Dublin City University

Electronic and Computer Engineering

EE00 Network Performance

Notes

Author

Michael Lenehan michael.lenehan4@mail.dcu.ie
Student Number: 15410402

Contents

1 Modeling and Simulations

1.1 Modeling

1.1.1 Need for Modeling: Difficulties

- Understanding and predicting complex systems behaviour
  - Many properties
  - many input parameters
  - Various environmental conditions
  - Different constraints
  - Diverse outputs
- Building real-life systems during design or for testing
  - Expensive
  - Requires personnel
  - Difficult to modify
  - Not sure how

1.1.2 Modeling as a Solution

- Building an abstract representation of the real system
  - Reduced complexity
  - Important characteristics only
  - Cheaper
  - Highly modifiable

1.1.3 Model Definitions

- A representation of a system from a certain point of view and at a certain level of abstraction
  - CPU of a computer
- A representation containing the essential features of an object or event in the real world
  - Airplane, train network, weather system

1.1.4 Modeling Definition

- Process of building a model
- Designing and analyzing a representation of a system to study the effect changes to system variables have

1.1.5 Modeling Benefits

- Allows for investigation of the properties of the system
- Enables prediction of future systems behaviour and outputs

1.1.6 Modeling Limitations

- Most models are inherently inexact (due to the simplifications and assumptions made)
- Accuracy is limited as:
  - Most parameters and equations used only estimate the real world situation
  - Initial conditions are not known
  - Environment influence is either ignored or limited

1.1.7 Simulation Definition

- Process of performing experiments using a model in order to determine the outcome

1.1.8 Analysis Definition

- Processing and interpreting the results of experiments in order to draw conclusions

1.1.9 Studying a System

- Experiments with the actual system
- Experiments with a model of the system
  - Prototyping
  - Modeling
    - Mathematical modeling
    - Modeling and Simulation

1.1.10 Model Types

- Deterministic or Stochastic
  - Deterministic: all variables are deterministic
  - Stochastic: Some model variables or behaviours are random

- Static or Dynamic:
  - Static: the model does not change in time
  - Dynamic the model is modified in time
- Continuous or Discrete:
  - Continuous: the system state evolves continuously
  - Discrete: the system state changes at discrete points in time

1.1.11 Stages in Modeling - Take A

- Simplification and Abstraction
  - A model contains essential characteristics of real-life objects or events
  - This stage identifies relevant features of real system to be modeled
  - Assumptions are made
  - Input parameters are determined
  - Output measures are listed
- Representation and Measurements
  - Object, events, numbers and relationships in the real system are associated model components
- Manipulation
  - Implementation of real world objects and relationships are determined
  - New objects and relationships are represented
- Verification
  - Outcomes from the model are compared with real world outcomes
  - It is determined if the model is adequate for the desired purpose

1.1.12 Stages in Modeling - Take B

- Determine the goals and objectives
  - Level of abstraction
  - Relevant features to be modelled
  - Required input and expected output
- Build a conceptual model
  - Very high level
  - Determines how comprehensive the model will be

  - Determines state variables if they are dynamic, how important they are etc.

- Create the specification model
  - Average detailed level
  - May involve equations, pseudocode, etc.
  - Indicates input and output
- Convert into a computational model
  - Low detail level
  - Involves a general purpose or a simulation programming language
  - It is the actual useful model
- Verification and validation
  - Verification
    * Did we build the model right? According to Specification
  - Validation:
    * Did we build the right model? Relative to the real system

1.2 Simulation

1.2.1 Network Simulators

- Network Simulator V2
  - Discrete event simulator
  - Includes many models for protocols at various network layers:
    * TCP UDP RTP
    * FTP CBR VBR
  - Support for wired and wireless delivery
  - Extended by many reasearchers worldwide
- Network Simulator version 3
  - Discrete event simulator
  - Includes increasing number of different protocols
  - Support for wired and wireless delivery

2 Introduction

2.1 Current Environment

- Cause:
  - Advances in mobbile devices, easy to use, affordable and powerful
  - People can connect to Internet anytime, anywhere
  - Popularity of video-sharing websites
- Effect:
  - Mobile users demands increasing
  - Exponential growth in video traffic
  - Explosion in data traffic
- Problems:
  - Application requirements
  - Multiple Device Types
  - Different technologies
  - Different User preferences (cost, energy, quality)
- Solution
  - Coexistence of multiple technologies
  - Deployment of different radio access technologies in overlapping areas
  - Accomodate more and more subscribers
- Challenges:
  - Offer always best connectivity to the interet for mobile users
  - Ne on best availabel radio access network
  - Network optimization especially for video traffic
  - Provide continuous and smooth video streaming, minimal delay, jitter, and packet loss
  - Avoid degredation in video quality and user experience

2.2 What is QoS?

- What is quality?
  - "The totality of characteristics of an entity that bear on its abuility to satisfy states and implied needs" ISO 8402
  - "Degree to which a set of inherent characteristics fulfils requirements" ISO 9000
- What is QoS?
  - A subset of overall quality
  - "The collective effect of service performance which determine the degree of satisfaction of a user of the service" ITU-T Rec. E.800

3 Service Level Agreement

- Contract between ISP and Client
- ISP gives guarantees for delivery of service
- Service Level Objectives (SLO)
  - Goals needed to be met for service
  - Used to specify QoS desired
- Service Level Guarantees (SLG)
  - Promise to meet SLOs
- Service Level Managements (SLM)
  - Approach of ISP for operation and delivery of services
  - Integrated management of functionalities in SLA life cycle

3.1 Service Level Objectives

- QoS Parameters
  - Instance to represent QoS to customers
  - Different according to type of service
- Generic QoS params required in network service:
  - Availability, Delivery, Latency, Bandwidth, MTBF (Mean Time Between Failures), MTTR (Mean Time to Recover)

3.1.1 QoS Parameters

- Availability
  - % of feasibility of service in every service request
  - key parameter for customers
- Delivery
  - Converse of packet loss
  - % of each service delivered without packet loss
- Latency
  - δt packet to travel from service access point (SAP) to target and back
  - includes transport t and queuing delay
- Bandwidth
  - Used/Available capacity - Stated in SLA

- MTBF - Mean Time Between Failure
- MTTR - Mean Time To Recover
  - Avg. t device/sys takes to recover from failure

3.2 Service Level Guarantees

3.2.1 Customer requirements of QoS

- Focus on user-percieved effects
- Not depend on assumptions of internal net design
- Take into account all aspects of service from cusomers PoV
- Assured to user by ISP
- Described in net-independent terms, creates common lang. understandable by both user and ISP
  - ITU-TG.1010

3.2.2 QoS Offered by the Service Provider

- QoS metrics for web browsing
- Requirements:
  - Mainly influenced by response time (!$>$ 5s)
  - Delay $< 400ms$ expected for best effort net traffic
  - Jitter not applicable to HTTP
    * Little impact on txt/picture web browsing
  - Data rate & required b.w. $< 30.5kbps$
  - Expected loss rate & error rate 0 since HTTP is reliable
    * Error reTX
- QoS Metrics for Video
  - Under diff. codec tech and quality req. diff. req. for net TX
  - VCR quality MPEG-1 stream:
    * B.W $1.2 - 1.5Mbps$
    * Jitter recommended $< 100ms$ for broadcast quality
    * Residual bit error rate $< 10^5$ for broadcast quality stream using compressed format
    * Loss/Error rates $< 10^5$
  - HDTV quality MPEG-2 video streams:
    * B.W $40Mbps$

    - Jitter $< 50ms$ for HDTV quality
    - Residual bit error rate $< 10^6$ for HDTV quality stream using compressed format
    - Loss/Error rate $< 10^6$
  - MPEG-4 video streams:
    - B.W $28.8 - 500kbps$
    - Jitter $< 150ms$ due to lower quality req.
    - MPEG-4 has higher comp. rate, $\therefore$ less residual error
    - Loss/Error rate $< 10^5$

- Statement of level of quality actually achieved and delivered to customer
- should be same as offered QoS
  - Determine what was actually achieved to asses level of performance achieved
- Performance figures summarised for specified periods of time

3.2.3 QoS Percieved by Customer

- Statement expressing level of quality exp.
- Perceived QoS - Degrees of Satisfaction, not in tech. terms
- Mean Opinion Score (MOS) specified by ITU-T Rec. P.800

3.3 Service Level Management Functions

- SLM categorized into seven functions:
  - SLA creation
    - Create SLA template for specified services
  - SLA Negotiation
    - Selecting applicable QoS params. in SLA
    - Negotiating penalty in case of SLA violation
  - SLA Provisioning
    - SP configure the network element/topology to provide service
  - SLA Monitorimg
    - SP must verify degree of SLA assurance
    - Perform surveillance on QoS parameter degredation/violation
  - SLA Maintenance
    - In case of QoS violation, analyses readon why degredation has occured, which params. degraded
    - Notifies SLA provisioning to restore service

  - SLA Reporting
    * Provides performance info to customers, periodically or on-demand
  - SLA Assessment
    * Demands payments to customers
    * Accommodates customers with penalty when violation occurs
- SLA provisioning and monitoring most important in net management layer

3.3.1 SLA Monitoruing

- Input
  - QoS Parameters
  - SLA Contract
- SLA Monitoring
- Output
  - Problem Notification
  - Performance

4 Network Performance Metrics

- Network Performance Metric (NPM)
  - Basic metric of performance metric in net management layer
- Four Types:
  - Availability:
    * % spec. t interval in which sys was available for normal use
    * What is supposed to be available?
      · Service, Host, Network
    * Reported as single monthly figure
      · 99.99% means service is unavailable for 4 minutes during a month
    * Test by sending syutable packets, observing answering packets (latency, packet loss)
    * Metrics:
      · Connectivity: Physical connectivity of network elements
      · Functionality: Whether associated sys works well or not
  - Loss:
    * Fraction of packets list in transit from host to another during specified t.
    * Packet transport works on best-effort basis

    * Moderate level of packet loss not in itself tolerable
        - Some real-time services can tolerate some losses e.g. VoIP
        - TCP resends lost packets at slower rate
    * Metrics:
        - One way loss
        - Round Trip (RT) Loss
- Delay:
    * t taken for pkt to tracel from host to another
    * $RTDelay = ForwardTransportdelay + Serverdelay + backwardtransportdelay$
    * Forward transport delay often $\neq$ backward transport dfelay
    * Ping still most commonly used to measure latency
    * Delay changes as conditions on net. vary
        - e.g. Server load, traffic load, router load, routing function
    * For streaming, high delay/jitter (delay variation) can cause degredation on user-perceived QoS
    * Metrics
        - One Way delay
        - RT Delay
        - Jitter
- Utilization:
    * Throughput for link expressed as % of access rate
    * Throughput:
        - Rate data is sent through net. (b/s, pkt/s, flows/s)
    * Metrics:
        - Capacity
        - B.W
        - Throughput

5 Performance at Lower Network Layers

5.1 Network Layer - Overview

Goal:

- Transports data from src to dest, across multi. hops
- Every major net. component has net. layer concerns

Design Principles:

- Services provided by network layershould be indep. of net. topology

- Transport layer should be shielded from member, type and topology of net. components
- Network addresses avail. to the transport layer should use uniform numbering plan

Service Types:

- Connectionless
  - e.g. IP: Internet PRotocol
- Connection-oriented
  - ATML Asynch. Transfer Mode Protocol

5.2 Internet

5.2.1 Characteristics

- Initial Design
  - Connection-oriented
  - Peer-peer topology
  - Circuit swithing-based communication
  - e.g. Telegraph and telephone
- Current Design
  - Best Effor Service
    * More appropriate for data transfers
    * No RT requirements
    * End-points can adapt to net. conditions, if they want/need to
  - Connectionless packet-switching based
    * Preferred to circuit-switvhing
    * No set-up delay
    * No blocking (fire and forget, forward if possible, deliver as received)
      · No guarantee that any data reaches dest.
    * Flex. in TX bit rates
      · Circuit-switching usually has few pre-determined bit-rates
    * No stable "path"
      · More reliable (route around problems
    * More efficient use of net. resources when traffic bursty

5.3 IP-based Network Layer

- Based on IP
- Connectionless: uses datagram packet switching
- Open design
- Open implementations
- Open standardisations process
- Independent of physical medium
- Scalable: as evidenced by its growth
- Extensible: protocols have evolved over time, as problems arose and/or req. changed

5.4 IP Router Architecture

5.4.1 Router Basic Functions

- Forwarding
  - Move pkts from routers input to output port
- Routing
  - Determine route taken by pkts from src to dest.
- Routing Activity (When datalink frame arrives)
  - Line card applies datalink layer logic to ensure frame is valid and pkt was successfully received
  - If pkt arrival rate > routers forwarding cap. pkt queued, waits for processing
  - If queue buffers full, pkt discarded
  - If space in queue, after waiting, validity check performed on IP header
  - If dest address non-local host, routing table lookup performed to determine how to forward pkt.
  - Pkts classified into predefined service classes (if defined)
  - TTL field decremented, new header checksum computed, pkt sent to approp. output port
  - Datalink layer login on output ports line card inserts datalink layer header, TX pkt inside a frame
  - If process fails, error msg sent to pkts sender

5.5 Internet Protocol Version 4 (IPV4)

5.5.1 IPv4 Header

- Ver indicates IP V num.
- ID is the same for all fragments of given datagram
  - Fragmentation of a datagram needed when an intermediate net. has a max frame size too small to carry datagram
- Fragmentation offset indicates place of each fragment in datagram
- Time-to-Live decreased by 1 at each hop
- Options field carrys fields that control routing, timing, management, security, etc.
  - Padded to a multiple of 4 bytes

5.5.2 IPv4 Address Format

5.5.3 Special IPv4 Addresses

Loopback useful for debugging/testing network software as IP pkts with loopback addresses are processed by the machine which generated them as if they were incoming pkts

5.6 Internet PRotocol Version 6 (IPV6)

5.6.1 Motivation

- IPv4 Limitations
  - Limited address space
    * Despite subnetting, Network Address Translation (NAT)
    * Classless Inter-Domain Routing (CIDR)
  - No special tratment for real-time traffic
    * Despite IPv4 Type of SErvice field which is ignored by routers
  - No wide usage of security issues
    * Despite IPv4 security ffeatures which are not widely used

5.6.2 Action

- In 90s, following an open design process IPv6 was standardised

5.6.3 ISsues

- IPv6 and v4 not compatible
- IPv6 deployment takes time
  - Both will coexist for a long time

5.6.4 Features

- Increased address space
  - Uses 128 bit address
  - 2^{128} addresses
  - $5 * 2^{28}$ addresses for each person on earth
- Simple pkt header
  - Routers don't do fragmentation
  - No header checksum to be checked
- Support for more options
  - e.g. routing, hop-by-hop, fragmentation, etc.
  - extension headers can be present
- Support for per-flow handling and traffic classes
  - Flows defined by src address, dest addres and flow num.
- Mandatory authentication and security
  - Internet Protocol Security (IPsec) was specially developed (then deployed in IPv4)
- Compatability with existing TCP/IP protocol stack
  - E.g DNS, TCO, UDP, OSPF, BGP, etc.

5.7 Other Network Layer Protocols

5.7.1 Motivation

- IP is in charge with data transport
- IP reqs. support from other transport layer protocols
  - Control functions (ICMP)
  - Multicast signalling (IGMP)
  - Routing table setup (TIP, OSPF, BGP, PIM)

5.7.2 ICMP

- Internet Control Message PRotocol facilitates:
  - Error reporting
  - Simple Queries
- ICMP msgs. carried by IP datagrams

5.8 Internet Control Message Protocol (ICMP)

5.8.1 ICMP Message Format

- Header (4bytes)
- Fields:
  - Type (1 byte): msg type
  - Code (1 byte): msg subtype
  - Checksum (2 bytes): calculated for entire msg
- Payload (min 4 bytes)
- Content
  - Related to msg type
  - If no data, content includes 4 bytes set to 0
- Note:
  - ICMP msgs have min. length of 8 byte

5.8.2 ICMP Message Types

- Query
  - Request-reply
  - e.g. Echo request, echo reply, timestamp request, timestamp reply, router solicitation, router advertisement
- Error reporting
  - Informs about error in transporting data
  - Sent by routers to hosts or routers
  - Processed at higher layers (e.g. application)

5.9 Routing Algorithms

- Definition
  - Determine route taken by pkts from src to dest
- Desirable Properties
  - Correctness
  - Simplicity
  - Efficiency
  - Robustness
  - Stability - Routing alg. reaches equilibrium in reasonable time
  - Fairness
  - Optimality
- Least-Cost Routing
  - Cost - A value assigned to each link in the net.
  - Cost of a route - Sum of values of all routes links
  - BEst route - Route with lowest cost
- Meaning of cost
  - 1 for each link - best route = fewest hops
  - Financial cost of using link - best is cheapest route
  - delau on link - bes is min.-delay route
  - pkt tx time on link - best is max.-bw route
  - Some comb. of these
- Pkt fprwarding
  - Towards the best route

5.9.1 Types

- Non-adaptive or Static
  - Routing decisions pre-determined, not based on measurements (or estimates) of current net. topology and traffic load
- Adaptive
  - routing decisions may be changed when net. topology and/or trafic load change
    - Extreme case: select new route for each pkt
    - May get info from neighbouring routers, or from net. routers
    - Routes are changed
      - Periodically

      - When topology changes
      - When traffic load changes significantly

- Centralised
  - Routing decisions taken in centralised manner for whole network
- Distributed
  - Routing decisions taken separately by each router, independent from neightbours

5.9.2 Decentralised Routing Algorithm

- Distance-vecor
  - Each router exchanges info about entire net. with neighbour routers at regular intervals
  - Neighbour - connected by direct link
  - Regular interval - every 30 seconds
- Link-state
  - Each router exchanges info about neighbourhood with all routers in net. when there is a change in the topology
  - Neighbourhood of router - set of neighbour routers
  - each routers neighbourhood info is flooded through the net.
  - Change in topology occurs hwen:
    * Neighbouring router not accessibe anymore
    * New router has been added
- Note
  - Link state algorithm converges faster and therefore more widely used

5.10 Distance Vector Routing

Principle

- Assume several LANS represented by "clouds" and routers/gateways by "boxes"
- Num. in each cloud represents net. ID
- Letter in each box represents router (or gateway) names
- Every router sends its info to its neighbours
- Each neighbor router adds this info to its own and send to its neighbours

- In time all routers learn about the net. struct.
- Each router stores info. about the net. in its routing able
- Routing table includes
  - Net. ID = final pkt dest
  - Cost = Num of hops from this router to final dest.
  - Next hop = neighbouring router to which pkt should be sent
- Initially each router knows net IDs of the net. to which it is directly connected only

5.10.1 Router Table Update

- Distributed Bellman-Ford Algorithm
  - Add 1 to cost of each incoming route (each neighbour 1 hop away)
  - If new dest learned, add its info to routing table
  - If new info received about existing dest.
    * If next hop field is same, replace existing entry with new info even if cost is greater
    * If next hop field not same, replace existing entry with new info if cost is lower

5.11 Link-State Routing

Principle

- Each router sends info about is neighbourhood to every other router
- Each router updates its info about the net. based on info received
- In time, all routers learn about net. struct
- Makes use of link costs (usually a weighted sum of various factors
  - e.g. traffic level, security level, pkt delay
- Link cost is from router to net. connecting it to another router
  - When pkt sent in LAN, every node - including router - can receive it
  - No cost assigned when going from a net. to router

Routing tables

- All routers get their info about their neighbourhood by sending short echo pkts to their neighbours, monitoring response

- All routers share info about their neighbours by sending link-state pkts to all routers in network (flooding)
- Pkts include
  - Advertiser: sending reouter ID
  - Network: Dest. network ID
  - Cost: Link cost to neighbour
  - Neighbour: Neighbour router ID
- Every router prepares a link-state pkt and floods it through the net.
- When router receives all these pkts. it can save the data in a link-state DB
- Assuming that every router receives same pkts, same content will be found in all link-state DBs
- Using info from DB, each router can fill it's routing table

5.11.1 Dijkstra's Shortest Path Algorithm

- ID all link costs in net. either from link-state DB, or using fact that cost of any link from a network to a router is 0
- Build shortest-path spanning tree for router running the alg.
  - Tree has route from router to all possible dest. and no loops
- Router is root of its shortest-path spanning tree
- Node either a net. or a router: nodes connected by arcs
- Algorithm keeps track of 2 sets of nodes and arcs, Temp. and Perm.
- Initially router is in Perm. set and Temp. set contains all neighbour nodes of router itseld, arcs connecting them to router
- Identify Temp. node whose arc has lowest cumulative cost from root: move to Perm set
- All nodes connected to new PErm node and not already in Temp. set along with their arcs, moved to Temp.
- Any node already in Temo set has lower cumulative cost reom root by using a route passing through the new Perm node, this new route replaces the existing one
- Repeat until all nodes and arcs are in Perm set
- NoteL even if all routers link-state DBs are identical, tree determined by routers are different

5.11.2 Building the Routing Table

- Once a router has found its shortest-path spanning tree it can build its routing table
- In large net. memory required to store the link-state DB and the computation time to calc. the link-state routing table can be significant
- In practice, since link-state pkt receptions not synchronised, routers may be using different link-state DBs to build their routing tables
- Result accuracy depends on how different the various routers DB content is

5.12 Routing in the Internet

5.12.1 Centralised Routing

- Initially Internet buiilt around Core system which enabled interconnectivity via core gateways
- Routing info collected, exchanged between core Gateways using Gateway-Gateway protocol
- Routing data processed by Core and result were distrib. back to external routers
- Major weakness of model - Scalability and vulnerability

5.12.2 Decentralised routing

- Internet build as a set of hierarchical inter-connected independent network groups known as Autonomous systems (AS)
- Two level routing
  - Intra-AS: each AS responsibe for own routing
    - Major protocols used in practice
    - Routing Info Protocol (RIP) - based on distance vector alg.
    - Open Shortest Path First (OSPF) - based on link-states alg.
  - Inter-AS: enables routing between AS
    - Major protocol used in practice
    - Border Gateway Protocol

5.13 Multicast Routing

- Definition
  - Delivery of a copy of a packet to a group of receivers
- Types
  - Multicast unicast
    * Mult. pkts travel from src to each dest.
  - Multicast
    * Single pktstravel on common routes
- Multicast in practice
  - Requires multicast addresses for multicast groups
    * Start with "10" in binary
  - Requires multicast enabled routers
    * Maintain and pass lsit of addresses assoc. with multicast group address
  - Requires multicast routing protocols
    * Distance vector mulicast routing protocols
    * Multicast open shortest path first protocol
  - Requires multicast routers to know about their own multicast groups
    * Internet Group Management Protocol

5.14 Performance Issues

5.14.1 Distance-Vector Routings count-to-infinity problems

- Slow convergence in some conditions
- Slow reaction to link/router failure as info travels in small steps
- Many ad-hoc solns. have been tried, but either also fail to solve count-to-infinity problem or are hard to implement

5.14.2 Link-State Routing Performance

- Link costs can be configured in OSPF (hop, reliability, delay, cost, bw)
- Large mam. req.
- Dijkstra alg. computations are highly processor intensive
- High BW req. if network topology changes often

5.14.3 Need for Intra- Inter-AS routing

- Policy
  - Inter-AS: Concerned with policies
  - Intra-AS: Under same admin, control so policy is less important
- Scalability
  - Inter-AS: Scale for routing among large num. of net.
  - Intra-AS: Scalability less of a concern
- Performance
  - Inter-AS: difficult to focus on performance metrics
  - Intra-AS: highly focused on performance metrics and costs

5.15 Wireless Routing PRotocols

5.15.1 Classification

- Topology-Based Routing
  - Table-Driven (proactive)
  - On-Deman (Reactive)
  - Hierarchical Routing
- Location-based routing
  - Greedy Routing

5.15.2 Table-Driven (Proactive) Routing

- Based on distance-vector and link-state protocols
- Nodes maintain routes to other nodes
- Periodic or event triggered route updates
- Relatively low latency, routes known in advanfe
- Higher overhead and longer route convergence

5.15.3 On-Demand (Reactive) Routing

- Src node inits routing discovery on demand
- Only active routes maintained
- Relative reduced routing overhead
- Long delays when new routes fount

5.15.4 Hierarchical Routing

- Net. divided into clusters
- Nodes talk to cluster head only
- Better scalability (descreases routing overhead), unfair use of resoutces

5.15.5 Location-Based (Geographic Routing

- Routing performed according to position of node
- Routing overhead can be small but optimal routing may not be found

5.15.6 Destination Sequenced Distance Vector (DSDV)

- Proactive routing protocol
- Each node maintains routing table with entries for each node in net.
  - dest addr, seq num., next-hop, hop-count)
- Nodes transmit pkts according to routing table
- Each node has seq num, updated when routing info changes (new node joins, line break)
  - Used to avoid routing loops
- Each node periodically broadcasts routing table updates

5.15.7 Dynamic Source Routing (DSR)

- Reactive protocol
- Srv wamts tp TX, does not know route to dest, inits route discovery
- Route request pkt broadcast, once dest receives, send back route reply, in pkt header ID's each forwarding hop in next node field
- Entire route stored in pkt headers
- At nodfes, route cache used to store most recent routes

5.15.8 Ad Hoc On-Demand Distance Vector (AODV)

- Essentially combo of DSR and DSDV
- DSRs on-demand mechanisms for route discovery and route maintenance
- Uses DSDVs table of precursor, next hop for each route during hop-by-hop routing and sequence numbers (to prevent loops)

- Improve DSR by keeping routing tables at nodes (pkts do not contain entire route)
- Routing table entries have lifetime in contreast to DSR cache

5.15.9 Temporally-Ordered Routing Algorithm (TORA)

- Adaptive routing protovol for muli-hop net.
- Designed to min comms overhead via localization of algorighmic reaction to topological changes (distribd execution)
- Uses directed acyclic graphs instead of shortest path soln
- Each node assigned unique height, pkts flow from high noes to low nodes along path towards dest.

5.16 Performance Issues

5.16.1 Throughput

- Throughput of DSDV decreases drastically with increases in mobnility. DSR outperforms all other protocols

5.16.2 Overhead

- In general routing overhead increases with mobility (topology changes)
- For DSR overhead dependent on num of diff. routes
- For DSDV overhead higher as routing tables need to be maintained

5.16.3 Delay

- DSDV delay lowest, constant (see routing tables)
- DSR high delay (see reactive protocols)
- TORA highest delay (see short-lived and long lived loops)

5.16.4 Optimality

- DSDV and DSR find optimal paths
- TORA and AODV use suboptimal paths even under low mobility

5.17 Quality of Service Support

5.17.1 Buffering

- Significant traffic burstiness when Tx over net.
- Buffering reduces loss, enables control over Tx rate

5.17.2 Packet Scheduling

- Enables selection of packets for differentiated Tx
- Arrival based: First in First Out (FIFO), Last In First Out (LIFO)
- Priority based: Src or pkts have different priority
- Weight based: Weighted Fair Queueing (WFQ)

5.17.3 Traffic Shaping

- Controls flow of data
- Time-based: Leaky bucket alg
- Token-based: Token bucket alg

5.17.4 Admission Control

- Enables access if certain performance metrics are met
- Otherwise refuses admission
- Maintains certain level of performance e.g. quiality

5.18 Traffic Engineering

5.18.1 Motivation

- Network traffic highly dynamic
- Network resources variable
- No network control
- No guaranteed QoS
- No efficient use of network resources
- No guaranteed security, reliability, resilience, etc.

5.18.2 Definition

- TE is concerned with optimizing performance of telecomms network by dynamically analyzing, predicting, and regulating the bhavour of dat TX over that network

5.18.3 Goal

- Optimisation in terms of efficiency (i,e, costs and quality)

5.18.4 Major Solutions

- Intergrated Services
  - Focus on providing QoS delivery guarantees per-flow (using resource reservation: RSVP)
  - Concerns on: complexity, scalabity, business model, etc.
- Differentiated Services
  - Focus on providing QoS support per-class
  - Routers on the network differentiate traffic treatment based on it's class, ensuring preferential treatment for higher priority traffic
  - No advance setup, no reservation, no negotiations for each flow, easier to implement
- Other solutions: MLPS

5.19 Performance of Datalink and Physical Network Layers

- Wireless PANs (BT - IEEE802.15)
  - v. low range
  - wireless connection to printers etc
- Wireless LANs (WiFi - IEEE 802.11)
  - Infrastructure as well as ad-hoc net. possible
  - Home/office net.
- Wireless MANs (WiMAX - IEEE 802.16)
  - Large scale network
  - Base station-based infrastructure

5.20 WiMax IEEE 802.16

- Group formed in 98
- Standards
  - Air-interface for wireless broadband
  - Line of Sight comms
  - Ooperates in 10-66GHz range
- 802,16a amendment
  - Included Non LOS version in 2-11 GHz freq. band
  - PHY layer uses orthogonal freq. division multiplexing
  - MAC layer supports Orthogonal Frequency Division Multiple Access
- 802.16d
  - Further amended standard
  - Formed basis for first WiMax soluions
- Above standards supported fixed wireless applications
  - No mobility support
- 802.16e - 2005
  - added support for mobility and improved performance
  - Enable soft and hard handover between base stations
  - Introduce scalable OFDMA
    * Enables higher sppectrum efficiency in wide channels
    * Cosst reduction in narrow channels
  - Improces coverage using
    * Antenna diversity schemes
    * Hybrid ARQ (hARQ)
  - Improving capacity and coverage using
    * Adaptive Antenna Systes (AAS)
    * Multiple Input Multiple Output(MIMO) tech
  - Into'd high performance coding techniques to enhance security and NLOS performance
    * Turbo coding
    * Low density parity check
  - Intro's downlink sub-channelization alling admins trade coverage for capacity or vice versa
  - Increases resistance to multipath interference using enhances FFT alg. which can tolerate larger delay spreads
  - Adds extra QoS classs (enhanced rtPS) more appropriate for VoIP apps

5.21 WiMax 802.16e Service Classes

5.21.1 Unsolicited Grant Service (UGS)

- Fixed size pkt carried periodically without requiring explicit req. for bw allocation every time. Real-time high bw (T1) CBR applications (e.g. VoIP)

5.21.2 Extended Real-Time Poling Service (ertPS)

- Newly intro'd scheduling service in 802.16e complement periodic bw allocations with possibilities for mobile stations to req. additional resources during original allocation. Supports applications whose bw req. vary in time (e.g. VoIP, streaming)

5.21.3 Real Time Polling Service (rtPS)

- Intro'd to support real time services with variable zide data pkts fenerated periodically, such as MPEG video delivery applications. Frequent unicast polling opps are provided such as movile stations can req. bw and satisfy their timing req.

5.21.4 Non-Real-Time Polling Service (nrtPS)

- Similar with rtPS, unicast polling opps less freqent. Contention based polling can also be used to req. bw resources

5.21.5 Best Effort Service (BE)

- Designed for services with no strict QoS requirements such as email and web apps. Mobile stations use contention based polling to request resources

5.22 WiFi IEEE 802.11

- First std published in 97 for WLAN comms
- Since, various extensions proposed to address different issues - higher bit rate, QoS support, security
- Tech gained popularity because of low deployment and maintenance cost, as well as relatively high bitrate
- IEEE 802.11 - 1997
  - supports data rates up to 2Mbps, initially developed for best effort traffic only

  - Each host connects to an IEEE802.11 access point
  - Wireless medium shared with other nodes associated with same AP point
  - Contention for medium access which determines increased collision rates and consequently lower data rates especially when num of mobile hosts involved in sumultaneous data comms increases
  - IEEE 802.11 MAC layer provides mech. for medium access coordination:
    * Distributed Coordination Function (DCF) - distributed
    * Point coordination Function (PCF) - partly centralised

- IEEE 802.11b
  - Increased max data rate to 11Mbps, operating in 2.4 GHz freq. band
- IEEE 802.11g
  - Increase max. data rates to 54Mbps
- IEEE 802.11a
  - Data rates up to 54Mbps operating in 5GHz freq. band
- IEEE 802.11e
  - QoS extesion provided by two new mechanisms
    * Hybrid Coordination Function (HCF) - PCF extension
    * Enhanced Distributed Coordination Function (EDCF) - DCF extension

5.22.1 Other 802.11 extensions

- IEEE 802.11n
  - Higher bitrates up to 600Mbps
  - QoS support similar with 802.11e
- IEEE 802.11p
  - Wireless comms in vehicular environments
  - Short to medium range comms at high data transfer rates
- IEEE 802.11ac VHT
  - Offers data rates up to 1Gbps for low velocity mobile hosts

5.23 WiFi IEEE 802.11 Issues

5.23.1 Hidden Station Problem

- Consider that station B has TX range indicated by left oval, C by right oval. Any station in these ranges can hear TX from B and C respectively
- Station C, outside TX range of B cannot hear B, likewise B cannot hear C. Station A in range of both. Assuming B TX to A, C cannot hear B, believes medium is free, also TX data to A. Neither TX successful
- RST and CTS frames introduced to solve this problem. Before sending, B sends RTS to A (includes duration of TX). A hears RTS and replies with CTS which also includes TX duration info. As C is in range of A it gets CTS msg, learns of hidden station will be using channel, refrains from TX.

5.24 WiFi IEEE 802.11e

5.24.1 QoS Support

- Access Class (AC)
  - AC_VO (Voice), AC_VI (video), AC_BE (best effort) and AC_BK (Background)
- Transmission Opportunity (TxOP)
  - Time duration dring which station is allowed Tx turst of data frames
- Arbitration Interframe Space (AIFS[AC])
  - Period of time a wireless node has to wait before alloewd TX next frame
  - Dependent on access class
- Contention Window (CWmin, CWmax)
  - Deoendent on access class

5.25 WPAN

5.25.1 IEEE 802.15

- Bluetooth
  - Interconnects various protale devices and their accessories
  - 2.4GHz band
  - Data rates of up to 1Mbps (BT v1.0) and up to 3Mbps (v2.0)

  - Future rates expected to be between 53Mbps and 480Mbos
  - IEEE802.15.1 based on BT v1.1

- IEEE 802.15.4
  - Low-range, low-power wireless network comms
  - Based on this standard, Zigbee protocol defines the network layer specialized on ad-hoc networking and the application layer targeting wireless sensor networks as well as other monitoring and control applications
  - IEEE 802.15.4/Zigbee offers data rates up to 250 Kbps in the 2.4GHz band

- Ultra-Wideband (UWB)
  - WiMedia Alliance defined UWB wireless comms tech sipporting wide range of data rates from 53Mbps to 480Mbps over short range using low power transceivers
  - PHY/MAC protocols developed by WiMedia became ECMA 368 standard and later on ISO/OEC 26907

- Wibree
  - Ultra-low power wireless net. comms tech
  - Ranges up to 10m and data rates of 1Mbps

6 Performance at Transport Layer

6.1 TCP

Characteristics

- Connection-oriented reliable byte-stream service
  - Two comms end points must establish, maintain connection
  - Byte stream data exchanged between end points
  - Reliable data delivery ensured

6.1.1 Principles

- Data broken into segments of certain size
  - Max. Segment Size (MSS) set (negotiated) at conn. estab.
  - MSS val carried by SYN segment
  - End point never TX segment larger than MSS

- Higher MSS, better performance (min. OH vs payload ratio)
- If not indicated, default val of 536 bytes is used for MSS
- In reality, seg size 40 byteslarger as also includes
  - 20 bytes TCO header
  - 20 bytes IP header

6.1.2 Problem

- Data broken into segments of certain size
  - COmpute efficiency considering OH and payload when TX 4GB video and MSS of 1460and 536 used:
    - Case 1: No pkts: $4 * \frac{1024}{1460} = 2873; Headers : 40 * 2873 = 114920$
      - Efficiency = useful data/total data = $\frac{4194304}{4309224} = 97.33\%$
    - Case 2: No pkts: $4 * \frac{1024}{536} = 7826; Headers : 40 * 7826 = 313040$
      - Efficiency=useful data/total data= $\frac{419304}{4507344} = 93.05\%$

6.1.3 Principles

- Reliability through ack and reTX
- When TX seg, timer set
- RX expected to ack seg
- If ack not RX, seg is reTX

6.1.4 Issues

- ReTX TimeOut (RTO) period is variable
  - RTO set in relation to RTT
  - RTT estimated using smoothed estimator (SRTT) using a low-pass filter
  - After unsuccessful reTX, TO period doubled (exponential backoff) with an upper limit
- Adter series of unsuccessful reTX, conn. is reset
  - TCP implementation have Keepalive timer, not present in TCP standard

6.1.5 Problem

- Exponential backoff reTX
    1. List times at which reTX occurs if there is a need for 6 reTX and the first two are 2s apart
        - ReTX: 1,3,7,15,31,63
    2. List times at which reTX occur if there is need for 10 reTX and the first two are 1.5s apart
        - ReTX: 1,2.5,6.5,11.5,23.5,47.5,96.5,159.5,223.5,287.5

6.1.6 RTT Estimation

- Calculated every time new measurement performed
- $STT = \alpha * SRTT + (1 - \alpha) * MRTT$, where
    - SRTT is RTT estimator
    - α is smoothing factor with rec. val between 0.8 and 0.9
    - MRTT is measured RTT

6.1.7 RTO Value

- Calculated every time there is need for reTX
- $RTO = min(RTOMax, max(RTOMin, (\beta * SRTT)))$, where
    - RTOMax is upper bound on timeout (e.g. 1m, 64sec)
    - RTOMin is lower bound on timeout (e.g. 1s)
    - β is delay variance factor with dixed val between 1.3 and 2
    - If ack not RX, seg is reTX

6.1.8 ISsues

- RTT estimation accuracy problem
    - RTT estimation alg assumes RTT variations are small, constant
    - Loses accuracy with wide fluctuations in RTT, causing unnecessary reTX
    - ReTX add traffic to already loaded net.
- Jacobson's soln.
    - Keep track of both mean and variance of RTT, compute RTO based on both

6.1.9 RTT Average and Mean Deviation

- Calc every time new measurement performed
- $Err = MRTT - ARTT$
  - Err is error between measured val and smothered value for RTT
  - ARTT is smothered RTT average
  - g is gain factor with rec. value of 1/8
  - MRTT is measured RTT

6.1.10 RTT MEan Deviation

- Calc. every time new measurement performed
- $DRTT = DRTT * h * (|Err| - DRTT)$
  - DRTT is smothered mean deviation
  - h is difference factor set to 0.25

6.1.11 RTO value

- Calc. every time need for reTX
- $RTO = ARTT + r * DRTT$, where
  - r is constant set to 4
  - Initial val set for r was 2, later changed to 4

6.1.12 Issues

- RTT measurement accuracy problem
  - RTT measured between sending of data pkt and its ack
  - When Large delays occur, timer goes off, reTX takes place
  - When RX ack, no way to know if it was delayed res. to orig data seg or res. to reTX seg
- Karn's soln
  - Not to update RTT estimator with info on reTX seg's performance
- Limitations of Karn;s soln
  - When RTT increases sharply, normal reTX resumed after series of reTX and TCP does to receive ack, for a while RTT not updated, reTX would happen considering old RTT val
- Limitations soln

    - Exponential backoff timer timout val employed: timout=2*timout

- Solution isse
    - If to increases too much, delays added with no correlation with actual net. delay
- Solution fix
    - Upper limitations added to to value > 1 min: 64s

6.1.13 Computation of RTT estimation

6.2 Congestion control

- Modern TCP std include 4 major alg
    - Slow start
    - COngestion avoidance
    - Fast reTX
    - Fast recovery

6.3 Slow Start

6.3.1 Principle

- Slowly probes net in order to determine available capacity
- Employed at beginning of transfer/after loss detected by TX timer
- Uses following var.
    - COngestion window (cwnd) - sender side limit on amount which can be TX before receiving ack
    - Receiver window (rwnd) - Receiver-side limit on outstanding data
    - Slow start threshold (ssthresh) - limit to decide using slow start or congestion avoidance
    - Sender Maximum Segment Size (SMSS) - Max seg size at sender
    - Flight Size - amount of unack data in TX between sender, receiver
- TX should exchange min of cwnd and rwnd amount of data
- Slow start used when cwnd > ssthresh, Congestion Avoidance emploued for cwnd < ssthresh and either alg when cwnd = ssthresh

6.3.2 MEchanism

-
-
-
-
-

6.3.3 Note

-

6.3.4 Problem: ACK Division

- ‘
-
-

6.3.5 UPdated Mechanism

-
-
-

6.3.6 Performance Issues

- - *
- - *
  - *
- - *
  - *
  - *
    *
    *
    *
    *

6.4 Congestion Avoidance

6.4.1 Principle

6.4.2 Mechanism

6.4.3 Updated MEchanism

6.4.4 Note

6.5 Fast Retransmit

6.5.1 Principle

6.5.2 Mechanism

6.6 Fast Recovery

6.6.1 Principle

6.6.2 Mechanism

6.6.3 Note

6.7 Fast Retransmit and Fast Recovery

6.7.1 PRinciple

- Two major alg types that improve Fast reTX and Fast recovery
- Based on TCP selective Ack
  -

7 TCP Tahoe

7.1 Characteristics

- Fast recovery not included
- Fast reTX not included
- TXP old tahoe did not have fast reTX either
- Implemented in Unix 4.3 BSD Tahoe

7.2 ISsues

- ONly mechanism to detect loss is through reTX timer timeout
  - Introduces potential delays
- TCP old tahoe by not emplying dast reTX alg, slow start has to be used
  - Rates kept low
- Every lost pkt determines cwnd reste to min
  - Severe reduction in rates

8 TCP Reno

8.1 Characteristics

8.2 Issues

9 TCP NEw Reno, SACK and Vegas

9.1 TCP New Reno

9.1.1 Characteristics

9.1.2 ISsues

9.2 TCP SACK

9.2.1 Characteristics

9.2.2 Issues

9.3 TCP Vegas

9.3.1 Characteristics

9.3.2 Issues

10 SCTP

10.1 Motivation

- TCP limitations with wireless and mobile comms
- Need for multi-streaming
- Need for multi-homing

10.2 OVerview

- Series of IETF 2960 (2000), IETF RFC 3286 (2002)

10.3 Features

- Reliable transport protocol
- Uses association instead of conn.
- Designed for message oriented applications
  - Framing (preserve message boundaries)
- Ack error free transfer of msg
- Detection of data corruption, data loss and data duplication
- Selective reTX to corect lost or corrupted data
- Active monitoring of session conn. via heartbeat
- Resistance to DOS attacks
  - 4-way handshake
- Supports multi-streaming
  - Up to 64K indp. ordered streams
- Supports multi-homing
  - Set of IP addresses per endpoint

10.4 Message Format - 1:HEader

- Src Port and Dest Port (2+2 bytes)
  - Same port concept as TCP and UDP
- Verification Tag (4 bytes)
  - Exchanged etween endpoints at startup to validate the sender
- Checksum (4 bytes)
  - Uses CRC32 alg

10.5 MEssage Format - 2: Chuncks

- Type (1 byte)
  - Control or Data: e.g. Data, Init, SACK
- Flags (1 byte)
  - Carry info depending on type
- Length (2 bytes)

  - Chunk length, including data payload length
- Data (N bytes)
  - Variable length payload

10.6 Message Format - 3: Important Chunk Types

- DATA
  - IDs chunks carrying data
- INIT, INIT-ACK, COOKIE-ECHO, COOKIE-ACK
  - USedfor association establishment
- HEARTBEAT, HEARTBEAT-ACK
  - Used for keep-alive chacking
- SHUTDOWN, SHUTDOWN-ACK
  - USed for graceful disconn.

10.7 Establishing an Association

Association Establishment Procedure

-

10.8 INIT Chunk

- Initiate Tag
  - Receiver stores Initiate Tag Value
  - Must be placed in VErification Tag field of every SCTP pkt receiver sends
- Advertised Receiver Window Credit (a_rwnd)
  - Indicates dedicated buffer space sender reserved for this association
- Number of Outbound Streams (OS)
  - Number of outbound streams sender wishes to create in this association (max 64k)
- Number of Inbound Streams (I-TSN)
  - Defines initial TX seq number the sender will use
  - Field may be set to value of Initiate Tag Field
- –

10.9 INIT-ACK Chunk

10.10 COKIE ECHO and COKIE ACK Chunks

10.11 DATA Chunk

10.12 Terminating an Association

10.13 SHUTDOWN Chunks

10.14 Multihoming

SCTP Association:

- Comm. hosts use set of IP addr. instead of single one each
- Multi comms path may be set up
  - One primary path
  - No. of secondary paths
- Lists of IP addrs exchanged between hosts during init of assoc.
  - Both INIT and INITACK msgs include list of IP addrs
- Source of INIT msg is dest of INIT-ACK
  - In general, determine primary path

SCTP Operation:

- HOsts monitor data TOs and No. of reTX to determine path's transmission quality
- ReTX Data chunks may be sent over multipaths if status of one path is suspect
- Faulty paths marked "Out of Service"
- HEartbeat chunks sent periodically to all inactive IP addr
- Non-responding IP addrs will be marked "Out of Service"

11 mSCTP

Mobile SCTP

- Extends SCTP
  - Adds Dynamic Address Reconfiguration (ADDIP)
  - Enables SCTO to add, delete, and change existing IP addrs attached to an assoc. during an acrive conn.
  - Enables support for seamless handover for mobile hosts that are moving between IP networks
  - Uses ASCONF and ASCONF-ACK
    * Add new IP addrs to assoc
    * Change primary IP of assoc
    * Delete old IP addr from assoc

12 DCCP

Motivation

- UPD and TCP limitations with realtime transport of data
- Need to support real-time data transfers over wireless links

Overview

- DCCP is novel non-reliable transport layer protocol
-
-

Features

-

Datagram Format 1:

- Headers - Long Sequence No.

Datagram Format 2:

- Headers - Short seq no.
- Acknowledgements - Short seq no.
- Options and Data

Datagram Fields

-

Packet Types

-

Connection Setup

- 3-way handshake

Data exchange

- Two endpoints exchange Data pkts and ack pkts acking data
- Optionally DataAck pkts containing data and acks can be exchanged
- If one endpoint has no data to send it will send ack pkts exclusively

Connection Close

- 3-way handshake

13 Congestion Control-Related Schemes

Drop Tail

- Involves default queue mechanisms
- Drops all pkts exceeding queue length
  - Any TCP-based receiver reports loss in ACK pkt
  - Most often sender adapts to loss by multiplicatively decreasing
- One loss event is very likely to be dollowed by series of loss events
  - Little or no space in queue
- If adaptive senders need some time to respond

Random Early Detection (RED)

- Uses active queue management

- Drops pkt in intermediate node based on av. queue legnth exceeding a thresh
  - Any TCP receiver reports loss in ACK pkt
  - Most often sender adapts to loss by multiplicatively decreating rate
- RED experiences mostly singular loss events
- Gives time to adaptive senders to respond

Early Congestion Notifications

- End-End congestion avoidance mechanism
  - Implementedin routers and supported by end-systems
  - Not multimedia-specific, very TCP-specific
- Uses two IP header bits
  - ECT - ECN Capable Transport, set by sender
  - CE - COngestion Experienced, may be set by routers
- If pkt has ECT bit 0,
  - ECN acts as RED
- If pkt has ECT bit 1:
  - ECN node sets CE bit
  - Any TCP receiver sets ECN bit in ACK
  - As result most often sender applies multi decrease
- EXN-pkts never lost on un-congested links
- Distinction between loss and marked pkts
  - TX window can decrease
  - No pkt loss and no reTX

Early Congestion Notification (ECN) Nonce

- Optional addition to ECN
- Improvies robustness of congestion control
- Prevents receivers from ecploiting ECN to gain unfair share of net. BW
- Protects against accisdental/malicious concealment of marked pkts from sender

eXplicit Congestion Notiication (XCN)

- Protocol for Connections with high BW-delay product
- Routers return explicit feedback to host
- Hosts use feedback from routers to change their congestion window

14 TCP over Wireless

Motivation

- LArge percentage of traffic is reliable:
  - File Trandfer (FTP)
  - Web Traffic (HTTP)
  - Command Based (TELNET, SSH)
- TCP very popular in wired networks
  - Very good congestion control
  - Very good congestion avoidanve

TCP in Wireless Networks

- Pkt loss in wireless networks occurs due to:
  - Bit errors due to wireless channel impairments
  - Handovers due to mobility
  - Congestion (rarely)
  - Pkt reordering (rarely)
- TCP assumes pkt loss is due to:
  - COngestion in the net.
  - Pkt reordering (rarely)

Problems with TCP over Wireless NEtworks

- Congestion avoidance can be triggered by pkt loss
  - TCPs mechanisms do not respond well to pkt loss due to bit errors and handoffs
  - Efficiency of TCP-based transfers suffer
- Error bursts may occur due to low signal stregth or longer period of noise
  - More than one pkt lost in TCP
  - More likely to be detected as TO -> TCP enters slow start
- Delay is often very high and variable
  - RTT can be very long and variable
  - TCPs TO mechanisms may not work well
  - Problem exacerbated by link-level reTX

- Links may be asymmetric
  - Delayed ACKs in slow dirn. limit throughput in fast dirn

Solutions for TCP over Wireless Networks

- Link-Layer approaches (A)
  - Hide losses not caused by congestion from the transport-layer sender
  - Makes link appear to be more reliable than it is in reality
  - Solns:
    - Use frame reTX
      - Link-level automatic reTX request (ARQ)
    - USe error correction codes
      - Forward Error Correciton (FEC)
    - Use hybrid solutions
      - ARQ and FEC
- Advantages
  - Requires no change to existing sender behaviour
  - Matches layered protocol stack model
- Disadvantages
  - Negative TCP effect:
    - Delays due to link-level TO and reTX may trigger TCP fast reTX
    - TX efficiency decreases
  - Soln to negative TCP effect
    - Make link-level protocol TCP-aware
- Example: Snoop TCP
  - Advantages
    - Attempts to reTX locally, suppress duplicate ack
    - State is soft, handoff simplified
  - Disadvantege
    - May not completely shield TCP from effects of mobility and wireless loss

Split Connection Approaches (B)

- Divide single TCO conn. into two conn.
- Isolate wired net. from wireless net

- OFten split at base station or access point
- soln
  - Use TCP on wired net
  - Enhanced protocol over wireless net
- Advantages
  - Clarity of approach
  - Each of the protocols performs best in its setup
- Disadvantages
  - Extra protocol OH
  - Violates end-end semantics of TCP
  - Complicates handoff due to state info at access point or base station where protocol is "split"
- Example
  - Indirect TCP

End-to-End Approaches (C)

- Make sender aware that some losses are not due to congestion
- Avoid congestion control when not needed
- Solns
  - Selective ack (SACKs)
  - Explicit loss notificaiton (ELN) distinguishes between congestion and other losses
- Advantages
  - Maintains end-end semantics of TCP
  - Intros no extra OH at base stations for protocol processing or handoff
- Disadvantages
  - Requires modified TCP
  - May not operate efficiently e.g. for pkt reordering versus pkt loss
- Example
  - SMART

15 Snoop TCP

OVerview

- Link-layer protocol that snoops passing TCP data and acks
- Employs Snoop agent between two endpoints
- Data from Fixed Host to Mobile Host
  - Cache unack'd TCP data
  - Perform local reTX
- Data from Mobile Host to Fixed Host
  - Detect missing pkts
  - Perform negative ack

Architecture

-

Fixed Host to Mobile Host Operation

- If new pt rec. in normal TCP seq
  - Add to snoop cache
  - Forward to Mobile Host
- If out of seq pkt cached earlier arrives
  - Fast reTX/TO at send due to:
  - if last_ACK < crt_seq_no
    - Loss in wireless link - Forward to Mobile Host
  - if last_ACK > crt_seq_no
    - Loss of previous ACK - send ACK to Fixed Host with Mobile Host addr and port
- If out of seq pkt not cached earlier arrives
  - if seq_no far from last_seq_no
    - Congestion in fixed network
      - Forward to Mobile Host
      - Mark as reTX by sender
  - if seq_no close to last_seq_no
    - Out of order delivery

Mobile Host to Fixed Host Operation

- If new ack rec. in normal TCP operation
  - Normal Case
    - Clean snoop cache
    - Update RT estimate
    - Forward ack to Fixed Host
- if spurious ack rec.
  - Discard
- If duplicate ack rec.
  - If pkt not in snoop cache
    - Lost in fixed net.
      - Forwared to fixed host
  - If pkt marked as sender reTX
    - Forward to Fixed Host
  - If unexpected (first after a pkt loss)
    - Lost pjt on wireless link
      - ReTX ar higher priority
  - If expected (subsequent adter one lost)
    - Discard

Advantages

- Improved performance in wireless net.
- No change to TCP at fixed host
- No violaiton of end-end TCP semantics
- No recompiling/re-linking of existing applications
- Automatic fallback to standard TCP
  - No need to ensure all foreign net. provide Snoop agent

Disadvantages

- Does not fully isolate wireless link errors from the fixed net.
- Mobile host must be modified to handle NACKs for reverse traffic
- Cannot snoop encrypted datagrams
- Cannot be used with authentication

16 Indirect TCP (I-TCP)

Overview

- Hides pkt loss due to wireless from sender
- Wireless TCP can be independently optimized
- Good performance in case of wide-area net.
- reTX occurs only on bad link
- Faster recovery due to relativelty shortRTT for wireless link
- Handoff requires state transfer
- Buffer space needed, extra copying at proxy
- End-end semantics violation needs to be augmented by apllication level

Architecture

-

Advantages

- No changes to TCP at fixed hosts
- Wireless link errors are corrected at the TCP proxy and do not propagate to the fixed net.
- New "wireless" protocol affects only limited part of internet
- Possible further optimizaitons over wireless link
- Delay variane between proxy and mobile host is small -> optimised TCP
- Opportunity for header compression
- Opportunity for different transport protocol

Disadvantages

- Loss of TCPs end-end semantics
- Addition of third point of failure (proxy) apart from fixed, mobile hosts
- Handover can be significant
- OH at proxy for per pkt processing
- TCP proxy must be trusted
- Opportunities for snooping and DOS attacks
- End-end IP-level privacy and auth. must terminate at proxy
- Proxy failure may cause loss of TCP state

17 Other Approaches

18 Next Genneration Networking

18.1 Mobile Key Features

- High performance: Processing and storage
- High quality multimedia
  - 4K UHD video player/recorder
  - High resolution cameras
- Long battery Life

18.2 Fundamental Goal: COnnectivity

18.3 1G

- Introd in 1980s
- Established foundation of mobile net
- Used analog radio signals
- Used Freq Div Multi Acces (FDMA)
  - 1 user per channel
  - Neighbouring cells assigned diff freq to avoid interference
- AMPS, NMT, TACS

18.4 1G Limitations

- Large freq gap req. between users to avoid interference
  - Inefficient use of spectrum
  - Scalability Issues
- Analog Phones large/heavy, power inefficient, expensive

18.5 2G

- Introd in 1990s
- Used digital readio signals
- Combines FDMA with Time Div Multi Access (TDMA)

  - Multi Users per channel
  - Small, power saving, inexpensive phones
- Introduces data service for mobile
  - SMS
  - MMS
- D-AMPS, GSM

18.6 TDMA Limitations

- Still req. large freq gaps to reduce interference
- Rigid slots assignment, whether or not users have voice/data to send
- Potential for call drop when switching channels between adj cells

18.7 Code Division Multiple Access (CDMA

- Each subscriber has unique code
- Multiple simultaneous users per channel
- Same radio channel can be used in ad cells
- Spectrum allocated to inactive users used to support new users
- Established foundation of 3G

18.8 Why 3G?

- With 2G more perope had subscriptions
- Advances in device tech lead to era of smartphones
- Internet widely adopted at homes/offices
- People wanted more than voice and simple data

18.9 3G

- Introd in early 21st century
- Accommodate web-based apps and phone-based audio and video files
- 2 competing standards
  - CDMA2000/EV-DO
  - WCDMA/HSPA

18.10 CDMA2000/ED-VO vs. WCDMA/HSPA

18.11 EV-DO and HSPA Benefits

- Delivered achievable throughput > 2Mbps
- Reduced operator cost for device services
- Continuous evolution for enhanced services

18.12 4G: Faster and better broadband experience

- Introd in early 2010s
- Compleents 3G to boost data cap
  - $\geq$1Gbps for stationary users
  - $\geq$100Mbps for mobile users
- LTE to bridge gap
  - Labeled 4G because provides substantial improvement over 3G
  - Net started advertising connections as 4G LTE
- Multimode 3G/LTE is foundation for successful 4G LTE

18.13 4G LTE

- Allows for downloading, browsing, streaming, gaming faster than ever
- 2 goals
  - Connect daster
    * Wider channels (up to 20MHz) with OFDMA
    * More antennas (2x2 MIMO mainstream)
  - Connect real-time
    * Simpolified core network (flat IP architecture)
    * Low latency

18.14 4G LTE TDD

- Time Division Duplexing
- Single freq for up/downloading
  - Up/download ratio can be changed dynamically depending on data needs
  - Works better with high freq (from 1850MHz to 3800MHz)

        * Cheaper to acces, less traffic
        * Overlap with WiMax bands
            · Easy upgrade of WiMax to LTE-TDD
    - Popular for ISP with no 2G/3G services

18.15 4G LTE FDD

- Frequency Division Duplexing
- Uses paired frequencies to up/download data simultaneously
    - Works better at lower frequencies (from 450MHz to 3600MHz)
    - Efficient in syummetric traffic
    - Easier and efficient radio planning
    - Popualar for cell operators having established 2G/3G services

18.16 LTE Advanced

- Considered "real" 4G tech
- Data transfer speeds $\geq$ 3xLTE (300Mbps)
    - Carrier/channel aggreagation
        * 20 MHz channels cannot provide 1Gbps throughput
        * Increase bandwidth used by aggreadgating carriers
        * Up to 5 20MHz carriers can be aggregated, up to 3 in practive
        * When carriers aggreagated, can either primary or secondary

18.17 3G and 4G Evolution

18.18 5G

- Next major phase of mobile telecoms and wireless systems
- Will provide higher speeds, greater cap, lower latency
- Will be capable of supporting billions of connected devices
- Will be a heterogeneous network of many wireless technologies

18.19 5G: General Requirements

18.20 5G: PErformance Requirements

18.21 5G: Use Cases

18.22 Enhancing Mobile Broadband Experience

18.23 Connecting Massive Number of Devices

18.24 Enabling Critical Control of Remote Devices

18.25 5G: Spectrum

- Below 1GHz
  - Very good coverage, cannot enable dastest data rates
- Between 1 and 6GHz
  - Mix of coverage and cap.
  - Carrier aggregation needed to support 5G data rates
- Beyond 6GHz
  - Extremely fast data rate, very limited coverage

18.26 5G Standardization (ITU and 3GPP)

18.27 Internet of Things (IoT)

- "A global infrastructure for the information society, enabling advanced services, by interconnecting (physical and virtual)thigns based on existing and evolving interoperable information and communication technologies" - ITU-T, 2012
- Thing are objects capable of being ID'd and integrated into comm lauer
  - Physical things: devices with comms capability eg. surrounding environment, sensors, actuators, electrical equipment
  - Virtual things that are capable of being stired, processed and accessed, e.g. multimedia content, Facebook and twitter accounts, etc

18.28 IoT Characteristics

- Interconnectivity
  - Devices should be able to communicate with other devices to offer remote control, monitoring, sensing
  - Control temp at home while at office, car updateing maps for nav sys while in garage, etc
- Heterogeneity
  - Devices with diff HW and connected through diff tech
  - Interoperability should be supported
- Self-adapting
  - V. Large number of connected devices
  - Huge amounts of data $\rightarrow$ Big Data

18.29 IoT Reference Model

- Devices TX sensed data to cloud via diff networks (LTE, WiFi, Zigbee)
- Data processed and stored at cloud computing infrastructure
- Cloud deploys processing techniques to extract ingo and provide services to users
- Security modules
  - Decides which services to provide to which users
  - How data from/to clout is TX and how its stored

18.30 Edge Computing

- Goal: Optimize cloud computing sys
- IdeaL distib data provessing and storage by putting resources near src of data
- Advantages:
  - Reduce comms BW needed between sensors nad cloudd
  - Reduce latency

18.31 IoT Applications

- Smart citiesL manage assets and resources efficiently via data collection from citizens and IoT devices
- Intelligent TransportationL enhance road safecty and traffic management
- Smart energy: designm new ways to save energy
- Smart agri: enhance cap of agri sys
- Smart Healthcare: Improce clinical care, research and puoblic health

18.32 Machine-to-Machine Communicaiton (M2M)

- Direct comms between devices using any comms channels w/o manual assistance of humans
- Often used for remote monitoring: warehouse management, traffic control, robotics, fleet management, telemetry
- Key components: sensors, RFID, non-IP based net (e.g. Zigbee, BT), and a SW to help remote receiver interpret data and make decisions
- Not standardized as many M2M systems are built to be task or device specific

18.33 IoT vs. M2M

- M2M
  - almost synonymous with isolated systems of sensors
- IoT
  - Try to marry disparate systems into wider sys view to enable new applications
- When considere in larger context with IP connectivity, M2M becomes IoT

18.34 Software-Defined Networks (SDN)

- Trad net cannot cope up and meet net req.
  - Very exensive (CAPEX and OPEX)
  - Cannot be dynamically config.
    - Manual config
  - Net elements lack ability to customize features
  - Do not support dynamic scalability

- Decouples control plane from forwarding plane
- Control plane hosted in centrlized entity, called SDN controller
  - Has global view of network
- Forwarding plane kept at switches
  - Also called data plane
- Extremely scalable, easily config's/managesd, programmable and inexpensive

18.35 SDN architecture

- Application plane
  - Programs that proide instructions and req.
  - Abstract view of net
- Control plane
  - Relays app layer instructions and req. to net component
  - Collects info from net devices and comms it to app layer
- Data Plane
  - Forwarding data and collecting net state info

18.36 SDN and OpenFlow

- OpenFlow: open protocol that provides a standard interface for programming data plane of switches
  - PRovides definition of abstract swithes so that swithces of diff vvendors can be manages by single protocol
- Considered as enabler to SDN
- Based on Ethernet switches that has 2 components:
  - Secure channel: interface that connects each OpenFlow swithc to controller
  - Flow tables: define what actions should be applied to packets received by OpenFlow switches

18.37 OpenFlow Tables

- Various fields
  - Rule: matching criteria against which packets are compared
  - Action: Instructions to be executed when packaet matches entry
  - Stats: keeps track of num of pkts that match the entry
  - PRiority: enables switch to select action with highest priority when multiple matches are found
  - HArd TO: time adter which entry will be removed

18.38 Network Functions Virtualization (NFV)

- Current networks have custom hardware appliances for each network function (e.g. switches, routers, firewalls, load balancers, servers, etc.)
  - Complex, hard to maintain
- NFV decouples net functions from dedicated HQ to run them on standard servers and switches
- Advantages:
  - Standard HW architecture
  - V. flexible, scalable and inexpensive
  - Reduced power consumption
  - Test new apps

18.39 NFV Framework

- VNFs (Virtualized NEtwork Functions)
  - SW used to virtually create the various net functions (switch, firewall, etc.)
- NFVI (NFV Infrastructure)
  - All HW and SW components contained within environment in which VNFs are deployed
  - Can be located across several physical locations
- NFV-MANO
  - Functional blocks that run and manage NFVI and VNFs

18.40 Difference between NVF and SDN

- NVF and SDN very closely linked, not the same
- SDN replaces standardised netwroking protocols with centralised control
  - Central view for more efficient implementation and running of the net serviecs
- NFV replaces proprietary net HW with SW that can run on standards HW
  - Optimizing the network services themselves
- NFV and SDN are complementary, but not dependent on one another
  - One can exist without the other