

# Challenges in Wireless Network Measurement

David Kotz  
Dartmouth College  
April 3, 2005

*WinMee 2005*  
*Riva del Garda, Italy*

# Wireless is not Wired

- Many inherent differences
  - Wired medium: clear points of connection
  - Wireless medium: physically dispersed
- Mobility inspires new usage patterns
- Novel devices inspire new usage patterns

# Why measure?

- To improve our understanding of user and network behavior.
- This understanding leads to better models.
- Better models are critical to innovation:
  - network protocols
  - distributed algorithms and applications
  - deployment strategy

# What do we measure?

- We measure *production networks*
  - to learn about real users and real traffic
- We measure *controlled networks*
  - for careful study of network behavior

# Measuring real wireless networks

# Measuring real networks: Practical challenges

- Lack of portable tools for collection, analysis
- Lack of information about network hardware
- Lack of common data formats
- Reluctance of network administrators
- Avoiding, identifying, and handling data “holes”

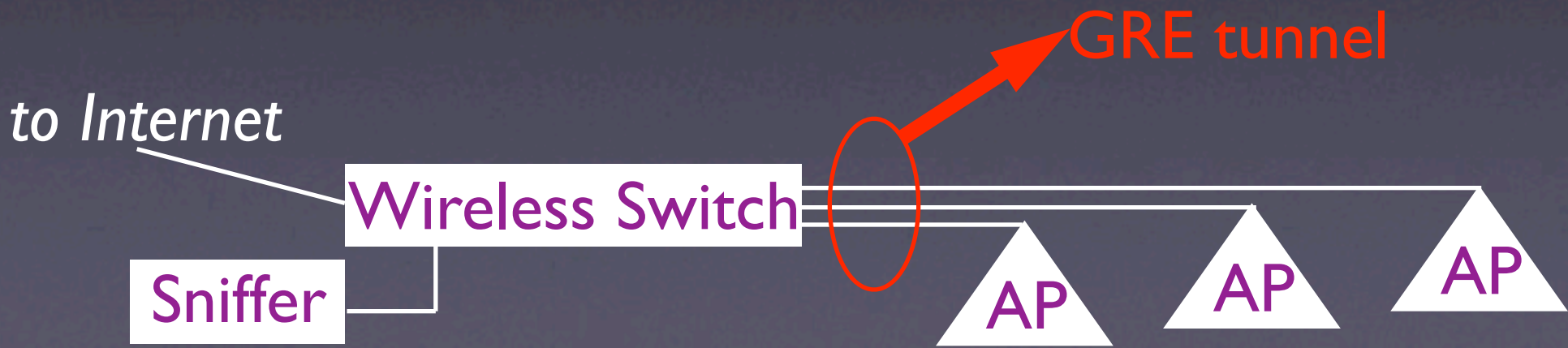
# Capturing traffic: “sniffing the wire”

- One sniffer captures traffic from many APs
- But...
  - Does not capture intra-AP traffic
  - Does not capture 802.11 control frames
  - Does not capture collisions, drops



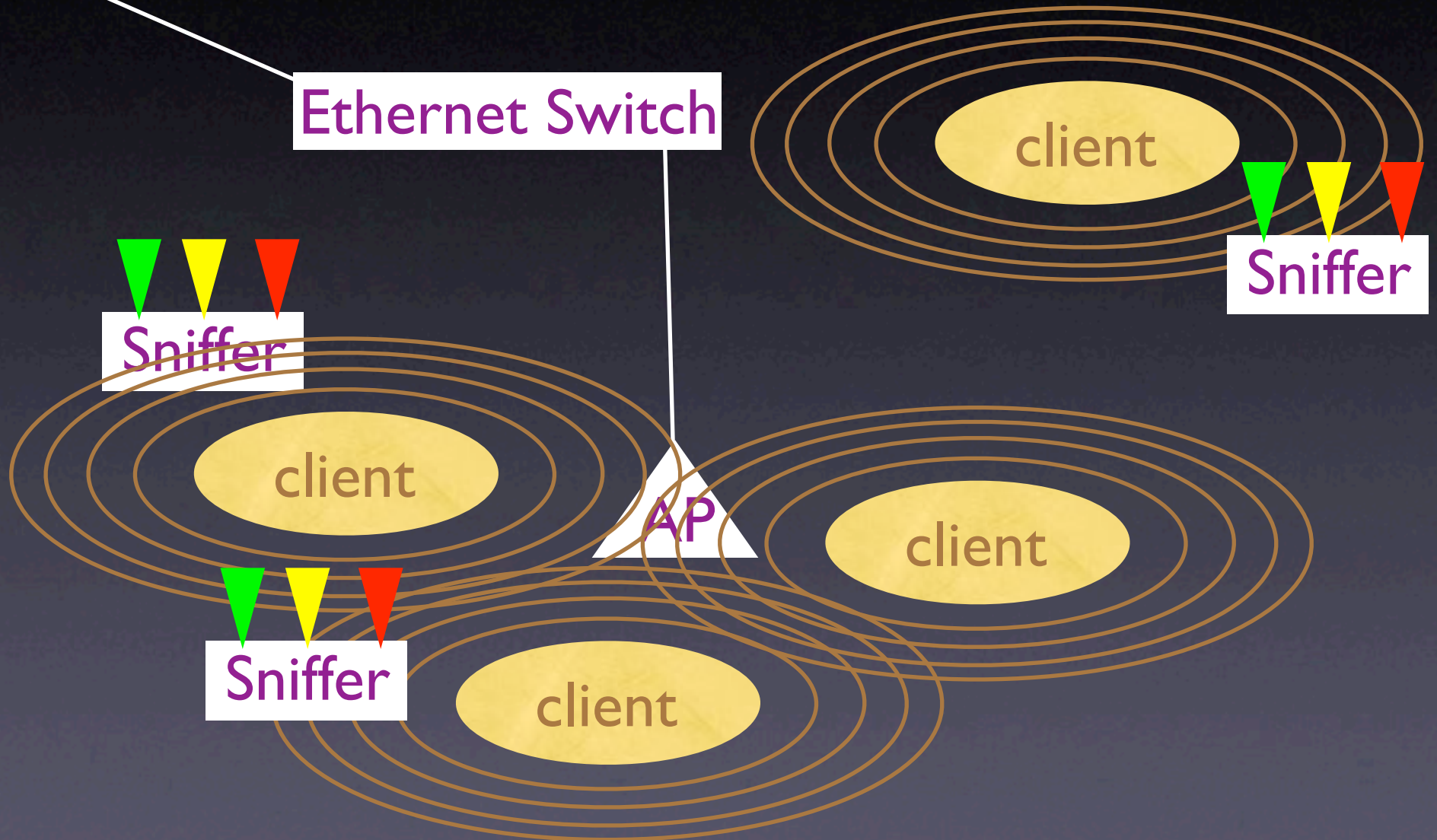
# Capturing traffic: “switched wireless”

- Can capture nearly all MAC-layer traffic
- But...
  - Needs explicit support from switch
  - Today’s switches are underpowered



# “sniffing the air”

to Internet



# Capturing traffic: “sniffing the air”

- Can capture full MAC-layer traffic
- But...
  - Need multiple radios, multiple locations
  - Still might not capture all traffic
  - Frames may be encrypted

# Understanding traffic

- Encryption limits what we can see
  - WEP and WPA encrypt traffic in the air
  - VPNs and other tunnels encrypt the wire
- Firewalls and NAT may block traffic
- Identifying P2P traffic is hard
- Identifying VoIP traffic is hard

# Correlating sources

- Hard to match data across sources
  - syslog: device movements
  - SNMP: traffic counts (poor granularity)
  - CDR: call detail records
  - tcpdump: packet traces
  - RADIUS: authentication records

# Network structure

- Must know network structure– and history
  - location of all APs
  - subnet structure
  - switched wireless AP structure
  - channel assignments, power levels?

# Devices

- Tracking device movements
  - syslog, SNMP: lack of common formats
  - no clean way to identify device departure
  - no clean way to tie “cards” to “users”
- Identifying device type
  - laptop, palmtop, VoIP phone, ...?

# Authenticated users

- allows us to link devices of same user
- may define “user session” more clearly
- But...
  - not always available

# Human subjects

- IRB approval required
- must secure the collection infrastructure
- must encrypt the data storage
- must anonymize data where possible

# Real user behavior

- Ultimately, it is hard to map observed network activity to real user behavior.

# Mesh networks

- Where to monitor them?
- How and where to collect the data?
- What, additionally, to monitor?

# Measuring controlled wireless networks

# Controlled networks

- Carefully specify experimental conditions
- Can we develop standard conditions?
  - standardized environment?
  - standardized hardware + software?

# What can we *control*?

- What factors do we control?
  - number and placement of nodes
  - mobility of nodes
  - radio and antenna selection?
  - ...
  -
- What factors are assumed or unidentified?
  - Do these factors affect results?

# Modeling wireless networks

# Building models

- Models should be derived from *real data*
  - Then, how are the models validated?
- What is modeled, and what is assumed?
  - Carefully define assumptions
  - Clearly identify usable range of the model
- Is the model portable?
  - translates to other places, other times, other sizes

# Mobility models

- The MANET world is full of fake models!
- We need new models from real users
- *Mobility model:*
  - the path of users in geographic space
- *Association model:*
  - sequence of APs associated by a device

**The needs of  
our community**

# We need...

# Data collection

- Standardized formats and interfaces
- Documentation from network vendors
- Portable tools for data collection
- Portable tools for network mapping

# We need...

# Data processing

- Effective, portable tools for anonymization
  - avoid data-mining attacks
  - but don't lose the "tail" of the data
- Identifying holes and cleaning data

# We need...

# Data analysis

- Portable tools for data analysis
- Precise definitions: e.g., “session”
- Standardized metrics: e.g., diameter, prevalence

# We need...

# Data sharing

- Archives of measurement data for research
- ... and the tools to manage archives
- ... and encourage contributions of new data
- ... and staff to manage archives and tools

# We need...

## Wireless testbeds

- Ideal testbed should
  - allow repeatable experiments
  - be flexible to variety of experiments
  - be remotely accessible
  - represent indoor, outdoor, or both
  - recognize its own limitations

# We need...

## A scientific process

- Every wireless-network paper should
  - clearly state its experimental conditions
  - clearly state its assumptions
  - identify how these assumptions and conditions limit the conclusions
  - contribute its data to an archive
  - make source code available

# We need...

# A community!

- We should focus energy on one conference
  - WinMee
  - WitMeMo
  - IMC
  - PAAM
  - Mobicom, Mobisys, SIGCOMM, WiOpt...

# Thank you

David Kotz

<http://www.cs.dartmouth.edu/~dfk>