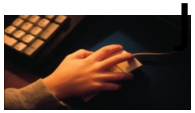
Keamanan Sistem Wireless

Budi Rahardjo

Mengapa Wireless?

- Karena terpaksa, sulit mendapatkan layanan wired.
  - Wireless populer di dunia di mana layanan wired susah diperoleh (Eropa dan Asia)
  - Di Amerika Serikat, infrastruktur wired sudah mapan sehingga kurang insentif untuk menggunakan wireless (meskipun akhirnya populer juga)



Mengapa Wireless [2]

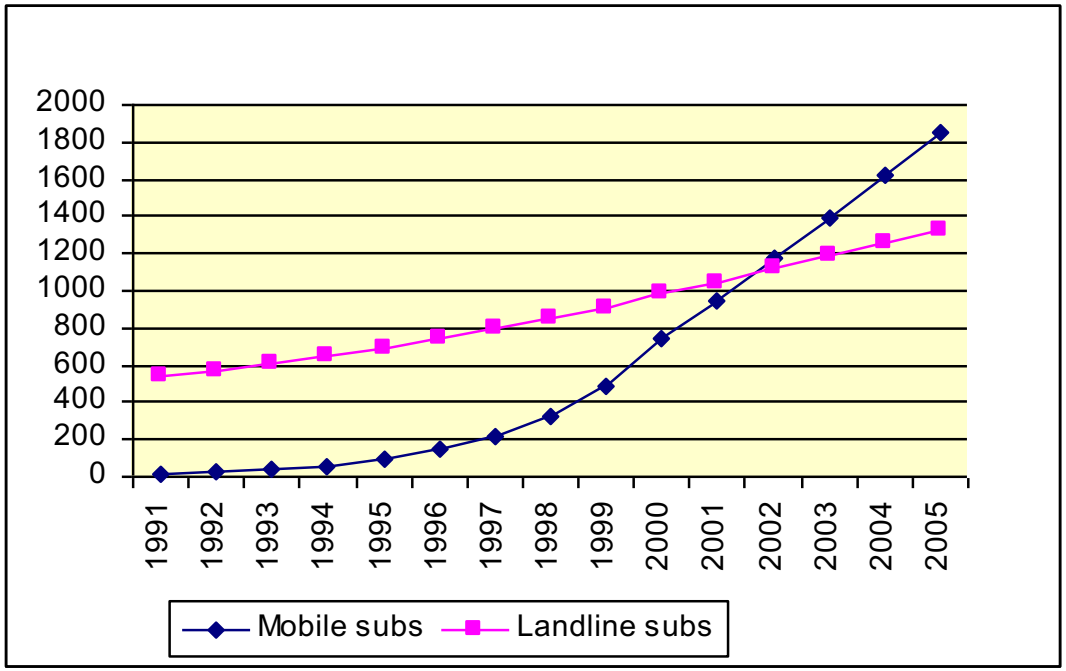
- Kemudahan
  - Kenyamanan: bergerak (mobile) & always connected, roaming
  - Lebih murah dan cepat untuk dimiliki
  - Layanan lebih mudah dan cepat untuk diluncurkan

Mengapa Wireless [3]

- Untuk layanan berbasis data dari telepon (3G, CDMA, HSDPA, LTE), kecepatan mulai nyaman untuk berbagai aplikasi
- Mulai muncul aplikasi wireless. Mulai banyak aplikasi baru yang sebelumnya tidak dimungkinkan karena batasan bandwidth.
- Aplikasi baru ini menghasilkan banyak pengguna lagi. Terjadi siklus saling memperkuat

Mengapa Wireless [4]

- Jumlah pengguna layanan telepon seluler (handphone) sudah melampaui jumlah pengguna telepon biasa
- Handphone sudah menjadi style



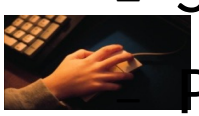
World Telecom Statistics

Mengapa Wireless [5]

- Teknologi WiFi dan regulasi mendukung
- Hotspot sudah menjadi bagian dari layanan umum
- Muncul WiMax yang lebih baik jangkauan dan kecepatannya
- LoRa yang jangkauannya lebih jauh lagi
- Adanya gabungan teknologi telekomunikasi dan komputer
  - LTE
  - EVDO

Aplikasi Baru

- SMS merupakan killer application
- **Facebook** & **twitter** awalnya merupakan killer application berbasis internet di Indonesia (kemudian Instagram, messaging, TikTok)
- Aplikasi lain?
  - Banking
  - Sekedar akses internet
  - Photo/ story sharing



Instagram
Fast beautiful photo sharing

Bayar via handphone

Traffic Data > Voice

- ~~Diperkirakan~~ Jumlah traffic data akan melebihi voice
  - Saturasi traffic voice
  - Machine to Machine communication
- Voice diubah menjadi data dan terlihat sebagai data (misal Skype, Zoom)
- Diskusi akan lebih fokus ke data

Three major changes in telecomunications

Menurut Nicholas Negroponte:

1. Digital (70s): multimedia
2. Packet switching: always on connectivity
3. Wireless: functional mobility

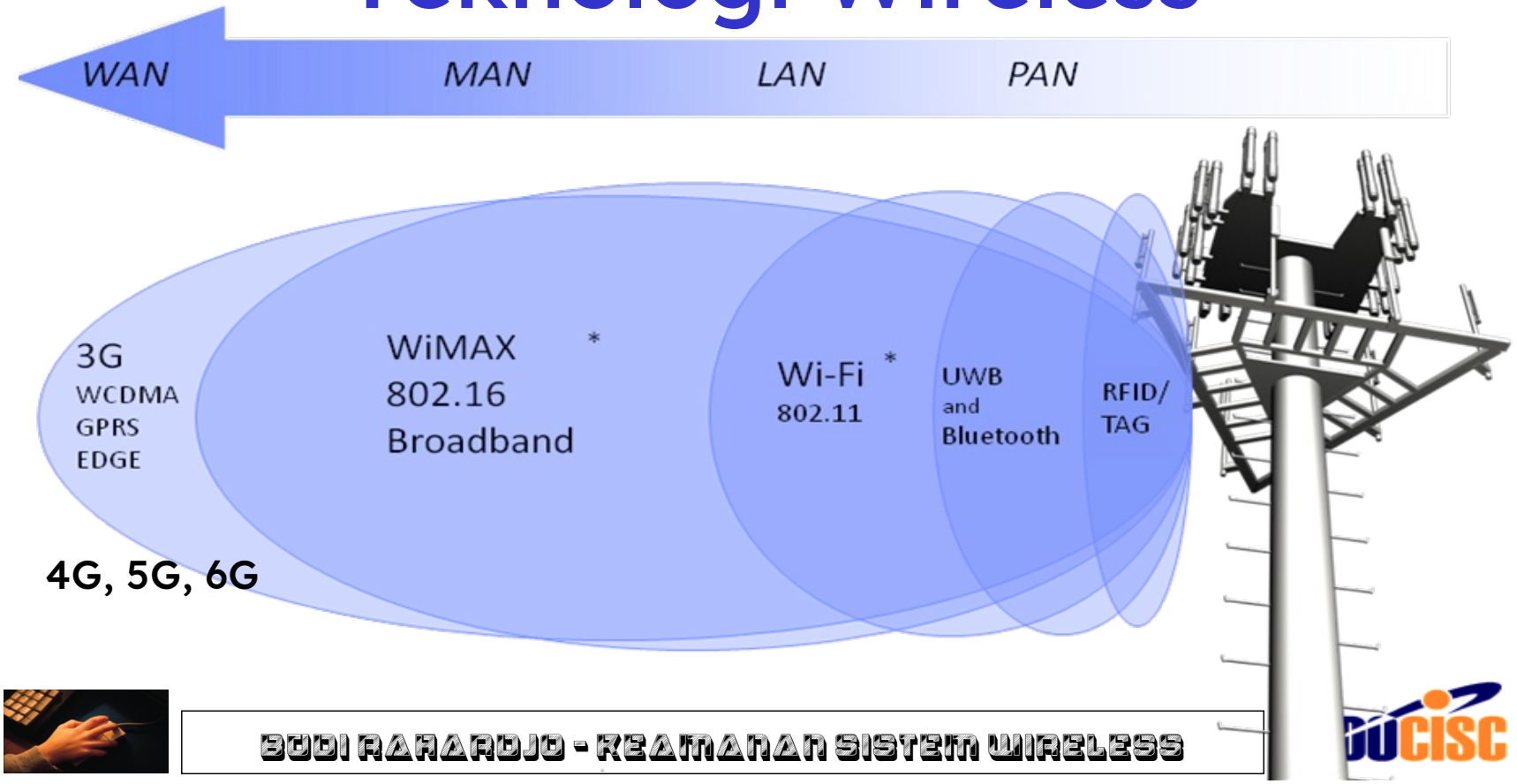
THE WATER LILIES:
THE REAL NEXT GENERATION

http://www.wired.com/wired/archive/10.10/wireless.html

Jenis Wireless

- Wireless technology:
  - Cellular-based wireless data solutions
    - Mempergunakan saluran komunikasi cellular/pager yang sudah ada untuk mengirimkan data
  - Wireless LAN (WLAN) solutions
    - Hubungan dalam lingkup area yang terbatas, biasanya 10 s/d 100 meter dari base station ke Access Point (AP)
    - Mulai meningkat sampai ke 15 mil (WiMax, LoRa)
- ~~Akankah~~ terjadi konvergensi?

Teknologi Wireless



Konflik Teknologi

- Banyaknya teknologi & standar yang berbeda (dan konflik)
  - Cellullar: GSM, CDMA, TDMA, CDPD, GPRS/EDGE, 2G, 2.5G, 3G, UMTS, EVDO
  - LAN: keluarga 802.11 (802.11b, 802.11a, 802.11g), HomeRF, 802.15 (Personal Area Network) based on Bluetooth, 802.16 (Wireless Metropolitan Area Network) – WiMax, LoRa
- Batasan jangkauan Radio, interferensi

Konvergensi

- Yang dominan adalah yang berbasis IP
  - Cellular based: CDMA / GPRS/3G / HSDPA, EVDO, LTE
  - Wireless LAN: WiFi, WiMax, LoRa

Mulai muncul masalah security

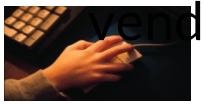
- Cloning handphone AMPS untuk curi pulsa
- Cloning simcard

Mulai muncul masalah security

- Airsnort dapat menyadap paket WLAN. Tools lain seperti Netstumbler, WEPcrack, dll mulai banyak tersedia
- NIST di Amerika melarang penggunaan WLAN untuk sistem yang memiliki data-data confidential
- Bluetooth jacking, bluestumbler: mencuri data-data melalui bluetooth

Masalah keamanan wireless

- Pencurian fisik (perangkat wireless yang biasanya kecil ukurannya) dan data
- Penyadapan, *man-in-the-middle attack*, passive attack dapat dilakukan. Contoh: informasi seperti daftar nomor telepon, calendar, dan data-data lainnya bisa dibaca melalui bluetooth tanpa pengaman
- Resources perangkat wireless yang terbatas (CPU, memory, kecepatan) sehingga menyulitkan pengamanan dengan *encryption* misalnya
- Pengguna tidak dapat membuat sistem sendiri, bergantung kepada vendor



Masalah keamanan wireless [2]

- DoS, *active attack*, *injection of new (fake) traffic*, mengirimkan pesan sampah (*bluejacking*), hijacking information
- Fokus utama dari wireless adalah transfer data secepat mungkin. **Speed!** Pengamanan dengan enkripsi (apalagi dengan resources terbatas) menghambat kecepatan sehingga menjadi nomor dua
- Pengguna tidak tahu ada masalah keamanan

Masalah keamanan wireless [2]

- Fokus
  - *Identity* & *Authentication*, belum pada *Confidentiality*
  - Biasanya yang dideteksi adalah *device* (perangkat) bukan usernya
  - Pengelolaan sistem dengan banyak *Access Point* menyulitkan (misal bagaimana dengan single sign-on, penggunaan dynamic firewall untuk akses ke jaringan internal)

Pengamanan Wireless

- Segementasi jaringan. Masukkan wireless ke sisi extranet yang dianggap kurang aman
  - Masuk ke LAN via VPN
- Pembatasan akses berdasarkan *MAC address* (namun masih mudah di-*spoof*)
- Menambahkan *digital certificate* atau agent di perangkat mobile untuk mengidentifikasi perangkat

Pengamanan Wireless

- Encryption:
  - WEP (Wired Equivalent Privacy)
    Masih ada masalah dengan Initial Vector (IV) yang bisa ditebak jika banyak data
    - Ada tools untuk cracking
  - Ganti dengan WPA
- Penggunaan end-to-end encryption pada level aplikasi

Penutup

- Penggunaan wireless tidak dapat dihindari
- Teknologi wireless masih “bayi”, membutuhkan pengembangan lebih lanjut, khususnya pada aspek keamanan
- Kesadaran akan masalah keamanan wireless ini masih perlu disosialisasikan