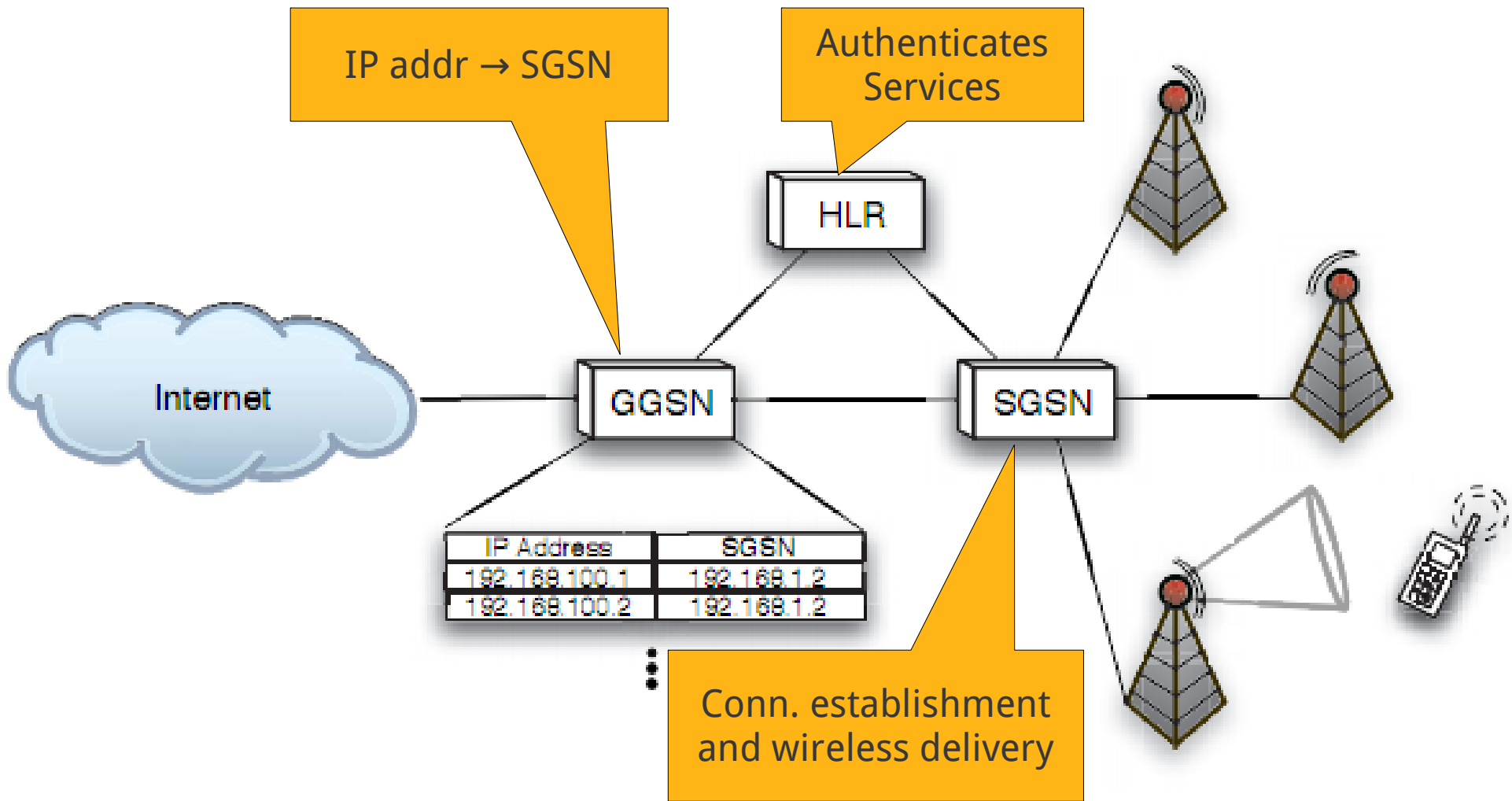
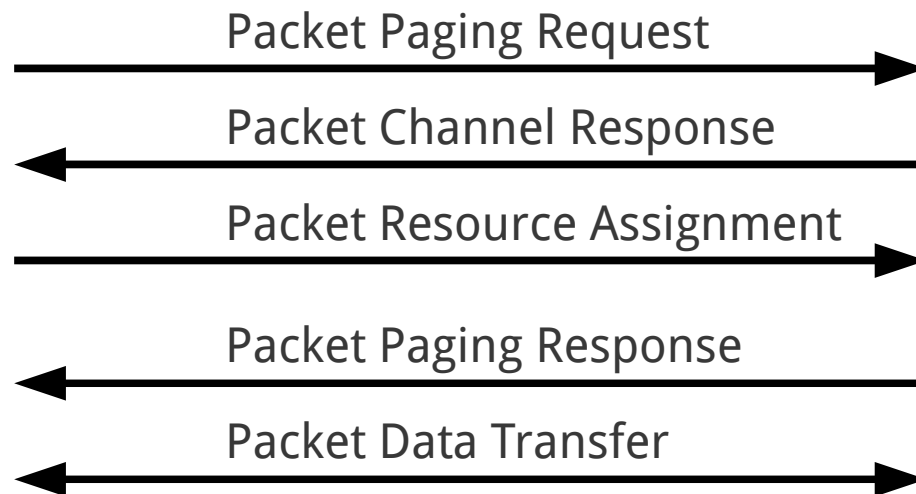
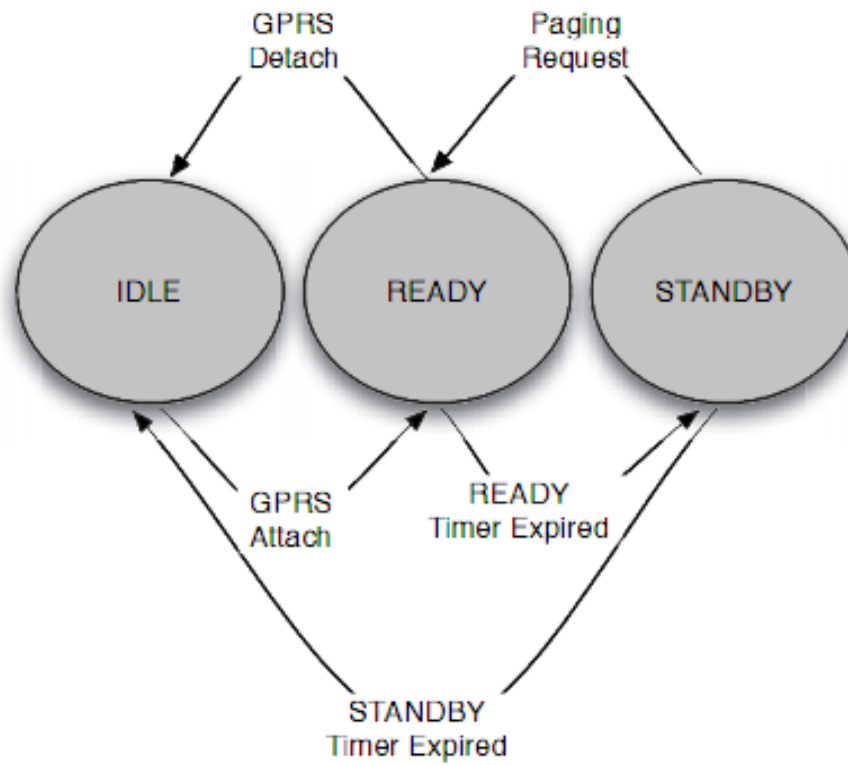


# On Attack Causality in Internet-Connected Cellular Networks

Patrick Traynor, Patrick McDaniel and  
Thomas La Porta

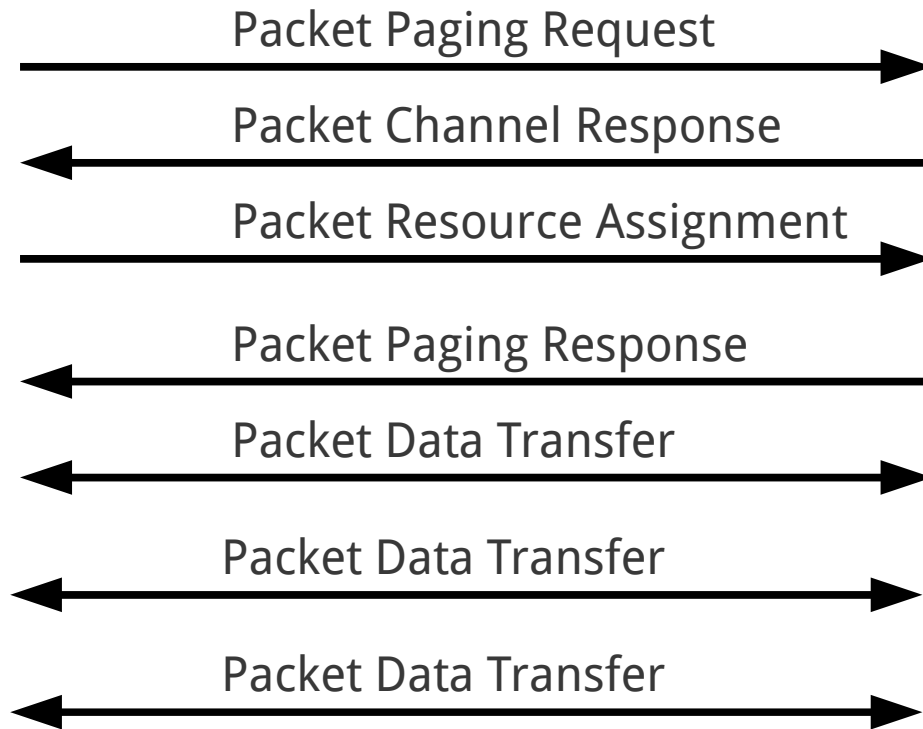


Internet → Cellphone architecture





Temporary Flow Identifier Assigned (5 bits)



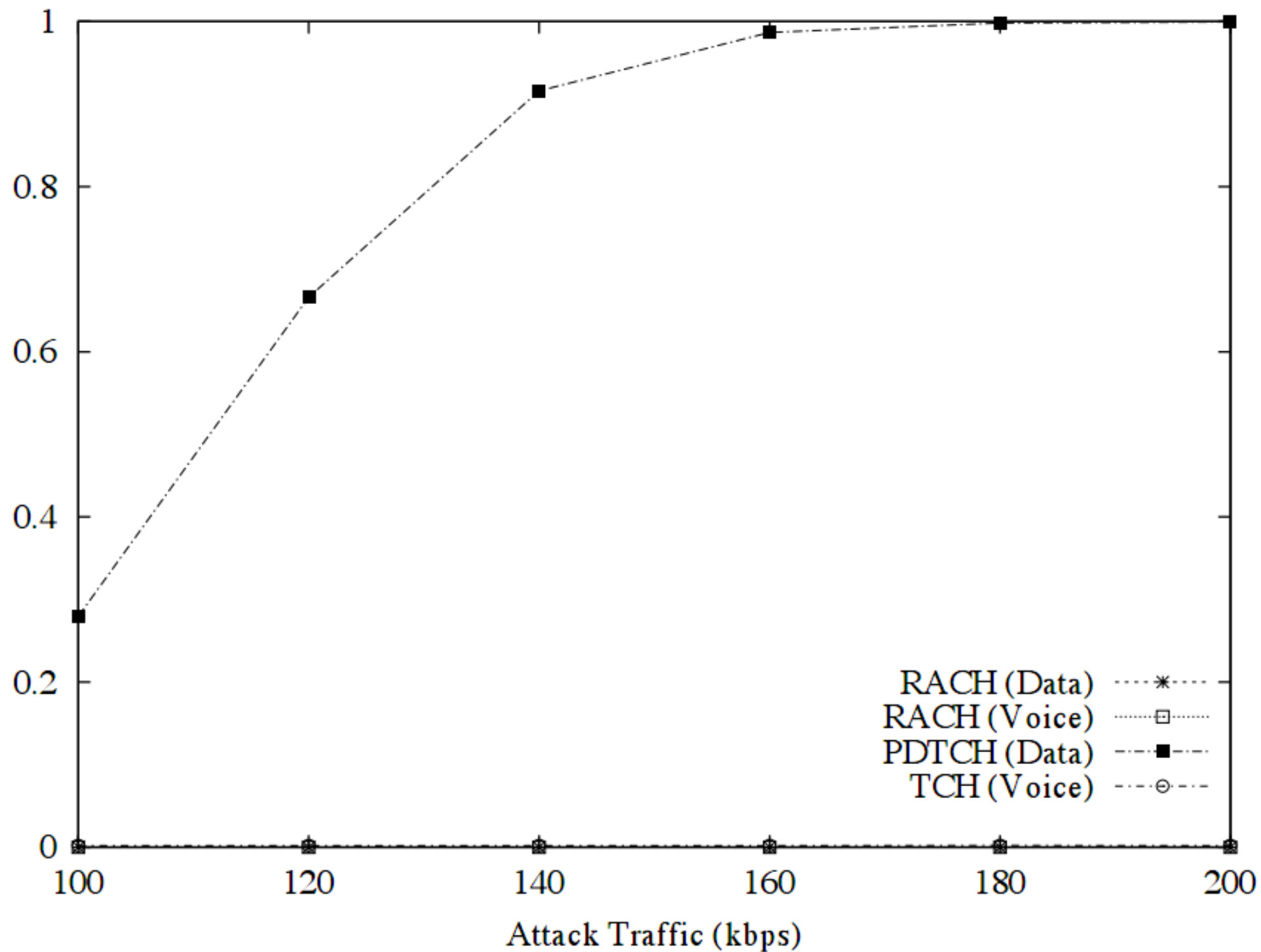
5 seconds

Temporary Flow Identifier Recovered

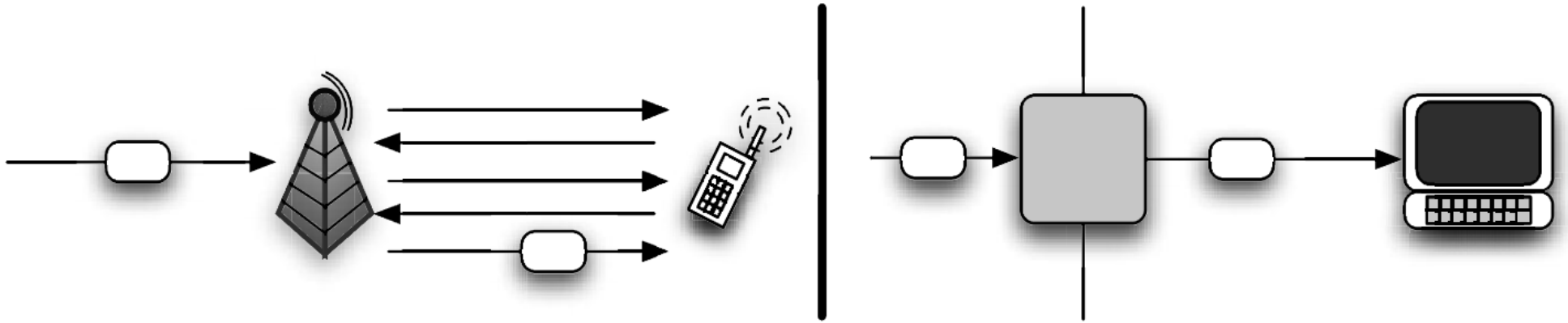
# Temporary Flow Identifier Exhaustion Attack

- Building on TDMA
- Each flow has a Temporary Flow Identifier (TFI)
  - 5 bit field
  - 5 second timer (reset to 0 each time a packet is delivered)
- Manhattan
  - $(55 \text{ sectors}) \times (32 \text{ msgs / sector}) \times (41 \text{ bytes / msg}) \times (1 / 5 \text{ sec})$
  - $\approx 110 \text{ Kbps}$
- If brute force attack on physical channels (frequency)
  - $(55 \text{ sectors}) \times (172 \text{ Kbps / freq}) \times (8 \text{ freq / sector})$
  - 73 Mbps

Average Percent Blocking During Attack



# Architecture Choices



- 5 bits – restricted bandwidth available to GPRS / EDGE
- Attack vulnerability + violation of end-to-end principle → connection setup
- Connection setup ← power saving  
(idle ↔ ready ↔ standby)
- Laptops → power saving?