Automating Cross-Layer Diagnosis of Enterprise 802.11 Wireless Networks

Yu-Chung Cheng
Department of Computer Science & Engineering
University of California, San Diego
Diagnosing distributed systems

- Simple systems
  - Few components
  - Inputs/Output observed
  - Cause of failure usually obvious

- Distributed systems
  - Many interdependent components
  - Hard to monitor all interactions
  - Cause of failure/degradation is non-obvious
The promise of enterprise 802.11

Blanket AP coverage = seamless connectivity
A familiar story...

“The wireless is being flaky.”

“Flaky how?”

“Well, my connections got dropped earlier and now things seem very sloooow.”

“OK, we will take a look”

“Wait, wait … it’s ok now”

“Mmm… well let us know if you have any more problems.”
Our story: new CSE building at UCSD

- 150k square feet
  - 4 floors + basement
  - >500 occupants

- Building-wide WiFi
  - 40 APs (802.11b/g)
    - Channel 1, 6, 11

- Users complain about wireless performance since we moved in July 2005
  - Admins and vendors can not solve the issues
Why is it hard to figure out?

- Problems can be in anywhere
  - Across layers – protocols
    - Even in the same layer – 802.11 {a,b,f,g,h,i,n,s}
  - Software incompatibilities – vendor variations
  - Transient or persistent – time
  - Radio propagates in free space – locations
  - Radio spreads across channels – frequencies
    - Shared spectrum makes it worse
  - APs bridge wireless and wired worlds – infrastructure

- To diagnose
  - Gather data everywhere
  - Analyze across all layers

- Need a system to do this job automatically
Better world

The wireless is being flaky

User

Your SSH has over 200ms response time in average, 8% TCP packet is lost due to the interferences from the microwave oven nearby

This problem is logged for sys admins
Shaman

- **Goal**: Develop a system to automatically diagnose problems in wireless networks
- **Pervasive data collection (Jigsaw)**
  - Extensive passive monitoring system
    - Observe all transmissions across locations, channels, and time
  - Provides a unified synchronized trace of every packet transmission
- **Explicitly model protocols on critical path**
  - DHCP, 802.11 MAC, TCP, etc.
  - Provides complete delay and loss breakdown
    - For every packet transmission, all protocol stages
- **Framework for diagnostic tools**
  - Use model outputs to determine root cause of problems
  - Users can query on demand, also alert admins
Shaman system architecture

Gather and merge traces from monitors into one global trace

Do all in real-time

Trace sync & merging

Protocol modeling

Critical path diagnosis

Infer protocol states

Identify problems on the critical path
Why pervasive monitoring?

- Protocol states are often not directly observable
  - Inferred from packet traces and protocol state machines
  - Packet delay and losses
    - PHY/MAC interactions with each other and the environment

- Capturing **all wireless events** provide the ground truth to model protocol states
  - Require a global perspective = one clock
  - Require high resolution timestamp for 802.11 timing analysis

- How?
Jigsaw passive monitor system

- Overlays existing WiFi network
  - Series of passive monitors
  - Blanket deployment for best coverage

- Monitor
  - PoE box w/ 266Mhz P4 + 128MB ram
  - 2 b/g radios

- 96 monitors (192 radios)
  - Monitors are paired in each location
    - Covering all channels in use
  - Captures all 802.11 activity (including PHY/CRC errors)
  - Stream back to centralized storage
Trace merging (ideal)
Not all monitors see all packets
Trace merging (reality)
Challenge 1: sync at 10us precision

- Why 10us precision?
  - Critical evidence for 802.11 layer analysis

- 802.11 channel access mechanism
  - Carrier-sense multiple access (CSMA)
    - Channel busy → wait
    - Channel idle → send
  - Timing unit is ~10us

- Precise trace timestamps reveal 802.11 internal states
  - Ex1: if A and B send at same time, they could interfere → A can’t hear B
  - Ex2: if A sends right after B’s transmission → A can hear B

- How?
  - Create a global clock
  - Monitors timestamp packets w/ local HW clocks
  - 802.11 HW clocks has 1us granularity
  - Estimate the offset between local and global clock for each monitor
Challenge 2: sync across 192 radios

- **Goal:** estimate the offset between local and global clock for each monitor
  - Time route from one monitor to the other
- **Sync across channels**
  - Ch. 1 monitor does not hear packet sent in ch. 6.
  - Dual radios on same monitor slaved to same clock

---

Jigsaw: Solving the Puzzle of Enterprise 802.11 Analysis
Cheng, Bellardo, Benko, Snoeren, Voelker, and Savage
SIGCOMM 2006
Trace merging (reality)

Time

Shaman sync’d’d trace

Frame 1
Frame 2
Frame 3
Frame 4
Frame 5

5/13/07
Part of a sync’d’d trace

<table>
<thead>
<tr>
<th>Row</th>
<th>User 1</th>
<th>User 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Traces synchronized
Shaman system architecture

- Wireless monitor
- Wireless monitor
- ... 
- Wireless monitor
- Wired gateway monitor

Gather and merge traces from monitors into one global trace

Trace sync & merging

Protocol modeling

Critical path diagnosis

Infer protocol states

Identify problems on the critical path
Modeling protocols

- Now we have fully sync’d global traces
  - What protocols must we model?
- Critical path
  - Mobility management
    - Scan/associate w/ AP
    - DHCP
    - ARP
    - Portal page login
  - Data transport protocols
    - TCP
    - 802.11 Mac delay/loss
Mobility Management

- Create the illusion of a single AP
  - Proprietary system w/ site specific policy
- Most components are simple protocols
  - 1-2 request-response transactions
    - Easier to model compared to TCP
  - Very reliable in wired network
    - ARP, DHCP, DNS
    - Seldom suspected as the culprits in wireless
- Users expect seamless connectivity
  - People often suspend/resume laptops while moving in the office building
Mobility overhead in UCSD CSE

Major Problem: (Gratuitous) ARPs & Scans
Protocol Modeling

- Distribution is not enough
  - Want to diagnose any user’s problem by finding the root cause

- Need to track *per packet* delay and loss
  - Essential to model e2e protocols like TCP
    - Complex mechanisms to accommodate delay and loss

- Example:
  slow SSH response →
  high TCP losses →
  most 802.11 retries failed →
  microwave ovens operating nearby
The journey of a packet in 802.11

- Wired packet
- 802.11 Data
- 802.11 Ack
Modeling 802.11 packet delays

- Emulate AP queue
  - Based on input/output events

- Events observed directly
  - Ethernet packet on wires
  - 802.11 data/ack on wireless

- Need to infer when a packet ...
  - Reaches head of TxQ
  - Is scheduled to the TxQ
  - Is received by the AP
Applying 802.11 delays to TCP diagnosis

**Scenario**

- 3 users downloading same large tar ball through same AP from the CSE website
- 1 user complains about download performance in spite of having 54Mbps 802.11g connectivity

**Major performance bottleneck is queue competition**
Modeling packet losses

- Delay alone is not enough for diagnosis
- Loss is another major factor
  - 802.11 performs retransmission on loss
  - Loss happens on both ways
    - Data or Ack
  - Must model 802.11 conversations
- Loss causes
  - Attenuation (e.g. not enough signal strength)
  - Interference from other 802.11 devices (hidden-terminals)
  - Interference from other devices in 2.4GHz
Broadband interference

~9 am

12-2 pm
Interference fingerprints
TCP performance measures

- Want to measure TCP performance bottlenecks
  - Compares actual goodput with (modeled) ideal goodput [JP98]

- Major problems in UCSD CSE TCP bulk flows
  - 30% small receiver window
  - 19% AP retry bug
  - 30% AP 802.11b/g compatibility policy (protected mode)

Automating Cross-Layer Diagnosis of Enterprise Wireless Networks
Cheng, Afanasyev, Benko, Verkaik, Snoeren, Voelker, and Savage.
SIGCOMM 2007 (To appear)
Putting everything together

Critical path diagnosis

Scan/Association

DHCP

ARP

TCP

Diagnose

802.11 Delay/Loss

Broadband Interference
System status

- Real-time monitoring and diagnosis of UCSD CSE wireless network
  - 30 seconds delay
- Serving UCSD CSE wireless users
  - Resolved 67 tickets
    - Validated manually
  - Discovered various implementation bugs and protocol problems
    - Only retry once
    - Do not respect CSMA, burst frames in a row
    - Very large transmission duration
    - Overly conservative 802.11g protection policy
    - ...
  - Working w/ vendors and admins to fix AP bugs
- Re-deployed in city 802.11 mesh network in the bay area
Related Work

- WiFiProfiler [Mobisys06]
  - Peer diagnosis among clients
- DAIR [NSDI07]
  - Distributed monitors but application-spec traffic summaries
    - No centralized merging/sync
  - Fine-grained location system
- Wit [SIGCOMM06]
  - Automatic protocol states inference engine
- Airmagnet
  - Troubleshooting user problems (PHY/MAC)
    - Detect interferences, security problems, protocol incompatibilities
  - Special devices to perform active probes
- Airtight/Airdefense/Kismet
  - Detect rogue APs and security problems
Conclusions

- Wireless diagnosis is tough
  - Especially for large enterprise network
  - Need to check a lot of factors
  - Need a system to do the job automatically

- Shaman: an automatic comprehensive wireless diagnosis system
  - Large-scale 24x7 monitoring
  - High resolution synchronization
  - Models protocol states on the critical path
    - Mobility management
    - TCP
    - 802.11 delay and losses
  - Automatically diagnose user problems in real-time
Other work

- Metropolitan-scale Wi-Fi location system
  Cheng, Chawathe, LaMarca, Krumm. *Mobisys 2005*

- Monkey See, Monkey Do: A tool for TCP Tracing and Replaying
  Cheng, Hoezle, Cardwell, Savage, Voelker. *USENIX 2004*

- Fatih: Detecting and Isolating Malicious Routers
  Mizrak, Cheng, Marzullo, Savage. *DSN 2005*

- Total Recall: System Support for Automated Availability Management
  Bhagwan, Tati, Cheng, Savage, Voelker. *NSDI 2003*
Q & A

- Collaborators (since Jan 2005)
  - John Bellardo
  - Mikhail Afanasyev
  - Peter Benko
  - Patrick Verkaik
  - Jennifer Chiang
  - Harrison Duong
  - Alex Snoeren
  - Geoff Voelker
  - Stefan Savage

- Live traffic monitoring
  [sysnet.ucsd.edu/wireless/](http://sysnet.ucsd.edu/wireless/)