Exploiting Opportunistic Scheduling in Cellular Data Networks

Radmilo Racic, Denys Ma
Hao Chen, Xin Liu

University of California, Davis

3G Cellular Networks

- Provide high speed downlink data access
- Examples
  - HSDPA (High Speed Downlink Packet Access)
  - EVDO (Evolution-Data Optimized)
- Approach: exploring multi-user diversity
  - Time-varying channel condition
  - Location-dependent channel condition
- Opportunistic scheduling
  - Embracing multi-user diversity

TDM (Time Division Multiplexing)

- Base station use TDM to divide channels into time slots
- TTI (Transmission Time Interval)
  - HSDPA: 2 ms
  - EVDO: 1.67 ms

Opportunistic Scheduling

- Assumptions
  - Phones' channel conditions fluctuate independently
  - But some varying set of phones may have strong channel conditions at any moment
- Opportunistic scheduling
  - Phones measure and report their CQIs (Channel Quality Indicators) to base station periodically
  - Base station schedules a phone with good channel condition

Proportional Fair (PF) Scheduler

- Motivation: strike a balance between throughput and fairness in a single cell
- Goal: maximize the product of the throughput of all users

PF Algorithm

Base station schedules $\arg\max_i \frac{CQI_i(t)}{R_i(t)}$

$CQI_i(t)$: Instantaneous channel condition of user i

$R_i(t)$: Average throughput of user i, often calculated using a sliding window

$$R_i(t) = \begin{cases} \alpha CQI_i(t) + (1-\alpha)R_i(t-1) & \text{if } i \text{ is scheduled} \\ (1-\alpha)R_i(t-1) & \text{otherwise} \end{cases}$$

PF Vulnerabilities

- Base station does not verify phone's CQI reports
  - Attack: malicious phones may fabricate CQI
- PF guarantees fairness only within a cell
  - Attack: malicious phones may exploit hand offs
- Design flaw: cellular networks trust cell phones for network management

Attacks

- Goal: malicious phones hoard time slots
- Two-tier attacks
  - Intra-cell attack: exploit unverified CQI reports
  - Inter-cell attack: exploit hand off procedure
- We studied attack impact via simulation

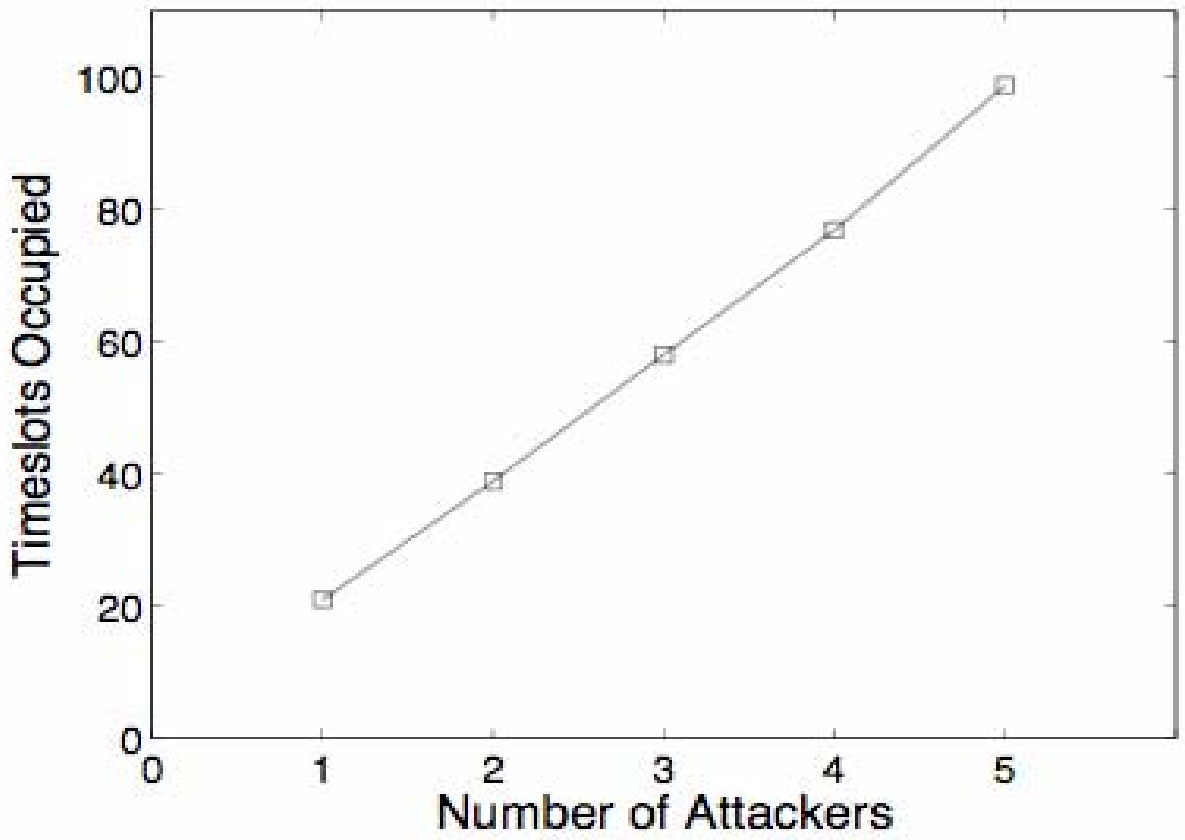
Threat Model

- Assumptions
  - Attackers control a few phones admitted into the network, e.g.:
    - Via malware on cell phones
    - Via pre-paid cellular data cards
  - Attackers have modified phones to report arbitrary CQI and to initiate hand off
- We do not assume that attacker hacks into the network

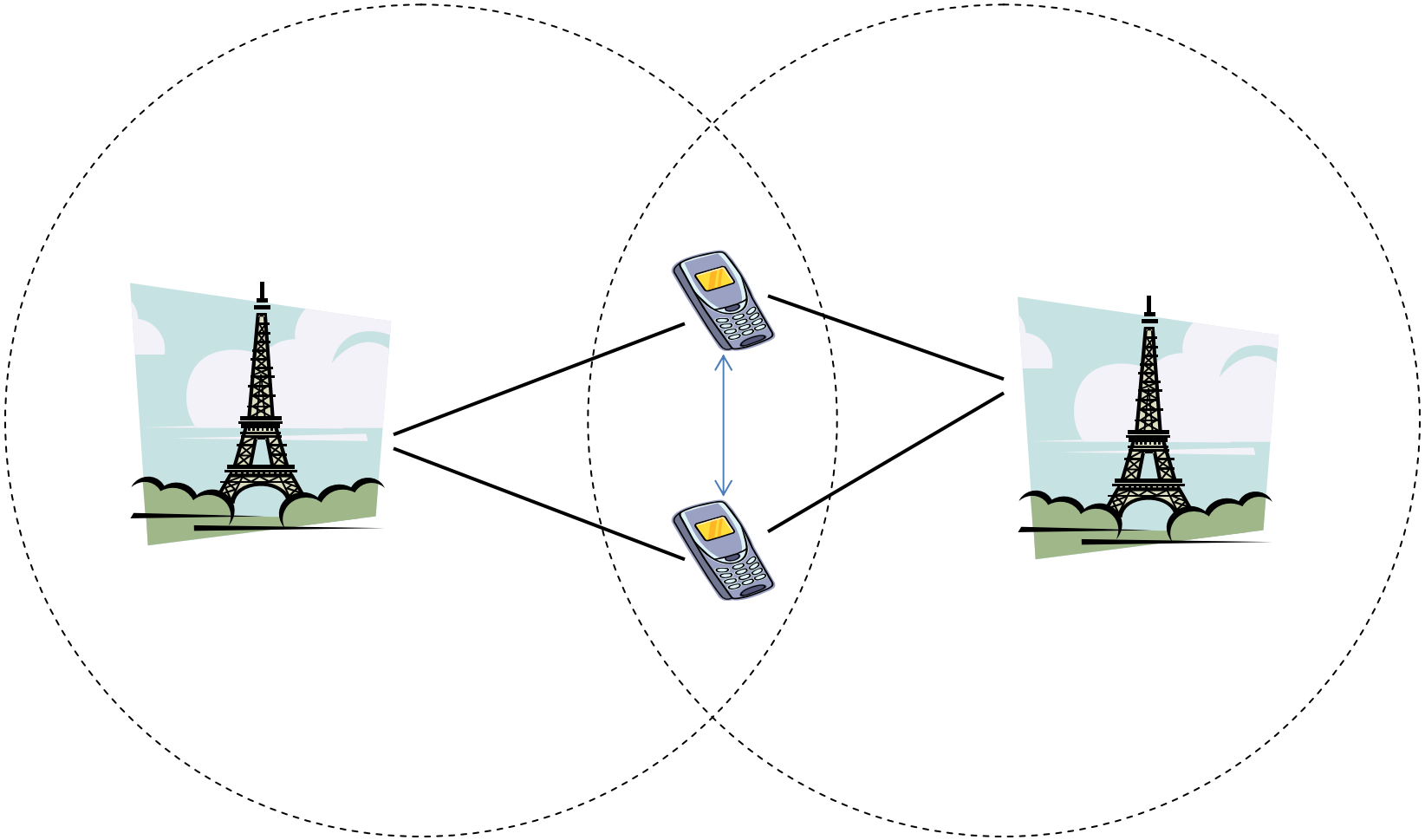
Intra-cell Attack

- Assumption: attacker knows CQI of every phone (we will relax this assumption later)
- Approach: at each time slot, attackers
  - Calculate $CQI_i(t)$ required to obtain max $\frac{CQI_i(t)}{R_i(t)}$
  - Report $CQI_i(t)$ to base station

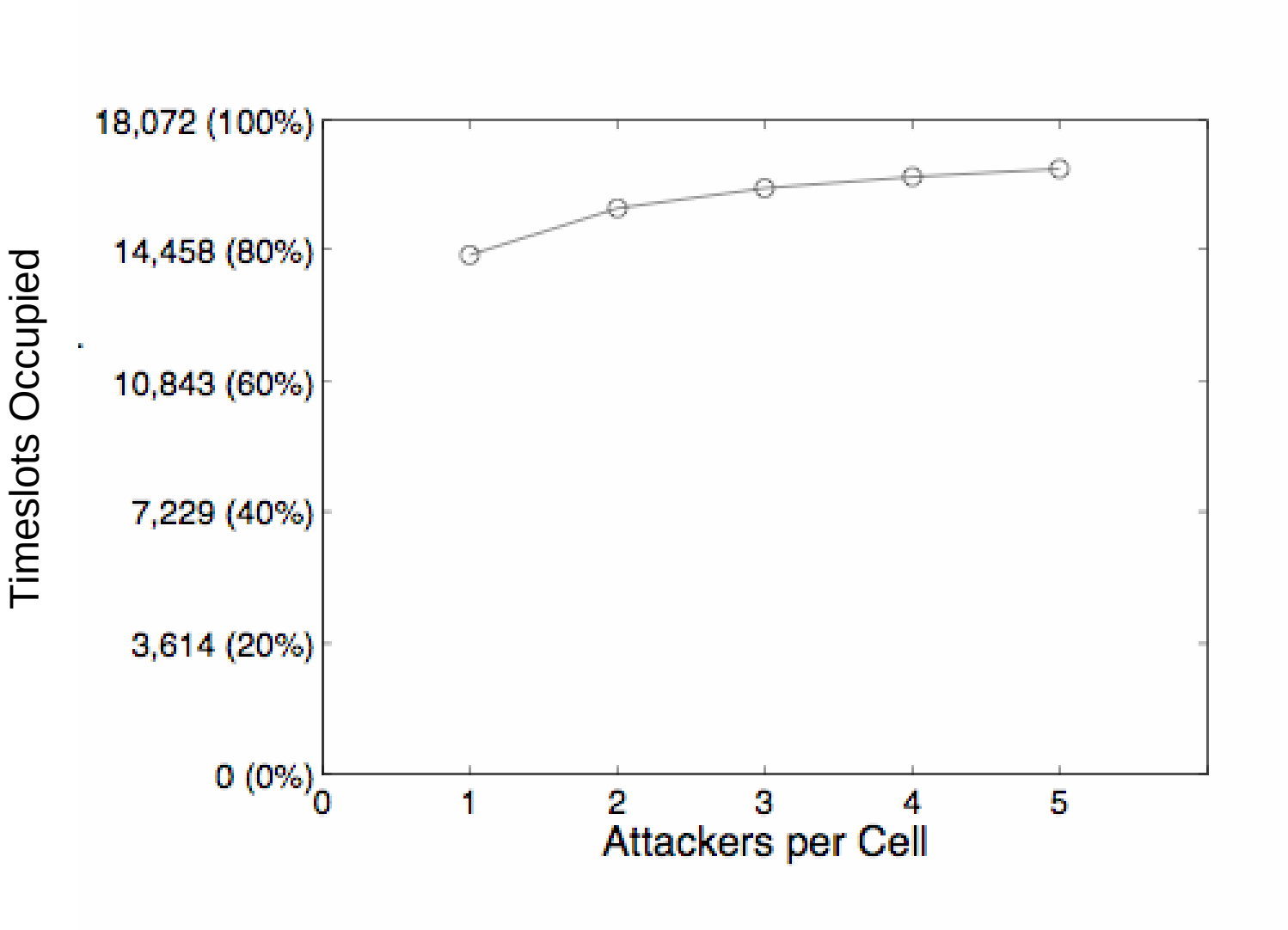
Results from Intra-cell Attack



Inter-cell Attack



Results from Inter-cell Attack

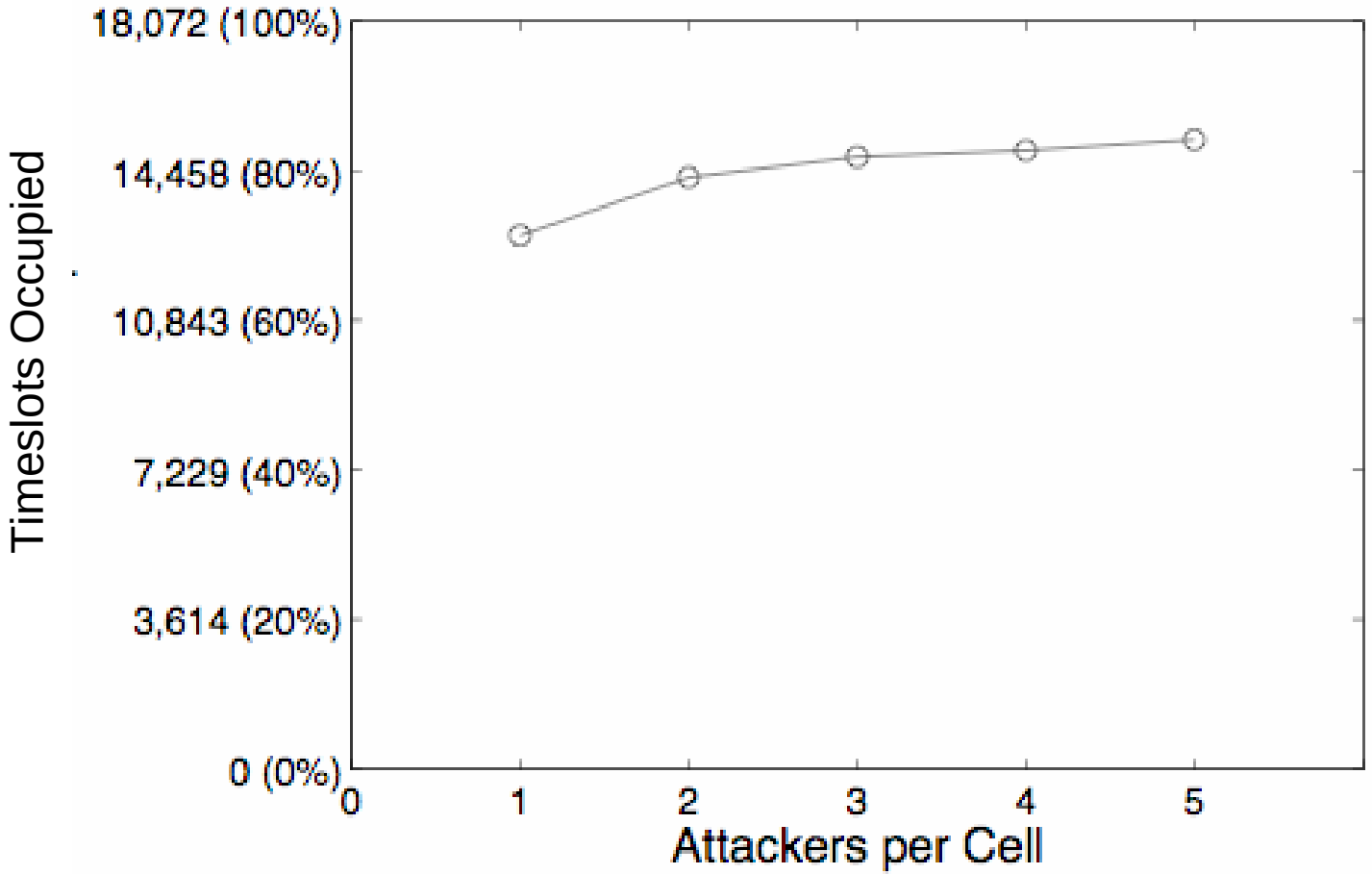


Attack without Knowing CQIs

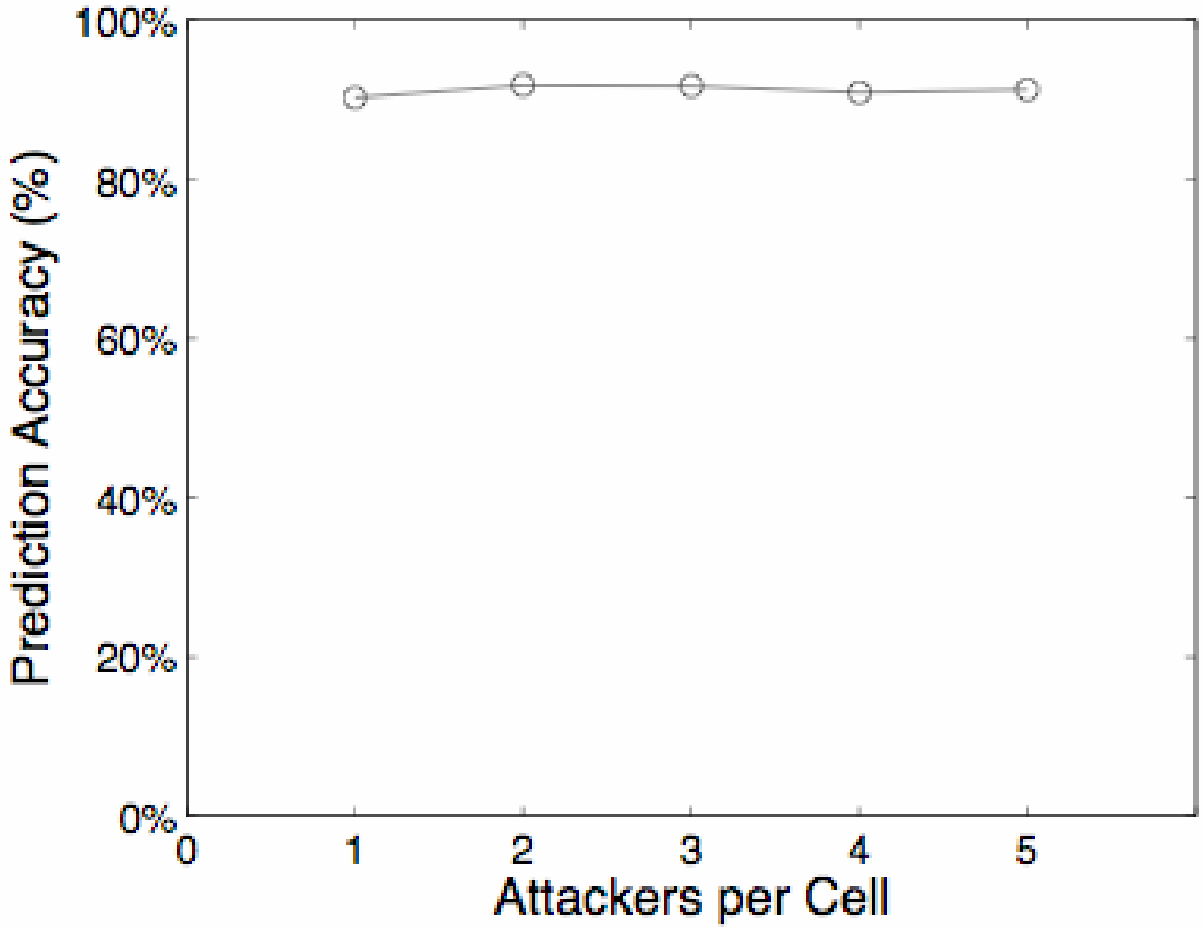
- Problem
  - Attack needs to calculate $\max_i \frac{CQI_i(t)}{R_i(t)}$
  - But attacker may not know the every phone's $\frac{CQI_i(t)}{R_i(t)}$
- Solution: estimate $c(t) = \max_i \frac{CQI_i(t)}{R_i(t)}$

$$c(t+1) = \begin{cases} c(t)/(1-\varepsilon) & \text{if attacker is scheduled} \\ c(t)/(1+\sigma(c(t)-1)) & \text{otherwise} \end{cases}$$

Results from Unknown CQI Attack



CQI Prediction Accuracy



Attack Impact on Throughput

- Before attack
  - 40-55 kbps
- After attack (1 attacker, 49 victim users)
  - Attacker: 1.5M bps
  - Each victim user: 10-15 kbps

Attack Impact on Average Delay

- Before attack
  - 0.01s between two consecutive transmissions
- After attack (in a cell of 50 users)
  - One attacker causes 0.81s delay
  - Five attackers cause 1.80s delay
- Impact: disrupt delay-sensitive data traffic
  - E.g.: VoIP useless if delay > 0.4s

Attack Detection

- Detect anomalies in
  - Average throughput
  - Frequency of handoffs
- Limitations
  - Difficult to determine appropriate parameters
  - False positives

Attack Prevetion

- Goal: extend PF to enforce global fairness during hand-off
- Approach: estimate the initial average throughput in the new cell
- Estimate average throughput as:

$$R = E(CQI)\frac{G(N)}{N}$$

$E(CQI)$: expection of CQI

$G(N)$: opportunistic scheduling gain

N: number of users

Attack Prevention (cont.)

$$\frac{R_B}{R_A} = \frac{E(CQI_B)\dfrac{G(N_B)}{N_B}}{E(CQI_A)\dfrac{G(N_A)}{N_A}} \approx \frac{\dfrac{G(N_B)}{N_B}}{\dfrac{G(N_A)}{N_A}}$$

Related Work

- Attacks on scheduling in cellular networks
  - Using bursty traffic [Bali 07]
- Other attacks on cellular networks
  - Using SMS [Enck 05] [Traynor 06]
  - Attacking connection establishment [Traynor 07]
  - Attacking battery power [Racic 06]

Conclusion

- Cellular networks grant unwarranted trust in mobile phones
- We discovered vulnerabilities in PF scheduler
  - Malicious phone may fabricate CQI reports
  - Malicious phone may request arbitrary hand offs
- Attack can severely reduce bandwidth and disrupt delay-sensitive applications
- Propose to enforce global fairness in PF to prevent attack