CSE and EE 461
Lecture 13

Summer Quarter 1998

Evaluating Protocols

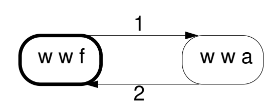
- Correctness
  - No duplicates
  - No gaps
  - Data delivered in order to network layer
  - No deadlock - protocol gets in a set of states where no progress can be made
- Performance
  - Good utilization of channel
  - Maximum delay encountered by the protocol is on small
  - Smooth flow in implies smooth flow out
  - Buffers not too large

  Naturally performance depends on the characteristics of the channel such as loss rate, propagation delay, and bandwidth. But, one wants to get the best possible under the circumstances.

Finite State Analysis

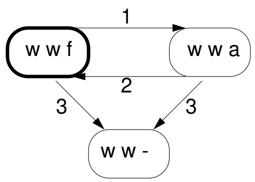
- Protocol is modeled by a finite state system which includes:
  - state of sender
  - state of receiver
  - state of the channel
  - transitions which move the system from state to state
  - start states
- Reachability analysis - examples
  - No deadlock - no set of states is reachable in which nothing is accomplished in the set and there is no way out.
  - Zipper property - the system moves from one set of states to another properly.

Stop-And-Wait Example



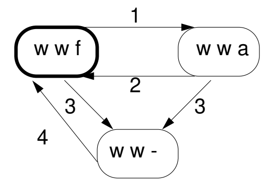
Trans	Who runs	Frame accepted	Frame emitted	To network layer	From network layer
1	receiver	f	a	yes	
2	sender	a	f		yes

Stop and Wait with Lost Frames



Trans	Who runs	Frame accepted	Frame emitted	To network layer	From network layer
1	receiver	f	a	yes	
2	sender	a	f		yes
3		lost frame	lost frame		

Adding Timeouts at Sender



Trans	Who runs	Frame accepted	Frame emitted	To network layer	From network layer
1	receiver	f	a	yes	
2	sender	a	f		yes
3		lost frame	lost frame		
4	sender		f		no

A Correctness Conditions

- **Safety Condition**: In any sequence of transitions, transition which are "from the network" must alternate with those "to the network"

  Example: 1, 3, 4, 1 has two "to the network'' in a row
- **Liveness Condition:** From any reachable state it is possible to get to a state where progress can be made. Progress means that we can get data through.
- Importance of verification

  - Companies like ATT are spending lots of money on this.

  - Very active research area

    Symbolic Model Checking
    Petri Nets
    Temporal Logic

HDLC

- HDLC - High-level Data Link Control - old standard used in X.25

  - variable length frames

  - Uses flags 01111110 and bit stuffing

  - 16 bit checksum

  - 3 bit sequence numbers for sliding window protocol. Can use either go-back-N strategy or selective repeat.

  - piggy backing allowed

  - unacknowledged service is allowed

PPP

- PPP - Point-to-Point Protocol used in the internet between hosts and router and between routers.

  - variable frame length - default is about 1500 bytes

  - uses flags 01111110 and character stuffing

  - frames are always in multiples of bytes in length

  - 16 or 32 bit checksum - normally 16 bits.

  - LPC - Link Control Protocol - must handle dynamic links well because hosts come and go often

  - NCP - Network Control Protocol - must handle different network protocols
    Typical problem is that the host needs an IP address

  - Can support acknowledged or unacknowledged frames.

ATM

- ATM - Asynchronous Transfer Mode - link protocol needed between host and switches and between switches.

  - fixed length cells - 53 bytes including 5 bytes of header

  - no flags delinating frames - a mechanism using the checksums keeps things synchronized

  - 8 bit checksum only checks for an error in the header - data is not checked for errors.

  - There is no resending of damaged or lost cells. Damaged cells are just thrown away. Any error control on data is done end-to-end, not point-to-point.