Congestion Control in Data Networks

Dr Steve Gordon

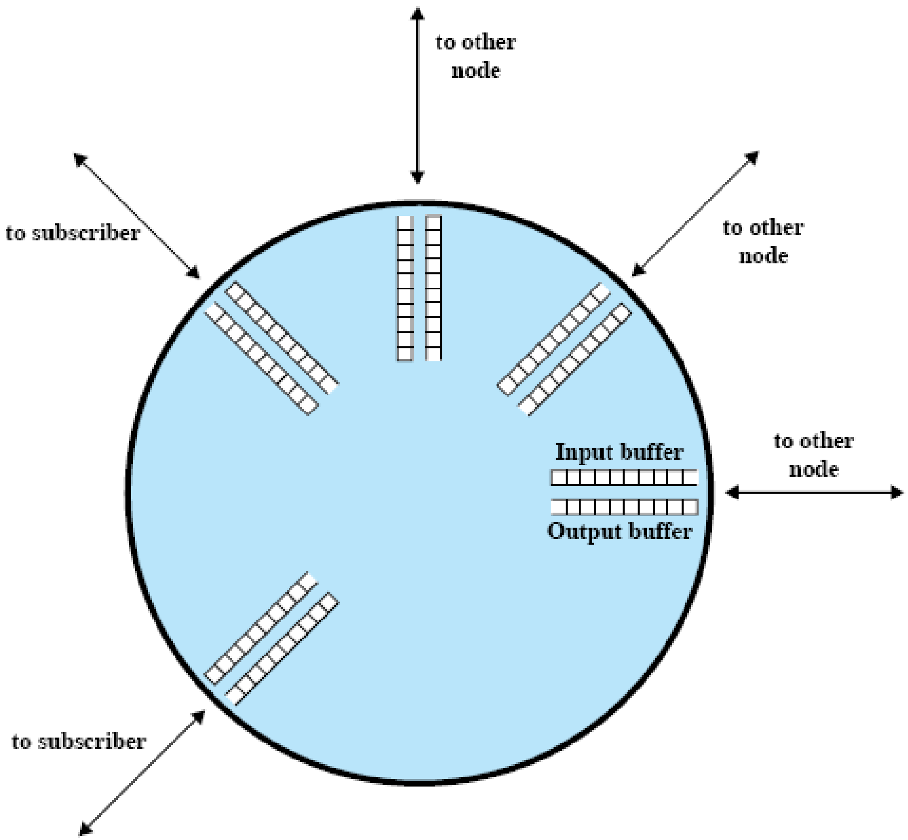
ICT, SIIT

What Is Congestion?

- Congestion occurs when the number of packets being transmitted through the network approaches the packet handling capacity of the network
  - What is the packet handling capacity of a network?
  - What happens when capacity is approached?
- Congestion control aims to keep number of packets below a level at which performance falls off dramatically
  - How to keep number of packets below level?
- Consider from a queuing perspective:
  - A data network is a network of queues
    - At each node, a queue of packets arriving and queue of packets leaving
  - Queuing theory tells us that generally 80% utilization is critical
    - When 80% utilization, queue length grows rapidly
      - Delay in queue increases
      - Since queue is finite length, overflow (drop) occurs

Effects of Congestion

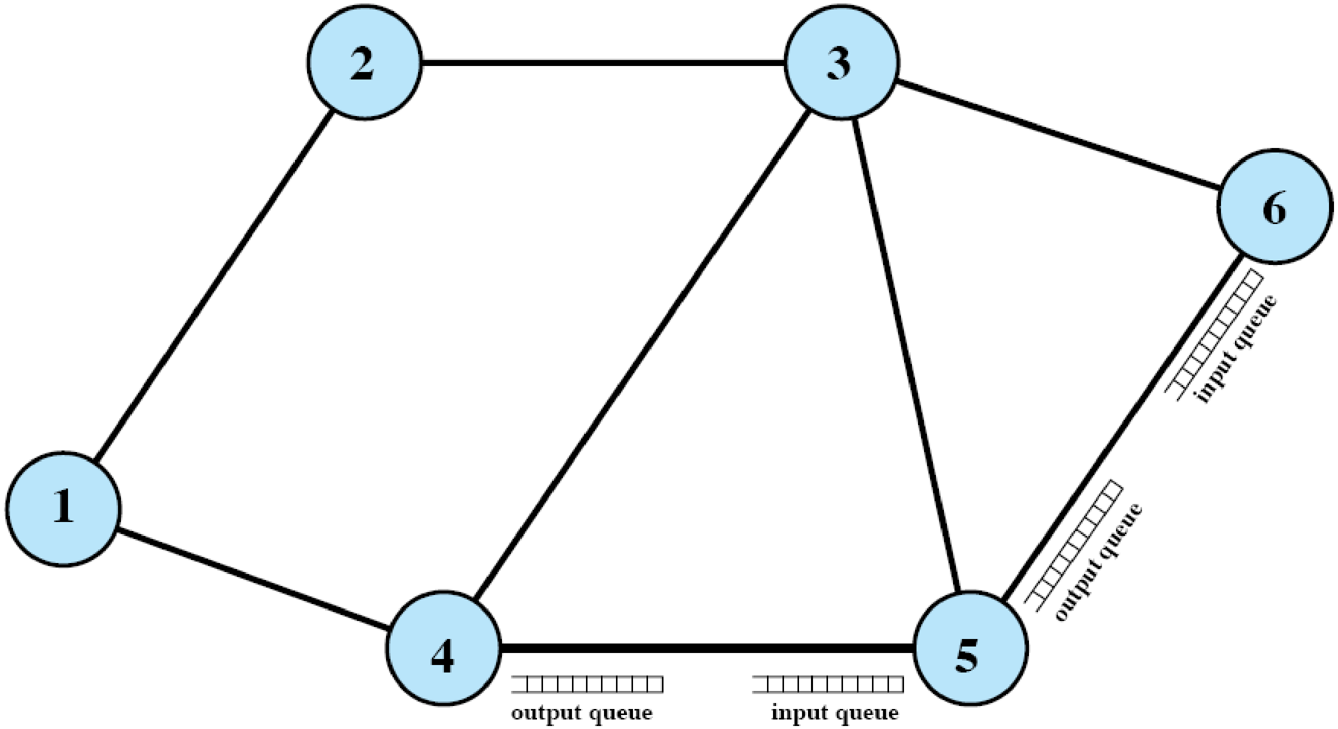
Queues at a Node



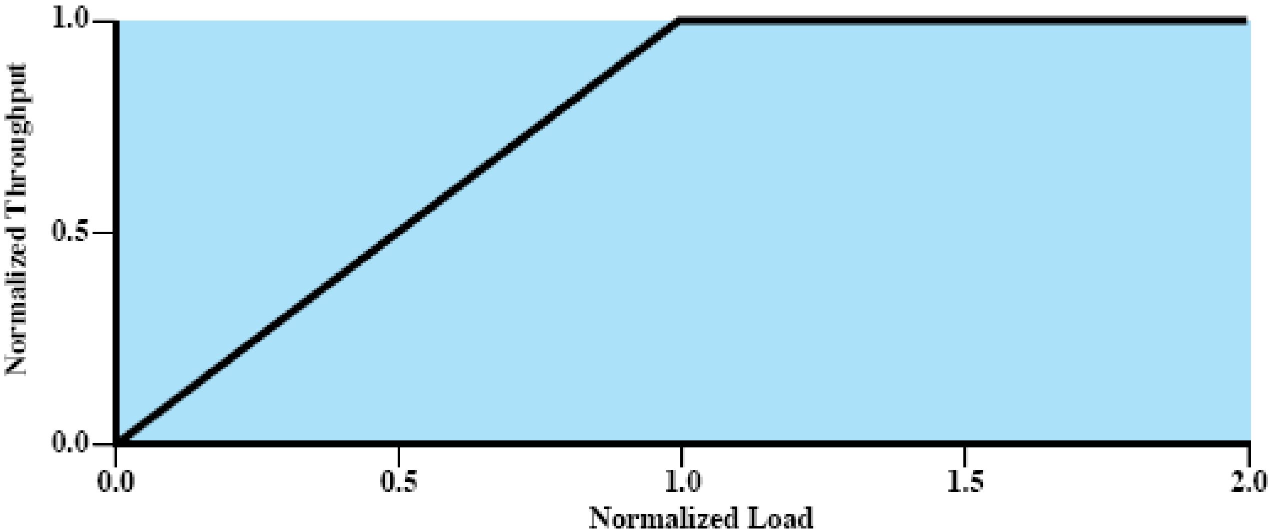
- Each I/O port has a queue for arriving packets and queue for sending packets
  - Node makes routing decision on packets that arrive and moves packet to output queue
- Queues are memory in computer
  - Total size is limited (because of delay, not cost of memory)
- Queues are full if packets arrive:
  - Too fast for node to process
  - Faster than queued packets can be sent
- This is saturation

Interaction of Queues

- Two options when saturation point is reached:
  - Discard any incoming packets if no queue space available
  - Apply flow control to slow neighbours down
- But flow control is difficult in network
  - If node 6 tells node 5 to slow down, then output queue on node 5 will fill up
  - Congestion is now present at node 5

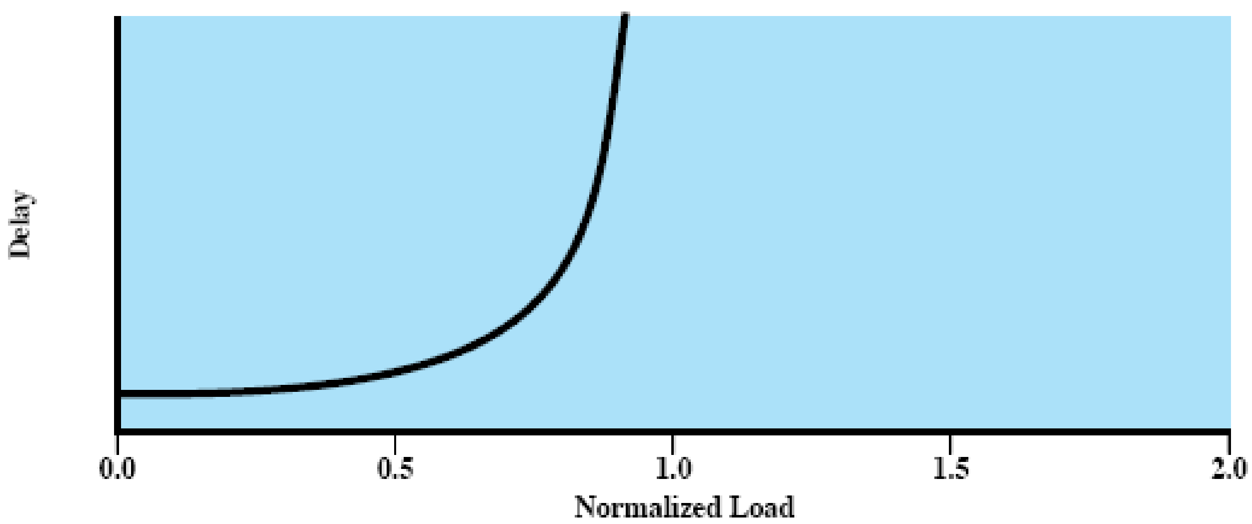


Ideal Network Utilization



- Throughput: number of packets/bytes delivered to destinations
- Load: number of packets/bytes sent by sources
- Network should handle all traffic sent, up to capacity (1.0)

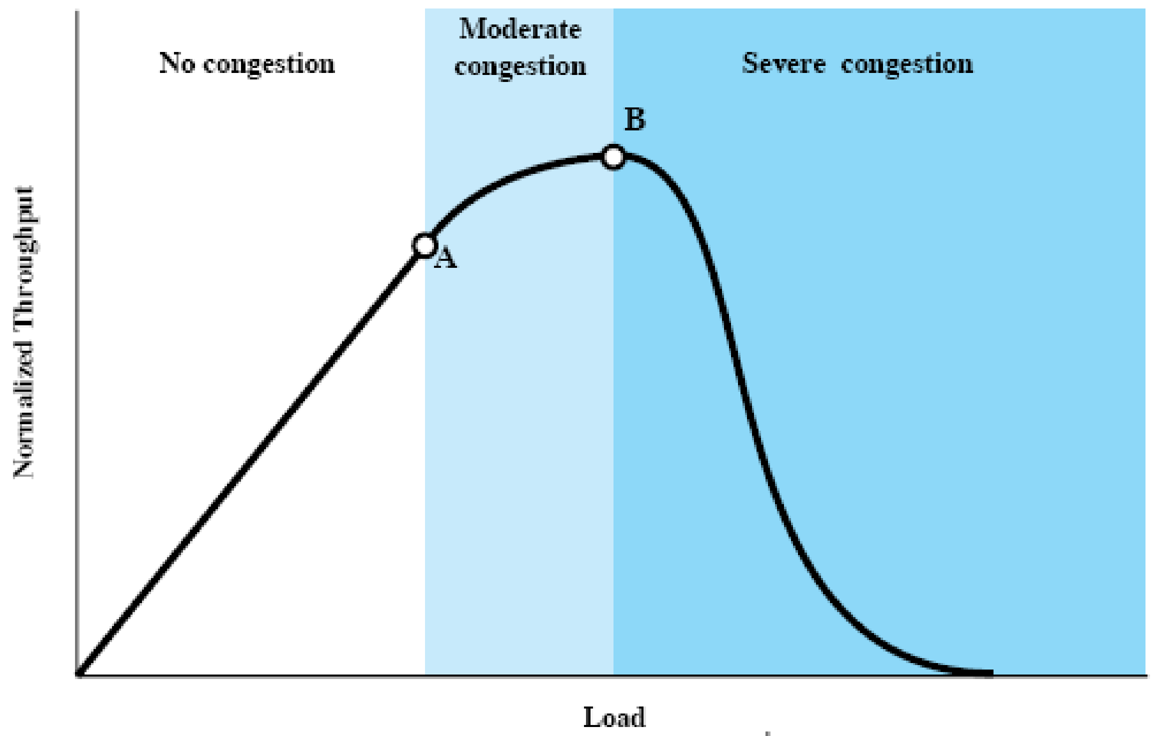
- With small load, delay is small (constant)
- As load increases, packets must wait in queues longer
- With overload, more packets enter network than leave
  - Queue size increases
  - Delay increases

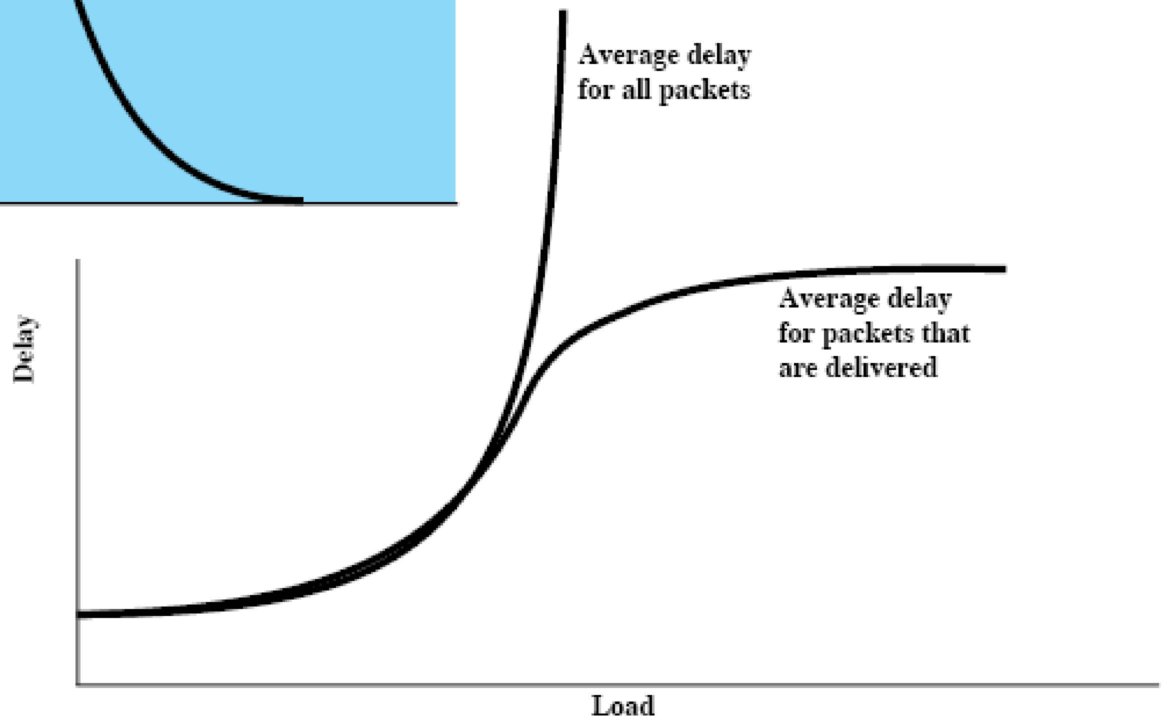


Effects of Congestion

- In practice:
  - Queues are finite length
  - Congestion control mechanisms (including routing) contribute to network overhead (e.g. number of routing packets increases)
- The effect:
  - At light loads, throughput increases linearly with load; delay is almost constant – everything is OK
  - As load increases (point A onwards), throughput degrades slightly (not linear increase with load) although delay is increased because:
    - In practice, load is not uniform; some nodes may experience minor congestion, others severe congestion discarding traffic
    - Routing to find paths that avoid congestion contributes to overhead (hence decrease throughput)
  - Eventually (point B onwards) throughput decreases as buffers are full and more packets are dropped:
    - With dropped packets, retransmissions occur, hence increasing the load (and more dropped packets, and more retransmissions, and …)
    - Effective capacity can decline to 0 as the load increases

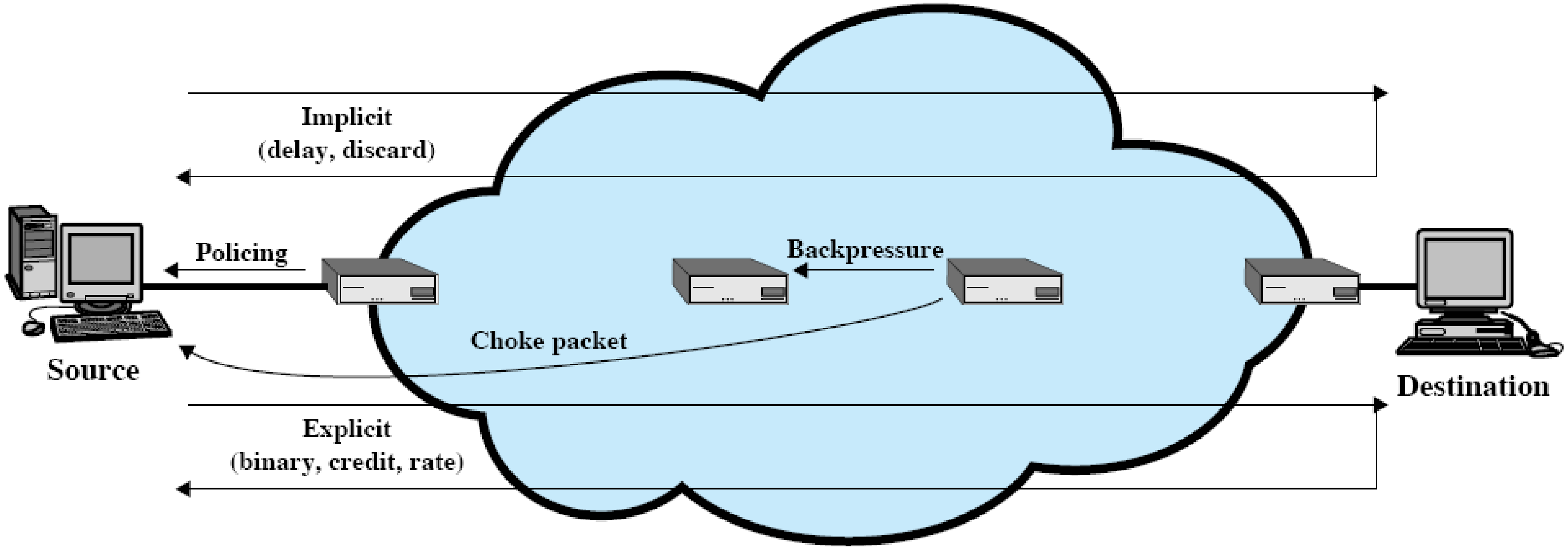
Effects of Congestion





Mechanisms for Congestion Control

- Backpressure
  - Node tells previous node to slow down; the previous node tells its previous node to slow down; and so on until source slows down
  - Useful if hop-by-hop flow control: ATM, Frame Relay and IP do not support this
- Choke Packet and Explicit Congestion Signalling
  - A control packet is sent from congested node to source node to slow it down
  - Different types: Binary (Slow or not); Credit-based; Rate-based
- Implicit Congestion Signalling
  - If packet is discarded or packet delays increase, assume congestion



Examples of Congestion Control Mechanisms

- Choke Packet
  - In the Internet, the Internet Control Message Protocol (ICMP) can be used to send a "choke" packet to the source, telling it to slow down
    - This choke packet is called *Source Quench*
  - Upon receiving Source Quench, the source slows down
    - The source will keep slowing down until it no longer receives more Source Quench packets
  - This mechanism is relatively simple, but not very effective
- Implicit Congestion Signalling
  - Useful in connectionless, datagram packet switching networks
    - Datagram packet switching: packets take different routes, so difficult to use explicit mechanisms at each router
  - TCP uses the loss of a packet to indicate congestion

TCP Congestion Control

- A very simple explanation …
  - The TCP sender starts by sending very slow
    - Sends 1 packet, and waits for an ACK (e.g. window size of 1)
  - After receiving ACKs, the TCP sender increases the number of packets it can send
    - Example:
      - Window size doubles to 2
      - Receive another ACK – window size doubles to 4, and so on
    - Why? If the TCP sender receives an ACK, it assumes the network can handle the traffic (no congestion), so it tries to send faster
  - TCP sender keeps increasing the rate it sends (that is, keeps increasing its window size) until either:
    - An upper limit is reached (usually determined by the speed at which receiver can receive)
    - Or, an ACK is not received, that is a packet is lost
      - TCP assumes a lost packet is due to congestion
      - Therefore the TCP sender reduces its sending rate to reduce congestion
  - We will cover TCP in more detail in later lectures and courses …

Traffic Management

- Congestion control often concerned with efficient use of network at high load
- But other things to consider as well:
  - Fairness
    - Provide equal treatment of various flows
    - Two users (or applications) should experience on average the same delay, throughput
  - Quality of Service (QoS)
    - As an enhanced network service, different treatment can be given for different connections
    - Voice calls should experience low delay; network management traffic should have highest priority
  - Reservations
    - Related to QoS, a way to avoid congestion is to reserve available resources on a connection
    - Traffic contract between user and network