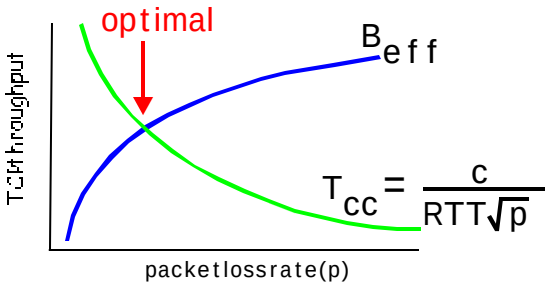
Secure and Wireless Networks

http://www-net.cs.umass.edu/

Improving TCP performance over wireless links

- FEC reduces packet loss (p) but also usable bandwidth (B_{eff})
- optimal FEC point: $T_{tcp} = B_{eff}$
- TCP thruput = min(T_{cc}, B_{eff})
- cross layer coupling improves TCP performance



Secure leader election in wireless networks

- elect leader with maximum ID or with performance preference
- synchronous, and asynchronous (self-stabilizing)
- provable correctness, and security (cheat-proof) properties

Inter-Area Rekeying Algorithms for mobile networks

- scalable rekeying: group members move between "areas," each area has key
- four rekeying algorithms identified
- comparative performance analysis
  - communication: key msg rate within, out-of area
  - computation: area key rekey rate
  - security: # (area keys) held by area member
- delayed rekey algorithm provides low overhead, with few extra area keys being held

Additional Projects

- performance analysis of hierarchical, subset difference rekeying (joint with Nortel)
- hidden Markov model characterization of wireless link packet loss
- capacity analysis of hybrid wireless/wired network