Specific Systems:

Cellular
#13
Part 2: EV-DO

Victor S. Frost
Dan F. Servey Distinguished Professor
Electrical Engineering and Computer Science
University of Kansas
2335 Irving Hill Dr.
Lawrence, Kansas 66045
Phone: (785) 864-4833   FAX:(785) 864-7789
e-mail: frost@eecs.ku.edu
http://www.ittc.ku.edu/

Outline

- Part 1
  - Basic components
  - 3G
  - Overview of W-CDMA/UMTS
  - HSPDA
- **Part 2**
  - **EV-DO overview** (Slides provided by Soshant Bali, Ph.D. candidate-EE, University of Kansas)
  - **Case study: Mitigating scheduler-induced starvation in 3G wireless networks**

Slides provided by Soshant Bali, Ph.D. candidate, University of Kansas

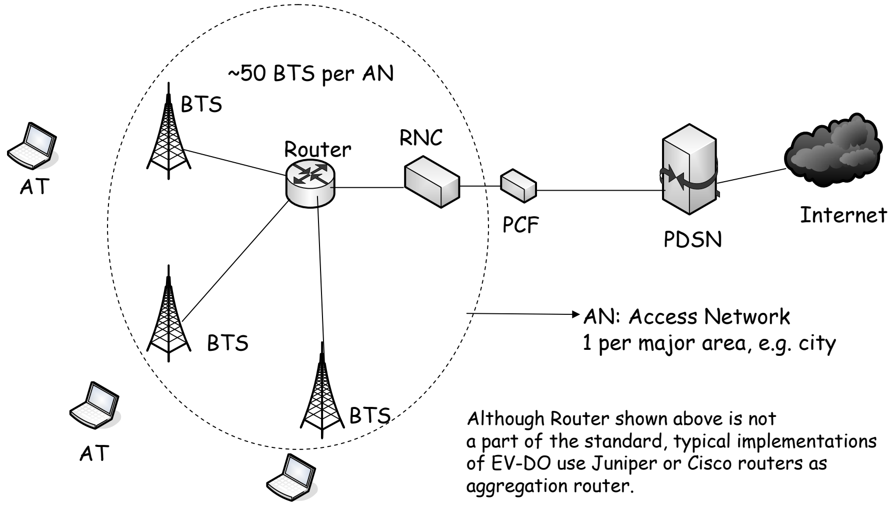
EV-DO overview-Outline

- Introduction
- Network Architecture
- Simplified Protocol Stack
- Air Interface Protocol Layers
- Forward Link
  - MAC Layer
  - PHY Layer
- Reverse Link
  - MAC Layer
  - PHY Layer
- Some Interesting Features
  - Radio Link Protocol
  - Adaptive modulation and coding
  - Hybrid ARQ

Introduction

- 1xEV-DO: 1x Evolution for Data Optimized
  - 3G data rates: up to 2.45Mbps downlink, 153.6Kbps uplink
  - Natural evolution from IS-95, IS-2000
  - Evolution: leverage existing network elements
  - Optimized for data transfer
    - IS-2000 needs 3.75MHz spectrum for 2.07 Mbps
    - EV-DO only 1.25MHz spectrum for 2.45 Mbps
- Data service characteristics
  - Rates asymmetric
    - EV-DO: higher rate in forward link
  - Latency can be tolerated
    - EV-DO: uses link layer ARQ
    - EV-DO: powerful error-correcting codes (e.g., turbo codes)
  - Transmissions are in burst
    - EV-DO: uses time-division multiplexing

EV-DO network architecture



AN: Access Network
1 per major area, e.g. city

Although Router shown above is not a part of the standard, typical implementations of EV-DO use Juniper or Cisco routers as aggregation router.

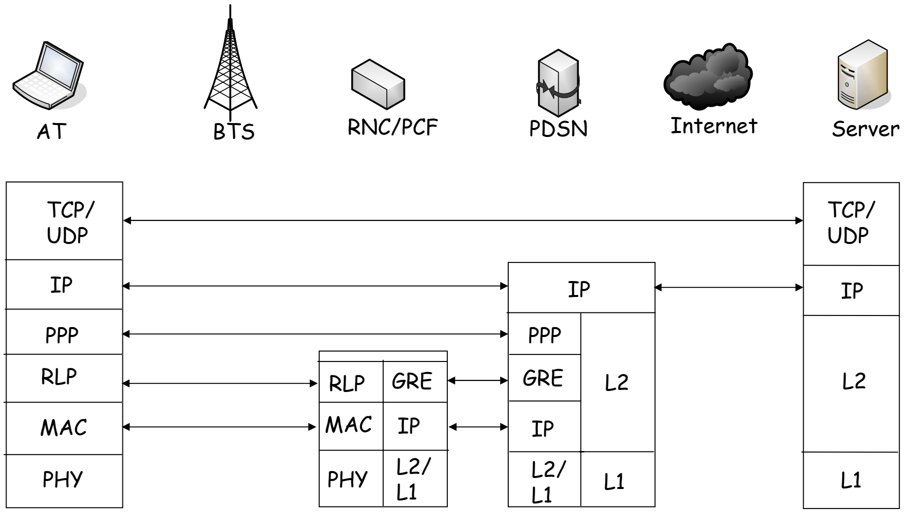
AT = Access Terminal

PCF = Packet Control Function

Network architecture

- Base Transceiver Station (BTS)
  - RF components for transmitting/receiving signals
  - Software/hardware for digital communications/DSP
  - Connected to RNC with backhaul links
- Radio Network Controller (RNC)
  - Session establishment and release
  - Frame selection
  - Radio Link Protocol (RLP) processing
- Access Network (AN)
  - BTS and RNC form the AN
- Packet Control Function (PCF)
  - Allows RNC functions to interface with PDSN
- Packet Data Service Node (PDSN)
  - Interfaces with Internet
  - Home/Foreign agent for mobile IP
  - Terminates PPP connection with AT

Simplified protocol stack



GRE= Generic Routing Encapsulation

Air interface – protocol layers

Application	Flow control protocol Location update protocol Radio link protocol	Signaling link protocol Signaling network protocol
Stream	Stream protocol	
Session	Address management protocol Session configuration protocol Session management protocol	
Connection	Air link management protocol Connected state protocol Idle state protocol Initialization state protocol	Overhead message protocol Route update protocol Packet consolidation protocol
Security	Authentication protocol Encryption protocol	Key exchange protocol Security protocol
MAC	Access channel MAC protocol Control channel MAC protocol Forward traffic channel MAC protocol Reverse traffic channel MAC protocol	
Physical	Physical layer protocol	

Air interface protocol layers

- Application layer : Radio link protocol
  - Provides reliable octet stream service
- Stream layer
  - Multiplex application layer streams
  - Four possible application streams (00 to 11)
  - Stream 00 is signaling application stream
- Session layer
  - Manage logical session: AT address, protocol parameters
- Connection layer
  - Manages air-link connection: open, close connection, update route as AT moves between cells, etc.
  - Session lasts longer than connection: close connection to conserve air-link resources when not in use (idle state), but session is still open so that re-connection is quicker
- Security layer
  - Key exchange, encryption and authentication

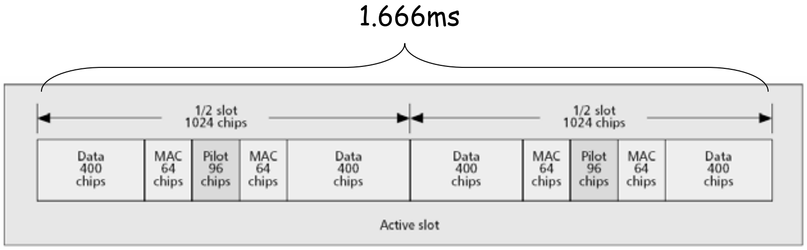
MAC Layer (forward link)

- Mechanisms to control access to the forward link
  - Open-loop rate control
    - AT’s send a request Data Rate Control (DRC) message
  - Adaptive data Scheduler-Opportunistic scheduling
  - Closed-loop rate control-Hybrid ARQ

MAC Layer (forward link)

- Forward traffic channel MAC
  - TDM on the downlink
  - Control rate of transmission
    - Each AT measures SINR
    - Reports to AN on data rate control (DRC) channel
    - AN sends at the requested rate
    - AN chooses appropriate modulation/coding for SINR
- Control channel MAC
  - Generates control channel MAC packets
  - Sent on shared control channel
  - ATs identified using AT identifier record in header
  - All ATs read identifier
  - If packet destined to that AT then read rest of packet

Downlink Slot Structure



Modified From: Naga Bhushan, Chris Lott, Peter Black, Rashid Attar, Yu-Cheun Jou, Mingxi Fan, Donna Ghosh, and Jean Au, "CDMA2000 1xEV-DO Revision A: A Physical Layer and MAC Layer Overview," IEEE Communications Magazine, February 2006

Physical Layer (forward link)

- Following channels are also used in forward link
  - Pilot channel
    - Sync- timing/phase infromation
    - SNIR
  - MAC channels
    - Reverse activity channel
    - Reverse power control channel
    - DRCLock channel (more later)
- Forward traffic channel PHY layer packet can contain 1 to 4 MAC layer packets (PHY packet can be 1024, 2048, 3072, 4096 bits long)

PHY pkt size (bits)	Data rate (kbps)	Code rate	Modulation type
1024	38.4,76.8,153.6,307.2, 614.4, 1228.8	1/5	QPSK
2048	307.2,614.4,1228.8	1/3	QPSK
3072	912.6,1843.2	1/3	8-PSK
4096	1228.8,2457.6	1/3	16-QAM

Physical Layer (forward link)

- Data (not voice) – delays ok – Turbo error correcting code can be used
- Traffic control channel
  - Use only QPSK
  - Either 76.8Kbps or 38.4Kbps
- Each PHY packet
  - Encoded: error correcting code
  - Scrambled: reduce peak-to-average ratio of RF waveform
  - Interleaved: to combat fading
  - Modulated: QPSK, 8-PSK or 16-QAM

Physical Layer (MAC channel)

- Reverse Activity (RA) channel
  - AN informs all ATs of activity on reverse channel
  - ATs decrease data rate if load is high
  - RA bits are time-multiplexed in forward channel
- Reverse Power Control (RPC) channel
  - Power control reverse channel (no power control in forward channel)
  - RPC bit time multiplexed in forward channel
- DRCLock channel
  - AN uses this channel to tell AT if AN received DRC information correctly
  - DRCLock "yes" or "no" for every time-slot
  - DRC information includes data rate (12 possible) and DRCCover (AT specifies best serving sector)

Physical Layer (Example)

- Consider a 1024 bit PHY packet
  - Data rate = 307.2Kbps
  - Code rate = 1/5
  - Modulation = QPSK
  - Length of preamble = 128 chips
- Turbo encoder converts 1024 bits to 5120 symbols
- QPSK outputs 1 symbol for every 2 input symbols
- QPSK outputs 2560 symbols
- Preamble tells: data channel or control channel
  - There are different preamble lengths
- Pilot channel: 96 chips
- MAC channel: 64 chips

MAC Layer (reverse link)

- Reverse link rate from 9.6 to 153.6 Kbps
- Power control on reverse link
- Soft handoff on reverse link
- Reverse link CDMA (not TDMA)
- Reverse traffic channel MAC determines rate
  - AT computes MaxRate based on several parameters
  - AN sends RateLimit to AT
  - AT's Max. transmission rate minimum of MaxRate and RateLimit
- Access channel MAC manages transmission and reception of signaling messages
  - AT keeps sending access probes at increasing power levels until it gets back acknowledgement from AN

Physical Layer (reverse link)

- Two PHY channels
  - Access Channel
    - Pilot channel
    - Data channel

    Used for first contact to the AN
  - Reverse Traffic Channel
    - Data channel
    - Pilot channel
    - Reverse rate indicator (RRI) channel
    - Data rate control (DRC) channel
    - ACK channel
- To conserve battery power: BPSK in reverse link (QPSK, 16QAM require high power)
- Similar to forward, reverse link
  - slot size 1.67ms
  - 2048 chips per slot (1.22Mc/s)

Physical Layer (reverse link)

- Reverse traffic channel
  - Transfers both data and signaling messages
  - One PHY packet contains one MAC packet
  - Length of PHY packet longer when length of MAC packet longer (256, 512, 1024, 2048, 4096 bits)
  - PHY packet size depends on achievable data rate

PHY pkt size (bits)	Data rate (kbps)	Code rate	Modulation type
256	9.6	1/4	BPSK
512	19.2	1/4	BPSK
1024	38.4	1/4	BPSK
2048	76.8	1/4	BPSK
4096	153.6	1/2	BPSK

  - Each PHY packet occupies 16 slots (26.67ms)
  - Turbo codes used in reverse link too (delay not a problem)

Physical Layer (reverse link)

- Data channel
  - Different Walsh code from all other channels
  - When data channel active, so is pilot & RRI channel
- DRC channel
  - AT notifies AN of AT’s home sector using DRC channel
  - Also AT requests AN to send at certain rates using DRC channel
  - AN sends on forward channel using rate requested by AT in DRC channel
  - AT may use the following chart (one implementation) to decide what rate to request

Data rate (kb/s)	E_c/N_t (dB)
38.4	–12.5
76.8	–9.5
102.6	–8.5
153.6	–6.5
204.8	–5.7
307.2	–4.0
614.4	–1.0
921.6	1.3
1228.8	3.0
1843.2	7.2
2457.6	9.5

Bender, P., et al., “CDMA/HDR: A Bandwidth Efficient High Speed Wireless Data Service for Nomadic Users,” IEEE Communications, Vol. 38, No. 7, July 2000, pp. 70-77.

Physical Layer (reverse link)

- Reverse rate indicator channel
  - Tells AN of the rate at which packet are sent in reverse-link data channel
  - 6 possible rates (including 0 Kbps)
  - Tell AN once every PHY packet (16 slots) so AN knows what rate data is coming at
- ACK channel
  - ACK/NACK a forward channel PHY packet based on CRC check success/failure
- Access channel
  - Used by AT to first contact AN
  - Rate fixed at 9.6 Kbps (access packet always 256 bits)
  - Access probe carries PHY access packet

Power control (reverse link)

- On reverse link, pilot channel, data channel, DRC channel and ACK channel are power controlled
- Both open-loop and closed-loop power control used
- Open-loop power control
  - AT receives forward pilot channel
  - AT uses this to compute mean output power in reverse link
  - Lower the received power of forward channel pilot, higher is the open-loop mean output power of reverse channels
  - Reverse link power also function of transmission rate
    - AT needs higher power to transmit at 153.6 than at 9.6 Kbps
- Closed-loop power control
  - AT receives power control bits from AN on RPC channel
  - AT changes mean output power based on these bits
  - AN has E_b/N_0 threshold
    - If received power less than threshold, send “power up” to AT
    - If received power more than threshold, send “power down”
    - Threshold is computed dynamically at AN

Adaptive modulation and coding

- Channel is time-varying: mobility, fading, etc.
- If adaptive modulation/coding not used then either
  - Design modulation/coding conservatively for good link quality but then high data rates cannot be achieved
  - Or design modulation/coding for high data rate but then link quality is low
- Adaptive: match transmission parameters to channel
  - Improves spectrum efficiency, system performance
- In EV-DO systems, AT reports DRC (based on SNR) in every time-slot (1.667 ms)
- AN uses this information to chose suitable modulation and coding for that time-slot (target packet error rate at less than 1%)

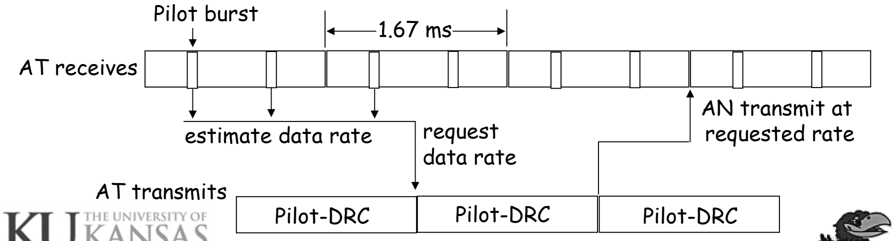
Adaptive modulation and coding

Data Rate (kbps)	Modulation type	Bits per encoder packet	Code rate	Number of slots used per packet
38.4	QPSK	1024	1/5	16
76.8	QPSK	1024	1/5	8
153.6	QPSK	1024	1/5	4
307.2	QPSK	1024	1/5	2
307.2	QPSK	2048	1/3	4
614.4	QPSK	1024	1/3	1
614.4	QPSK	2048	1/3	2
921.6	8-PSK	3072	1/3	2
1228.8	QPSK	2048	1/3	1
1228.8	16-QAM	4096	1/3	2
1843.2	8-PSK	3072	1/3	1
2457.6	16-QAM	4096	1/3	1

Forward link transmission characteristics

Adaptive modulation and coding

- AN sends pilot bursts in every time-slot
- AT estimates SNR using pilot bursts
- AT uses estimated SNR to request a data-rate on the data-rate request channel (DRC)
- AN sends at requested rate using suitable modulation/coding for that data rate



Pilot burst

1.67 ms

AT receives

estimate data rate

request
data rate

AN transmit at
requested rate

AT transmits

Pilot-DRC

Pilot-DRC

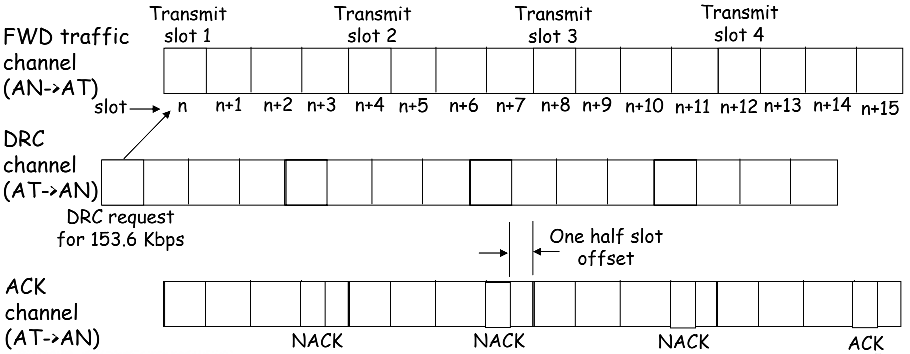
Pilot-DRC

Hybrid ARQ (PHY layer ARQ)

- PHY ARQ faster than link layer ARQ
- Makes adaptive modulation/coding more robust
  - DRC mechanism discussed previously provides initial estimate of redundancy required
  - Hybrid ARQ enables fine tuning of effective code rate
- For EV-DO multi-slot packets
  - AT ACKS or NACKS data received in each slot
  - Incremental coding is used to soft-combine data
  - Erroneous data is not discarded but combined with the data in next slot
  - Yields lower bit-rate than discarding erroneous data

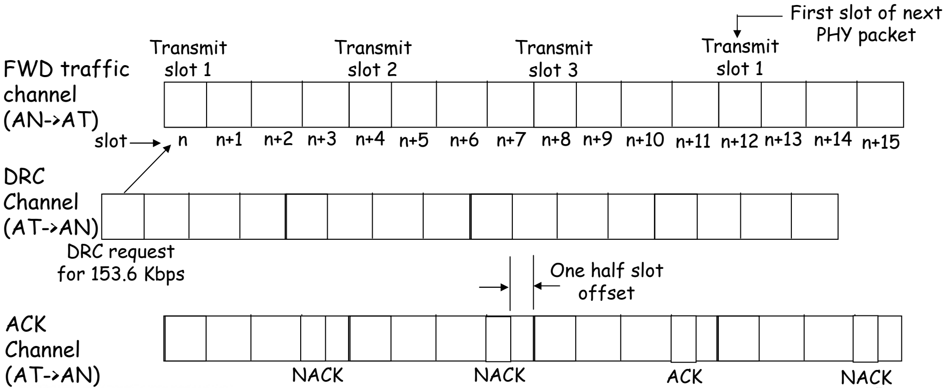
Hybrid ARQ (PHY layer ARQ)

- Multi-slot transmissions interleaved by 3 slots
  - Allows time to receive NACK/ACK
- Example case: 153.6kbps – QPSK – 4 slots – 1/5 coding



Hybrid ARQ (PHY layer ARQ)

- If channel conditions improve since DRC request
  - Data can be received correctly with less coding
  - Early termination possible in that case



Radio link protocol (RLP)

- Reliable octet-stream service to higher layers
  - Provides retransmission
  - Provides duplicate detection
- Transmitter
  - Creates RLP segments from octet-stream
  - Appends sequence number to each segment
- Receiver
  - Detects duplicate/missing segments
  - Delete duplicate segments
  - Send negative ack for missing segments (transmitter retransmits missing segment only once)
  - If no missing segments, send data to higher layer
  - If missing segment retransmitted and lost, send data to higher layer – it is up to the higher layers to recover now

---

Case study

Mitigating scheduler-induced starvation in 3G wireless networks

Soshant Bali*, Sridhar Machiraju**, Hui Zang**

See: A Measurement Study of Scheduler-based Attacks in 3G Wireless Networks
Soshant Bali, Sridhar Machiraju, Hui Zang, Victor Frost, Passive and Active Measurement. April 5-6, 2007, Louvain-la-neuve, Belgium

* ITTC, Univ. of Kansas, Lawrence, Kansas
** Sprint Advanced Technology Lab, Burlingame, California

Outline

- Introduction
- Problem: PF with on-off traffic
  - High jitter
  - Throughput reduction
  - Increased flow completion time
- Solution
  - Parallel PF
  - Shrinking alpha

Introduction

- 3G-wireless widely deployed
- Sprint and Verizon use 1xEV-DO
  - 1x Evolution for Data Optimized
  - Up to 2.45Mbps downlink, 153.6Kbps uplink
  - Natural evolution from IS-95, IS-2000
  - Evolution: leverage existing network elements
  - Optimized for data transfer
- Data service characteristics
  - Rates asymmetric
    - EV-DO: higher rate in forward link
  - Latency can be tolerated
    - EV-DO: uses link layer ARQ
    - EV-DO: powerful error-correcting codes (e.g., turbo codes)
    - PHY packet error rate < 1%, ARQ on top of that = Reliable link
  - Transmissions are in burst
    - EV-DO: uses time-division multiplexing

Introduction

- Scheduler
  - Time divided into time-slots
  - Scheduling problem: Base station has to decide which mobile it should send data to in next time slot
  - EV-DO and HSDPA use PF scheduler
    - Channel-aware scheduler
    - Improves system throughput
    - Very well researched, shown to have very good performance
    - Widely deployed (all major vendors implement and recommend using this algorithm)
- Contribution
  - PF scheduler can easily lead to starvation of mobiles
    - Deliberately (malicious user)
    - Accidentally (one mobile web browsing can cause impairments to other mobile users)
  - Propose and evaluate starvation resistant scheduler

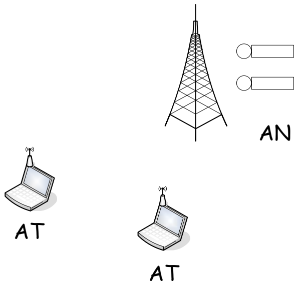
EVDO: adaptive modulation/coding

- Channel conditions are time-varying: mobility, fading, etc.
- If adaptive modulation/coding not used then either
  - Design modulation/coding conservatively for good link quality but then high data rates cannot be achieved
  - Or design modulation/coding for high data rate but then link quality is low
- Adaptive: match transmission parameters to channel conditions
  - Improves spectrum efficiency, system performance
- AT measures SINR every time slot (1.67ms) and in determines suitable DRC (data rate control)
- AT reports DRC in every time-slot
- AN uses this information to chose suitable modulation and coding for that time-slot

  (target packet error rate is less than 1%)

EVDO scheduler

- DRC tells AN what modulation/coding to use for an AT for each time slot
- However, DRCs can also be used by scheduler to make better scheduling decisions
- AN gets DRC information for each time slot from all K ATs
- Scheduler at AN must decide which AT to allocate the next time slot to
- If scheduler uses DRC information to make scheduling decision then channel-aware scheduler (e.g. PF)
- If does not use DRC information then not channel-aware (e.g., Round Robin)
- Channel-aware scheduling improves system throughput and throughput of achieved by individual ATs

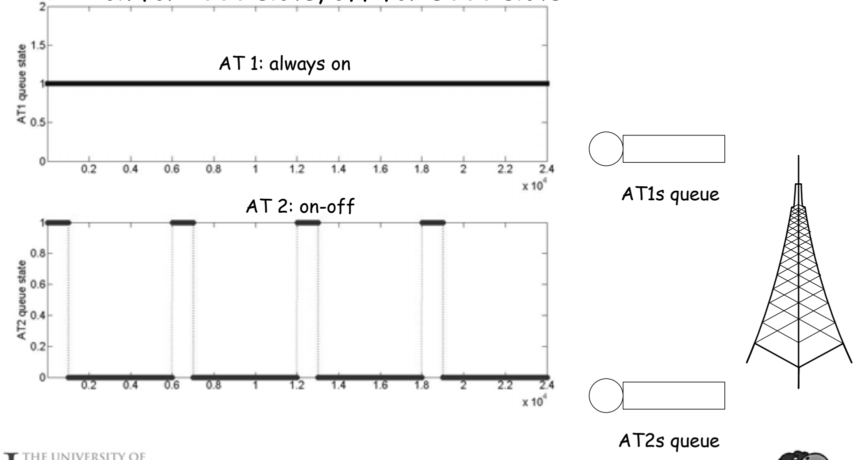


PF scheduler with on-off traffic

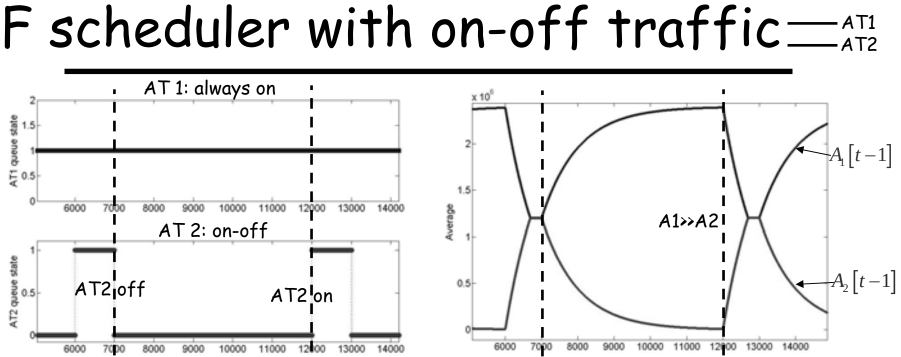
- PF design assumes infinite backlog, but…..
  - Traffic commonly on-off, e.g., web browsing
- Problem: on-off traffic causes starvation
  - When off, no slots allocated to that AT
  - Average decays when no slots allocated
  - When on after long off, average is very low
  - AT that goes on has highest R/A amongst all ATs (low A)
  - AT that goes on gets all slots until A increases
  - This starves other ATs
- PF widely deployed and can be easily corrupted
  - Deliberately (attacks using burst UDP)
  - Accidentally (web browsing)

PF scheduler with on-off traffic

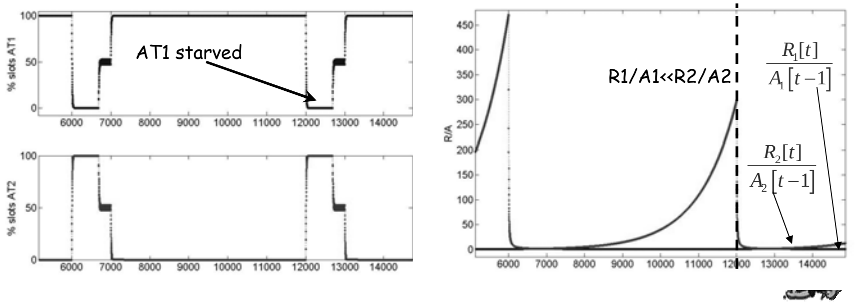
- AT1 infinitely backlogged
- AT2: on for 1000 slots, off for 5000 slots



PF scheduler with on-off traffic

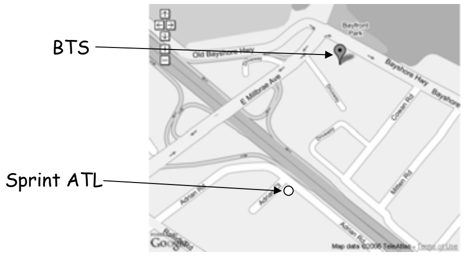


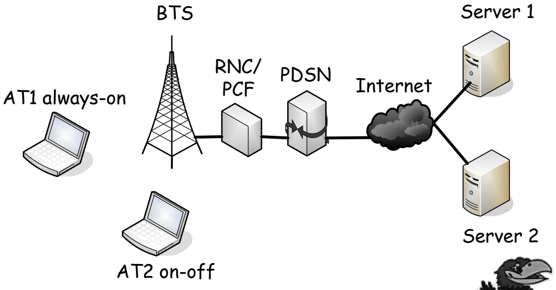
Conclusion: Sending on-off traffic to one laptop can lead to starvation in other AT's



Experiment configuration

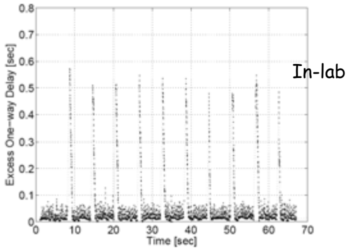
- Typical setup
  - AT1 always-on
  - AT2 on-off
- In deployed network
- In lab
  - AT1, AT2 the only users
  - No wireless cross traffic

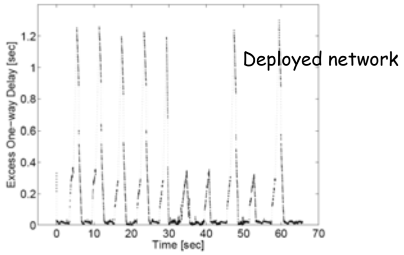


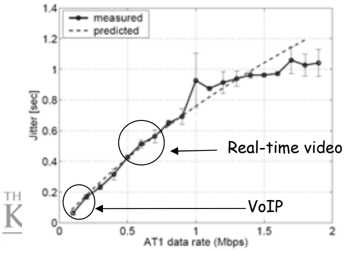


Starvation of real-time flows

- AT1: 1500 Byte UDP packet once every 20ms
- AT2: burst of 250 1500 Byte UDP packets once every 6 sec
- AT1's latency increases when burst for AT2 arrives
- Delayed packets may be lost if playout deadlines missed - impairments
- Increase in delay is a function of AT1's rate
  - Impact on VoIP
  - Impact on real-time video







Excess delay= Delay – Min_Delay
(Account for unsynchronized clocks)

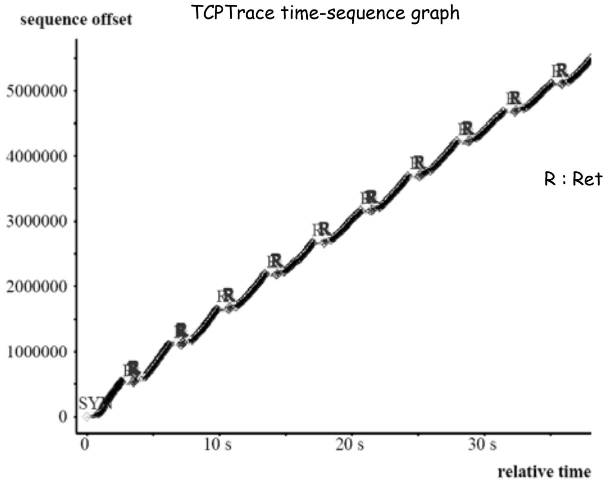
TCP throughput reduction

- Two-user case
  - AT1 downloads a file using TCP
  - AT2 sends periodic bursts of UDP packets
  - TCP to AT1 times out when UDP bursts to AT2 arrive
    - Reduces TCP throughput
    - Increases flow completion time

TCP throughput reduction

- TCP timeouts when burst arrives for another AT
- AT1 download 20MB file, AT2 sends 150 pkt. burst every 4 sec

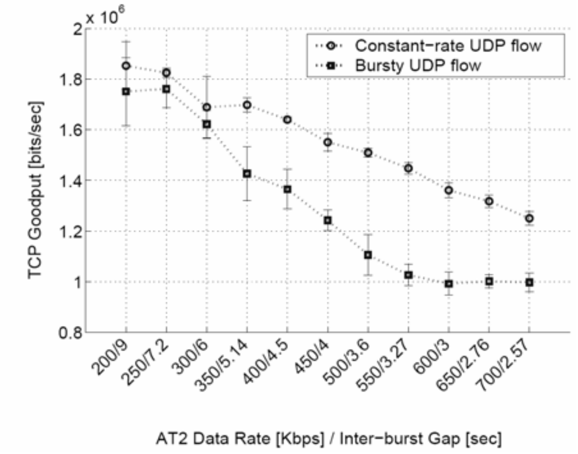
TCPTrace time-sequence graph



R : Retransmission

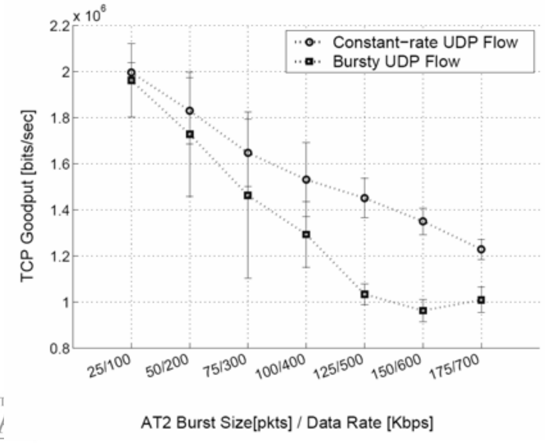
TCP throughput reduction: long flows

- AT1 downloads 20 MB file (using TCP), AT2 sends cbr or bursty UDP traffic; burst size = 150 packets
- Which inter-burst gap has maximum impact with minimal overhead?



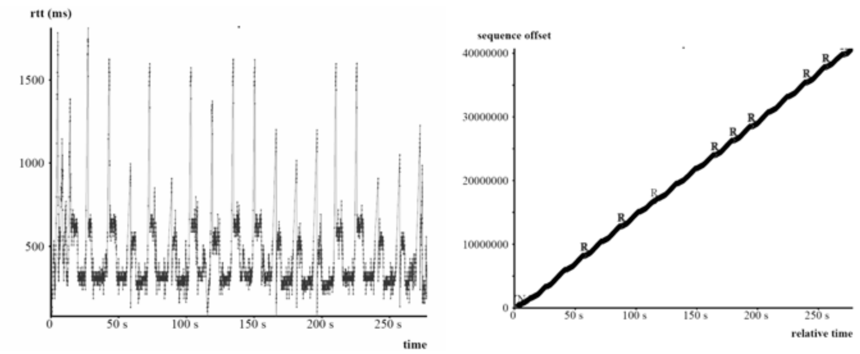
TCP throughput reduction: long flows

- AT1 downloads 20 MB file, AT2 sends cbr or bursty UDP traffic; burst size = variable, interval burst gap = 3 s
- Which burst size has maximum impact with minimum overhead?



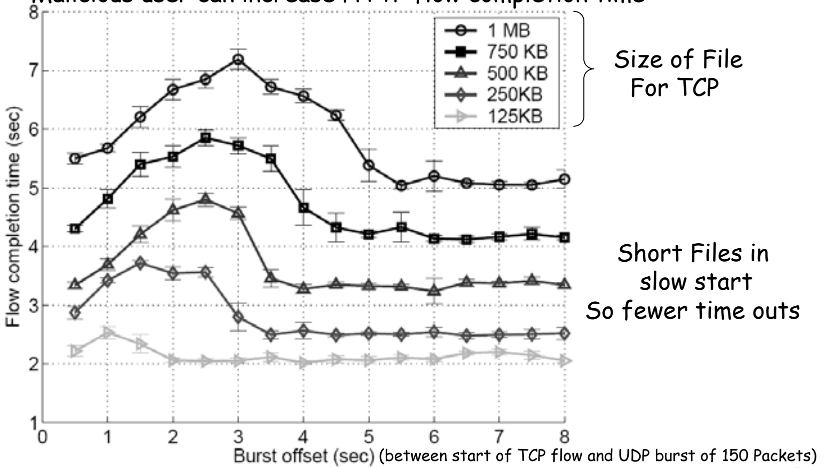
HTTP induced TCP throughput reduction

- AT1 downloads 20 MB file, AT2 downloads 500KB file every 15 sec
- Does not have to be malicious user: accidental due to web browsing



TCP increased flow completion time: medium flows

- For all but very short flows, significant effect
- Malicious user can increase HTTP flow completion time



Size of File
For TCP

Short Files in
slow start
So fewer time outs

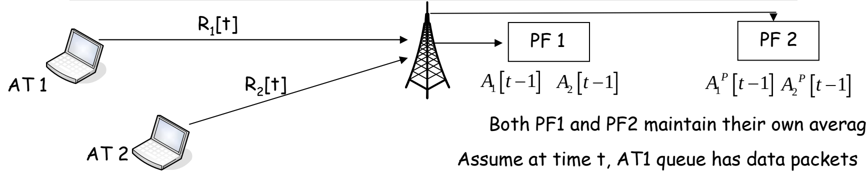
(between start of TCP flow and UDP burst of 150 Packets)

Solution: parallel PF scheduler

- Note that the PF scheduler analysis assumes that all ATs are backlogged (that is, in the on state)
- The normal PF scheduler implementation for an AT in the off state the A(k) is small.
- The PPF scheduler uses an additional parallel (virtual) instance of PF that assumes all ATs are backlogged
- When an AT changes from off to on then the average from the virtual PF scheduler is used
- The virtual PF scheduler needs an initial value of A(k)→ later

---

Solution: parallel PF scheduler



Both PF1 and PF2 maintain their own averages

Assume at time t, AT1 queue has data packets (always on)and AT2 queue is empty (in off state)
Note: packet > Time slot

Compute $R_k[t]/A_k[t-1]$ for AT k=1, since there is no data for AT2. Final scheduling decided by PF1	Compute $R_k[t]/A_k^P[t-1]$ for each AT k. PF2 does not look at the Queues. Assumes backlogged
Update $A_k[t]$ for all k	Update $A_k^P[t]$ for all k

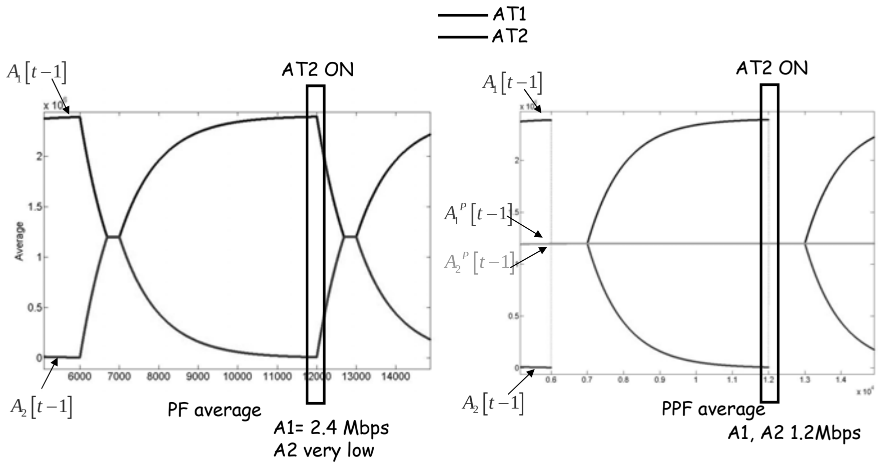
At time t+M, AT2 queue receives data for AT2

$A_k[t+M-1]= A_k^P[t+M-1]$

Compute $R_k[t]/A_k[t-1]$ for all k. AT with highest ratio gets slot.

Summary:-
- PF1 decides final scheduling
- PF2 only virtual scheduling
- PF1 aware of queue size
- PF2 unaware of queue size
- When on after off, copy averages from PF2 to PF1

Parallel PF scheduler



PF average

A1= 2.4 Mbps
A2 very low

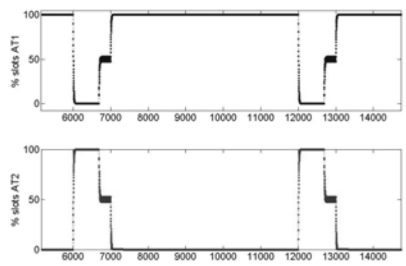
PPF average

A1, A2 1.2Mbps

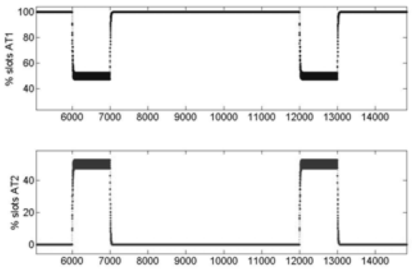
Parallel PF scheduler

- PF: AT1 starved when AT2 goes from off to on
- PPF: Both AT1 and AT2 get equal share of slots immediately after AT2 goes from off to on

PF

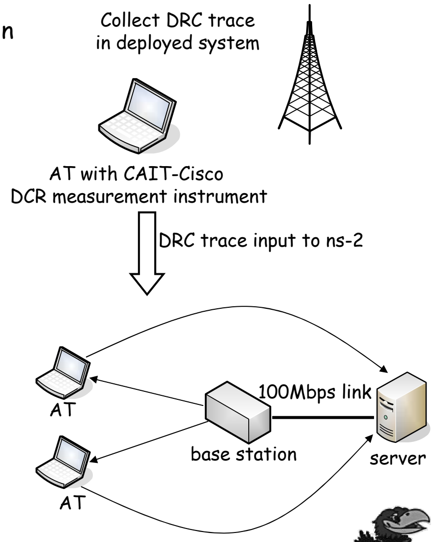


PPF



Simulation setup

- Collect stationary user DRC trace in deployed system using CDMA air interface tester (CAIT)
- DRC trace input to ns-2
- Server-base station 100Mbps
- Base station queue sizes > largest UDP burst (no losses)
- Base-station to AT DRC variable (from trace)
  - Loss probability = 0
  - RLP not implemented (not needed)
- High bandwidth link from AT to server
- Traced based simulation, DRC's from real channel measurements



Collect DRC trace in deployed system

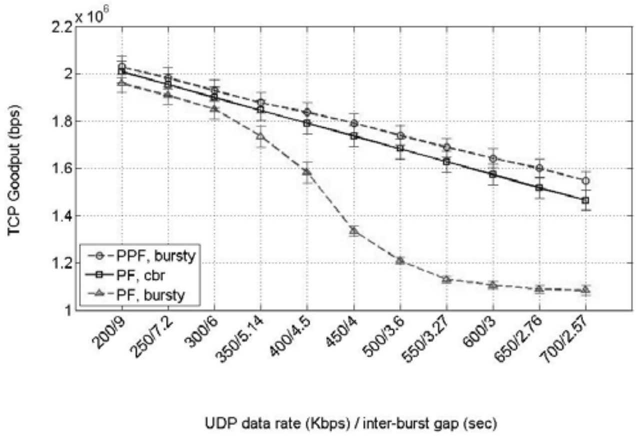
AT with CAIT-Cisco DCR measurement instrument

DRC trace input to ns-2

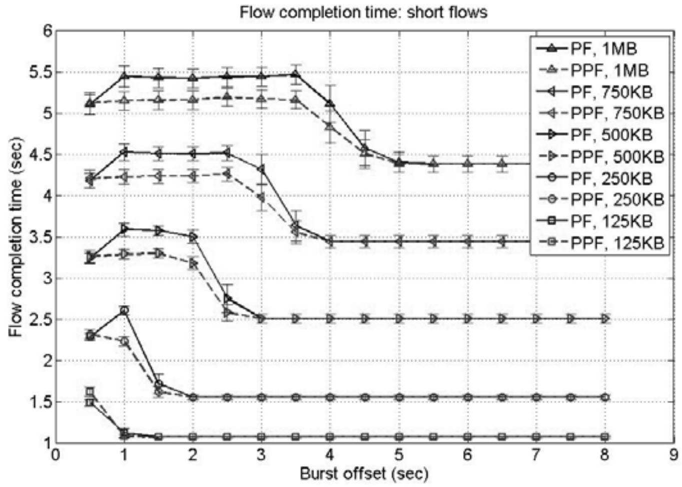
ns-2 model

TCP throughput reduction: long flows

- AT1 downloads 20 MB file, AT2 sends cbr or bursty UDP traffic; burst size = 150 packets
- Figure shows that PPF is robust to starvation due to UDP bursts

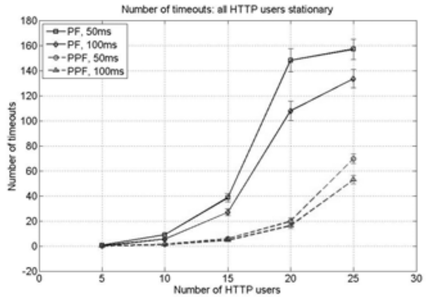


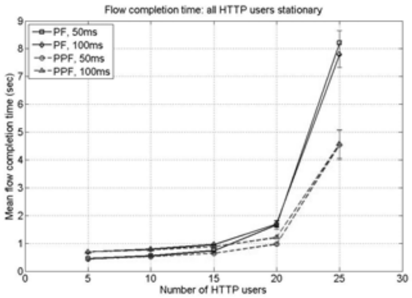
TCP increased flow completion time: medium flows



PF and PPF : HTTP users

- All users HTTP
- File size: uniform 10KB to 100KB
- Time b/w downloads: uniform 2 to 8 sec
- Stationary DRCs





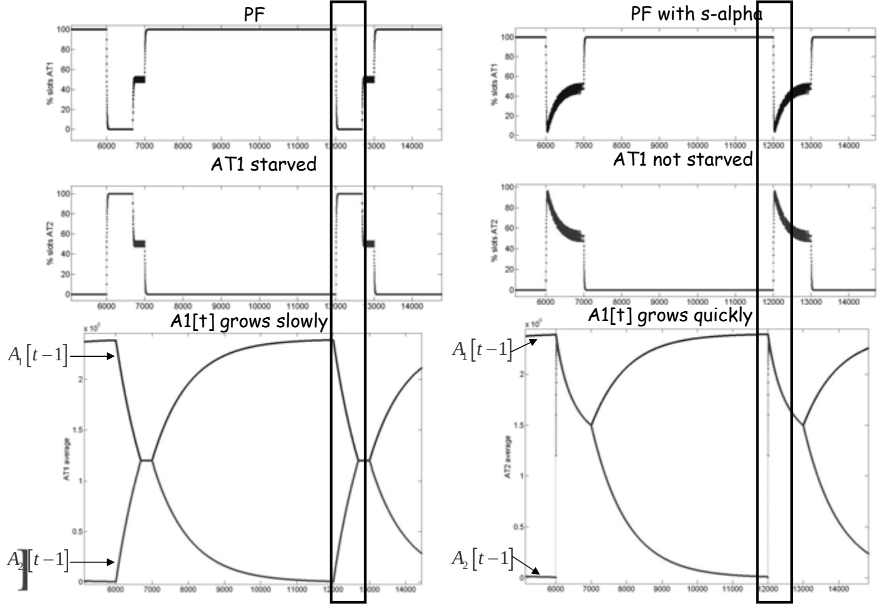
Initial values for A(k)

- If Off time small enough then can use last observation
- After about 12 sec inactivity
  - AT connection goes into sleep mode
  - DRC not reported
  - PPF cannot work
- If flow restarts after 12 or more sec
  - Average resets to zero
  - AT that restarts gets all slots for some time
  - Other ATs starved

Longer inactivity: shrinking alpha

- Solution: use s-alpha when flow restarts
  - Slot 1: average=0, alpha=1
  - Slot 2: alpha=1/2, slot 3: alpha=1/3 … slot 1000: alpha=1/1000
  - Average converges faster than if slot 1: alpha=1/1000

S-alpha



Conclusions

- PF can be easily corrupted
  - Deliberately (attacks using burst UDP)
  - Accidentally (web browsing)
- Solution
  - Parallel PF
  - Shrinking alpha
  - Combination makes PF robust to corruption
- Lessons learned
  - PF is well researched, widely deployed
  - Security issues were not considered
    - Design algorithms taking security into consideration
  - Infinite queue backlog assumption
    - Simplifying assumptions good for analytical optimality results
    - But evaluate algorithms for when assumptions violated
    - Specially when assumption does not represent the common-case scenario

References

- TIA/EIA/IS-856, cdma2000 High Rate Packet Data Air Interface Specification, Telecommunications Industry Association, January 2002.
- Samuel C. Yang, “3G CDMA 2000: Wireless System Engineering,” Artech House Inc.
- Kamran Etemad, “CDMA 2000 Evolution,” John Wiley and Sons Inc., 2004
- Mooi Choo Chuah and QinQing Zhnag, “Design and Performance of 3G Wireless Networks and Wireless LANs,” Springer Inc., 2006.
- Bender, P., et al., “CDMA/HDR: A Bandwidth Efficient High Speed Wireless Data Service for Nomadic Users,” IEEE Communications, Vol. 38, No. 7, July 2000, pp. 70-77.
- Soshant Bali, Sridhar Machiraju, Hui Zang, Victor Frost, “A Measurement Study of Scheduler-based Attacks in 3G Wireless Networks, Passive and Active Measurement,” April 5-6, 2007, Louvain-la-neuve, Belgium

---

References