Wireless Networks - Energy, Security

- Christine E. Price, Krishna M. Sivalingam, Prathima Agarwal and Jyh-Cheng Chen, "A Survey of Energy Efficient Network Protocols for Wireless and Mobile Networks", Accepted for ACM/Baltzer Journal on Wireless Networks, Jan 2001
- Nikita Borisov (University of California, Berkeley, USA); Ian Goldberg (Zero Knowledge Systems, Canada); and David Wagner (University of California, Berkeley, USA). "Intercepting Mobile Communications: The Insecurity of 802.11", Mobicom 2001

Motivation: Energy consumption for iPAQ

Operation		Energy (mW)
iPAQ (fully powered, no wireless, with serial)		**929**
Agere WNIC 802.11b (11 Mbps)	Sleep	**177**
	Idle	**1319**
	Recv	1425
	Send	1675

- Note:
  - Overall energy consumed depends on the components, peripherals and their energy states
  - iPAQ battery capacity – 2*950mAh (2*2850mWh @ 3V)

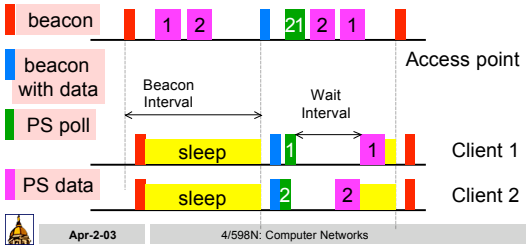
Source: Compaq researchers, Sukjae Cho, Paul Havinga, Mark Stemm

Energy conservation techniques

- Physical layer
  - Avoid collisions (wasted energy)
    - Packet delivery at well defined intervals
    - How do new nodes join? What about throughput?
  - Reduce switching between transmit and receiving
- MAC layer
  - IEEE 802.11 - scheduled rendezvous mechanism

IEEE 802.11b power saving mode (PSM)

- Scheduled rendezvous mechanism using beacons
  - Access point (AP) informs client of pending packets at predefined intervals (beacon interval)
  - Clients transition to lower energy consuming states between scheduled beacons



Energy conservation

- Network layer
  - Balance topology maintenance with energy overhead
  - Broadcast/unicast differences
  - Analysis of ad-hoc routing protocols from an energy perspective
- TCP
  - TCP probing - not all packet loss is congestion related

Security

- 802.11 networks utilize Wireless Equivalent Privacy protocol (WEP)
  - Confidentiality: Prevent casual eavesdropping
  - Access control: Protect access to wireless infrastructure
  - Data integrity: Prevent unauthorized tampering
- WEP utilizes a shared secret (WEP key, array of 4 shared keys)
  - Checksumming P = M,c(M)
  - Encryption C=P⊕RC4(v,k)
  - Transmission v,C

Risks

- Keystream reuse: If you know the keystream v, and information about the plain text message, then you can get the cipher text
  - Certain IP packets are predictable
  - Proactively create packets by sending known strings, say via SPAM
  - Buggy implementation - broadcasting encrypted and unencrypted
- Build a dictionary of known keystream values
  - By IEEE standard, v is only 24 bits wide
  - Dictionary valid irrespective of the encryption key width
  - Keystream can be reused many times
  - Some cards always start with 0
  - Shared keys are usually same for all clients

Message authentication failure

- WEP checksum is a linear function
  - Crypto experts would never use such a scheme
  - Protocol was developed like a network protocol - liberal
  - Use client association packets
  - IP redirection to have access point do the work for us
  - Use TCP client check summing mechanism
- End-to-end mechanisms such as VPN/IPSEC helps
- Treat wireless LANs as untrusted