More on wireless

Overview

- Multiple access networks
  - 802.11
    - Collision avoidance
    - Encryption
  - Bluetooth
  - Mobile telephone system

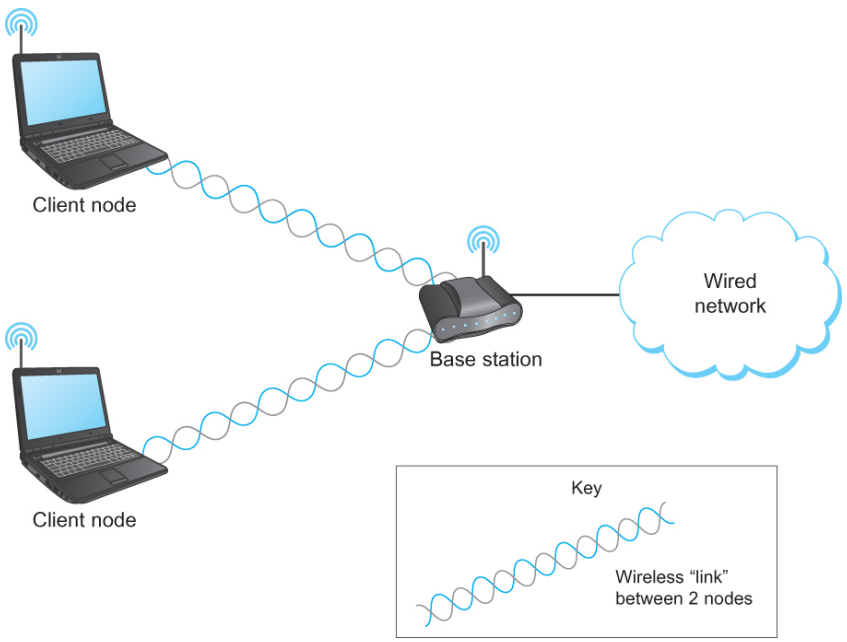
802.11 Wi-Fi

Standard	Released	Max bit rate (shared)	Frequency band	Indoor range
802.11	1997	2 Mbps	2.4 GHz	20 m
802.11a	1999	54 Mbps	5 GHz	35 m
802.11b	1999	11 Mbps	2.4 GHz	38 m
802.11g	2003	54 Mbps	2.4 GHz	38 m
802.11n	2009	600 Mbps	2.4 GHz 5 GHz	70 m

- Operate in license exempt bands
- More absorption at high frequencies (5 GHz)
- All support lower bit rates
  - Switch between modulation techniques & error correction codes
- 802.11n, multiple antennas
  - MIMO (Multiple Input Multiple Output)

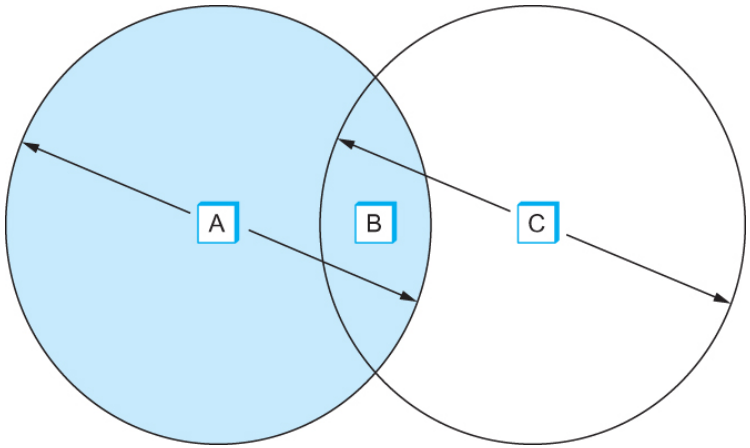
Wireless topology

- Base station topology
  - Typically all clients talk to base station
  - No direct communication between clients



802.11 collision avoidance

- Collision avoidance
  - Can't transmit and listen for collision
    - Transmission power swamps receiving circuit
    - Collision detection (CD) as in Ethernet not possible
  - Not everyone can hear everything
    - Hidden node problem:

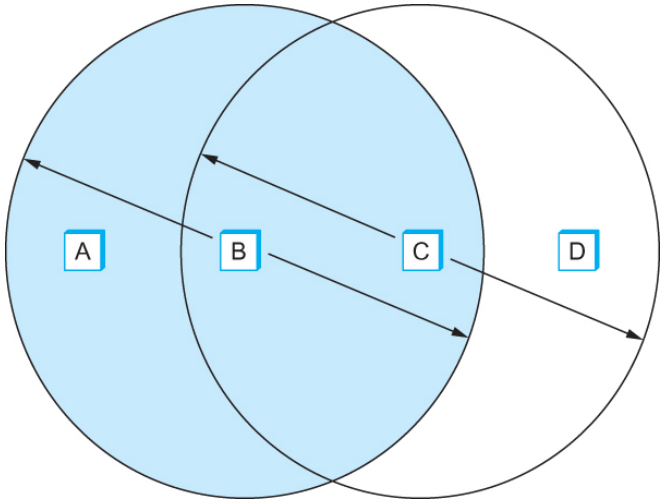


A and C both want to send to B.

A and C can't hear each other so can't detect their transmissions collided.

802.11 collision avoidance

- Collision avoidance
  - Lack of global information about who is in range of who
    - Exposed node problem:



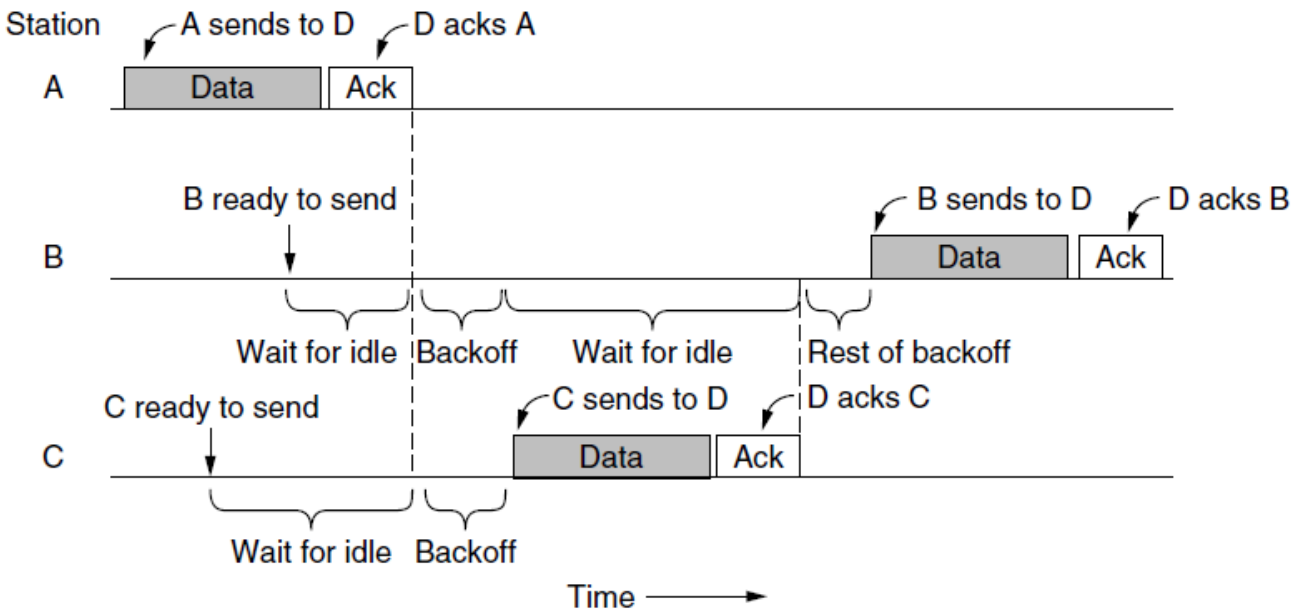
C wants to send to D.

But C can hear B transmitting to A.
But D cannot hear B,
and A cannot hear C.

So C could safely transmit to D.

Carrier Sense, Multiple Access w/ Collision Avoidance

- CSMA/CA
  - Don't send if you hear transmission
  - If you sent recently, don't be greedy
    - Use random backoff
  - Explicit ACK from receiver to sender
    - Exponential backoff if bad/missing ACK

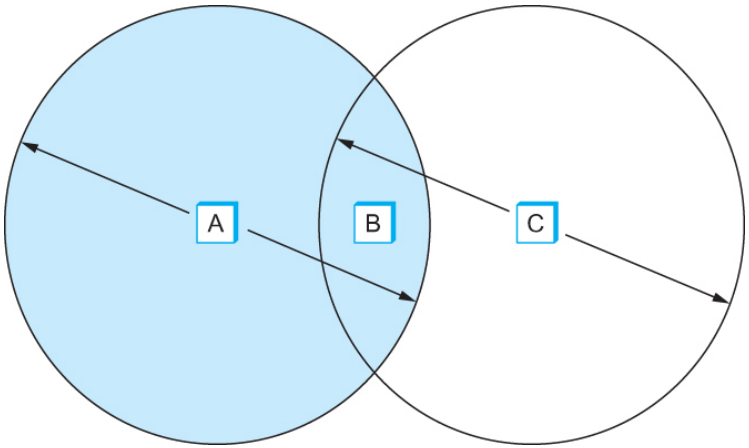


Ready to Send-Clear to Send

- Ready to Send-Clear to Send
  - Optional RTS-CTS protocol:
    - Exchange control frames before transmission
    - Informs nearby nodes about planned transmission
    - Request to Send (RTS)
      - Transmitter: "I want to send a frame of this length"
    - Clear to Send (CTS)
      - Receiver: "Okay, you're the man, send the data"
    - One-side usually an access point
      - Clients can hear either the RTS or CTS
      - Other clients stay off the air until after ACK

Ready to Send-Clear to Send

- RTS-CTS
  - Helps address hidden node problem:



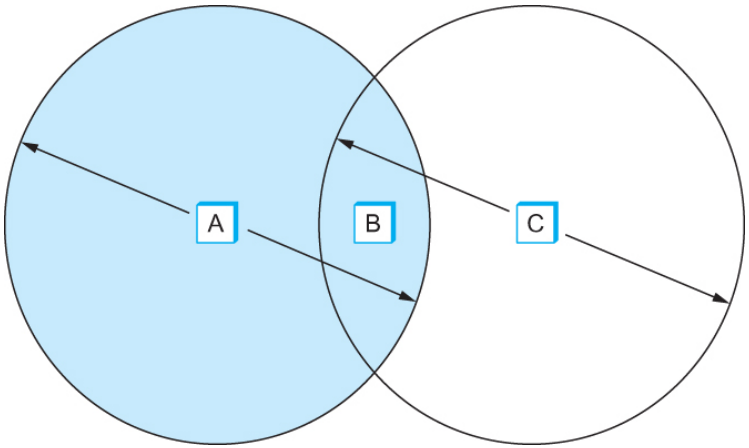
A wants to send to B.

A issues RTS.
B hears RTS, responds with CTS.

C wants to send to B.
But heard the recent CTS broadcast from B.
C waits until after length of A's communication (obtained from the CTS).

Ready to Send-Clear to Send

- RTS-CTS
  - RTS frames can collide



A wants to send to B.
C wants to send to B.

A issues RTS.
B issues RTS.

RTS's are mangled at B.
B doesn't send anything.

A and B wait and resend RTS using an exponential backoff algorithm.

Ready to Send-Clear to Send

- RTS-CTS
  - Good in theory, not used much in practice
  - Slows down:
    - Short frames and transmissions from access point (AP)

Why RTS-CTS is not your ideal wireless LAN multiple access protocol

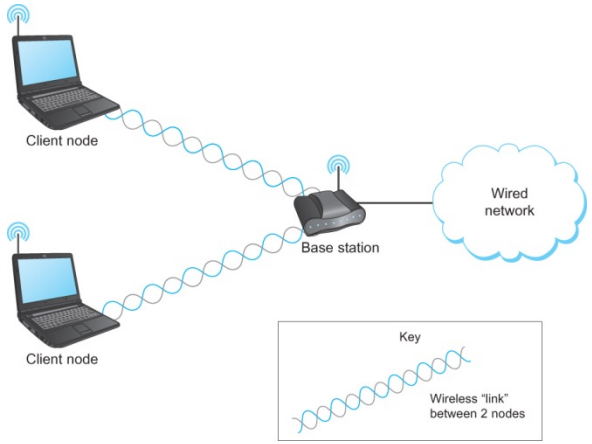
João Luís Sobrinho, Roland de Haan, José Manuel Brázio
Instituto de Telecomunicacões, IST
Lisboa, Portugal
Email: {joao.sobrinho, r.dehaan, jose.brazio}@lx.it.pt

***Abstract*— Although Request-To-Send Clear-To-Send (RTS-CTS) has been introduced as a uniform improvement over Carrier Sense Multiple Access (CSMA) in a wireless LAN environment it is not. As it tries to solve the hidden-stations problem of CSMA, it creates new problems derived from the interaction among its control and data packets. In this paper, we systematically identify and classify the sequences of events where CSMA and RTS-CTS depart from an ideal behavior, and we define a reference configuration and an analytical model on the basis of which a comparative study of protocol performance is made. The results show that RTS-CTS falls short of an ideal protocol, in some cases performing even worse than CSMA. This is especially noticeable in situations where the interaction between control packets in RTS-CTS prevents transmissions that under CSMA could occur concurrently and successfully.**

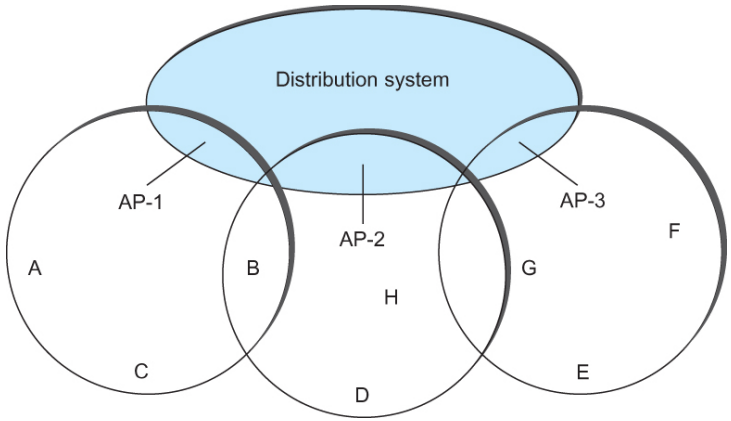
where CSMA and RTS-CTS deviate from the ideal behavior, and we define a reference configuration and an analytical model on the basis of which we make a comparative study of protocol performance. The configuration considered consists of a wireless LAN comprising two interfering cells and subject to several traffic scenarios. The analytical model builds on the work of [8] and [9] and, in contrast to most existing analytical work on RTS-CTS, accurately describes the space and time dependencies between the transmission activity at different stations in the network.

The paper is organized as follows. In Section II, we state the operation of an ideal protocol and closely examine the shortcomings of CSMA and RTS-CTS. Next, in Section III, we

802.11 distribution system



Simple distribution system. One access point (AP) and multiple clients.

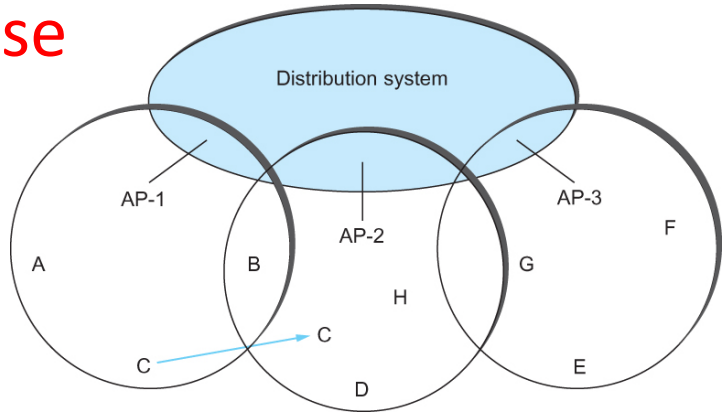


Distribution system with multiple APs. Clients can switch between APs.

- Distribution system
  - Operating at same link layer as Wi-Fi
    - Not using higher layer protocols (e.g. network layer)
  - Each client associates with one AP

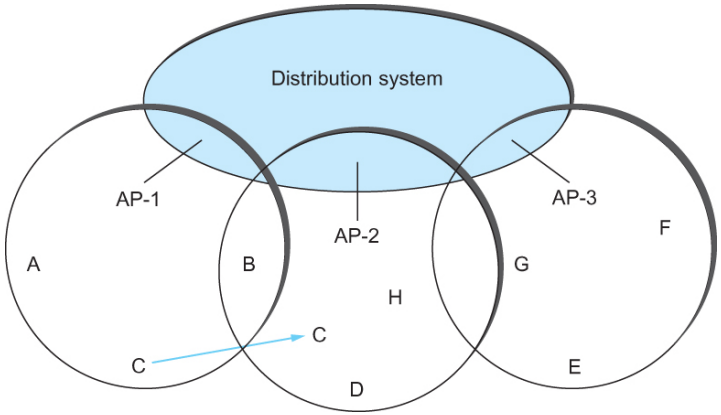
802.11 finding an AP

- Active scanning
  - Node sends a probe frame
  - All APs that hear probe, send a probe response
  - Node decides AP it likes best
  - Node sends AP association request
  - AP sends association response



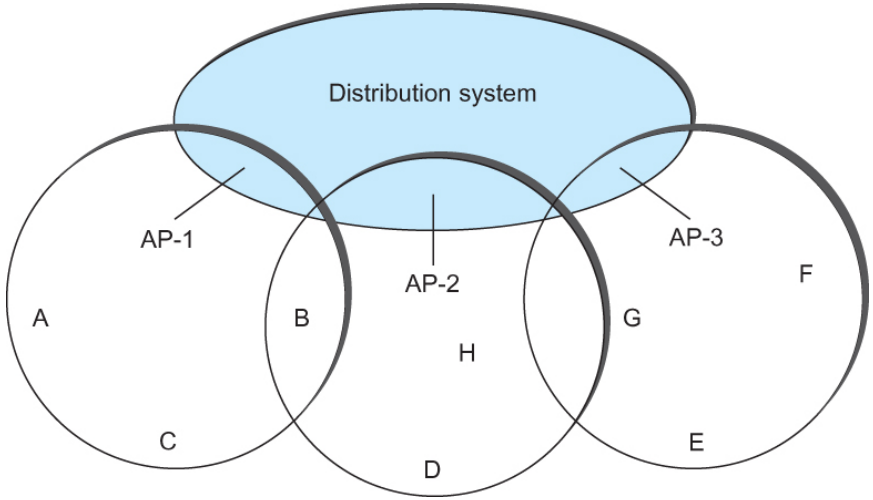
802.11 finding an AP

- Passive scanning
  - APs periodically send beacon frame
    - Advertise access point's capabilities
    - Transmission rate, etc.
  - Node can respond with association request

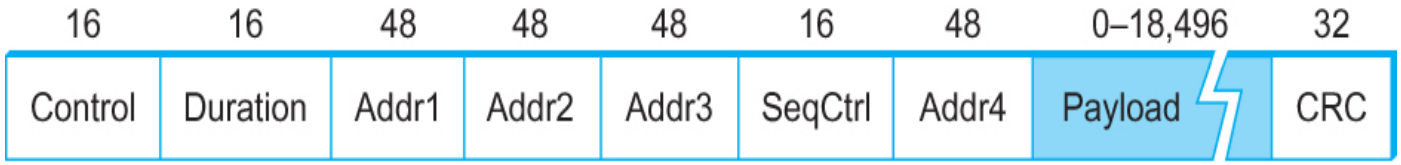


Node communication

- Node-to-node communication
  - Simple case:
    - A wants to talk to C
    - Send via AP-1
  - Complex case:
    - A wants to talk to F
    - Send to AP-1
    - Goes through distribution system
    - AP-3 sends to F

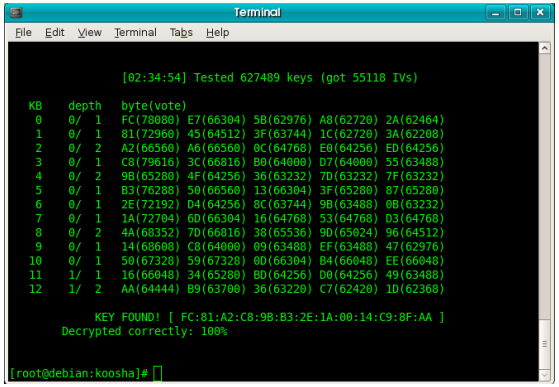


802.11 frame format

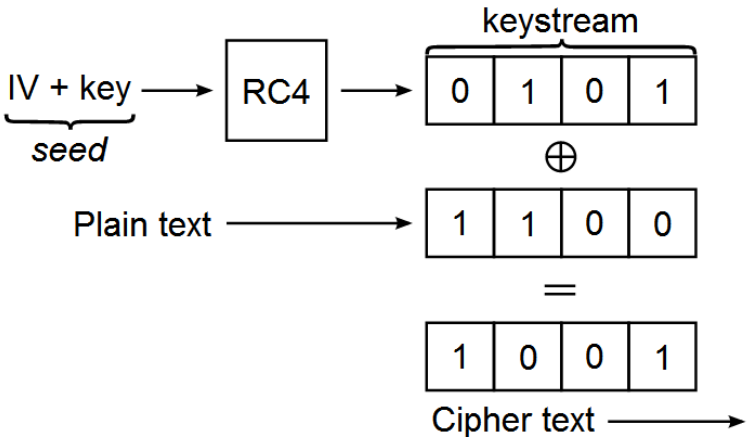


- Source and destination addresses
  - Four 48-bit MAC addresses:
    - Allows for frame going via distribution system:
      - Addr1 – ultimate destination
      - Addr2 – immediate sender, AP that forwarded to ultimate destination
      - Addr3 – intermediate destination, AP that accepted frame from sender
      - Addr4 – original sender

802.11 encryption



- Client in range can sniff frames
- Encryption schemes:
  - WEP (Wired Equivalent Privacy)
    - Encryption in original 802.11 standard (1999)
    - RC4 stream cipher
    - Shared and static 40 bit-secret, 104-bit secret "WEP2"
    - Random 24-bit initialization vector (IV)
    - Only protect wireless hop
  - 2001 exploit published
    - Cracking software freely available



Breaking 104 bit WEP in less than 60 seconds

Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin *
<e_tews,weinmann,pyshkin@cdc.informatik.tu-darmstadt.de>

TU Darmstadt, FB Informatik
Hochschulstrasse 10, 64289 Darmstadt, Germany

Abstract. We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40,000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85,000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of magnitude over the best known key-recovery attacks for WEP. On a IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately 2^{20} RC4 key setups, which on current desktop and laptop CPUs is negligible.

1 Introduction

Wired Equivalent Privacy (WEP) is a protocol for encrypting wirelessly transmitted packets on IEEE 802.11 networks. In a WEP protected network, all packets are encrypted using the stream cipher RC4 under a common key, the *root key*[1] Rk. The root key is shared by all radio stations. A successful recovery of this key gives an attacker full access to the network. Although known to be insecure and superseded by Wi-Fi Protected Access (WPA) [18], this protocol is still is in widespread use almost 6 years after practical key recovery attacks were found against it [5,15]. In this paper we present a new key-recovery attack against WEP that outperforms previous methods by at least an order of magnitude.

First of all we describe how packets are encrypted: For each packet, a 24-bit initialization vector (IV) IV is chosen. The IV concatenated with the root key yields the per packet key $\mathsf{K} = \mathsf{IV}||\mathsf{Rk}$. Over the data to be encrypted, an Integrity Check Value (ICV) is calculated as a CRC32 checksum. The key K is then used to encrypt the data followed by the ICV using the RC4 stream cipher. The IV is transmitted in the header of the packet. Figure 1 shows a simplified version of an 802.11 frame.

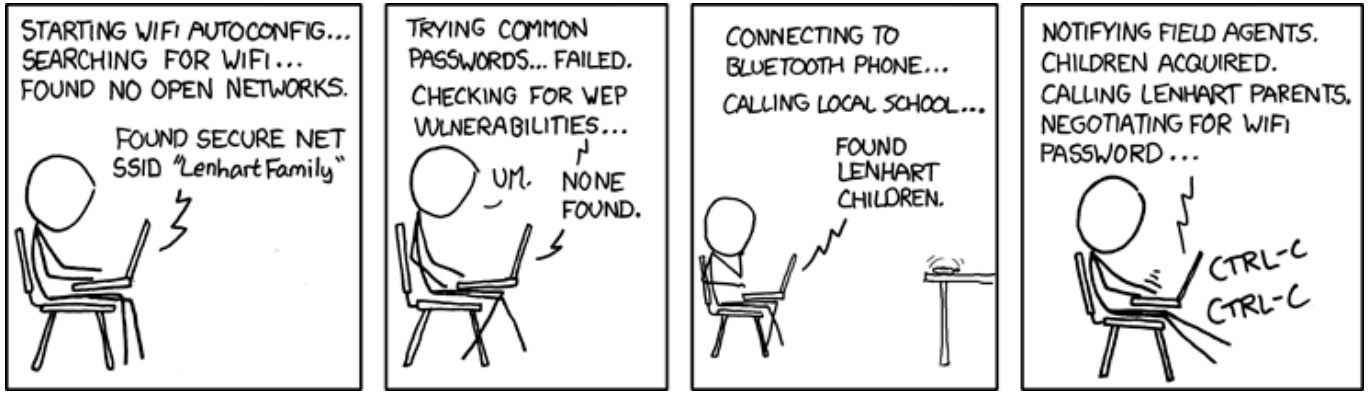
A first analysis of the design failures of the WEP protocol was published by Borisov, Goldberg and Wagner [2] in 2001. Notably, they showed that the ICV merely protects against random errors but not against malicious attackers.

* Supported by a stipend of the Marga und Kurt-Möllgaard-Stiftung.

[1] The standard actually allows for up to four different root keys; in practice however, only a single root key is used.

802.11 encryption

- WPA (802.11i)
  - WPA interim subset of 802.11i
  - WPA2 (WiFi Protected Access 2)
    - Initial authentication via pre-shared key
    - New key generated for a particular session
    - 128-bit key, 48-bit IV
    - Enterprise version using 802.1x authentication



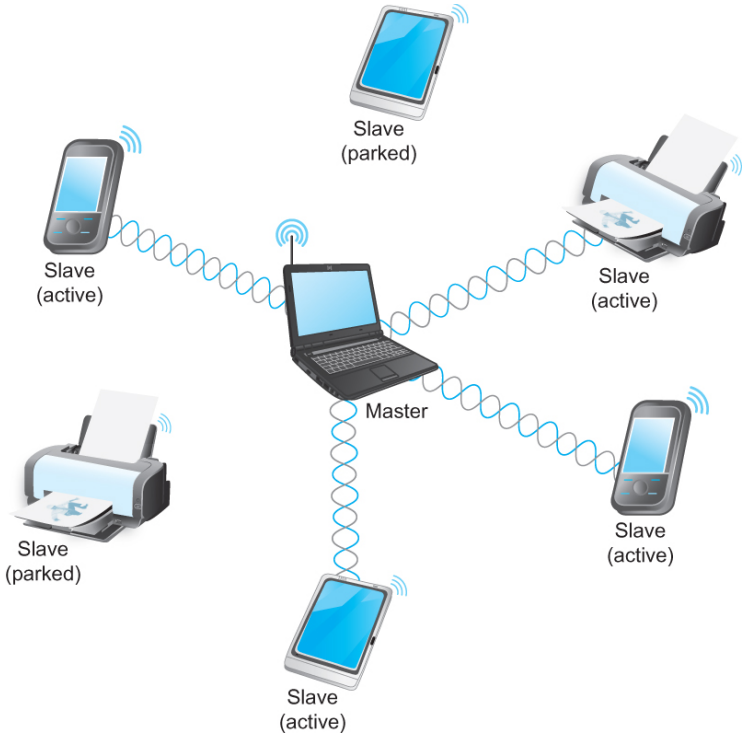
http://xkcd.com/416/

Bluetooth™

- Bluetooth wireless
  - 802.15.1
  - Replace wired connections
    - Connect small, battery-powered devices
  - Short range (<10m)
  - Low bandwidth (1-3 Mbps)
  - 2.45 GHz license exempt band

Bluetooth™

- Piconet
  - Master device
    - Initiates all communication
  - Slave devices
    - Up to seven
    - Only talk to master
    - Can be parked, inactive low-power state
    - Up to 255 parked devices



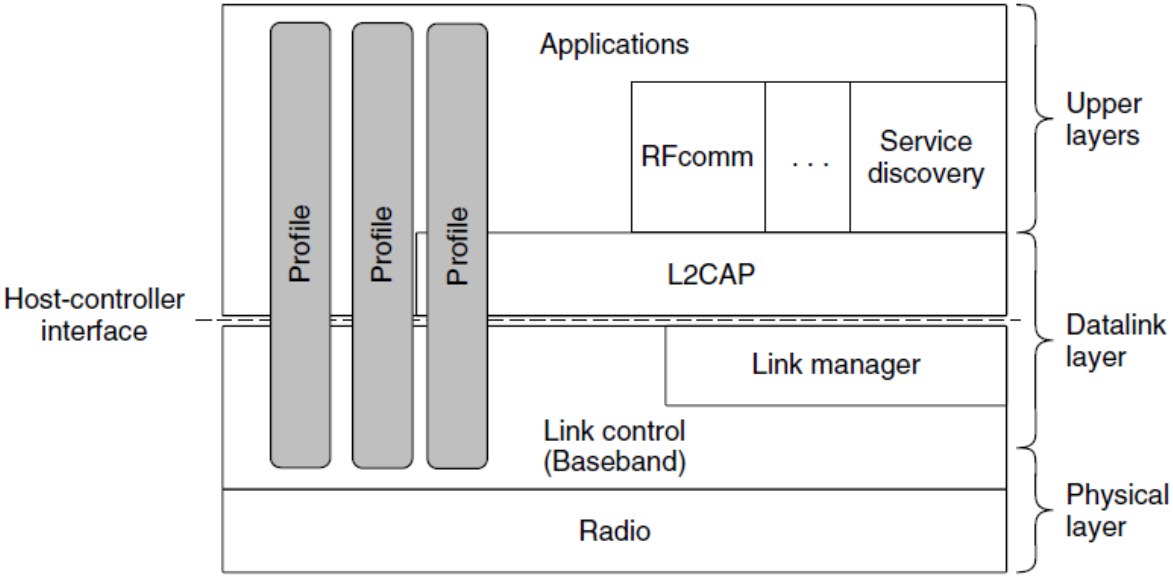
Bluetooth™

- Profiles
  - Bluetooth SIG specifies supported applications as profiles (currently 25):
    - Intercom - two telephones connect as walkie-talkies
    - Headset/hands-free - headset to base station
    - Human interface device - connect keyboard/mouse
    - Networking - share files
    - Dial-up networking - use phone as a modem
    - …
  - Conway's law in action?

"organization which design systems…are constrained to produce designs which are copies of the communication structures of these organization."

Bluetooth™

- Protocol architecture:



Bluetooth™

- Radio layer
  - 79 bands, 1 Mhz each, 2402-2480 Mhz
  - Spread spectrum, frequency hopping
    - 625 µs per slot
    - Master transmits only in odd time slots
    - Slave uses even, but only when asked by master
    - Early version collided with 802.11
      - Bluetooth amended to avoid channels with RF signals
  - Bandwidth
    - Bluetooth 1.0, FSK 1-bit symbol, 1 Mbps
    - Bluetooth 2.0, PSK 2-3 bits symbol, 2-3 Mbps

Mobile telephone system

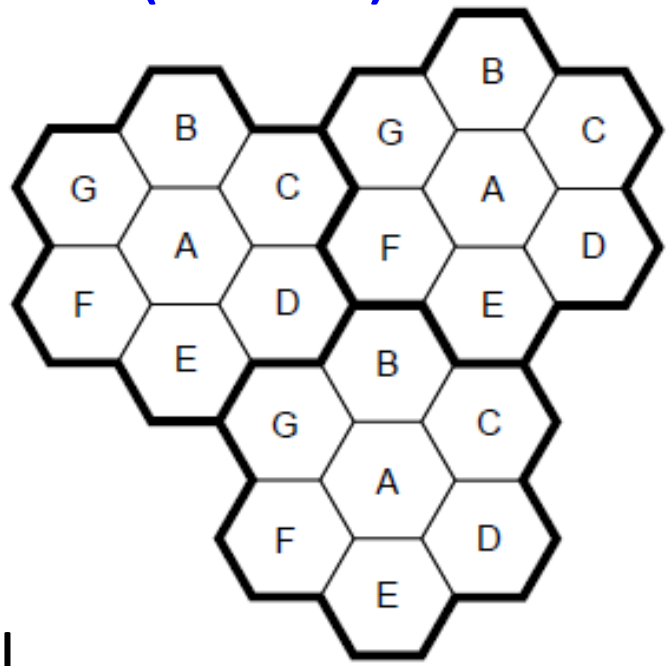
- Generations:
  - 1G, analog voice
  - 2G, digital voice, SMS
  - 3G, digital voice and data
  - 4G, faster data

1G

- Mobile radiotelephones
  - Maritime and military, early 20th century
  - 1946 first car-based system in St. Louis
  - Single channel, push-to-talk
- Improved Mobile Telephone System (IMTS)
  - 1960s
  - One channel send, one channel receive
  - 23 channels, 150-450 Mhz
  - Single hilltop transmitter

1G

- Advanced Mobile Phone System (AMPS)
  - 1980s
  - Divide region into cells
    - 10-20 km
    - Different frequencies per cell
    - Increased capacity
    - Reduced transmit power
  - Device controlled by single cell
    - Handoff when base station notices weak single
  - Frequency division multiplexing
    - Around 45 calls per cell

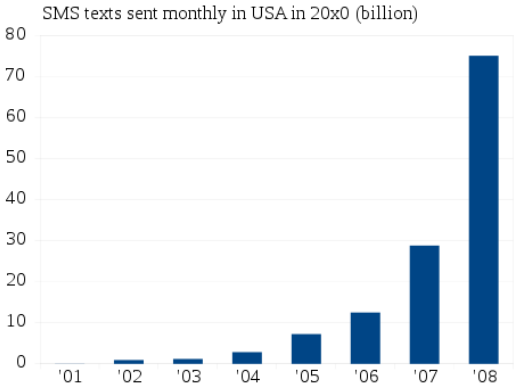


1G

- AMPS
  - Analog transmission
  - Each phone
    - 32-bit serial #, 10-digit phone #
  - To place a call:
    - Sends identify and destination # on access channel
    - Base station responds with allocated idle channel
  - To receive a call:
    - Base station broadcasts packet on paging channel of cell in which phone currently registered
    - All phones listen on paging channel
    - Negotiate idle channel via access channel

2G

- 2nd generation wireless
  - Digital voice
  - 1990s
  - Various systems:
    - GSM (Global System for Mobile communications)
    - CDMA (Code Division Multiple Access)
    - iDEN (Nextel)
  - Short Message Service (SMS)
  - High cell densities
  - GSM, CDMA, EDGE, GPRS



3G

- 3rd generation wireless
  - Digital voice and data
  - Early 2000's
  - ITU's IMT-2000 vision:
    - Go into service in 2000
      - Reality: at least a few years late
    - Frequency of 2000 Mhz all over the world
      - Reality: only China allocated spectrum
    - Bandwidth of 2000 kbps
      - Reality: peak data rates ~200 kbps
  - UTMS, CDMA2000, EVDO

4G

- 4th Generation wireless
  - Fast data
  - Long term evolution (LTE)
    - Verizon, AT&T
      - 12 Mbps downstream, 5 Mbps upstream
  - HSPA+
    - T-Mobile, AT&T
      - 21 Mbps downstream, 6 Mbps upstream
  - WiMAX (802.16)
    - Sprint, Nextel
      - 10 Mbps downstream, 6 Mbps upstream

Summary

- 802.11 WiFi
  - Widely adopted short-range wireless
- Bluetooth
  - Very short range wireless
  - Replacement for wires
- Mobile telephone technologies
  - Multiple generations
  - Every increasing speeds