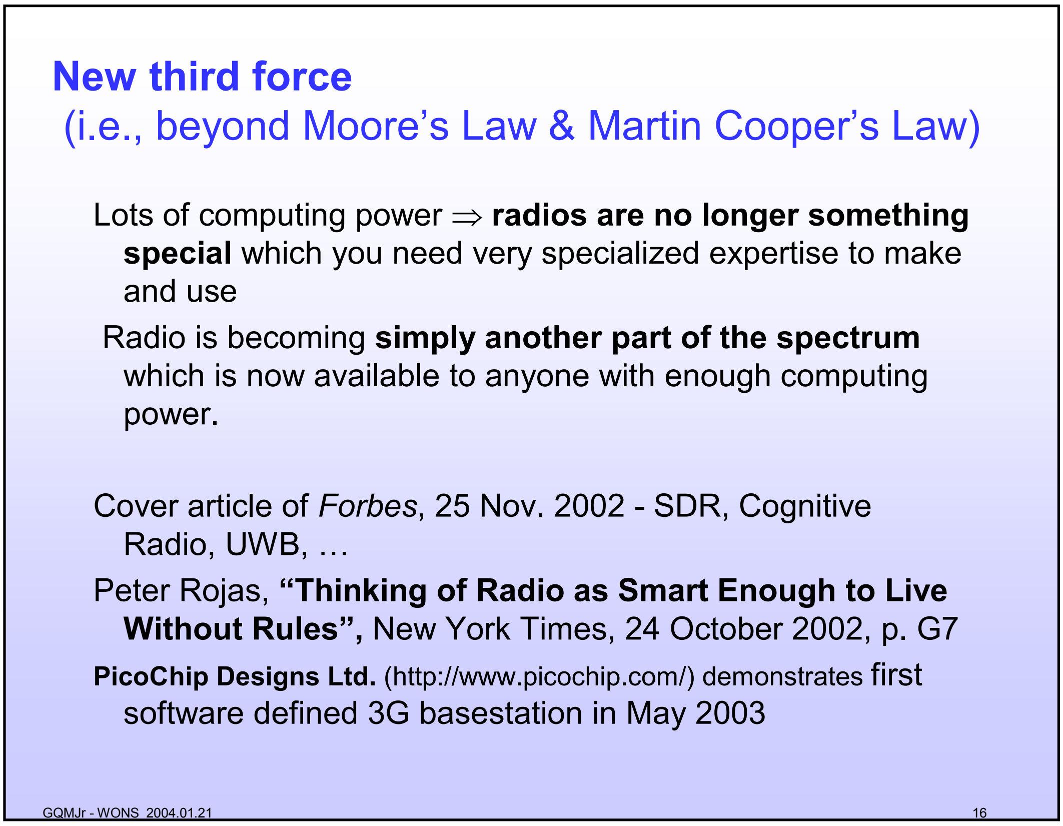
Practical problems and issues

- Ericsson GC75 card (a PCMCIA GPRS card) surges 1A when you power on the radio [this is not just an Ericsson problem]
- Operating power demands are very high, on some devices this means you can **not** transmit from both the GPRS and WLAN cards at the same time.
- Guilio Mola will release his MobileIP client (which supports both IP-in-IP and IP-in-UDP {for **NAT traversal**}) and policy manager
- unoptimized horizontal handoffs take 4.8 s (other students have shown how to reduce this (via improved DHCP and avoiding WLAN scanning) to ~30 ms -- Mobile IP registration time)
- upward vertical handoff dominated by time to recognize L2 connectivity is lost, can use L1 triggers + but should also use L3 and L4 information
  - Using information from the links provides a lot of information which can be used by a policy based manager to control which interface is used - often this permits handoff to be **completely hidden**
- downward vertical handoffs can be completely hidden - at a cost in traffic across GPRS (hence lower bandwidth, higher delay, and traffic charges)
- Having link (L2) connectivity is not enough, due to authentication failures need to see that packets are actually getting through (.e., **user** L3 connectivity)



Future work

- Exploiting knowledge of the playlist (of multimedia content)
  - provide information to policy driven interface manager
- Exploiting knowledge of the likely networks (based on your own past experience and that of others)
- Exploiting information to avoiding unnecessary handoffs -- based on knowledge of what the use is likely to do and what resources are likely to be available
- Exploiting context information and other information with aware applications
- Adaptive Personalization
- *Extending* the individual
  - extending the user's senses and knowledge (mixed reality)
  - Hive/cooperative applications (games/entertainment/news/...)



New third force
(i.e., beyond Moore’s Law & Martin Cooper’s Law)

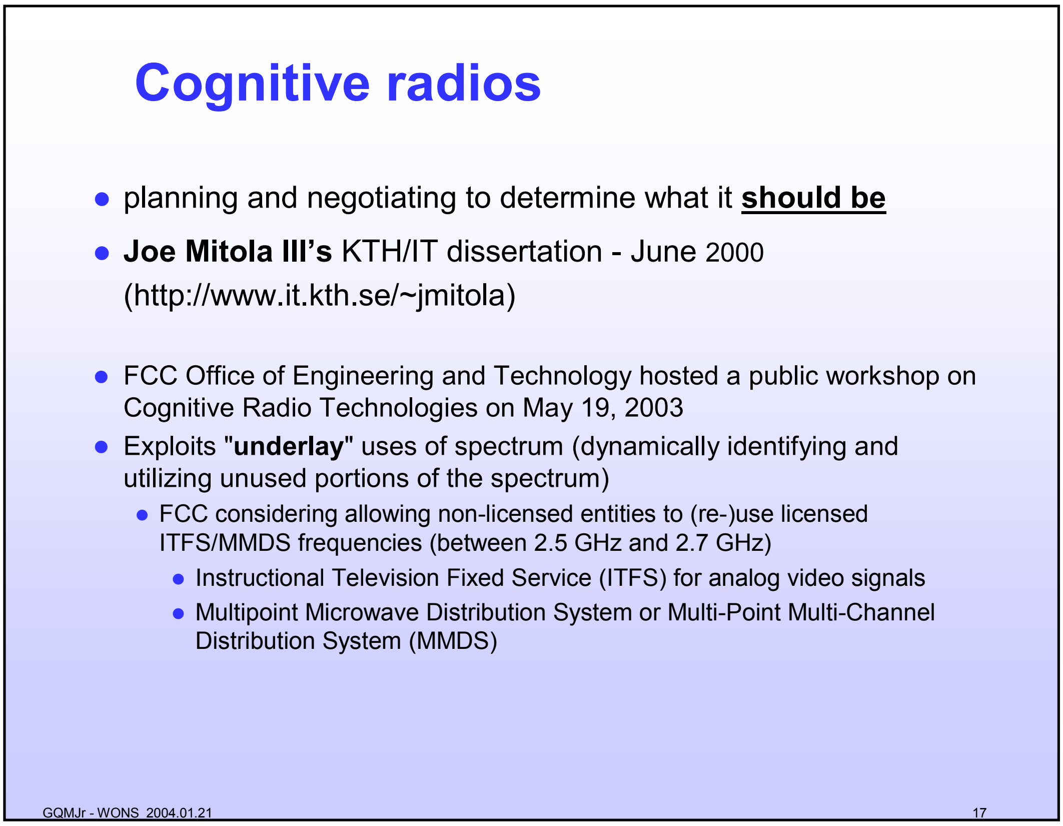
Lots of computing power ⇒ **radios are no longer something special** which you need very specialized expertise to make and use

Radio is becoming **simply another part of the spectrum** which is now available to anyone with enough computing power.

Cover article of *Forbes*, 25 Nov. 2002 - SDR, Cognitive Radio, UWB, …

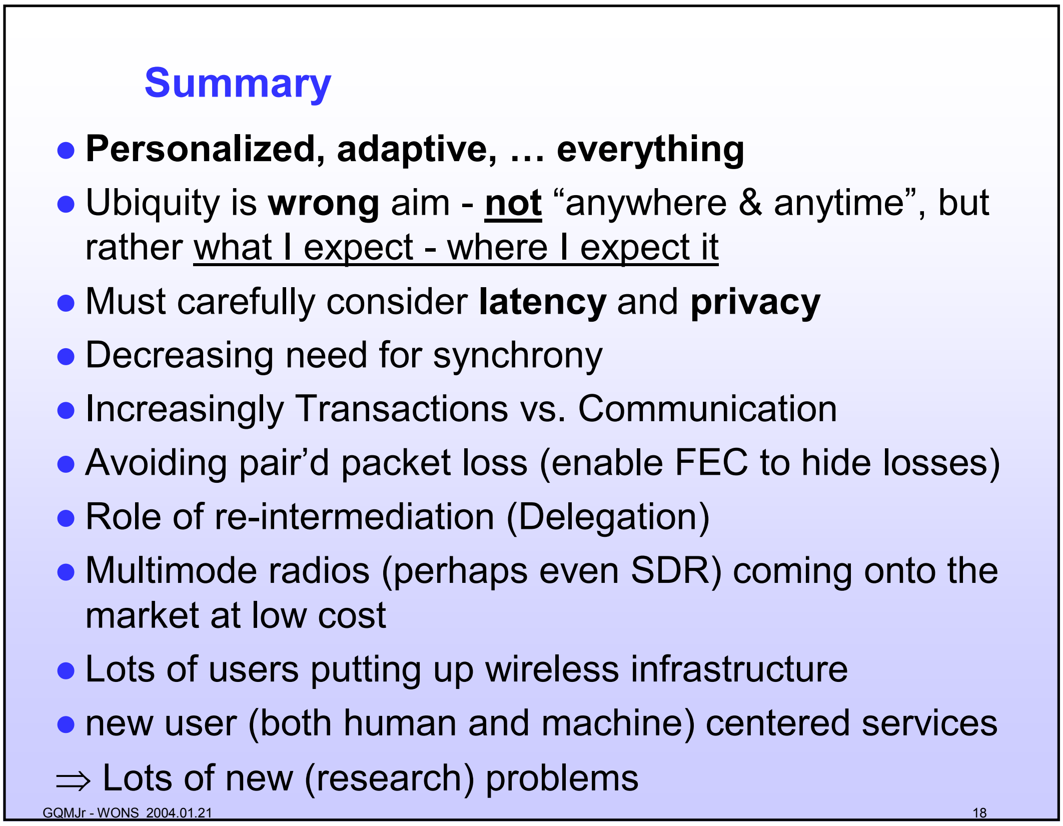
Peter Rojas, **“Thinking of Radio as Smart Enough to Live Without Rules”,** New York Times, 24 October 2002, p. G7

PicoChip Designs Ltd. (http://www.picochip.com/) demonstrates first software defined 3G basestation in May 2003



Cognitive radios

- planning and negotiating to determine what it **should be**
- **Joe Mitola III’s** KTH/IT dissertation - June 2000 (http://www.it.kth.se/~jmitola)
- FCC Office of Engineering and Technology hosted a public workshop on Cognitive Radio Technologies on May 19, 2003
- Exploits "**underlay**" uses of spectrum (dynamically identifying and utilizing unused portions of the spectrum)
  - FCC considering allowing non-licensed entities to (re-)use licensed ITFS/MMDS frequencies (between 2.5 GHz and 2.7 GHz)
    - Instructional Television Fixed Service (ITFS) for analog video signals
    - Multipoint Microwave Distribution System or Multi-Point Multi-Channel Distribution System (MMDS)



Summary

- **Personalized, adaptive, … everything**
- Ubiquity is **wrong** aim - **not** “anywhere & anytime”, but rather what I expect - where I expect it
- Must carefully consider **latency** and **privacy**
- Decreasing need for synchrony
- Increasingly Transactions vs. Communication
- Avoiding pair’d packet loss (enable FEC to hide losses)
- Role of re-intermediation (Delegation)
- Multimode radios (perhaps even SDR) coming onto the market at low cost
- Lots of users putting up wireless infrastructure
- new user (both human and machine) centered services

⇒ Lots of new (research) problems

¿Questions?