

1 Introduction

1.1 Protocol performances

G: Total load, S arrival rate of new packets.

1.1.1 Pure ALOHA

If you have data to send, send the data. If the message collides with another transmission, try resending later. On collision, sender waits random time before trying again.

P(k trans. in 2Xs) = (2G/k!) * e^-2G

S = G * P(0) = Ge^-G

1.1.2 Slotted ALOHA

Probability of k packets generated during a slot: P(k) = G^k * e^-G / k! Throughput: P(1) = Ge^-G

1.1.3 CSMA

Goal: reduce the wastage of bandwidth due to packet collisions. Principle: sensing the channel before transmitting (never transmit when the channel is busy).

Non-persistent If channel is busy, directly run back off algorithm.

p-persistent If it is busy, they persist with sensing until the channel becomes idle. If it is idle:

- With probability p, the station transmits its packet
- With probability 1 - p, the station waits for a random time and senses again

Performance of Unslotted nonpersistent CSMA : For a = t_prop/X, the normalized one-way propagation delay. S = G / (G(1+2a) + e^-aG)

Performance of Slotted nonpersistent CSMA : S = aG - aG / (1 - e^-aG + a)

Approach	Idea	Terminals	Signal separation	Advantages	Dis-advantages	Comment
SDMA	segment space into cells/sectors	only one terminal can be active in one cell/one sector	cell structure, directed antennas	very simple, increases capacity per km²	inflexible, antennas typically fixed	used in all cellular systems
TDMA	segment sending time into disjoint time-slots, demand driven or fixed patterns	all terminals are active for short periods of time on the same frequency	synchronization in the time domain	established, fully digital, flexible	guard space needed (multipath propagation), synchronization difficult	standard in fixed networks, together with FDMA/SDMA used in many mobile networks
FDMA	segment the frequency band into disjoint sub-bands	every terminal has its own frequency, uninterrupted	filtering in the frequency domain	simple, established, robust	inflexible, frequencies are a scarce resource	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)
CDMA	spread the spectrum using orthogonal codes	all terminals can be active at the same place at the same moment, uninterrupted	code plus special receivers	flexible, less frequency planning needed, soft handover	complex receivers, needs more complicated power control for senders	higher complexity

1.2 Exercises

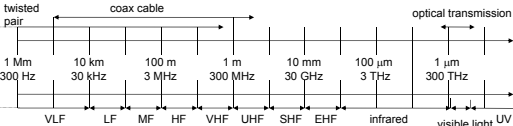
Capacity of a link vs Transmission capacity (=total capacity of all the links). Wire : C_t = min{C_1, C_2} Wireless : d/C_t = d/C_1 + d/C_2 ↔ C_t = (c_1c_2/c_1 + c_2) ALOHA : Aloha channel with infinite number of users gives 94% of idle slots. P(0) = e^-G = 0.94 → G = 0.062

S = P(1) = Ge^-G ≈ 5.8%

G < G_peak = 1 : channel underloaded.

Ration of busy slots occupied by collisions : (1-P(0)-P(1))/(1-P(0)) = 3.3%

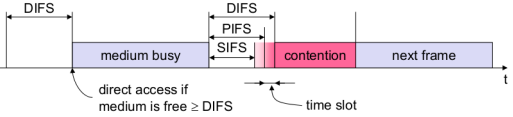
2 WLAN Engineering aspects



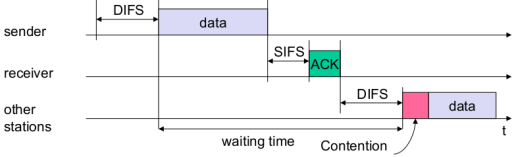
Frequency(f) and wave length(λ), c = 3 × 10^8 m/s : λ = c/f

2.1 802.11

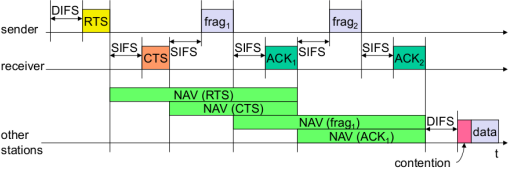
Physical layer : DSSS or FHSS, MAC Layer : best effort asynchronous data service, DCF CSMA/CA (mandatory), DCF with RTS/CTS or PCF (optional)



CSMA/CA Unicast :



DCF with RTS/CTS (with fragmentation) :



MAC address format :

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

2.2 Exercises

Wireless LAN use polling between M workstations and a central access point. Channel at 25Mbps. Stations 100 m away from AP, polling messages 64 bytes long. Packet length : 1250 bytes. No more packet indicated with 64-byte message. Maximum arrival rate λ_max = p_max * Br / Plength p_max = Efective*time / Wholetime = M*(NT_packet + T_poll + T_end + 2t_prop) / (1250*8 / 25*10^6) One station A sends a frame to another station B in a different BSS in an IEEE 802.11 infrastructure network with DCF access method without RTS/CTS. A → AP1

To	From	Type	Dur	A1	A2
1	0	Data	T_d + SIFS + T_A	BSS1	A

API1 → A
To DS From DS Type Duration Addr. 1
0 0 ACK 0 A
API1 → API1 : 1, 1, Data, T_d + S + T_A, API1, B, A
AP2 → API1 : 0, 0, ACK, 0, API1
AP2 → B : 0, 1, Data, T_d + S + T_A, B, BSS2, A
B → AP2 : 0, 0, ACK, 0, BSS2

3 Bianchi model

π, probability of transmission, p, probability of collision, b_i,k stationary probability of state i, k: p = 1 - (1 - π)^{N-1}

$$\pi = \frac{\sum_{i=0}^m b_{i,0}}{1-p} = \frac{b_{0,0}}{1-p} = \frac{2(1-2p)}{(1-2p)(W_{min}+1)+pW_{min}(1-(2p)^m)}$$
$$= \frac{2}{1+W_{min}+pW_{min} \sum_{k=0}^{m-1} (2p)^k}$$
$$b_{i,k} = \frac{CW_i - k}{CW_i} \cdot \begin{cases} (1-p) \sum_{j=0}^m b_{j,0} & i=0 \\ p \cdot b_{i-1,0} & 0 < i < m \\ p \cdot (b_{m-1,0} + b_{m,0}) & i=m \end{cases}$$

3.1 Saturation throughput

$$\tau = \frac{E[\text{Payload Transmitted by user i in a slot time}]}{E[\text{Duration of slot time}]}$$
$$= \frac{P_s P_{tr} L}{P_s P_{tr} T_s + P_{tr} (1 - P_s) T_c + (1 - P_{tr}) T_{id}}$$
$$P_s = \frac{N \pi (1 - \pi)^{N-1}}{1 - (1 - \pi)^N}$$
$$P_{tr} = 1 - (1 - \pi)^N$$
$$T_s = t_{header} + t_{payload} + SIFS + t_{ACK} + DIFS + 2\sigma$$
$$T_c = t_{header} + t_{payload} + SIFS + \sigma$$

3.2 DOMINO Cheating detection

Cheating Method	Detection Test
Frame scrambling	Number of retransmissions
Oversized NAV1	Comparison of the declared and actual NAV values
Transmission before DIFS	Comparison of the idle time after the last ACK with DIFS
Backoff manipulation	Actual Backoff/ Consecutive Backoff
Frame scrambling with MAC forging	Periodic dummy frame injection

4 Antennas & Propagation

Free space propagation, received power: P_R = P_T * A_R / (4 * π * d^2) * η_R with η_R an efficiency parameter, A_R the receiving antenna area. Focusing capability, depends on size in wavelength λ: G_T = 4 * π * η_T * A_T / λ^2 Directional emitter, received power: P_R = P_T * G_T * A_R / (4 * π * d^2) * η_R Free space received power: P_R = P_T * G_T * G_R / (4 * π * d^2) Loss: L = P_T / P_R = ((4 * π * d)^2) / (G_R * G_T * λ^2) c = 3 * 10^8 Parabola: G = (7 * A) / λ^2 Mobnet Decibels : B = 10 log((P / P_0)) Propagation modes Ground Wave: f ≤ 2 Mhz, Sky Wave, Line of Sight: f ≥ 30 Mhz 4.0.1 Line of sight equations Horizon distance d[km] in kilometers, antenna height h[m] and refraction adjustment factor K = 4/3: Optical LOS : d = 3.57 * √h Effective LOS : d = 3.57 * √K h Max LOS distance for two antennas : 3.57 * (√K h_1 + √K h_2)

4.1 Free Space Loss

Free space loss, ideal isotropic antenna:

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f d)^2}{c^2}$$

Free space loss equation can be recast:

$$L_{DB} = 10 \log \frac{P_t}{P_r} = 20 \log(f) + 20 \log(d) - 147.56 dB$$

Free space loss accounting for gain of other antennas:

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{G_r G_t \lambda^2} = \frac{(cd)^2}{f^2 A_r A_t}$$

G_t = gain of transmitting antenna
A_r = effective area of receiving antenna

Categories of noise : Thermal Noise, Intermodulation Noise, Cross-talk, Impulse Noise.

Thermal Noise N_0 = kT (W/Hz)

For signal power S, bitrate R, k = 1.3806 * 10^-23 JK^-1 the Boltzmann constant and T the temperature: E_b / N_0 = S / R / N_0 = S / (kTR)

4.2 Forward Error Correction (FEC)

Redundancy in packets to allow limited error correction at the receiver: used in 802.11a (Convolutional), HSDPA (Turbo Codes) and 802.11n (LDPC).

5 Cellular Networks

For a trunk of N channels, an offered load A = λE[X], X the call duration, Y the call arrival per sec ~ Poisson(λ) and ρ the traffic carried by each channel:

$$P_{\text{Blocking}} = P(\text{Drop a call because busy line})$$
$$= \frac{A^N}{N! \sum_{i=0}^N \left(\frac{A^i}{i!}\right)}$$
$$\rho = \frac{(1 - P_{\text{blocking}})A}{N}$$

Cellular efficiency E = Conversations / (cells * MHz)

Area: A = 1.5R^2 √3

Distance btw. adjacent cells: d = √3R

5.1 Co-channel interference

Co-channel reuse ratio : Q = D / R = √3N with D the distance to the nearest co-channel cell, R the radius of a cell and N the cluster size.

Signal to Interference ratio (SIR) : SIR = S / I = (S / (∑_{i=1}^{i_0} I_i)). With S the desired signal power, I_i the interference power from the i-th interfering co-channel base-station, i_0 the number of co-channel interfering cells.

Signal to Interference plus Noise ratio (SINR) : SINR = S / (I + N_0)

Average received power P_r : P_r = P_0 (d / d_0)^{-α} or P_r (dBm) = P_0 (dBm) - 10α log(d / d_0) with P_0 the power received from a small distance d_0 from the transmitter and α the path loss exponent.

SIR in the corner of a cell : S / I = (R^{-α} / (∑_{i=1}^{i_0} D_i^{-α}))

First interfering layer approximation : S / I = (D / R)^α = ((√3N) / i_0)^α eg. = (D / R)^{2 1/2} for two first layer interferers (cell divided into 3 sectors with directional antennas.)

5.2 Capacity of a cellular network

For B_t the total allocated spectrum and B_c the channel bandwidth:

m = Bt / (Bc * Q^2/3) = Bt / (Bc * ((6/alpha) * (S/T))_min)^(2/alpha) = floor(C/N)

For a cluster size N, N = (i + j)^2 - ij for i, j = 0, 1, 2, ... and number of channels C.

5.2.1 CDMA Capacity: single cell case

For the bitrate R, available bandwidth W, noise spectral density N0, thermal noise eta, received user signal (at base station) S, we have a possible number N of users:

N = 1 + (W/R) / (Eb/N0) - (eta/S)

With a duty cycle delta (Discontinuous transmission mode: takes advantage of intermittent nature of speech):

N = 1 + (1/delta) * (W/R) / (Eb/N0) - (eta/S)

And if we have m sectors, the effective capacity becomes m.N.

5.2.2 CDMA multiple cells

Frequency reuse factor on the uplink f = N0 / (N0 + sum_i U_i N_ai) where N0 = total interference power received from N - 1 in-cell users, U_i = number of users in the i^th adjacent cell and N_ai = average interference power from a user located in the i^th adjacent cell

Average received power from users in adjacent cell N_ai = sum_j N_ij / U_i where N_ij = power received at the base station of interest from the j^th user in the i^th cell

5.3 Ad-hoc Networks

Upper Bound for the Throughput If we have n identical randomly located nodes each capable of transmitting W bits/s. Then the throughput lambda(n) obtainable by each node for a randomly chosen destination is lambda(n) = O(W / (sqrt(n) log n))

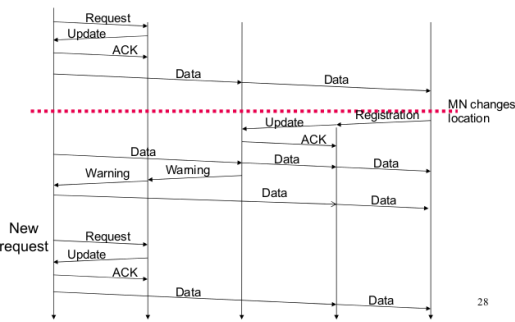
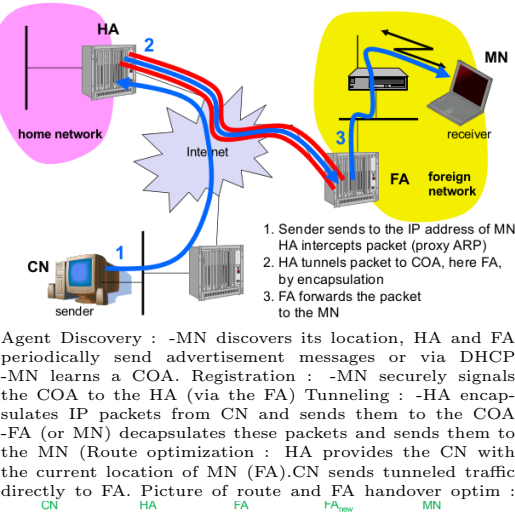
Routing proactive: DSDV, OLSR. reactive: AODV, DSR DSR : Route discovery only when source S attempts to send a packet to destination D, by flooding Route Requests (RREQ). Route maintenance by allowing S to detect when a link is broken with a Route Error message RERR, S try other route in its cache, otherwise route disc. AODV : Similar to DSR but maintains routing tables at the nodes (smaller header). AODV ages the routes and maintains a hop count.

6 Mobile Network Layer

Mobile Network Layer : Transparency, Compatibility, Security, Efficiency, Scalability.

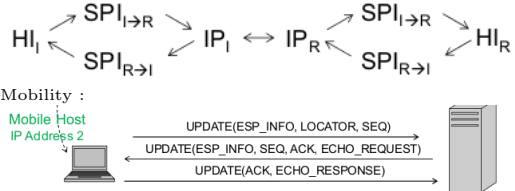
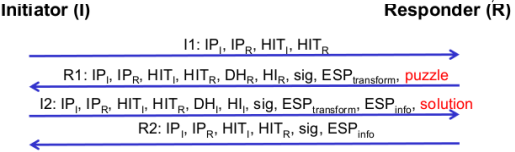
Network Layers Top-down: Application, Transport, (HIP layer), Network, Data-link, Physical.

Mobile IP :Issues : Security(Authentication to FA is problematic), Firewalls, QoS. IPSec can provide CIA by adding layer btwn IP and TCP/UDP. Mobile IPv6 : no FA, COA always co-loc, IPSec, route optim, bidirectional tunnel HA<->COA.



HIP New layer btw IP and transport, integrate security, mobility and multi-homing, decouple name and locator role of IP HI = public key. HIT=h(HI), DH : Diffie-Hellman key

material, sig signature generated with private key of HI_I/R



7 TCP

7.1 Standard

Tahoe Basic TCP. Three duplicate ACK's provoke fast retransmit (resend 1st missing packet), set ssthresh to cwnd/2, cwnd to 1 and provoke slow start.

Reno Three duplicate ACK's provoke fast retransmit, ssthresh to cwnd/2, cwnd to ssthresh + 3 and enter fast recovery.

Fast Recovery Increase cwnd by 1 segment for every received duplicate ACK. (Warning, unlogical: When new ACK is received, cwnd = ssthresh and enter congestion avoidance). If a timeout occurs, set cwnd to 1 and enter slow start.

New Reno Fast Recovery More intelligent fast recovery where you remember the last received ACK.

7.2 Mobile

Indirect TCP (I-TCP) Connection split at FA. Standard TCP on the wire line, wireless optimized TCP on the wifi side: shorter timeout, faster retransmission. Loss of end-to-end semantics, security issues.

Mobile TCP (M-TCP) Split connection at FA. Monitor packets, if a disconnect is detected, report receiver window = 0: sender will go into persist mode and doesn't timeout or modify his congestion window. Preserves end-to-end semantics. Disadv.: wifi losses propagate to the wire network, link-errors pkt loss must be resent by sender, security issues. Summary: only handles mobility errors, no transmission errors.

Snooping-TCP TCP-aware link layer: Split connections, FA buffers and retransmits segments, does not ACK buffered packets (preserves end-to-end semantics). Performance enhancing proxy (content caching, compression): breaks security end-to-end semantics. Link layer retransmission only if error detected (FEC)

Transaction oriented TCP (T-TCP) TCP phases: connection setup, data transmission, connection release. T-TCP combines these steps and only 2-3 packets are needed for short messages. Efficient for single packet transactions, but requires TCP modifications on all hosts.

SIP Application layer protocol

SIP invite : Port number, IP, Preferred encoding. 200 OK : Port number, IP, Preferred encoding. (over TCP or UDP). How to find IP ? User register to a SIP registrar server. Then use SIP proxies to find IP (similar to DNS). RTP is an alternative to SIP. VoIP over IEEE 802.11 DCF : Best effort service.

8 Security

Security Requirements : Confidentiality, Authenticity, Replay Detection, Integrity, Access Control, Jamming Protection.

GSM Shared secret and challenge responses, one-way authentication.

3GPP (Improvements from GSM) Two-way authentication, avoid fake base station, cipher keys and auth data is now encrypted, integrity. Privacy/Anonymity not completely protected however.

9 Privacy

Privacy Related Notions Anonymity, untraceability, unlinkability, unobservability, pseudonymity

Best to worst against information leakage: GPS: no third-party, determined 'alone'. Cell-ID: requires the operator database that is relatively protected (they won't easily mine you). Wireless: requires one or several third-party owned databases that can track you, and it is relatively precise due to short radio range.

9.1 Privacy Metrics

Entropy-Based Anonymity A the anonymity set (set of subjects that might have performed the action), p_x the probability for an external observer that the action was performed by x:

sum over x in A of p_x log(p_x)

Entropy-Based Unlinkability I_1, I_2, sets of elements to be related, p_r, the probability two elements are related for an external observer: sum over R subset I_1 x I_2 of p_r log(p_r)

Expected error-based measure for correctness sum over v in V of p_v x d(v, v_0)

This cheat-sheet is an update by Aubry Cholleton of the amazing work of Julien Perrochet, Christopher Chiche and Tobias Schlatter. GitHub:https://github.com/aubry/mobnet2012

ACO Authenticated Cipher Offset	DECT Digital Enhanced Cordless Telecommunications	FDD Frequency Division Duplex	LEAP Light EAP	PIN Personal Identification Number	SIP Session Initiation Protocol
AIFS Arbitrary Inter-Frame Space	DHCP Dynamic Host Configuration Protocol	FDMA Frequency Division Multiple Access	LSFR Linear Feedback Shift Register	PLCP Physical Layer Convergence Protocol	SPI Security Parameter Index
AMF Authentication and Key management	DH Diffie-Hellman	FEC Forward Error Correction	LF Low Frequency	PMD Physical Medium Dependent	SSR Slow Start Threshold
AOV Ad Hoc On-demand Distance-Vector	DNS Domain Name System	FHSS Frequency Hopping Spread Spectrum	LTE Long Term Evolution	PMK Pairwise Master Key	STA Station
AP Access Point	DQPSK Differential Quadrature Phase Shift Keying	FQDN Fully Qualified Domain Name	MACA-BI MACA By Invitation	PN Pseudo-random Noise	STA Station
AV Authentication Vector	DSDV Destination Sequenced Distance Vector	GFSK Gaussian Frequency Shift Keying	MACA Multiple Access with Collision Avoidance (RTS-CTS(+ACK))	PSN Public Switched Telephone Network	TCP Transmission Control Protocol
ATIM Ad-hoc Traffic Indication Map	DSRC Dedicated Short Range Communications	GMK Group Master Key	MAC Message Authentication Code	PTK Pairwise Transient Key	TDD Time Division Duplex
AUTN Authentication Token	DSR Dynamic Source Routing	GPRS General Packet Radio Service	MAHO Mobile Assisted Handover	QoS Quality of Service	TDMA Time Division Multiple Access
BO BackOff	DSSS Direct Sequence Spread Spectrum	GSM Global System for Mobile Communications	MAP Mobility Anchor Point	RA User Service	TIM Traffic Indication Map
BSS Basic Service Set Identifier	DS Distribution System	HA Home Agent	MD Mobile Device	RADIUS Remote Authentication Dial-In User Service	TKIP Temporal Key Integrity Protocol
CA Collision Avoidance	DTIM Delivery Traffic Indication Map	HCCA HCF Controlled Channel Access	MF Medium Frequency	RERR Route ERROR	TLS Transport Layer Security
CCA Clear Channel Assessment	EHF Extra High Frequency	HCF Hybrid Coordination Function	MH Mobile Host	RFID Radio Frequency Identification	TMSI Temporary Mobile Subscriber Identity
CDMA Code Division Multiple Access	ESP Electronic Product Code	HF High Frequency	MIB Management Information Base	RREQ Route REQuests	TOS Type Of Service
CH Correspondent Host	EAP-TLS TLS over EAP	HIP Host Identity Protocol	MIC Message Integrity Code	RSN Robust Security Network	TSF Timing Synchronisation Function
CN Correspondent Node	EAPOL EAP Over LAN	HIT Host Identity Tag	MN Mobile Node	RTCP Real Time Control Protocol	TTL Time To Live
COA Care-Of Address	EAP-Extensible Authentication Protocol	HI Host Identifier	MSC Mobile service Switching Center	RTM Retransmission Timeout	UHF Ultra High Frequency
CRC packet received CoReCtly	EDCA Enhanced Distributed Channel Access	HMIP Hierarchical Mobile IP	MTSO Mobile Telecommunications Switching Office	RTP Real Time Protocol	UMTS Universal Mobile Telecommunications System
CSMA/CD CSMA with Collision Detection	EHF Extra High Frequency	HSDPA High Speed Downlink Packet Access	NAASS Normalized Average Anonymity Set Size	RSR Request To Send	UV Ultraviolet Light
CSMA/CA Carrier Sense Multiple Access	ESP Encapsulating Security Payload	ICMP Internet Control Message Protocol	NAT Network Address Translation	RVN Rendez-Vous Server	VANET Vehicular Ad-hoc Network
CTS Clear To Send	ESPInfo Contains SPI	IFS Inter Frame Spacing	NAY Net Allocation Vector	RWND Receiver Window	VHF Very High Frequency
CW Contention Window	ESS Extended Service Set	IHL Internet Header Length	OFDMA Orthogonal Frequency-Division Multiple Access	SACK Selective ACKnowledgment	VLF Very Low Frequency
DAMA Demand-Assigned Multiple Access	FAMA Floor Acquisition Multiple Access	IMI International Mobile Subscriber Identity	OLSR Optimized Link- State Routing	SA Security Association	WAP Wireless Access Point
DA Destination Address	FA Foreign Agent	ISI InterSymbol Interference	OT One-Time Password	SDMA Space Division Multiple Access	WEP Wired Equivalent Privacy
DBPSK Differential Binary Phase Shift Keying		KISS Keep It Simple and Stupid	PCF Point Coordination Function	SIFS Super High Frequency	WMN Wireless Local Area Network
DCF Distributed Coordination Function		LDPC Low Density Parity Check	PEAP Protected EAP	SIFS Short Inter Frame Spacing	WPAN Wireless Personal Area Network
			PEP Performance Enhancing Proxies	SIM Subscriber Identity Module	WPA Wi-Fi Protected Access