Many don't have broadband due to out of service and expense. Broadband slow. Disaster recovery network needs rapid deployment, efficient resource/energy, flexibility, resilience. Wireless links are less reliable and vary over time/space. Interference, hidden terminals, exposed terminals, security, intermittent connectivity. Limited battery, bandwidth, processing, storage. Internet Protocol Stack: Application, Transport - process data transfer, Network - routing, Link - neighbor data transfer, Physical - bits on wire. Allows rapid app development through easy reuse/maintenance but constrains optimization/troubleshooting with layering overhead and less transparency.

1 Physical Layer

Sender: bit stream $\implies$ source/channel coding, modulation $\implies$ analog signal. Receiver: analog signal $\implies$ demodulation, channel/source decoding $\implies$ bit stream.

1.1 Signals

Data's physical representation. Function of time/location. Analog continuous, digital discrete. Parameters: period T, frequency $f = \frac{1}{T}$, amplitude A, phase shift ϕ. $A_t \sin(2\pi f_t + \phi_t)$. Fourier transform: every signal can be decomposed as harmonics collection $\frac{c}{2} + \sum_{n=1}^{\infty} a_t \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_t \cos(2\pi n f t)$. Digital need infinite frequencies for perfect transmission.

1.2 Frequency Allocation

$c = \lambda f$, $c = 3 * 10^8 m/s$, wavelength λ, frequency f. Need wide spectrum due to Shannon Channel Capacity: max bit number transmitted per second by physical channel $W \log_2(1 + \frac{S}{I+N})$, frequency range f, signal S, noise(thermal, background radiation) N, interference I.

Conversion: dB - difference between power levels($\frac{P2}{P1}[dB] = 10\log_{10}(\frac{P2}{P1}) \iff \frac{P2}{P1} = 10^{\frac{\frac{P2}{P1}[dB]}{10}}$). dBm/dBW - power level relative to 1mW/1W($P[dBm] = 10\log_{10}(\frac{P}{1mW})$, $P[dBW] = 10\log_{10}(\frac{P}{1W})$).

1.3 Signal Propagation

Transmission range: communication possible, low error rate. Detection range: no communication possible. Interference range: signal not detected, adds to background noise. Straight line propagation in free space. Received power proportional $\frac{1}{d^2}$, distance d. Shadowing, large(small) obstacle reflection(scattering), medium density refraction, edge diffraction, frequency dependent fading.

Path Loss Models: Free space - $P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2 L}$, Two-Ray Ground Reflection - $P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$, Log-Normal Shadowing - $P(d)[dB] = \overline{P}(d)[dB] + X_\sigma$, Indoor - $P_r(d)[dBm] = P_t(d)[dBm] - 10n\log(\frac{d}{d_0}) - \begin{cases} nW(WAF) & nW < C \\ C(WAF) & nW \geq C \end{cases}$, $d_c = \frac{4\pi h_t h_r}{\lambda}$.

Time disperses signal, inter-symbol interference(ISI). Signal reaches receiver phase shifted. Channel characteristics change over time. Quick(slow) changes in received power - short(long) term/fast(slow) fading. Short-term fluctuation due to multipath propagation in/out phase.

1.4 Multiplexing

Multiple use of shared medium in space, time, frequency, code. Guard spaces needed.

Space: Assign each region a channel. Pros - no dynamic coordination and works for analog signals. Cons - inefficient.

Frequency: Separate spectrum into bands. Pros - no dynamic coordination and works for analog signals. Cons - uneven traffic wastes bandwidth and inflexible.

Time: Channel gets spectrum for a time. Pros - one carrier in medium at a time and throughput higher than code. Cons - precise synchronization necessary.

Time/Frequency: Channel gets a band for a time. Pros - better against tapping and frequency selective interference and higher data rates then code. Cons - precise synchronization necessary.

Code: Channels have unique codes and use spectrum simultaneously, implemented by spread spectrum. Pros - bandwidth efficient and no coordination and protects against interference/tapping. Cons - complex signal regeneration and precise power control(main practical challenge).

1.5 Modulation

Digital Modulation: data translated into baseband analog signal. Analog Modulation: shifts baseband signal center frequency up to radio carrier. Antenna size on order of signals wavelength, more bandwidth available at higher frequencies, medium characteristics depend on the signals wavelength.

Digital Modulation: Amplitude Shift Keying(ASK), Pros - simple, Cons - noise susceptible. Frequency Shift Keying(FSK), Pros - less noise susceptible, Cons - requires larger bandwidth. Phase Shift Keying(PSK), Pros - Less noise susceptible and bandwidth efficient and most widely used, Cons - require frequency/pjase synchronization $\implies$ complicates receivers/transmitter. Binary Phase Shift Keying(BPSK), bit value 0 sine, bit value 1 inverted sine, low spectral efficiency, robust so used in satellites. Quadrature Phase Shift Keying(QPSK), 2 bits code a symbol, needs less bandwidth compared to BPSK, often transmission of relative phase shift - Differential QPSK(DQPSK). Quadrature Amplitude Modulation(QAM), combines amplitude/phase modulation, possible to code n bits a symbol, 2^n discrete levels, used in modem.

1.6 Spread Spectrum

Frequency dependent fading wipes out narrow band signals for interference duration. Spread narrow band signal into broad band using special code. Coexistence of several signals without dynamic coordination, tap-proof.

Direct Sequence Spread Spectrum(DSSS): XOR signal with pseudorandom number(chipping sequence), generate signal with wider frequency range - spread spectrum.

Frequency Hopping Spread Spectrum(FHSS): Discrete sequence of carrier frequency changes determined via pseudo random number sequence. Fast Hopping, several frequencies per user bit, Pros - More narrowband interference immune, Cons - tight synchronization increases complexity. Slow Hopping, Several user bits per frequency, Pros - cheaper, Cons - less narrowband interference immune. Frequency selective fading/interference limited to short period, simple implementation, uses only small spectrum portion at a time.

2 Link Layer and IEEE 802.11(WiFi)

2.1 MAC Layer

Services: Framing - encapsulate datagram into frame(adding header/trailer) and physical addresses used in frame headers to identify source/dest, coordinate shared medium access, reliable delivery between physically connected devices, error detection/correction, flow control.

Multiple Access Protocols: Determine how stations share channel - single shared communication channel so multiple simultaneous transmissions by nodes is interference. synchronous vs. asynchoronous, centralized vs. decentralized, efficiency and fairness.

Taxonomy: Channel Partitioning - divide channel into pieces and allocate piece to node for exclusive use (TDMA, FDMA, CDMA). Random Access - allow collisions and recover. Taking Turns - nodes with more to send take longer turns.

Random Access Protocols: Transmit at full channel data rate, no a priori coordination, multiple transmitting nodes collide, specifies how to detect/recover from collisions via delayed retransmissions, (Pure ALOHA, Slotted ALOHA, CSMA, CSMA/CD).

Pure ALOHA: Transmit whenever message ready, retransmit when collision.

Slotted Aloha: Time divided into slots, transmit at beginning of next slot, retransmit in future slots on collision. Success by N node $Np(1-p)^{N-1}$. Optimal $p = \frac{1}{e}$ as $N \to \infty$. Collision duration half that of pure.

Carrier Sense Multiple Access(CSMA): Listen before transmit, transmit if channel idle, defer transmission if channel sensed busy. Persistent CSMA - retry immediately with probability p when channel idle(may cause instability). Non-persistent CSMA - retry after random interval. Collisions can occur when nodes not hear each other, propagation delay and distance determine collision probability.

Collision Detection(CSMA/CD): Collisions detected and transmissions aborted, reducing channel wastage, persistent or non-persistent, compare transmitted/received signals in wired LANs. Difficult in wireless LANs - receivers cannot send/receive simultaneously and receivers channel condition different from sender's.

2.2 IEEE 802.11

Characteristics: Advantages - Very flexible and Ad-hoc networks without previous planning possible and no wiring difficulties and more robust against disasters. Disadvantages - typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium and less reliable

Design Goals: Global/seamless operation, low power for battery, no special licenses needed, robust transmission technology, simplified spontaneous cooperation at meetings, easy to use, simple management, wired networks investment protection, security, privacy, safety, transparent higher layers, location aware.

Infrastructure: Station(STA) - terminal with access mechanisms to wireless medium and radio contact to AP. Access Point(AP) - station integrated into wireless LAN and distribution system. Basic Service Set(BSS) group of stations using same AP. Portal bridge to other wired networks. Distribution System - interconnection network to form one logical network(Extended Service Set - EES) based on several BSSs.

Ad-Hoc: Direct communication within a limited range. Station(STA) - terminal with access mechanisms to wireless medium. Independent Basic Service Set(IBSS) - group of stations using same network.

MAC: Access mechanisms, fragmentation, error control, encryption. MAC Management: synchronization, roaming,Management Information Base(MIB), power management. Physical Layer Convergence Protocol(PLCP): clear channel assessment signal(carrier sense). Physical Medium Dependent(PMD): modulation, coding. PHY Management: channel selection, MIB. Station Management: All management function coordination.

2.2.1 Physical Layer

Security: Limited, WEP insecure, SSID. Connectionless/always on. QoS - Best effort with no guarantees (unless polling used). Manageability: Limited with no automated key distribution and symmetric encryption. 802.11 flavors differ in physical. 802.11a increases data rate of 802.11b but limits range.

WLAN IEEE 802.11b: Availability many products/vendors. Pros many installed systems/vendors and available worldwide on free ISM-band. Cons heavy interference with no service guarantees and relatively low data rate.

WLAN IEEE 802.11a: Availability some products/vendors. Pros - less crowded free 5 GHz ISM-band on simple systems with higher data rates. Cons - shorter range.

WLAN IEEE 802.11n: Multiple input multiple output (MIMO) so 20MHz/40MHz bands. Availability many products/vendors. Pros free dual ISM-band on simple system with higher data rates. Cons - interference.

2.2.2 MAC Layer

802.11 Distributed Function Wireless MAC (DFWMAC): Mandatory Asynchronous Data Service - best effort exchange of data packets that supports broadcast/multicast. Optional Time-Bounded Service - implemented using Point Coordination Function(PCF). ACK/retransmission for reliable unicast, not for broadcast/multicast. Mandatory Distributed Coordination Function(DCF) - collision avoidance via randomized back-off with minimum distance between packets and ACKs. Optional RTS/CTS - avoids hidden terminal. Optional PCF - AP polls terminals according to list. Priorities defined through inter-frame spaces, no guarantee. Short Inter Frame Spacing(SIFS) - highest priority for ACK/CTS/polling response. PCF IFS(PIFS) - medium priority for time-bounded service using PCF. DCF IFS(DIFS) - lowest priority for asynchronous data service.

Collision Avoidance (CSMA/CA): CSMA/CD impossible to detect collision using half-duplex radios and hidden terminal. Both physical/virtual carrier sense. Nodes hearing RTS/CTS stay silent for transmission duration. Once channel idles nodes wait a randomly chosen duration before transmit attempt. Physical carrier sense has threshold. Virtual carrier sense use Network Allocation Vector(NAV) updated by overheard RTS/CTS/DATA/ACK.

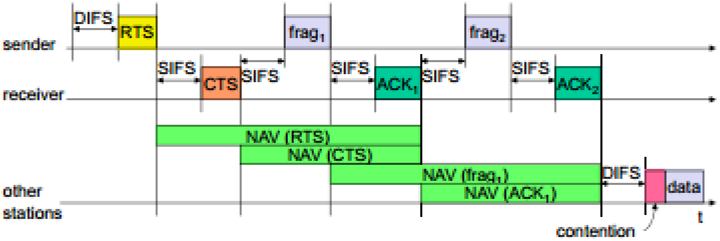
Hidden Terminal: B can communicate with both A/C, A/C can't hear each other. When A transmits to B C cannot detect transmission. Collision occurs at B when transmits. Hidden sender C needs to defer. MACA: A first sends Request-to-Send(RTS) to B which responds by sending Clear-to-Send (CTS). C overhears CTS and keeps quiet for transfer duration indicated in RTS/CTS. SINR more important in transmit range than carrier sense range which must be greater than interference range for RTS/CTS to work.

Reliability: Wireless links error prone, high loss rate detrimental to transport layer performance. B ACKs data packet from A, A retransmits when no ACK.

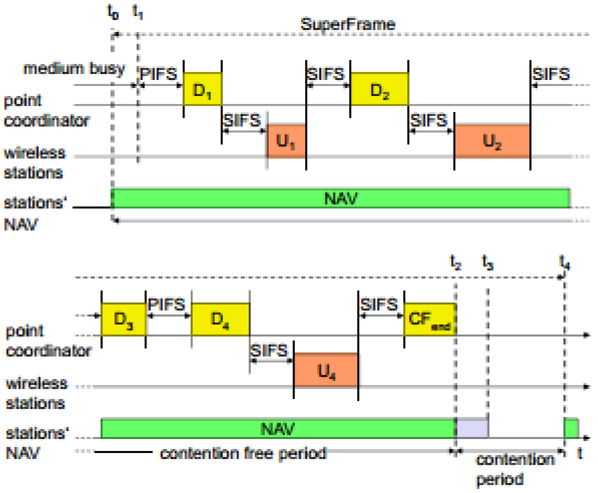
Backoff Interval: Reduce collision probability, choose a in the range [0, Contention Window(CW)], count down when medium idle, suspend when medium busy, transmit when 0. Large CW $\implies$ large overhead, small CW $\implies$ many collisions, CW chosen dynamically depending on collision occurrence, doubled up to upper bound when no CTS in respons, more collisions $\implies$ longer waiting time to reduce collision, restore CW to CW_{min} on success.

MACAW MILD: Update CW by exponential increase linear decrease. Successful transfers reduce CW by 1, avoid wild CW oscillations when many nodes contend for channel.

Overhead: DIFS, random backoff, ACK, SIFS, RTS/CTS handshake often disabled, header. Improve by fragmentation since increasing data transmission increases collision probability.



DFWMAC-PCF:



2.2.3 Management

Association/Reassociation: integration into LAN, roaming -change networks by changing AP, scanning - active network search. Synchronization: timing. Power Management: periodic sleep without missing messages by frame buffering, traffic measurements. Management Information Base(MIB) - manage/read/write. Always associating with strongest signal could swamp AP or thrash between channels. Management packets aren't authenticated, can be spoofed.

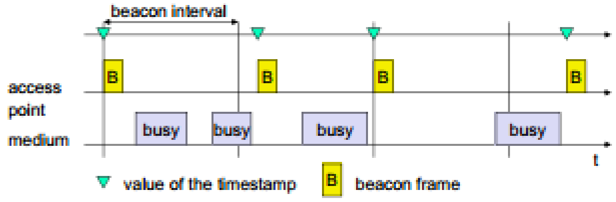
Scanning: Passive - move to each channel and listen for beacons. Active: Move to each channel and send Probe Requests to solicit Probe Responses from network.

Association: Request, Response, Data.

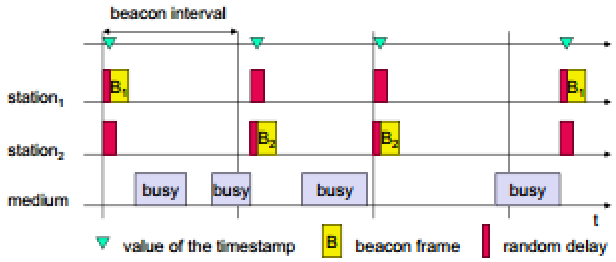
Roaming: Scan, Reassociaton request/response, AP signals new station to distribution system which updates location information and informs old AP to release resources.

Reassociation: Request, Verify Previous Association, Response, Send Buffered Frames, Data.

Infrastructure Synchronization:



Ad-Hoc Synchronization:



Power Management: Switch not needed transceiver off. Timing Synchronization Function (TSF) stations wake up at same time. Infrastructure - Traffic Indication Map(TIM) lists unicast receivers while Delivery Traffic Indication Map(DTIM) lists broadcast/multicast receivers. Ad-hoc - Ad-hoc Traffic Indication Map(ATIM) announces receivers by stations buffering frames so no AP(more complicated) and ATIM collisions possible.

3 Network Layer and MobileIP

Routing Protocols: Path selection for forwarding. Network Layer Protocol: Conventions for addressing conventions, packet format/handling. Control Protocols: error reporting, router signaling.

Functions: protocols in every host/router. Path Determination - algorithms route packets from source to dest. Switching - move packets from routers input to output. Call Setup - some network architectures require router call setup along path before data flows.

3.1 IP Addresses

IP Address: 32-bit identifier for host/router interface. Interface: connection between host/router and physical link, router have multiple interfaces, host has one. Subnet part high order bits, host part low order bits. Subnet - device interfaces with same subnet part of IP address and can physically reach each other without router. Classless InterDomain Routing(CIDR) - subnet portion of address arbitrary length with format a.b.c.d/x where x bits in subnet portion. Host get IP address hard-coded by system admin or Dynamic Host Configuration Protocol(DHCP) - dynamically get address from server. Network gets subnet from provider ISP address space. Hierarchical Addressing - route aggregation allows efficient routing information advertisement and more efficient routes. ISPs get address block from Internet Corporation for Assigned Names and Numbers(ICANN) - allocates addresses and manages DNS and assigns domain names and resolves disputes.

3.2 Virtual Circuit vs. Datagrams

Service Abstraction: guaranteed bandwidth, inter-packet timing preservation(jitter), loss-free/in-order delivery, congestion feedback to sender for channel. Most important network layer abstraction.

Virtual Circuits: Paths behaves like telephone circuit performance-wise and network actions. Call setup/teardown for calls before data flows, packets carries VC identifier(not destination host ID), every router path maintains state for passing connections, link/router resources(bandwidth/buffers) allocated to VC to get circuit-like perf. Initiate Call, Incoming Call, Accept Call, Call Connected, Data Flow Begins, Receive Data.

Datagram(Internet): No call setup at network layer. no network-level concept of connection(no state), packets routed using destination host ID, packets between same source-dest pair take different paths. Send Data, Receive Data.

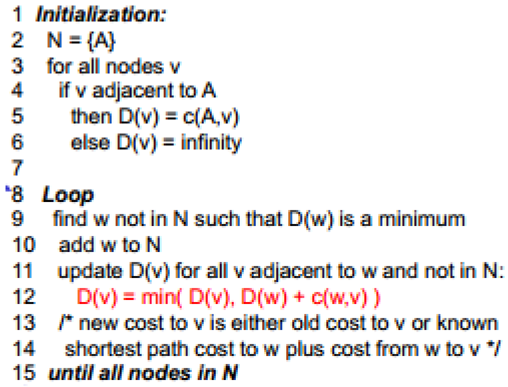
Internet: Data exchanged among computers, elastic service with no strict timing req, smart end systems (computers) can perform cong. control and error recovery, simple inside network complexity at edge, many link types with different characteristics so uniform service difficult.

ATM: Evolved from telephony, human conversation has strict timing/reliability requirements need for guaranteed service, dumb end systems (telephones),complexity inside network.

3.3 Routing Algorithms

Determine good path from source to dest, graph nodes are routers, graph edges are physical links with cost(delay, dollar, congestion level). good path means minimum cost but other defs possible. Max-flow algorithms used to find largest bandwidth path. Global: all routers have complete topology and link cost info(link state - LS). Decentralized: router knows link cost to physically connected neighbors , iterative computation process of, exchange of info with neighbors (distance vector - DS). Static: routes change slowly. Dynamic: routes change quickly with periodic update in response to link cost changes.

Link-State(Dijkstra's Algorithm): net topology and link costs communicated via link state broadcast, all nodes have same info, computes least cost paths(routing table) from one node to all other nodes, after k iterations know least cost path to k dest.s. $c(i,j)$ - link cost from node i to j and cost infinite if not neighbors, $D(v)$ - current path cost value from source to dest. v, $p(v)$ - predecessor node along path from source to v, N - set of nodes with known least cost path.

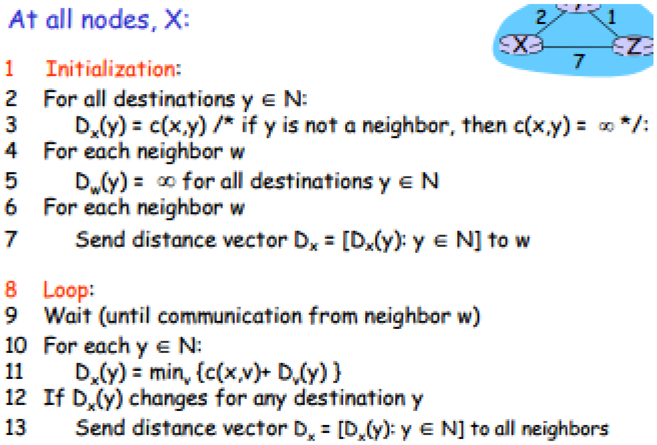


```
Initialization:
  N = {A}
  for all nodes v
    if v adjacent to A
      then D(v) = c(A,v)
      else D(v) = infinity

Loop
  find w not in N such that D(w) is a minimum
  add w to N
  update D(v) for all v adjacent to w and not in N:
     D(v) = min( D(v), D(w) + c(w,v) )
  /* new cost to v is either old cost to v or known
   shortest path cost to w plus cost from w to v */
until all nodes in N
```

n nodes E links needs $O(nE)$ msgs each, $O(n^2)$ algorithm. Node can advertise incorrect link cost but each node computes own table. Troubleshoot by comparing local topologies. ISPS use this.

Distance Vector: Iterative - continues until no nodes exchange info and self-terminating, Asynchronous - nodes not exchange info/iterate in lock step. Distributed - nodes communicate with neighbors. Each node x maintains cost $c(x,v)$ for each neighbor v, distance vector $D_x = [D_x(y) : y \in N]$ containing xs cost estimate to all destinations, distance vectors for each neighbor v $D_v = [D_v(y) : y \in N]$. Basic operation(Bellman-Ford) - $D_x(y) = min_v(c(x,v) + D_v(y))$ $y \in N$.



```
At all nodes, X:

Initialization:
For all destinations y ∈ N:
    $D_x(y) = c(x,y)$ /* if y is not a neighbor, then $c(x,y) = \infty$ */:
For each neighbor w
    $D_w(y) = \infty$ for all destinations y ∈ N
For each neighbor w
    Send distance vector $D_x = [D_x(y): y \in N]$ to w

Loop:
Wait (until communication from neighbor w)
For each y ∈ N:
    $D_x(y) = \min_v \{c(x,v)+ D_v(y) \}$
If $D_x(y)$ changes for any destination y
    Send distance vector $D_x = [D_x(y): y \in N]$ to all neighbors
```

Good news travels fast, bad news travels slow - count to infinity problem. Poisoned Reverse: If Z routes through Y to X Z tells Y distance to X infinite(Y wont route to X via Z). Convergence time varies, may be routing loops. Node can advertise incorrect path cost and each nodes table used by others so error propagate thru network. BGP uses this.

Hierarchical Routing: Cant store 200 million dests in routing tables, exchange would swamp links. Internet is network of networks so each network admin controls routing in own network. Aggregate routers into autonomous systems(AS), routers in same(different) AS run same(different) intra-AS routing protocol. Gateway Routers: run intra-AS routing with other routers in AS and inter-AS routing with other gateway routers.

3.4 MobileIP

Motivation: Routing - physical subnet xhange implies IP address change for topological correct address or needs special entries in routing tables. Routing table change for forwarding doesn't scale. Adjust host IP address is impossible to find mobile system, DNS updates take long time. TCP connections break. Security problems.

Requirements: Transparency - mobile end-systems keep IP address and communications continue after interruption with fixed network connection point changed. Compatibility - support same layer 2 protocols as IP so no current end-systems and router changes required and mobile end-systems communicate with fixed systems. Security - registration messages authenticated. Efficiency/scalability: little additional mobile system messages required with world-wide support of large number of mobile systems.

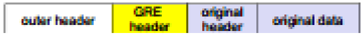
Terminology: Mobile Node(MN) - system that change connection point to network without changing IP address. Home Agent(HA) - router in MN home network that registers MN location and tunnels datagrams to COA. Foreign Agent(FA) - default router in MN foreign network of the MN that forwards tunneled datagrams to MN. Care-of Address(COA) - chosen address of current tunnel end-point for at FA/MN which is actual MN location from IP view point. Correspondent Node(CN)- communication partner.

Data Transfer: Sender sends to MN IP address, HA intercepts packet(proxy ARP) and tunnels to COA by encapsulation FA forwards the packet to MN. Receiver sends to sender IP address, FA default router. Not most efficient due to indirection but scales due to one contact point.

Integration: Agent Advertisement - HA/FA periodically send messages into physical subnets where MN listens and reads COA from FA advertisement. Registration(limited lifetime) - MN signals COA to HA via the FA and HA acknowledges MN via FA which are secured by authentication. Advertisement - HA advertises MN IP address (like fixed systems) and routers adjust entries which are stable for long time (HA responsible for a MN over long time) and packets to MN are sent to HA independent of COA/FA changes.

3.5 Encapsulation

Encapsulate one packet into another as payload like IPv6 in IPv4(6Bone), Multicast in Unicast(Mbone), IP-in-IP tunnel between HA/COA, minimal encapsulation, Generic Record Encapsulation(GRE). Optional Minimum encapsulation: avoids identical field repetition and only applicable for unfragmented packets.



3.6 Miscellaneous

Optimization: Triangular Routing - sender sending packets via HA to MN has high latency and network load. Solutions - HA informs sender about HA location for direct tunneling but big security problems. FA Change - packets on-the-fly during change lost so new FA informs old FA to forward remaining packets and release resources.

Reverse Tunneling: MN sends to FA, FA tunnels packets to HA by encapsulation, HA forwards the packet to the receiver(standard case). Router accept only topological correct addresses(firewall, encapsulate by FA) and solves problems with multicast and TTL(TTL in home network correct but MN too far away from receiver) and enjoy home network services. Does not solve problems with firewalls since reverse tunnel can abused to circumvent security(tunnel hijacking) and optimization since packets tunneled via HA to sender(double triangular routing). Backwards compatible and extensions implemented easily and cooperate with current extensionless implementations ans agent advertisements carry reverse tunneling requests.

IPv6: security integrated and not add-on, registration authentication included, COA assigned via auto-configuration and every node has address autoconfiguration, no separate FA since all routers perform advertisement which can be used instead of special agent advertisement, colocated addresses, MN signals a COA sender directly so sending via HA not needed(automatic path optimization), soft hand-over without packet loss between two subnets, MN sends new COA to old router which encapsulates/forwards all packets for MN and forwards to new COA, authentication granted.

Problems: Security - authentication with FA since it belongs to another organization and no key management/distribution protocol standardized in the Internet due to patent and export restrictions. Firewalls - cannot use with firewalls and special set-ups needed(reverse tunneling). QoS - tunneling makes it hard to give packet flows special treatment.

Security: Integrity - any changes to data between sender/receiver detected by receiver. Authentication - sender address really address of sender and all data received really data sent by sender. Confidentiality - only sender/receiver read data. Non-Repudiation - sender cannot deny sending data. Traffic Analysis - traffic and user profiles creation not possible. Replay Protection - receivers detect message replay.

Security Architecture: Multiple partners negotiate security mechanisms to setup security association, all partners choose the same parameters and mechanisms. Authentication-Header - guarantees packet integrity/authenticity and asymmetric encryption schemes guarantee nonrepudiation. Encapsulation Security Payload(ESP) - protects confidentiality between communication partners. Mobile Security Association for registrations gives parameters for MN/HA/FA. Extended registration authentication. Replay registration prevention with time stamps - 32 bit time stamps + 32 bit random number, and nonces - 32 bit random number(MH) + 32 bit random number(HA).

Key Distribution: FA has security association with HA, MN registers new binding at HA which answers with a new session key for FA/MN.

Micro-Mobility Support: Efficient local handover inside foreign domain without involving HA which reduces control traffic on backbone, needed for route optimization. Cellular IP, HAWAII, Hierarchical Mobile IP (HMIP). Efficiency, Security, Scalability, Transparency, Manageability.

4 Routing in Mobile Ad Hoc Network(MANET)

Infrastructure-less, multi-hop, mobility changes routes, easy/fast deployment. Military environments with soldiers, tanks, planes. Personal area networking with cell phone, laptop, ear phone, wrist watch. Civilian environments with taxi cab network, meeting rooms, sports stadiums, boats, small aircraft. Emergency operations like search-and-rescue, policing and fire fighting. Assumption: fully symmetric environment where all nodes have identical capabilities and responsibilities. Route stability despite mobility, energy consumption. Some protocols invented for MANET, others adapted from previous wired protocols. No protocol good in all environments so some try adaptive protocols. Proactive Protocols - determine routes independent of traffic. Reactive Protocols - maintain routes when needed. Route Discovery Latency - proactive lower since routes maintained constantly while reactive higher since route from X to Y found only when X sends to Y. Route Discovery/Maintenance Overhead - reactive lower overhead since routes determined only if needed while proactive higher(not necessarily) due to continuous route updating. Depends on the traffic/mobility patterns. Proactive(reactive) better static(dynamic) link overhead.

Flooding: Sender broadcasts packet P to all neighbors, each node forwards P to neighbors, sequence numbers avoid forwarding same packet more than once, P reaches destination D if reachable, D does not forward P. Pros - simplicity. Cons - high overhead. Many perform flooding of control packets used to discover routes instead of data packets. Control packet flooding overhead amortized over data packets between consecutive control packet floods.

Dynamic Source Routing(DSR): Node S wants to send to node D so initiates route discovery by flooding Route Request(RREQ), each node appends own identifier when forwarding RREQ, potential collision. D sends a Route Reply(RREP) on route appended to RREQ reversed if links bidirectional. Unidirectional(asymmetric) links need route discovery for RREP piggybacking. IEEE 802.11 MAC need bi-directional links for ACKs. Default uses first route since easy to implement and indicates performance. Routes cached by any means which speeds up route discovery and reduces RREQ flooding. Source Routing - entire route included in packet header for forwarding. Route Error(RERR) sent when forwarding fails which updates route cache. Time/mobility invalidates caches which adversely affects performance(TCP) since several stale routes tried. Pros - reduces route maintenance overhead and caching reduces route discovery overhead while yielding many routes. Cons - packet header grows with route length due to source routing and RREQ floods reach all nodes and RREP from neighbors collide/storm and caches polluted with stale RREP, need invalid cache purge like static/adaptive timeouts based on link stability. Reduce RREPs by discriminating CW.

Ad Hoc On-Demand Distance Vector Routing(AODV): Maintaining routing tables at nodes to rid source routing. At most one next-hop per destination at a node(DSR have several routes for a destination). Nodes set up reverse path towards the source which assumes symmetric(bi-directional) links(asymmetric links due to different transmission power or interference). Intermediate nodes RREP for more recent path than one known to sender(destination sequence numbers), new RREQs assigned higher destination sequence numbers. Reverse(forward) path routing table entry purged after a timeout(*active_route_timeout*) interval even if route still valid but unused. All active neighbors informed when next hop link breaks. RERR increments destination sequence number N, source initiates discovery with destination sequence number at least N, destination set sequence number to N if lower. Reactive failure to receive MAC-level ACK after several retries. Proactive neighbors periodically exchange hello message whose indicated link failure. Sequence numbers prevent loop formation in RREQ when RERR lost. Expanding Ring Search - RREQs sent with small Time-to-Live(TTL) field to limit propagation then larger TTL when no RREP(DSR includes similar optimization).

Destination-Sequenced Distance Vector(DSDV): Nodes maintain routing tables with next hop, cost metric, destination sequence number used to avoid loop formation. Nodes periodically forward routing table to neighbors and increments/appends sequence number attached to route entries created for this node. $S(X)/S(Y)$ destination sequence number for node Z as stored at node X and sent by node Y respectively. $S(X) > S(Y)$ X ignores Y's routing information. $S(X) = S(Y)$ and cost of Y smaller than X X sets Y as next hop to Z. $S(X) < S(Y)$ X sets Y as next hop to Z and $S(X)$ updated to equal $S(Y)$.

DSDV proactive so best no mobility. DSR(AODV) aggressive(selective) so best in low(high) mobility. DSR header bad or large networks. DSDV amortizes discovery cost so best for many destinations.

5 Routing in Wireless Mesh Networks

Improve network capacity for stationary nodes. Per-link delivery ratio product and bottleneck link throughput ignores hop count. End-to-end delay ghanges with network load as queue lengths vary causing oscillations.

Hop Count: Maximizes hop distance traveled which minimizes signal strength and maximizes loss ratio while higher Tx Power causes interference. Many shortest routes and intermediate loss rates.

ETX: predicted number of data transmissions to send packet over link, path ETX is sum of ETX link values over path. Expected probability of successfully received and acknowledged transmission is $d_f d_r$ where $d_f(d_r)$ forward(reverse) delivery ratio. ETX= $\frac{1}{d_f d_r}$. Delivery ratios affect throughput, detects asymmetry, uses(assumes) precise link loss measurements for finegrained decisions between routes, penalizes routes with more hops which have lower throughput due to inter-hop interference so assumes equal loss rates over links, minimize spectrum use which maximizes system capacity(reduce power) where nodes spends less time retransmitting. Values measured by broadcasting link probe packets with average period τ(jittered by 0.1τ), delivery ratio $r(t) = \frac{count(t-w,t)}{\frac{w}{\tau}}$ where $count(t-w,t)$ is probes received during window w and $\frac{w}{\tau}$ is probe number expected. Each probe contains this information. More throughput advantage with smaller probe packets since larger packets have higher corruption chance, underestimates ACK delivery ratios and overestimates total transmission number per packet. Probes interfere with data so can significantly decrease throughput so piggyback on data for different probe sizes and accurate delivery rate. Pros - better than hop count, accounts for bi-directional loss rates, easily incorporated into routing protocols. Cons - only considers link loss rates and may not be best metric for mobility/power-limited/adaptive rate(multi-rate)/interference while predictions not always accurate and incur overhead and doesn't incorporate interaction between routing/ETX change causing oscillation and sub-optimal paths.

Single radio nodes can not transmit/receive simultaneously, two radios tune to non-interfering channels, increased robustness due to diverse frequency fading characteristics, tradeoff between range and data rate.

Weighted Cumulative Expected Transmission Time(WCETT): Multi-Radio Link-Quality source routing (MR-LQSR) - link-state source routing protocol. Assume no power constraints, little mobility, nodes have multiple 802.11 radios tuned to noninterfering channels with fixed assignments. Nodes discovers/measure neighbors links, floods information through network. Maximize throughput by prefering high-bandwidth/low-loss links, selecting short channel diverse paths. Expected Transmission Time(ETT) - ETT= $\frac{S}{B}$ETX with packet size $S$and link bandwidth B so transmission lasts $\frac{S}{B}$. Lower ETT implies better link. Use link sum as path metric(SETT) which favors short paths but ignores channel diversity. Interference reduces throughput which is lower if many links on same channel so path metric should be worse for non-diverse paths. Assumption all links on same channel interfere. Group links on path using channel, add link ETTs in each group, bottleneck group is with largest sum so too many links is poor quality(Bottleneck Group ETT - BG-ETT) which favors high-throughput/channel-diverse but ignores short paths, largest sum is path metric so lower value implies better path. WCETT = $(1-\beta)$SETT+β BG-ETT, Higher(lower) β more preference to channel diversity(shorter paths). Loss rate measured using broadcast probes link ETX updated every second, bandwidth estimated using periodic packet-pairs updated every 5 minutes. Provides performance gain even with one radio, channel diversity more important for shorter paths, throughput better for lower β, better than HOP/ETX, gains more prominent over shorter paths and light loads, optimal β depends on load. Passive inference of loss rate and channel bandwidth, metrics measure link quality before changes which cause oscillation/sub-optimal performance and not globally good, need metrics for traffic impact on link quality and backoff overhead, WCETT assumes all links on path interfere(unrealistic), performance affected by more than routing metrics.

6 Introduction to Sensor Networks

Large number of low-cost/power, multifunctional, small sensor nodes consisting of sensing, data processing, communicating components. Node positions need not be pre-determined, protocols/algorithms self-organizing. Failure prone, frequent topology changes, broadcast communication whereas(most ad hoc networks use point-to-point), limited computation/memory, no global ID. collect/route data to sink which communicates with task manager via Internet/Satellite. Design factors: fault tolerance, scalability, production costs, operating environment, network topology, hardware constraints, transmission media, power consumption.

Hardware Constraints: Sensing Unit - composed of two subunits(sensors and analog to digital converters - ADCs). Processing Unit - manages collaboration procedures to carry out tasks. Transceiver Unit - connects to network. Power Units - most important. Location Finding System - routing techniques and sensing tasks require high accuracy location knowledge. Mobilizer - move sensors. Matchbox-sized module, consume extremely low power, operate in high volumetric densities, have low production cost, dispensable, autonomous, adaptive. Sink/sensor protocol stack has Power/Mobility/Task Management Plane spanning application, transport, network, data link, physical.

Topology: Pre-Deployment and Deployment Phase thrown in mass or placed one by one in sensor field. Post-Deployment Phase - topologies prone to frequent changes. Re-Deployment Phase addition new nodes poses and reorganize network.

Environment: Micro-sensors, onboard processing, wireless interfaces feasible at very small scale can monitor phenomena up close which enables spatially/temporally dense environmental monitoring. Embedded Networked Sensing reveal previously unobservable phenomena.

Transmission Media: Industrial Scientific and Medical(ISM) Bands 915 MHz ISM band widely suggested and most countries offer license-free communication. Infrared license-free and interference robust but requires line of sight between sender/receiver. Ultra Wide Ban(UWB).

Power Consumption: Limited power source (¡0.5 Ah 1.2V), lifetime strong dependent on battery lifetime, power consumption divided into three domains(sensing, communication, and data processing).

Large scale sensor networks require richer inter-node communication for In-network storage/processing/routing. Need point-to-point routing to scale to flows and different densities. Design goals are simple(minimum state), scalable(low control overhead, small routing tables), efficient(low routing stretch), and robust against node failure.

Greedy Perimeter Stateless Routing(GPSR): DSR/AODV suffer from out of date state and Hard to scale, use geographic information for routing by assuming every node knows position(x,y) and keep less network state in the network and requiring fewer update messages. Select neighbor geographically closest destination as next hop so keep state for neighbors. Beaconing mechanism provides all nodes with neighbors MAC/positions and minimize costs by piggybacking. Right Hand Rule - next edge traversed is sequentially counterclockwise about node x from edge (x, y) when arriving at x from node y(traverse exterior region in counter-clockwise edge order). Planar Graph - graph in which no two edges cross. Relative Neighborhood Graph(RNG) - $\forall w \neq u, v : d(u, v) \leq max[d(u, w), d(v, w)]$. Gabriel Graph(GG) - $\forall \neq u, v : d^2(u, v) < [d^2(u, w) + d^2(v, w)]$. Use greedy forwarding whenever possible, resort to perimeter routing when greedy forwarding fails, resume greedy forwarding when we are closer to destination. Implementation support MAC-layer feedback ,interface queue traversal, promiscuous network interface use, graph planarization. Pros - Low routing state and control traffic so scalable and handles mobility. Cons - GPS location not available everywhere and geographic distance doesn't correlate with network proximity and overhead in location registration/lookup and planarization algorithm limitations(works under unit disk model which doesnt hold in practical network and hard to handle mobility snd reduces network connectivity) and localization expensive and nodes need to update location somewhere.

Beacon Vector Routing(BVR): Create routing gradient from connectivity information rather than geography, assign positions based on connectivity and greedily forwarding on this space. Deriving Positions - r beacon nodes $(B_0, B_1 \ldots, B_r)$ flood network so node qs position $P(q)$ is hops to each beacon $P(q) = (B_1(q), B_2(q), \ldots, B_r(q))$ and q advertises coordinates using k closest beacons $C(k, q)$ so nodes know neighbors/beacon positions. Forwarding - $dist_k(p, q) = \sum_{i \in C(k,q)} \omega_i |B_i(p) - B_i(q)|$ choose neighbor to reduce $dist_k(*, q)$ to reach q but enter Fallback Mode(route towards beacon closer to destination) when no neighbor improves and scoped flood when Fallback fails and beacon reached. Each entry beacon vector has sequence number periodically updated by beacon between timeout so non-beacons nominate themselves as beacons when beacons $< r$. Store location mapping at beacons with hashing (H: nodeid → beaconid) so node k wanting to be destination periodically publishes coordinates to beacon $b_k = H(k)$ and route to k with lookup request to b_k with coordinates cached. Can achieve performance comparable to true positions, beaconing overhead grows slowly with network size (less than 2% nodes for larger networks), great benefit for deriving coordinates from connectivity, average stretch consistently low(< 1.1), robust to obstacles unlike geographic forwarding, costly floods but low density resilient, coordinates stable with few/small, sustained high throughput. Simple/robust/scalable/efficient so using connectivity for deriving routes is good for low density/obstacles, implementation indicates can work in real settings. Routing/transmission stretches high and no delivery guarantee with scoped flooding since may collide from multiple sources.

7 Delay Tolerant Networks(DTN)

Rural area(buses, mail trucks, infostations), Mobile routers with disconnection, Sensor networks, Deep space, Underwater, etc... Internet exists some end-to-end path with RTT At most a few seconds(typically less than 500 ms) and use retransmission for reliability and packet switching right abstraction. DTN May not exist e2e path with contact connectivity intermittent and arbitrary with large delay (hours, days) and high hink error and low capacity with resource budget limiting transmissions and different network architectures. Issues in naming, addressing, location management, dynamic graph routing, scheduling, security, applications, etc... Routing on time-varying topology have links unpredictable so use any/all links. Inputs topologies, traffic demands, vertex buffer limits, mobility patterns to determine route/schedule to optimize some metric(delay, throughput, resource consumption).

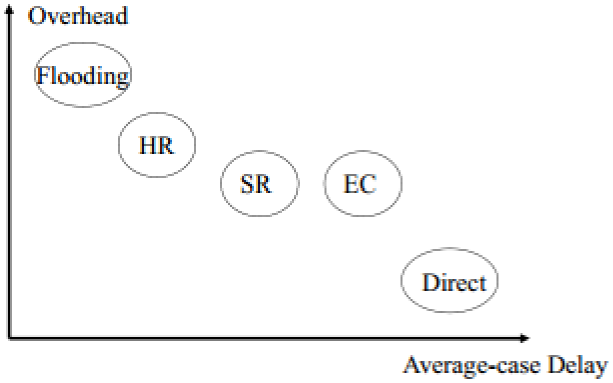
Flooding: Node forwards any non duplicated msg to any other node encountered. Pros - low delay. Cons - high transmission overhead and replicates messages after copy delivered.

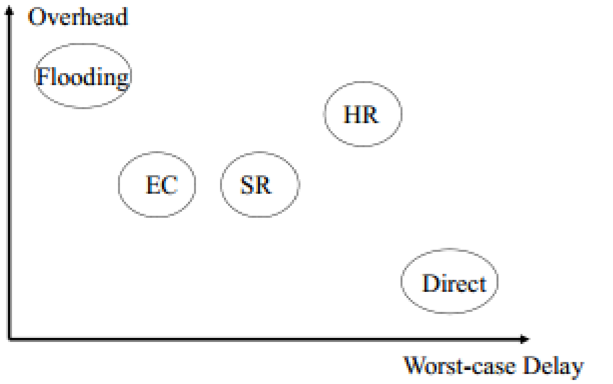
Direct Contact: Source holds data until contact with destination. Pros - minimal resources. Cons - long delay.

Simple Replication: Source sends r identical copies over first r contacts which Relay directly to destination so low average-case delay.

History-Based Replication: Nodes track message delivery probability for another node and replicates to r highest ranked relays. Record contact duration and inter-contact time for contact probability. Replicates messages after copy delivered. Simple relays relay once while history relays relay multiple times.

Erasure-Coding Based Replication: Split/distribute messages to more contacts to increase delivery chance instead of seeking good contacts. Same bytes number flow in network now in coded blocks which makes order insignificant. Given replication factor r any $\frac{1}{r}$ blocks reconstruct original data. Leveraging more contacts reduces worse-case latency risk of outlier bad contacts. Use first rk relays each get $\frac{1}{k}$ copy so $\frac{k}{rk}$ relays to succeed. $k \geq 1$ reatled to coding algorithm. Delay distribution converges to constant when k large so almost assured constant delay. Low success rate with small deadlines, high success rate for longer deadlines(due to lower 99th percentile latency distr), few very low delay cases.





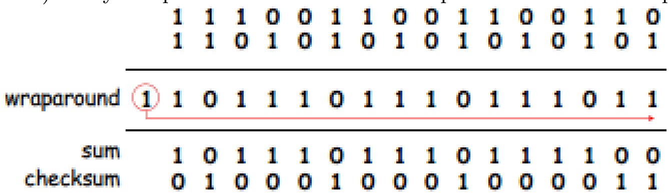
Enhancements: Optimize common case and guarantee worst-case. Replicate currently based on first r contacts but Could use delivery probability for selection, replicate quantity currently every node selected replicated equal amount but could use delivery probability for deciding amount, adapt coding parameters based on delivery probability and performance requirement, apply network coding, adapt/quantity/when to replicate based on message urgency.

8 Transport Layer

Provides logical communication between app processes on different hosts, runs in end systems. Send Side - breaks app messages into segments and passes to network layer. Rcv Side - reassembles segments into messages and passes to app layer. Internet uses TCP/UDP. Network Layer - logical communication between hosts. Transport Layer - relies/enhances network layer services. UDP - unreliable/unordered so no-frills extension of best-effort IP. TCP - reliable/in-order delivery with congestion/flow control and connection setup. Delay/bandwidth guarantees unavailable. Demultiplexing at Rcv - deliver received segments to correct socket. Multiplexing at Send -gather/envelope data from multiple sockets with header. Host receives IP datagrams with source/destination IP address, 1 transport-layer segment, source/destination port number. Host uses IP addresses and port numbers to direct segment to socket. Connectionless - create sockets with port numbers identified by (dest IP address, dest port number) and checks destination port number then directs UDP segment to socket with port number when host receives segment thus IP datagrams with different source IP addresses and port numbers directed to same socket. Connection-Oriented - TCP socket identified (source IP address, source port number, dest IP address, dest port number) used by receiver to direct segment to socket so server supports many simultaneous sockets and have different sockets for each client(non-persistent HTTP have different sockets for each request). Client Client- Create socket with socket() system an connects socket to server address using connect() and send/receive data using read()/write(). Server Side - create socket with the socket() and bind socket to address using bind()(Internet server socket address consists of port number on host machine) and listen for connections with listen() and accept connection with accept()(blocks until client connects with server and send/receive data.

UDP: no frills bare bones Internet transport protocol with best effort service so segments may lost/reordered to app. Connectionless - no handshaking between sender/receiver and segments handled independently. No connection establishment decreases delay, simple with no connection state at sender/receiver, small segment header, no congestion control so blast away as fast as desired. Used for streaming multimedia apps(loss tolerant rate sensitive), DNS, SNMP. Add reliability at application layer.

Checksum: Detect errors(flipped bits) in segment. Sender -treat segment as 16-bit integers sequence for 1s complement sum and puts checksum value into checksum field. Receiver - compute checksum and check if equals checksum field value (NO - error detected, YES - no error detected). Carryout from most significant bit added to result(ignores endianness). Easy computation with incremental update and endian-independent.



```
            1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
            1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

wraparound 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1

       sum  1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 0
  checksum  0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1
```

Unreliable channel characteristics determines reliable data transfer protocol complexity, checksum + NACK/ACK over eror channel, sequence no. + timeout over lossy channel. Stop-and-Wait works with stinky performance utilization $U_{sunder} = \frac{\frac{L}{R}}{RTT+\frac{L}{R}}$, L bits packet length, R bps transmission rate, network protocol limits physical resource use. Pipelining - sender allows multiple unacknowledged pkts in flight so increase sequence number range with buffering sender/receiver.

Go-Back-N: k-bit seq number in pkt header, window up to N consecutive unacked pkts allowed. ACK(n) - ACKs all pkts up to including seq number n(cumulative ACK) and may receive duplicate ACKs. Time each in-flight pkt with timeout(n) - retransmit pkt n and all higher seq number pkts in window.

Selective Repeat: Receiver individually acknowledges correctly received pkts and buffers pkts in-order delivery to upper layer. Sender resends pkts for which ACK not received(timer for each unACKed pkt) with N consecutive seq numbers window and limits unAcked pkts' seq numbers. Sender - send pkt when data from above and next available seq number in window and resent packet n and restart timer when timeout(n) and mark pkt n received and advance window base to next unACKed seq number if n smallest unACKed packet when ACk(n) in $[sendbase, sendbase+N]$. Receiver - send ACK(n) when $[rcvbase-N, rcvbase-1]$ and buffer out-of-order or deliver in-order (also deliver buffered) then advance window to next not-yet-received pkt when pckt n in $[rcvbase, rcvbase+N-1]$ and ignore otherwise.

Reliable Data Transfer Mechanisms: Checksum - detect bit errors. Timer - detect packet loss at sender. Sequence Number - Detect packet loss/duplicates at receiver. ACK(NACK) - inform sender pkt (incorrectly) received. Window/Pipelining - increase throughput and adapt to receiver buffer size and network congestion. NACK speeds up timeouts.

Congestion Control: Too many sources sending too much data too fast for network to handle. Manifestations through lost packets(buffer overflow at routers) and long delays(queuing in router buffers). One router with infinite buffers and no retransmission see large delays at maximum achievable throughput. one router with finite buffers and lost packet retransmission see more work(retrans) for given goodput and unneeded retransmissions since link carries multiple pkt copies. λ_{in} original data, λ'_{in} plus retransmissions, goodput($\lambda_{in} = \lambda_{out}$), perfect transmission only when loss($\lambda'_{in} > \lambda_{out}$), retransmission of delayed packet makes λ'_{in} larger (than perfect case) for same λ_{out}. Multihop paths with timeout/retransmit see upstream transmission capacity wasted when packet dropped. End-End - no explicit network feedback so congestion inferred from end-system observed loss/delay (approach taken by TCP). Network-Assisted - routers provide feedback to end systems with single bit indicating congestion (SNA, DECbit, TCP/IP ECN, ATM) or explicit sned rate(XCP).

TCP: Point-to-point with one sender/receiver, reliable/in-order byte steam with no message boundaries, pipelined with congestion/flow control that set window sizes, send/receive buffers, full duplex data so bi-directional data flow in same connection(maximum segment size MSS), connection-oriented with handshaking (exchange control msgs) inits sender/receiver state(sequence numbers, buffers, RcvWindow) before data exchange, flow controlled so sender not overwhelm receiver. Three Way Handshake - client host TCP SYN segment to server which specifies initial seq number with no data then server receives SYN and replies with SYNACK segment allocating buffers and specifies initial seq. number then client receives SYNACK and replies with ACK segment which may contain data(SYNCookie allows server allocate state after client's ACK). Closing Connection - client sends TCP FIN segment to server then server receives FIN and replies with ACK and closes connection and sends FIN then client receives FIN and replies with ACK and enters timed wait to respond with ACK to FINs then server receives ACK connection closed. Handles simultaneous FINs with modification. Seq. numbers are byte stream numbers of segment data's first byte. ACKs are seq number of next byte expected(cumulative). TCP spec doesnt say how to handle out-of-order segments so up to implementer. Timeout value longer than varying RTT, too short - premature timeout and unnecessary retransmissions, too long - slow reaction to segment loss. SampleRTT -measured time from segment transmission until ACK receipt (ignore retransmissions since ACKs ambiguous). EstimatedRTT = $(1-\alpha)$EstimatedRTT+αSampleRTT, exponential weighted moving average so influence of past sample decreases exponentially fast($\alpha = 0.125$). EstimatedRTT large variation needs larger safety margin, estimate of how much SampleRTT deviates from EstimatedRTT($\beta = 0.25$) with DevRTT= $(1-\beta)$DevRTT+β|SampleRTT−EstimatedRTT| then set TimeoutInterval=EstimatedRTT+4DevRTT. Sender - create segment with seq number of first data byte in segment then start timer if not already running(timer for oldest unacked segment) when data from app and retransmit segment then restart timer when timeout and if acknowledges previously unacked segments then update known acks and start timer for outstanding segments when ack. Receiver - wait up to 500ms for next segment but if no next segment then send ACK when in-order segment arrive with expected seq number and all data up to number ACKed or immediately send single cumulative ACK fro both in-order segments when in-order segment arrive with expected seq number and another segment has ACK pending or immediately send duplicate ACK next expected byte when out-of-order segment arrive with higher-than-expect seq. number(gap detected) or immediately send ACK if segment starts at gap's lower end when segment arrive that fills gap. Time-out period incurs long delay before resending lost packet so detect lost segments via duplicate ACKs since sender sends segments back-to-back have many duplicate ACKs for lost segment. Assumes segment after ACKed data lost on 3 ACKS for same data, Fast Retransmit - resend segment before timer expires. Flow Control - sender wont overflow receivers buffer by transmitting too much too fast with speed-matching service by matching sending rate drain rate and rcvr includes RcvWindow value in segments so sender limits unACKed data to RcvWindow and guarantees receive buffer doesnt overflow. Congestion Control - sender transmit as fast as possible without congesting network and decentralized so senders probe bandwidth by implicit feedback of ACK(segment received, network not congested, increase sending rate) or lost segment (assume loss due to congestion, decrease sending rate) since available bandwidth changes depending on other connections and limits rate by unACKed bytes in pipeline (LastByteSent-LastByteAcked $\leq$ cwnd, cwnd dynamic function of perceived network congestion) and min(cwnd,rwnd) with $rate = \frac{cwnd}{RTT}$ roughly so timeouts cut cwnd to 1 and 3 duplicate ACKs cut cwnd in half(less aggressively since some segments getting through) also Slow Start increases cwnd exponentially fast at connection start or following timeout at 1 MSS then quickly ramp up to respectable rate by doubling cwnd every RTT through incrementing cwnd by 1 for every ACK and Congestion Avoidance increase cwnd linearly when cwnd > ssthresh by increase cwnd by 1 MSS per RTT to approach congestion slower than slow start implemented by $cwnd = cwnd + \frac{MSS}{cwnd}$ for each ACK received(Additive Increase Multiplicative Decrease - AIMD)so in summary sender in slow-start(congestion-avoidance) phase with window grows exponentially(linearly) when CongWin <(>) Threshold and Threshold := CongWin/2 and CongWin := Threshold(1 MSS) when triple duplicate ACK(timeout) occurs.

9 TCP in Wireless Networks

9.1 Transmission Errors

Random Errors: Cause fast retransmit unnecessary reduces congestion window and throughput. Cause timeout when multiple packet lost with TCP-Reno and Selective ACK(SACK) to lesser extent.

Burst Errors: Window worth of data lost when wireless link unavailable for extended duration from passing truck or driving through tunnel. Timeout results in long idle time and slows start, which unnecessarily reduces congestion window to 1 MSS and ssthresh to 1/2.

Hide Loss: Link level Mechanisms, Split Connection Approach, TCP-Aware Link Layer, TCP-Unaware Approximation of TCP-Aware Link Layer. Find Loss Reasons: Explicit Notification, Receiver/Sender-Based Discrimination.

Link Layer Schemes: Recover wireless losses using FEC code, retransmission, and adapting frame size. Hide wireless losses from TCP sender so Link layer modifications needed at both ends of wireless link so TCP need not modified. Reliable link layer beneficial to TCP if provides in-order delivery and TCP retransmission timeout large enough to tolerate additional link level retransmits delays. Most widely used since easy and most links already do.

Split Connection Approach: End-to-end TCP connection broken into one connection on wired part and one over wireless part. Hides transmission errors from sender with responsibility at base station and if specialized transport protocol on wireless needs wireless host modification. Advantages - local/fast error recovery due to shorter RTT on wireless link and BS-MH connection optimized independent of FH-BS connection with different flow/error control two connections and good performance using appropriate BS-MH protocol since standard TCP on BS-MH performs poorly when multiple packet losses occur per window (timeouts occur on BS-MH connection, stalling during the timeout) but improve through selective acks. Disadvantages - end-to-end semantics violated since ack delivered to sender before data delivered to receiver and not useful if data/acks traverse different paths (both don't go through BS) and Extra copy/storage required at BS so not widely used.

TCP-Aware Link Layer: Snoop Protocol retains local recovery and end-to-end semantics, BS soft state instead of hard state. BS buffers packets to allow link layer retransmission and retransmit on wireless link when dupacks received from MH and prevent fast retransmit at TCP sender by dropping dupacks. If wireless link level delay-bandwidth product < 4 packets then simple(TCP-unaware) link level retransmission scheme suffices since can deliver lost packet without 3 dupacks from TCP receiver since delay-bandwidth product small. Hides wireless losses from the sender and requires BS modification(network-centric approach). Advantages - high throughput achieved and improved using selective acks with local recovery from wireless losses and fast retransmit not triggered at sender despite out-of-order link layer delivery and End-to-end semantics retained with soft state at base station so state loss affects performance not correctness. Disadvantages - link layer at base station needs TCP-aware and not useful if TCP headers encrypted (IPsec) and can't use if TCP data/acks traverse different paths (both don't go through BS).

TCP-Unaware Approximation of TCP-Aware Link Layer: Delayed Dupacks Protocol imitates Snoop without BS TCP-aware. TCP receiver delays dupacks (third and subsequent) when out-of-order packets received intended to give link level retransmit time. Pros - recovery from transmission loss without triggering TCP sender sender. Cons - Recovery from congestion losses delayed.

Explicit Notification: BS tags dup-ack with Explicit Congestion(Loss) Notification ELN(ECN) if wireless(congestion) related loss. Preferred over receiver/sender discrimination.

Receiver-Based Discrimination - Receiver guess packet loss cause. Sends notification to TCP sende when receiver believes packet loss due to errors. On notification TCP sender retransmits the packet without reducing congestion window.

Sender-Based Discrimination: Sender determine packet loss cause. Don't reduce congestion window if packet loss due to errors.

9.2 Mobility

Hide mobility from TCP sender or Make TCP adaptive to mobility. 0(1)-second Rendezvous Delay - beacon arrives 0(1) second after cell boundary crossed. TCP performance degradation in overlapping cells due to encapsulation/forwarding delay during handoff, additional degradation in non-overlapping cells due to packet sender loss and idle time. When MH the TCP receiver then after handoff complete sends 3 dupacks to sender which this triggers fast retransmit(special notification could replace dupacks), when MH is TCP sender fast retransmit after handoff completion. Smooth Handoffs - avoid packet loss with sufficient overlap between cells or buffer packets at BS and forward the packets to new BS before packets discarded after short interval.

M-TCP: Avoid shrinkage in the congestion window due to fast retransmit. Sender enters persist mode when new ack received with receivers advertised window 0 and doesn't send data before persist timer expires. exits persist mode when positive window advertisement received. RTO/cwnd same as before. Splits TCP connection into two logical parts with independent flow control as I-TCP. BS doesn't send to FH unless BS received ack from MH wich maintains end-to-end semantics. BS withholds ack for last byte acked by MH which sent with window advertisement 0 if MH moves away (handoff in progress) to put sender FH into persist mode. Last ack not withheld if BS doesn't expect other acks from MH when BS has no other unacked data buffered locally, prevents sender timeout at end of transfer(burst of data). Route changes with mobility and new route more congested so starting full speed after handoff not obvious right.

Mobile Ad Hoc Networks: Improve throughput by informing TCP of route failure by explicit message and let TCP know when route repaired with probing or explicit notification. Reduces repeated TCP timeouts/backoff. Route discovery returns cached route and TCP sender transmits after timeout but cached route broken, process repeats until good route found. Caching speeds route repair but incorrect repairs degrades caching performance so need mechanisms for determining when cached routes stale. Caching reduce route discovery overhead but low cache accuracy cause routing overhead gains offset by TCP performance loss due to multiple time-outs

10 Emergent Network

Wireless Communication: Medium: Radio frequency, Light(Images (e.g., QR code), Videos), Sound. Different medium has different characteristics and poses different challenges.**Climbing the Frequency Mountain** from 100KHz to 60 GHz to PetaHz. Light communication: directional interference-free wireless links.

1. QR Code. **UPC**1. Wallace Flint first suggested an automated checkout in 1932 2.UPC bar code formats developed in the 40s, 50s, 60s. 3.Grocery Industry adopted the UPC (based on an IBM proposal) April 3, 1973. 4.With computerized scanning, inventory, With computerized scanning, inventory, UPCs are ubiquitous on every product! **What is a QR Code?**. QR stands for Quick Response, Matrix or two dimensional bar code, It is a more advanced bar coding system, Very fast readability Instant access. Eliminates the memorization of URLs. **History**. Invented by Denso wave in 1994 for tracking vehicles during manufacture. Now is one of the most popular 2-D barcode. **Applications**. URL rediction . Virtual stores. Code payment . Web login. Encryption. **Uses for QR codes** 1. Advertisements 2. Guided tours 3. Creative ice breakers 4. Packing and organization of products and shipping 5. Uses in education: worksheet for students to cooperate with another student. Scavenger Hunts (help students solve problems and find correct answers.). Contact information for parents and students(post in classroom for studnets and parents to obtain phone number, email address and class website, etc). Notes: an easy way to post notes. Assignments: post homework assignments in codes for students to scan before leaving class. Hints/tutorials to assist on problems.**QR codes in Health and PE Body video** circulatory system is an organ system that passes nutrients (such as amino acids, electrolytes and lymph), gases, hormones, blood cells, etc. to and from cells in the body to help fight diseases, stabilize body temperature and pH, and to maintain homeostasis. Traveling Resource: Students are constantly on their devices. QR code readers save all searches and are able to be accessed at any time. **QR is very easy to create. Customizable. Use your imagination Risks**. Redirected URLs may host javascript, which can exploit vulnerabilities. QR code reader may allow use of the camera, Internet, read/write contact data, GPS, browser history, etc. In Russia, a malicious QR code caused phones that scanned it to send premium texts at a fee of US 6 each. **Open Issues**. Increase data rates. Resilient against blurring and viewing angle Blur: pixels bleed into each othe Perspective distortion: squeezed or stretched. Automatic rate adaptation.

2. Dhwani : PeerPeer Secure Acoustic NFC. **Near Field Communication** (NFC). Communication between physically proximate devices.. Key Advantage: No network configuration effort.. Association by proximity: devices are connected to each other by virtue of proximity. Used in contactless payments, short data transfer, ticketing, healthcare etc. NFC - Limitations . Low levels of penetration of NFC hardware today . NFC standard does not define security at the physical layer. **We can enable secure NFC-like communication in today's devices:**

2.1. **Dhwani - acoustic NFC system.** Uses phones speaker and microphone. Software only can be a downloadable app. Currently supports upto 2.4 Kbps data rate over 1 KHz bandwidth. 2.JamSecure secure communication. Information-theoretic approach to security. Security at physical layer by jamming and self-interference cancellation at the receiver. **Acoustic Communication - Challenges:** RF Communication: 1) Antenna frequency response is flat. 2) Multipath (in s) 3) Channel is defined interference is limited. Acoustic Communication: 1) Speaker-mic frequency selectivity 2) Echo (in ms) 3) Channel not defined ambient noise interference. **Challenge 1 : Frequency selectivity**. Imperfect electromechanical conversion. Frequency response is not uniform. Significant degradation above 12 KHz significant data loss in that band. **Challenge 2 : Ringing and rise time**. 5ms long sine wave was transmitted and received by a nearby device. **Challenge 3 : Ambient noise**. Ambient noise measured in various locations. Significant till 6KHz in noisy malls. Can cause interference. **Dhwani Design**: Software designed Acoustic OFDM radio. Ideal for frequency selective channels. Carrier-less design. 128 sub-carriers each 171 Hz width. Operating Bandwidth : 1 KHz (6-7 KHz) (No interference from ambient noise ¡6KHz). Band pass filter at the receiver.

2.2. **JamSecure : Secure NFC technique** . JamSecure - Idea. Scope and Limitations: Channel estimation based SIC Estimate the frequency dependant channel gain by sending a known sequence The frequency resolution depends on the reverberation in the channel. Since reverberation is high (¿15ms), these techniques does not give high SIC. **Limitations of JamSecure** The transmitter and the intended receiver are trusted devices. DoS attacks: Happens when the eavesdropper also starts jamming. But does not leak the private data. Directional antenna attacks: Eavesdropper focuses only on the transmitter. Hard in practice as it has to focus into ¡ 10cm.

2.3. **Dhwani : Performance**: Dhwani Communication range: ¡10cm.

2.4. **Conclusion: Dhwani**. Enables NFC in todays devices Software only solution. Provides security at physical layer.