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.
$P(k \text{ transm. in } 2Xs) = \frac{(2G)^k}{k!} e^{-2G}$
$S = G \cdot P(0) = Ge^{-2G}$

1.1.2 Slotted ALOHA

Probability of k packets generated during a slot: $P(k) = \frac{G^k e^{-G}}{k!}$ 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 $a = t_{\text{prop}}/X$, the normalized one-way propagation delay. $S = \frac{G^{-aG}}{G(1+2a)+e^{-aG}}$

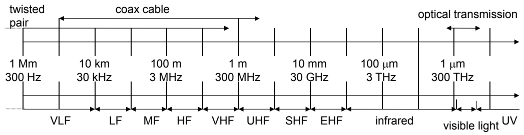
Performance of Slotted nonpersistent CSMA : $S = \frac{aG^{-aG}}{1-e^{-aG}+a}$

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	used in all cellular systems	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	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 : $d/C_t = d/C_1 + d/C_2 \leftrightarrow C_t = (c_1 c_2 / c_1 + c_2)$
ALOHA : Aloha channel with infinite number of users gives 94% of idle slots. $P(0) = e^{-G} = 0.94 \to G = 0.062$
$S = P(1) = Ge^{-G} \approx 5.8\%$
$G < G_{peak} = 1$: channel underloaded.
Ration of busy slots occupied by collisions : $\frac{1-P(0)-P(1)}{1-P(0)} = 3.3\%$

2 WLAN Engineering aspects



2.1 probabilities

π, probability of transmission, p, probability of collision, $b_{i,k}$ stationary probability of state i, k:

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

2.2 Saturation throughput

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

3 Trunk dimensioning

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

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

Cellular efficiency $E = \frac{Conversations}{cells \times MHz}$

4 Cellular Geometry: Hexagons

Area: $A = 1.5R^2\sqrt{3}$
Distance btw. adjacent cells: $d = \sqrt{3}R$

4.1 Co-channel interference

Co-channel reuse ratio : $Q = \frac{D}{R} = \sqrt{3N}$ 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) : $\text{SIR} = \frac{S}{I} = \frac{S}{\sum_{i=1}^{i_0} I_i}$. With S the desired signal **power**, I_i the **interference power** from the ith interfering co-channel base-station, i_0 the **number of co-channel** interfering cells.

Signal to Interference plus Noise ratio (SINR) : $\text{SINR} = \frac{S}{I+N_0}$

Average received power P_r : $P_r = P_0(\frac{d}{d_0})^{-\alpha}$ or $P_r(\text{dBm}) = P_0(\text{dBm}) - 10\alpha\log(\frac{d}{d_0})$ 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 : $\frac{S}{I} = \frac{R^{-\alpha}}{\sum_{i=1}^{i_0} D_i^{-\alpha}}$

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

4.2 Capacity of a cellular network

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

$$m = \frac{B_t}{B_c\frac{Q^2}{3}} = \frac{B_t}{B_c\left(\frac{6}{3^{\frac{\alpha}{2}}}\left(\frac{S}{I}\right)_{\min}\right)^{\frac{2}{\alpha}}} = \lfloor\frac{C}{N}\rfloor$$

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

4.2.1 CDMA Capacity: single cell case

For the bitrate R, available bandwidth W, noise spectral density N_0, thermal noise η, received user signal (at base station) S, we have a possible number N of users:

$$N = 1 + \frac{W/R}{E_b/N_0} - (\frac{\eta}{S})$$

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

$$N = 1 + \frac{1}{\delta}\frac{W/R}{E_b/N_0} - (\frac{\eta}{S})$$

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

4.2.2 CDMA multiple cells

Frequency reuse factor on the uplink $f = \frac{N_0}{N_0 + \sum_i U_i N_{ai}}$ where N_0 = total interference power received from $N-1$ in-cell users, U_i = number of users in thei^{th} adjacent cell and N_{ai} = average interference power from a user located in the i^{th} adjacent cell

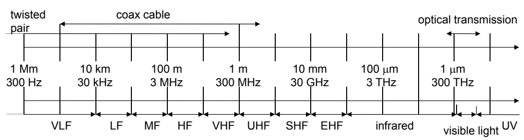
Average received power from users in adjacent cell $N_{ai} = \sum_j N_{ij}/U_i$ where N_{ij} = power received at the base station of interest from the j^{th} user in the i^{th} cell

5 Noise

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

Thermal Noise $N_0 = kT \quad (W/Hz)$
For signal power S, bitrate R, $k = 1.3806\cdot10^{-23}JK^{-1}$ the Boltzmann constant and T the temperature: $\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}$

6 Wireless Misc Stuff



Mobile IP Requirements : Transparency, Compatibility, Security, Efficiency, Scalability.

Mobile IP Issues : Security(Authentication to FA is problematic), Firewalls, QoS

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

6.1 Ad-hoc Netowrks

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 $\lambda(n) = \Theta\left(\frac{W}{\sqrt{n\log n}}\right)$

Routing *proactive*: DSDV, OLSR. *reactive*: AODV, DSR

6.2 Antennas & Propagation

Free space propagation, received power: $P_R = P_T\frac{A_R}{4\pi d^2}\eta_R$ with η_R an efficiency parameter, A_R the receiving antenna area.
Focusing capability, depends on size in wavelength λ: $G_T = 4\pi\eta_T A_T/\lambda^2$
Directional emitter, received power: $P_R = P_T G_T\frac{A_R}{4\pi d^2}\eta_R$
Free space received power: $P_R = P_T G_T G_R(\frac{\lambda}{4\pi d})^2$
Loss: $L = \frac{P_T}{P_R} = \frac{(4\pi d)^2}{G_R G_T \lambda^2}$
$c = 3\cdot10^8$
Parabola: $G = \frac{7A}{\lambda^2}$

Mobnet Decibels : $B = 10\log(\frac{P}{P_0})$

Propagation modes *Ground Wave*: $f \leq 2$ Mhz, *Sky Wave*, *Line of Sight*: $f \geq 30$ Mhz

6.2.1 Line of sight equations

Horizon distance d[km] in **kilometers**, antenna height h[m] and refraction adjustment factor $K = 4/3$:

Optical LOS : $d = 3.57\sqrt{h}$

Effective LOS : $d = 3.57\sqrt{Kh}$

Max LOS distance for two antennas :

$$3.57(\sqrt{Kh_1} + \sqrt{Kh_2})$$

6.3 Free Space Loss

Free space loss, ideal isotropic antenna:

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

Free space loss equation can be recast:

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

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

6.4 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

6.5 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).

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).

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.

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, p_x the probability for an external observer that the action was performed by x:

$$\sum_{\forall x \in A} p_x \log(p_x)$$

Entropy-Based Unlinkability I_1, I_2, sets of elements to be related, p_r, the probability two elements are related for an external observator:

$$\sum_{\forall R \subseteq I_1 \times I_2} p_r \log(p_r)$$

9.2 RFID

Standard tags possibilities : Kill, Sleep, Rename, Block, (Legislation).

Crypto enabled tags possibilities : Tree-approach, synchronization approach, hash chain based approach.

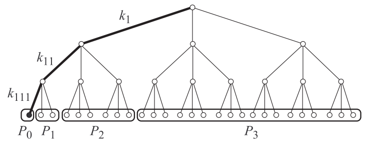
Singulation (determining which tags are present around the reader) Binary tree walking: reader first asks the tags to emit the first bit of their ID. If every answer is 0 (or 1) the reader knows on which side the ID's are. This is done recursively until all ID's are determined. A **collision** is the event where ID's on both sides of a node answer and both sides must be recursed upon.

Privacy zone A tag ID can be changed so that it lies in the *private* zone of the tree. A special device simulates collisions for every query in this area, so an exhaustive search would be required to find a tag.

Pseudonyms Tags can be set to use different ID's that an authorized reader would know how to correlate. To avoid having too complex tags, the reader will generally be responsible for *refilling* the pseudonyms. This will be done in cleartext and assumes an attacker does not always listen.

9.2.1 Key Tree

Tags are the leaves of a tree with branching factor b and depth d, and each edge to arrive to a tag has an associated key: hence, a tag has d associated keys. Maximize branching factor at the first level for strong anonymity.



Anonymity set has minimum size of 1, maximum size of all the tags. Compromising a tag yields all the keys leading to it and permit to partition the other tags (neighbors in the tree share common keys) : P_0 contains the compromised tag, P_1 contains the compromised tag's *brothers* not being in P_0, etc. Tags that belong to larger partitions have better privacy (e.g: tags in P_3 are not distinguishable, attacker only knows they don't use k_1.)

Expected size of the anonymity set for a random tag : for n the total number of tags and $|P_i|/n$ the probability of selecting a tag from partition P_i

$$\bar{S} = \sum_{i=0}^{d} \frac{|P_i|}{n}|P_i| = \sum_{i=0}^{d} \frac{|P_i|^2}{n}$$

Normalized expected anonymity : Using $n = b^d$ and $|P_0| = 1, |P_1| = b-1, |P_2| = (b-1)b, \ldots, |P_l| = (b-1)b^{l-1}$.

$$R = \frac{\bar{S}}{n} = \sum_{i=0}^{d} \frac{|P_i|^2}{n^2} = \frac{b-1}{b+1} + \frac{2}{(b+1)n^2}$$

For **one** tag in P_i, the linkability probability is $1/|P_i| \rightarrow$ global linkability in P_i is $|P_i|\frac{1}{|P_i|} = 1$. For l partitions, the probability that two transactions from a randomly chosen tag are linkable is (with $n = b^d$):

$$\frac{1}{n}\sum_{i=1}^{l}(|P_i|\frac{1}{|P_i|}) = \frac{l}{n}$$

10 Comparisons

This amazing cheat-sheet was brought to you by *Julien Perrochet*, *Christopher Chiche* and *Tobias Schlatter*. Follow us on GitHub: `https://github.com/Shastick/mobnet2012` !

Values of N: 0,1,3,4,7,9,12,13,16,19,21,25,27,28,31,36,37,39,43,48,49,52,57,61,63,64,67,73,75,76,79,81,84,91,93,97,100,103,108,109,111,112,117,124,127,129,133,139,147,148,151,156,169,171,175,192,193,196,217,219,243,244,271,300

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