Understanding Internet Routing Dynamics and Impact of Overlay Networks

Chen-Nee Chuah

Robust & Ubiquitous Networking (RUBINET) Lab
http://www.ece.ucdavis.edu/rubinet

Electrical & Computer Engineering
University of California, Davis

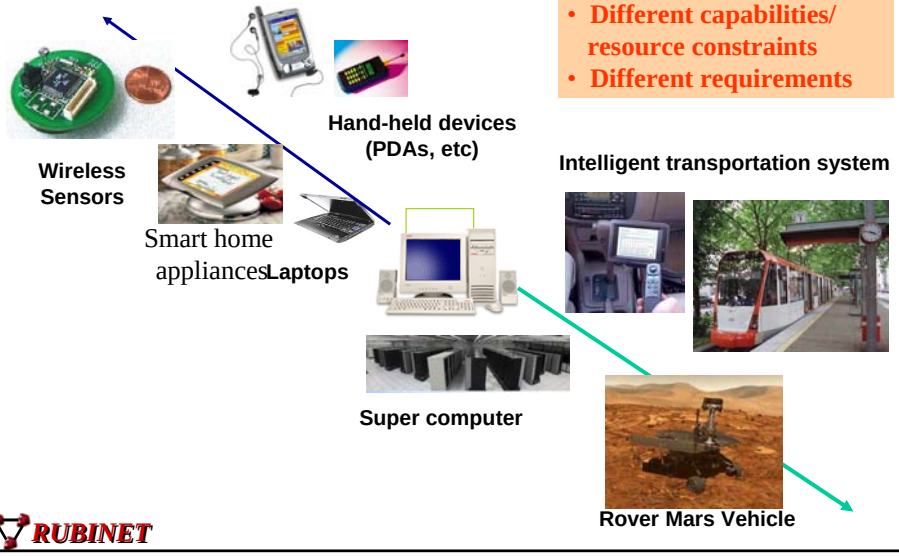
RUBINET

Outline

- RoSE: Project Overview & Lessons learned
- Overlays: friends or foe?
  - Co-existence between IP-Layer and Overlays
  - Race conditions between multiple overlays
    - Synchronizations due to external events
    - Cascading events
  - How often and how bad is it?
- Summary and Future Directions

RUBINET

Emerging Communication Paradigm



- **Different capabilities/ resource constraints**
- **Different requirements**

RUBINET

Challenges

- Scalability in number
- Scalability in heterogeneity
  - Access technologies, application requirements, protocols
- Performance Predictability
- Reliability, survivability, robustness
- Management/Complexity
  - Automated?
- Network evolvability and other X-ities
  - J. Kurose's Keynote Speech [INFOCOM04]

RUBINET

Current State of the Art

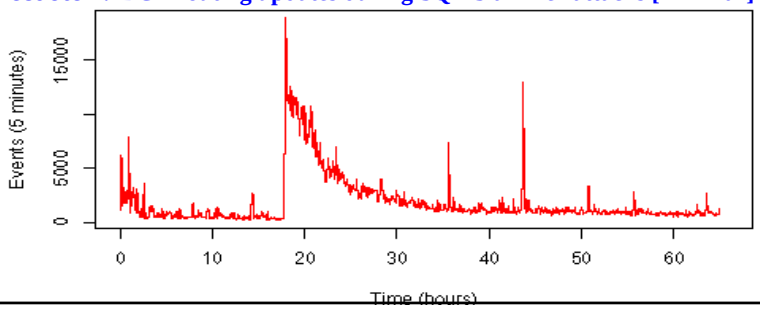
- What does the current IP-network look like?
  - Routing hierarchy: inter-domain vs. intra-domain routing
  - Different tiers of ASes (Customers vs. Tier-1/2/3 ISPs)
- Today's Service Level Agreements (SLAs)
  - Performance in terms of average delay and packet loss
    - 0.3% loss, speed-of-light end-to-end latencies
  - Port availability
  - Time to fix a reported problem
- What do Tier-1 ISPs do to meet SLAs?
  - Over-provisioning
  - Load balancing on per-prefix or per-packet basis

RUBINET

Internet routing infrastructure is fragile!

- Fiber cuts, faulty or mis-configured equipment can cause widespread losses of global connectivity
  - Baltimore tunnel fire, Ohio train wrecks, etc.
- Malicious attacks on servers cause routing instability
  - Code-red, Nimda worms, Slammer worms

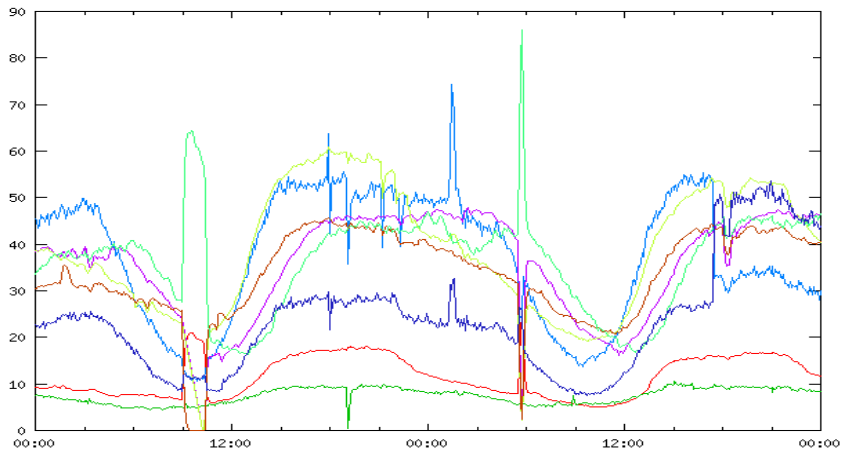
Anecdote 1: BGP routing updates during SQL Slammer attacks [PAM'04]



RUI

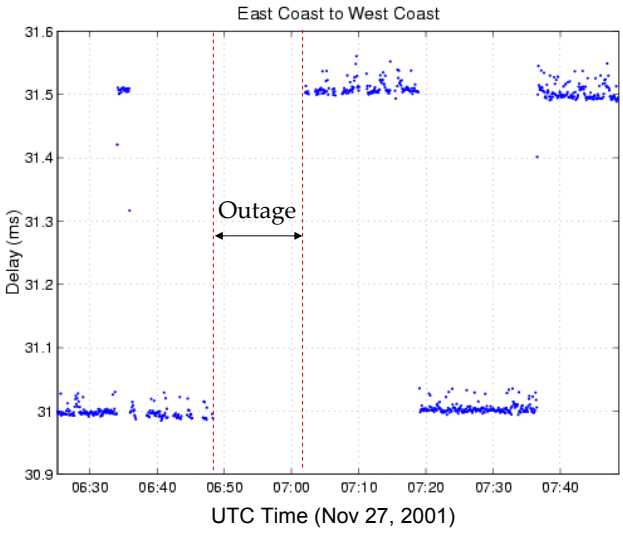
Anecdote 2: Transient Link Overload

- Even with over-provisioning => high variability in link load
  - Can find a link w/ load > 50% every 15 minutes; > 90% every 8 days



RUBINET

Anecdote 3: Traffic Pot-holes



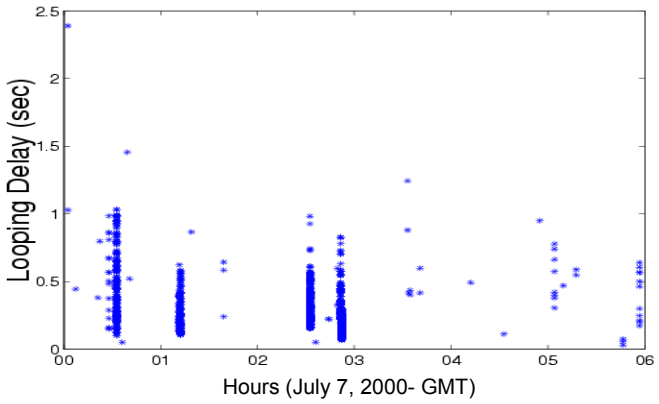
- Average delay over 5 sec intervals
- Traffic was blackholed for more than 10 minutes
- It took about 40 minutes for the network to reach a stable state
- Why?

Router Misconfigurations!

RUBINET

Anecdote 4: Routing Loops

- Loops due to link failure/new route advertisement
- Measurements from 3 backbone links
  - 25% packets caught in a loop in one failure instance
  - 1 % lost due to expire TTL; those that escape have long delays



RUBINET

* Graph courtesy of Sue Moon

RoSE: Robust, Secure, and Efficient Routing

Project goal: Improve availability and performance of the global Internet while maintaining the scalability and evolvability of IP

Phase 1: Modeling transient network dynamics, interactions between network components and across layers
- Large-scale Internet measurements (IGP, BGP, traffic, network, router configurations) over production networks

Phase 2: Exploring multi-layer information sharing & optimization
- Leverage results from #1 to optimize network planning, router design, traffic engineering practices, QoS mechanisms, overlays, and applications

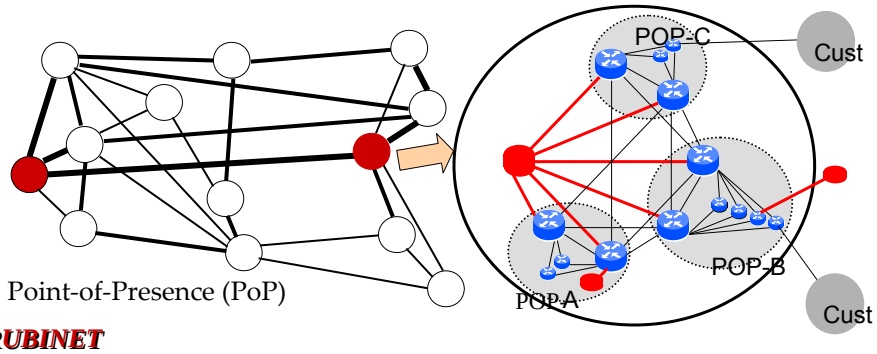
Phase 3: Re-architecting the Internet
- Design systems with built-in "sensors and actuators" to cope with increasing heterogeneity in access technologies and applications

RUBINET

Integrated Monitoring

Where?
- Tier-1 ISP backbone (600+ nodes), enterprise/campus networks

What?
- BGP/IGP passive route listeners, SONET alarm logs
- IPMON/CMON passive traffic monitoring & active probes
- Controlled failure experiments
- Router configurations and BGP policies



Point-of-Presence (PoP)

RUBINET

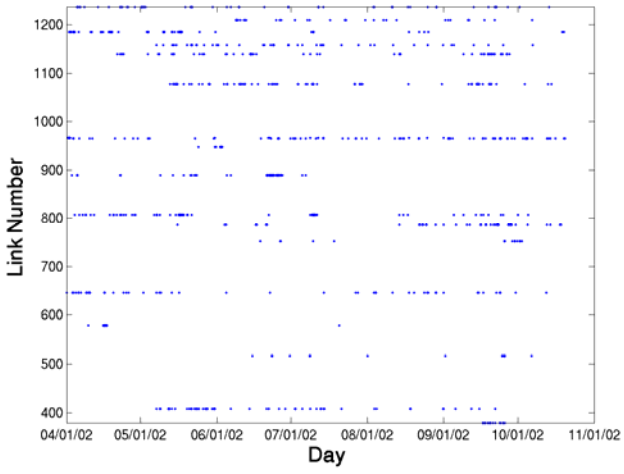
Questions we want to answer

- IGP/BGP routing behavior during sunny and rainy days
  - How frequent do failures occur?
  - How do they behave during convergence or routing instabilities
  - What are the causes?
  - Are there anomalies?
  - How do failures/instability/anomalies propagate across networks?
- How does the control plane impact the data forwarding?
  - What actually happens to the packets? What is the effect on end-to-end service availability?
- How do network components/protocols interact?
  - Unexpected coupling, race-conditions, conflicts?

RUBINET

Lessons Learned from Phase 1 (1)

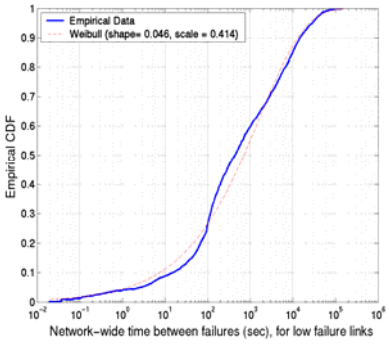
1. Transient, individual link failures are the norm
   - No, failures are not independent & uniformly distributed [INFOCOM'04]

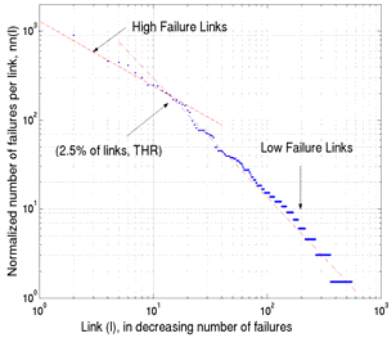


RUBIN

Backbone Failure Characteristics

- How often? (time between failures)
  - Weibull distribution: $F(x) = 1 - \exp(-(x/scale)^{shape})$
- How are failures spread across links?
  - Power law: $n_l \propto l^{-1.35}$ (link with rank l has n_l failures)





RUBINET

Lessons Learned from Phase 1 (2)

1. Transient, individual link failures are the norm

2. There are many reasons behind network failures
   - Fiber cuts, or mis-configured equipment, malicious attacks can lead to cascading instability & global meltdown [PAM'04]

3. Modeling individual component is not sufficient
   - End-to-end behavior (reachability, performance, security) depend on interactions between multiple entities and distributed sets of policies
   - Example: measuring service availability

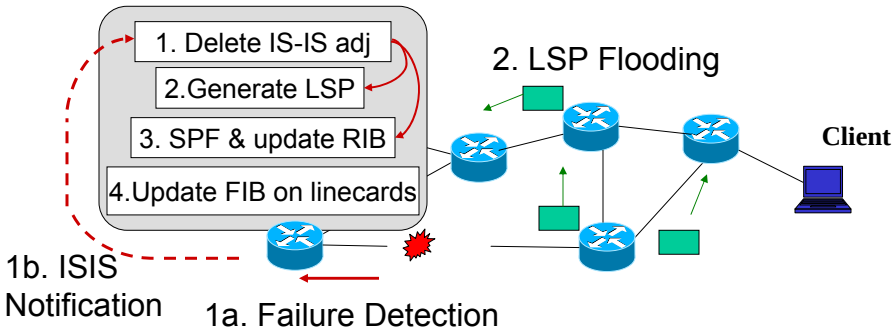
RUBINET

Service "Availability" of IP Networks

- 99.999 equivalent of PSTN
- Challenge: Typical *Service Level Agreements* (SLA) or static graph properties (like out-degree, network diameter) do not account for instantaneous network conditions
- Important factor for designing & evaluating
  - Failure protection/restoration mechanisms,
  - Traffic engineering, e.g., IGP weight selection, capacity provisioning
  - Network design e.g., topology, link/node upgrade,
  - Router configuration, e.g., tuning protocol timers
- Failure model is only one piece of the puzzle
  - Failure recovery is *NOT* instantaneous => forwarding can be disrupted during route re-convergence
  - Overload/Congestion on backup paths

RUBINET

Service Convergence After Failures



- Protocol convergence = 1+2+3, but data forwarding only resumes after step 4.
  - FIB updates depend on number of routing prefixes
- Invalid routes during route convergence (2-8 seconds) => complete black-hole of traffic => packet drops!

RUBINET

Service Convergence Delay

Detection of link down (SONET)	<100ms
Timer to filter out transient flaps	2s
Timer before sending any message out	50ms
Flooding of the message in the network O(network distance)	~10ms/hop
Timer before computing the new shortest paths	5.5s
Computation of the new shortest paths O(network size)	100-400 ms
→ **Protocol-level convergence:**	**Worst case: 5.9s**
Update of the Forwarding Information Base O(network size + BGP peering points)	1.5-2.1 s
→ **Service-level convergence:**	**Worst case: 8.0s**

→ Service availability depends on *topology, failure model, traffic matrix, protocol implementation, router architecture, traffic engineering policies location of peering points/customers* [IWQoS'04]

RUBINET

How to make networks more resilient?

- Improve routing design
  - MPLS-like fast reroute [BF+04]
- Improve forwarding plane
  - Order prefixes for updating [FB05]
  - Interface-specific forwarding [IWQoS'05]
- Application-layer approach
  - Smart applications, e.g., transcoding, FEC
  - Structured overlay networks, e.g., RON [AB+01], routing underlay [NPB03]

RUBINET

Lessons Learned from Phase 1 (3)

1. Transient, individual link failures are the norm

2. There are many reasons behind network failures
   - Fiber cuts, or mis-configured equipment, malicious attacks can lead to cascading instability & global meltdown [PAM'04]

3. Modeling individual component is not sufficient
   - End-to-end behavior (reachability, performance, security) depend on interactions between multiple entities and distributed sets of policies

4. There are problematic interactions between multiple control mechanisms
   - Multiple overlays compete with each other as well as the IP-layer to provide routing service without coordination [ACM Hotnets'04]
     => Race conditions => load oscillations => coupling of multiple ASes

RUBINET

Outline

- RoSE: Project Overview & Lessons learned
- **Overlays: friends or foe?**
  - **Co-existence between IP-Layer and Overlays**
  - **Race conditions between multiple overlays**
    - **Synchronizations due to external events**
    - **Cascading events**
  - **How often and how bad is it?**
- Summary and Future Directions

RUBINET

Overlay Networks

- Overlays are becoming popular
  - Allow application-level routing decisions, often designed to circumvent IP-layer routing problems
  - End-hosts only vs. infrastructure-based (pre-selected common overlay nodes)
  - Application-specific, e.g., multicast like Splitstream [CD+03], DHT like Bamboo
  - Generic structured overlays, e.g., RON [AB+01], routing underlay [NPB03], Detour

Our study focused on infrastructure-based overlays …

RUBINET

Motivation

- Overlay networks compete with IP-layer to provide routing service
- ISPs and overlay networks are unaware of key things happening at the other layer
- Multiple overlay networks co-exist and make independent decisions
- There are known problematic interactions between multiple control mechanisms
  - Seemingly independent period process can inadvertently become synchronized, e.g., routing update message [FJ94]
  - Control theory: multiple independent control loops reacting to same events is a classic situation for race conditions
- Big questions – *How does all this affect ISPs & overlay networks and the traffic they carry*?

RUBINET

Our Goals

- Identify, qualify and quantify potential interactions between: (a) ISPs & overlays and (b) Multiple overlays
- Focus is on network management issues rather than performance issues like throughput, loss, or delay
- Understand impact of large scale deployment of infrastructure-based overlays
  - Implicit assumption is that overlay traffic is a significant portion of the overall traffic
  - Identify conditions of race conditions and compute the likelihood of synchronizations through an analytical model
  - Explore techniques to avoid or limit harmful synchronizations
  - Provide guidelines for synergistic co-existence

RUBINET

Related Studies

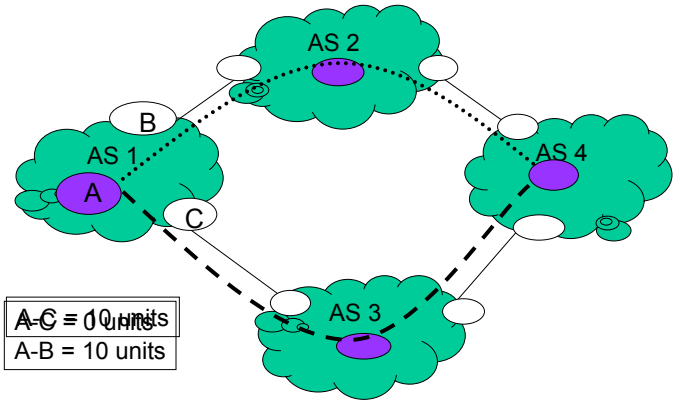
- Qiu et al investigate the performance of selfish routing of multiple co-existing overlays [QYZ03]
  - Optimal average latency is achieved at the cost of overloading some links
- Liu et al model interaction between IP traffic engineering and overlay routing as two-player game [LZ+05]
- Differences
  - Previous work study network state after the system reaches Nash equilibrium, we focus on dynamics in the transient period before system stabilizes
  - Instead of static network-layer routing, we consider external triggers like link/router failures that lead to dynamic re-routing at both IP and overlay layers

Potential "Side Effects" of Overlay Networks

- Challenges to ISP's Traffic engineering (TE)
  - Overlays *shift* and/or *duplicate* TM values, increasing the dynamic nature of the TM
  - Harder to estimate Traffic Matrix (TM) essential for most TE tasks.

Problem 1: Challenges to Traffic Engineering

- Traffic Matrix Estimation



- *Shifts* TM values by changing the exit point
- Increases the dynamic nature of TM

RUBINET

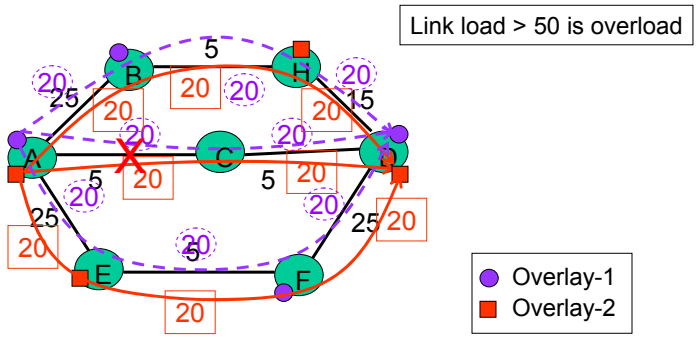
Potential "Side Effects" of Overlay Networks

- Challenges to ISP's Traffic engineering (TE)
  - Overlays *shift* and/or *duplicate* TM values, increasing the dynamic nature of the TM, making it harder to estimate
  - Harder to estimate Traffic Matrix (TM) essential for most TE tasks.
- Multiple overlays can get synchronized
  - Result of periodic nature of path probing process
  - Can impact both overlay and non-overlay traffic
  - Interfere with load balancing or failure restoration, leading to oscillations

RUBINET

Problem 2: Race Conditions & Load Oscillations

- Multiple overlays can get synchronized!



- Result of
  - Periodic nature of path probing process
  - Partial/full overlap of primary and alternate paths
- Could happen in real networks

RUBINET

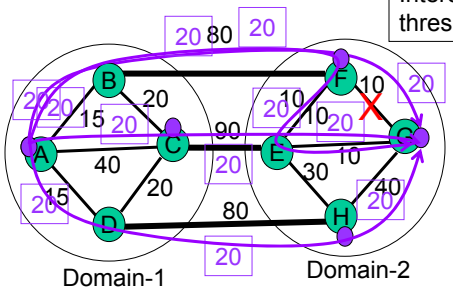
Potential "Side Effects" of Overlay Networks

- Challenges to ISP's Traffic engineering (TE)
  - Overlays *shift* and/or *duplicate* TM values, increasing the dynamic nature of the TM, making it harder to estimate
  - Harder to estimate Traffic Matrix (TM) essential for most TE tasks.
- Multiple overlays can get synchronized
  - Result of periodic nature of path probing process
  - Can impact both overlay and non-overlay traffic
  - Interfere with load balancing or failure restoration, leading to oscillations
- Coupling of multiple ASes
  - Overlay Networks may respond to failures in an AS by shifting traffic in upstream AS.

RUBINET

Problem 3: Coupling Multiple AS Domains

Link load > 50 is overload
Interdomain links have higher thresholds



- Defeats one of the objectives of BGP to decouple different domains by insulating an AS from events in neighboring ASes

RUBINET

Synchronization of Multiple Overlays

- Three main conditions for synchronization
  - Path performance degradation due to external triggers (e.g., failures, flash crowds)
  - Topology, i.e. partially overlapping primary and backup paths)
  - Periodic path probing processes
- The first two conditions are beyond the control of overlay networks
  - Frequent events that degrade path performance
  - Overlay node placement determines path overlap
- Focus on path probing
  - Derive analytic formulation for probability that two overlays get synchronized based on the parameters of their path probing procedures
    - Is it pathological or a more general problem?
  - Predicting how long the oscillations last before they disentangle

RUBINET

Modeling Overlay Path Probing Process

- For overlay network, ***i***
  - Probe Interval – $\boldsymbol{P_i}$
  - Timeout – $\boldsymbol{T_i}$
  - High Frequency Probe Interval – $\boldsymbol{Q_i}$
  - Number of High Frequency Probes – $\boldsymbol{N_i}$
- Additional parameter
  - Round trip time R_{ij} over path j
- By definitions: $P_i \geq Q_i \geq T_i \geq R_{ij}$

RUBINET

Detection Period & Approximation

- Under normal circumstances:
  - Probability of finding one low frequency probe in any time interval of length $\boldsymbol{P_i}$ is **1**
  - Probability of finding more than one low frequency probes in a time interval of length $\boldsymbol{P_i}$ is **0**
- Consider a failure event at time ***h***
  - Detection Period – Period of length $\boldsymbol{P_i}$ around the failure event when the overlay ***i*** sends a probe that detects the failure, i.e., $[\boldsymbol{h}-\boldsymbol{T_i}, \boldsymbol{h}-\boldsymbol{T_i}+\boldsymbol{P_i}]$
- Approximation
  - Ignore exact delays between the source, failed spot, and destination.
  - Approximate the time at which a probe is dropped by $R_{ij}/2$

RUBINET

Condition for Synchronization (1)

- Consider two overlay networks
- Time of occurrence of probes: β_i, $i=1,2$
- Final high frequency probes: $f_i = \beta_i + N_i Q_i$
- Overlays synchronize when:
  - O_1 moves traffic first. O_2 sends out the last high freq probe before O_1 moves its traffic, decides the path is bad, and move its traffic shortly after.

    $$f_1 < f_2 \text{ and } f_2 - f_1 < T_1$$
  - Or vice versa

RUBINET

Condition for Synchronization (2)

- Condition for synchronization of two overlays:

$$-T_1 < f_1 - f_2 < T_2$$
$$-T_1 < (\beta_1 + N_1 Q_1) - (\beta_2 + N_2 Q_2) < T_2$$
$$b < \beta_1 - \beta_2 < a$$

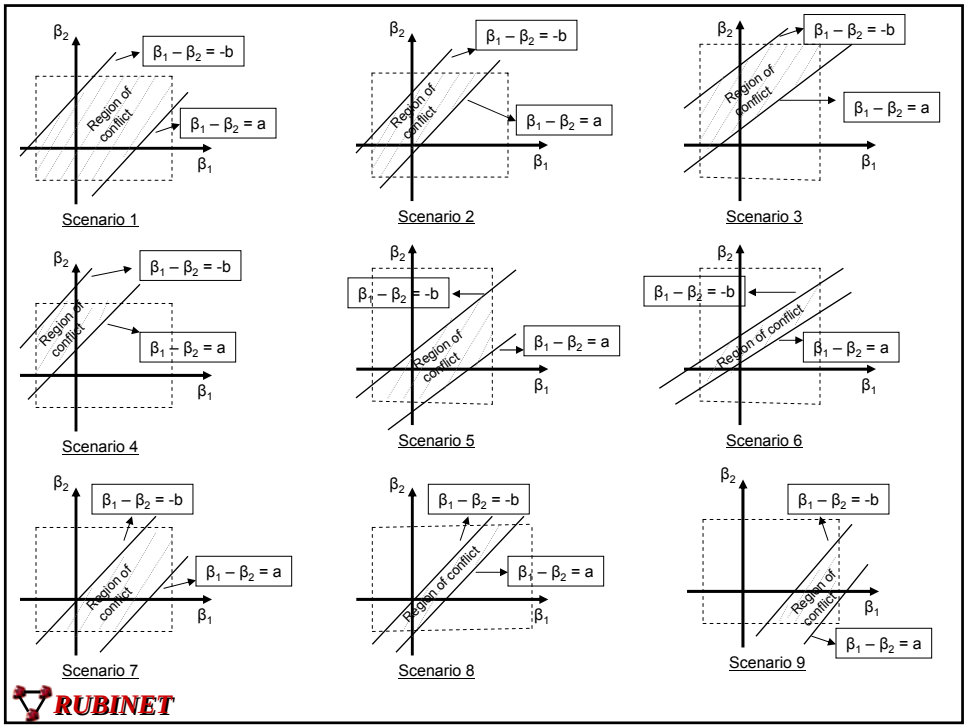
- where,

$$a = N_2 Q_2 - N_1 Q_1 + T_2$$
$$b = N_2 Q_2 - N_1 Q_1 - T_1$$

- Consider failure event happens at h=0. We assume that β_1 and β_2 are uniformly distributed in the detection period of length P_1 and P_2 respectively:

$$\beta_i \in [-R_i/2, P_i - R_i/2]$$

RUBINET



Probability of Synchronization/Oscillations

- Probability of Synchronization – Nine cases

$$A_C = A - A_1 - A_2$$

$$P(S) = \frac{A_C}{A}$$

  - For the simplest case:

$$\begin{aligned} A &= P_1 P_2 \\ A_1 &= 0.5(P_1 - R_1/2 - a + R_2/2)^2 \\ A_2 &= 0.5(P_2 - R_2/2 + b + R_1/2)^2 \end{aligned}$$

  - For identical overlays

$$P(S) = T(2P - T)/P^2$$

RUBINET

How long do oscillations last?

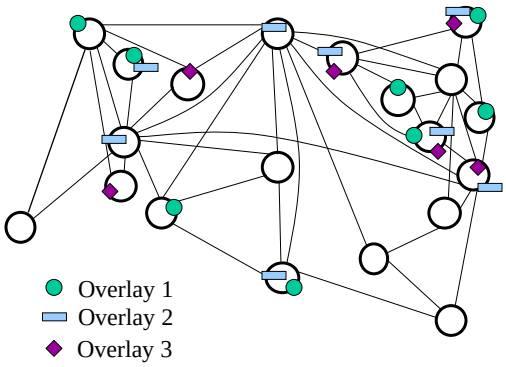
- Oscillations last until overlay networks
  - "Disentangle" themselves
  - "Influenced" by external event (e.g., link recovery)
- Assuming no external events
  - Bounds on the duration of oscillations and hence quantify the impact (in a probabilistic sense) on both overlay and IP traffic
- Length of oscillations

$$\bar{k} = \left\lceil \frac{T_1 + T_2}{|P_1 - P_2 + N_1 Q_1 - N_2 Q_2 + T_1 - T_2|} \right\rceil$$

RUBINET

Simulation Study

- Consider a Tier-1 ISP's pop-level topology
- Deploy five overlay networks on top of it
  - Different probing parameters, RTTs, and traffic demand

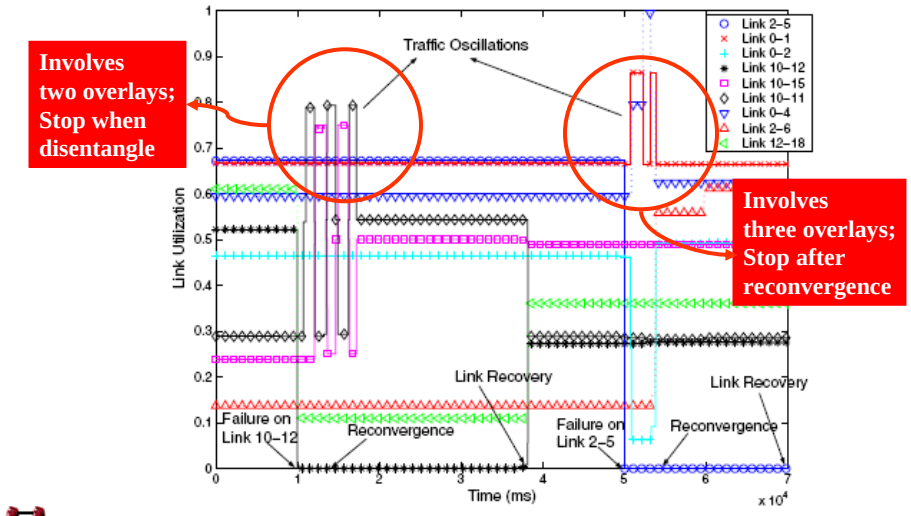


Timer	P(ms)	Q(ms)	T(ms)	N
O_1	2000	600	300	3
O_2	2000	1000	350	3
O_3	1000	500	200	3
O_4	800	400	120	3
O_5	700	300	100	3

RUBINET

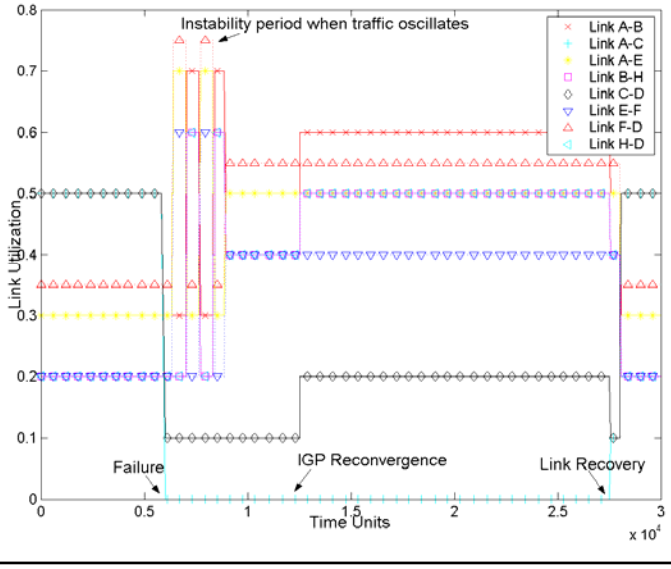
Illustrating Race Conditions

- Oscillations in link load

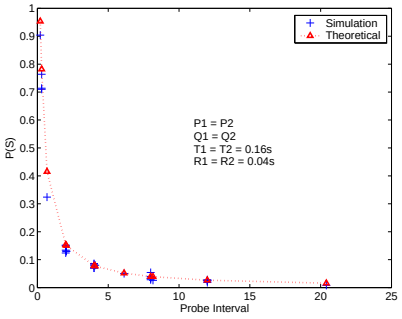


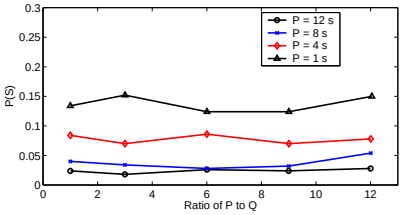
RUBINET

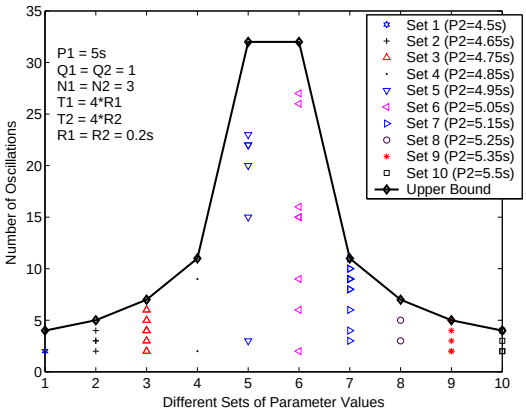
Another Example



Validation of Analytical Model



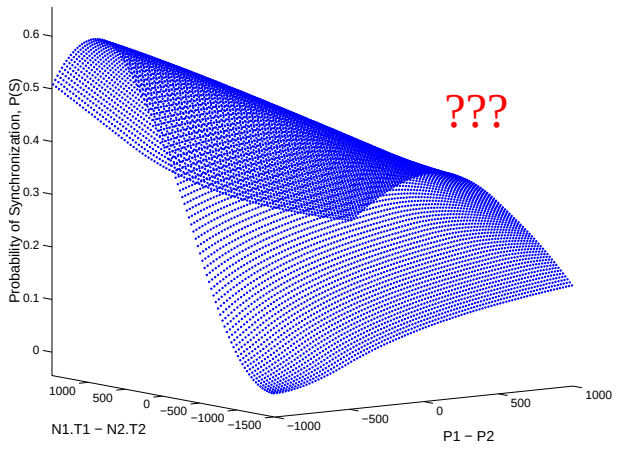




- When two overlays are identical (same probe parameters, *P(S)* only depends on *P* & *T*.

RUBINET

Probability of Synchronization (Oscillations)



RUBINET

Sensitivity to Probe Parameters

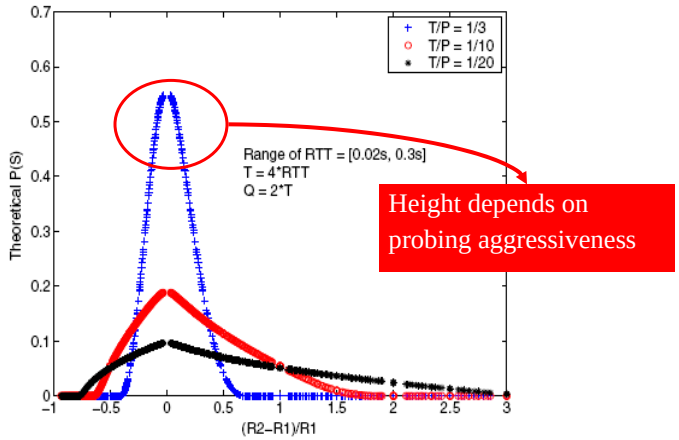
- Does the inherent randomness/variation in RTT help reduce *P(S)*?
- Is *P(S)* non-negligible in common Internet operating regions?
  - Consider it non-negligible if *P(S)* > 10%
- How do we choose the parameter settings to drive P(S) low?

First, some definitions …

- Aggressiveness factor: $\alpha_i = T_i / P_i$
- Assume *T*=4**RTT*
- Proportional overlays:
  P & *Q* multiples of *T* (different per path)
- Fixed overlays:
  P & *Q* values are set independent of *T* and *RTT*

RUBINET

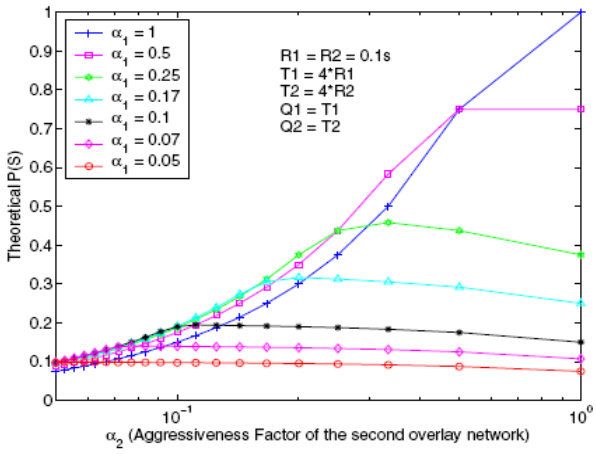
Proportional Overlays: Influence of RTTs



- When one RTT is more than twice the other, P(S) is close to zero.
- If two overlays span similar geographic region (similar RTTs), P(S) is non-negligible.

RUBINET

Proportional Overlays: Impact of Relative Aggressiveness on P(S)

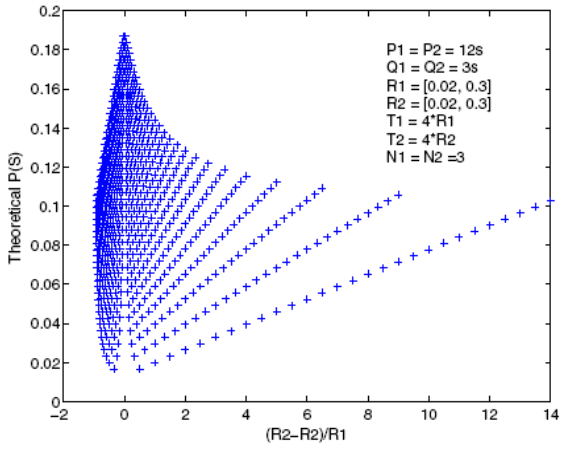


- As long as one overlay is non-aggressive, P(S) is low
- Caveat: Fairness issue

RUBINET

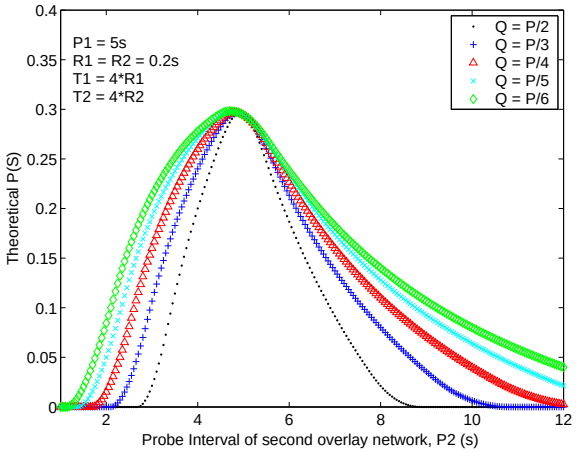
P(S) for typical overlays in today's Internet?

- Influence of RTT on P(S) in fixed parameter case
- Consider two RON-like overlays
- Unlike proportional overlays, absolute RTT values matter!
  - P(S) is non-negligible when both RTT are large (300 ms)



RUBINET

Fixed Overlays: Different Probe Parameters



- *P(S)* less sensitive to *Q*
- Smaller *Q* => wider range of cases where P(S) is non-negligible

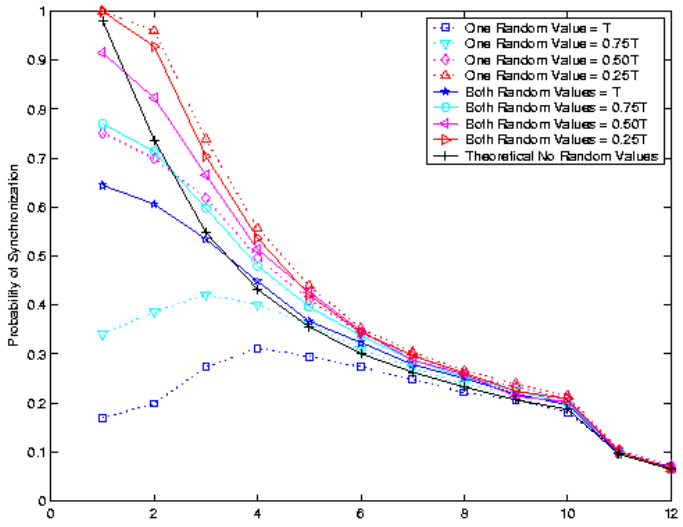
RUBINET

How to mitigate oscillations?

- Less aggressive probing to avoid synchronization
  - Cons: Fairness issues, slower reactions
- Break synchronization through randomization
  - Simply randomizing probe intervals or time-out values does *NOT* help

RUBINET

Randomize probe parameters doesn't help!



RUBINET

How to mitigate oscillations?

- Less aggressive probing to avoid synchronization
  - Cons: Fairness issues, slower reactions
- Break synchronization through randomization
  - Simply randomizing probe intervals or time-out values does *NOT* help
  - Back-off approach is promising
    - i.e., successively increase the time out/probe parameters each time an overlay decides to switch to the same destination
- Open problems:
  - How to share information between the IP layer and the overlays as well as among multiple overlay networks
  - What overlay topologies are most likely to have these problems? How to characterize good overlay network designs
  - How to contain oscillations/instability in one domain?

RUBINET

Outline

- RoSE: Project Overview & Lessons learned
- Overlays: friends or foe?
  - Co-existence between IP-Layer and Overlays
  - Race conditions between multiple overlays
    - Synchronizations due to external events
    - Cascading events
  - How often and how bad is it?
- Summary and Future Directions

RUBINET

Summary

- Initial understanding of Internet routing dynamics
  - Routing failure characteristics, transient behavior
  - Interactions between multiple entities (IGP/BGP, data forwarding plane, router configurations, etc.)
  - Findings have impact on
    - Network design, e.g., link/node upgrade
    - Traffic engineering, e.g., link-weight selection, BGP peering points
    - Router design, e.g., eliminating transient loops through failure inferencing techniques (FIFR) Monitoring for performance + Security
- Analyze impact of overlay network deployments
  - Identify potential harmful race conditions between IP & overlay layers, and between multiple overlays
  - Analytical model to predict likelihood of synchronization and length of oscillations (bounding performance impact)

RUBINET

RoSE: On-going and Future Work

- Design network monitoring for both traffic engineering and security
  - How does sampling affect anomaly detection?
  - Optimization and adaptation of distributed firewall configurations
    - Leveraging traffic statistics, routing topology, and policies
    - Collaborators: Zhendong Su and Hao Chen (Computer Science, UCD)
- Multi-layer information sharing and optimization
  - Routing introspection & feedback system (RIFS) for multimedia servers
  - Coordinating failure restorations at layer 2, 3, & 7
- Expanding the role of overlays
  - Coordination layer to protect/enhance IP infrastructure

RUBINET

Acknowledgement

- Sponsors:
  - NSF CAREER (2003-08)
  - UC MICRO program 03-04
  - Gifts from Cisco Systems, Fujitsu, Sprint ATL
- Research collaborators:
  - Sharad Agarwal (Microsoft Research)
  - Supratik Bhattacharrya (Sprint ATL)
  - Christophe Diot (Intel Research, Cambridge)
  - Gianluca Iannaconne (Intel Research, Cambridge)
  - Nina Taft (Intel Research, Berkeley)

RUBINET

References (1)

[PAM'04] S. Agarwal, C. N. Chuah, S. Bhattacharrya, and C. Diot, "The Impact of BGP Dynamics on Router CPU Utilization," *Passive & Active Measurement (PAM)*, vol. 3015, pp. 278-288, Apr 2004.

[IWQoS'04] R. Keralapura, C. N. Chuah, G. Iannaccone, and S. Bhattacharrya, "Service Availability: A New Approach to Characterizing Network Topologies," *IEEE Proc. IWQoS*, pp. 232-241, Jun 2004.

[BF+04] S. Bryant, C. Filsfils, S. Previdi, and M. Shand, "IP Fast Reroute using tunnels," Internet draft, draft-bryant-ipfrr-tunnels-00.txt, work in progress, 2004.

[FB05] P. Francois and O. Bonaventure, "Avoiding transient loops during IGP convergence in IP networks" IEEE INFOCOM, Mar 2005.

[IWQoS'05] Z. Zhong, R. Keralapura, S. Nelakuditi, Y. Yu, J. Wang, C-N. Chuah, and S. Lee, "Avoiding Transient Loops through Interface-Specific Forwarding," *Proc. IFIP/IEEE International Workshop on Quality of Service (IWQoS), Springer-LNCS*, vol. 3552, pp. 219-232, Jun 2005.

[AB+01] D. Anderson, H. Balakrishna, M. Kaashoek, and R. Morris, "Resilient Overlay Networks, *SOSP*, Oct 2001.

[NPB03] A. Nakao, L. Peterson, and A. Bavier, "A Routing Underlay for Overlay Networks," *ACM SIGCOMM* 2003.

RUBINET

References (2)

[SC+99] S. Savage, A. Collins, E. Hoffman, J. Snell, and T. Anderson, "The end-to-end effects of internet path selection," in *ACM SIGCOMM*, Aug.1999.

[CD+03] M. Castro, P. Druschel, A. Kermarrec, A. Nani, A. Rowstron, and A. Signh, "SplitStream: High-Bandwidth Multicast in Cooperative Environments," *SOSP*, Oct 2003.

[FJ94] S. Floyd and V. Jacobson, "The Synchronization of Periodic Routing Messages," *IEEE/ACM ToN*, 2(2):122-136, Apr 1994.

[QYZ03] L. Qiu, Y. Yang, Y. Zhang, and S. Shenker, "On Selfish Routing in Internet-Like Environments," *ACM SIGCOMM*, Aug 2003.

[LZ+05] Y. Liu, H. Zhang, W. Gong, D. Towsley, "On the Interaction between Overlay Routing and Traffic Engineering," *IEEE INFOCOM*, Mar 2005.

[HotNets'04] R. Keralapura, N. Taft, C. N. Chuah, and G. Iannaccone, "Can ISPs take the heat from Overlay Networks?" to appear in *ACM Workshop on Hot Topics in Networks (HotNets-III)*, Nov 2004.

[ICNP'05] R. Keralapura, C-N. Chuah, N. Taft, and G. Iannaccone, "Can co-existing overlays inadvertently step on each other?" to appear in *Proc. IEEE ICNP*, Nov 2005.

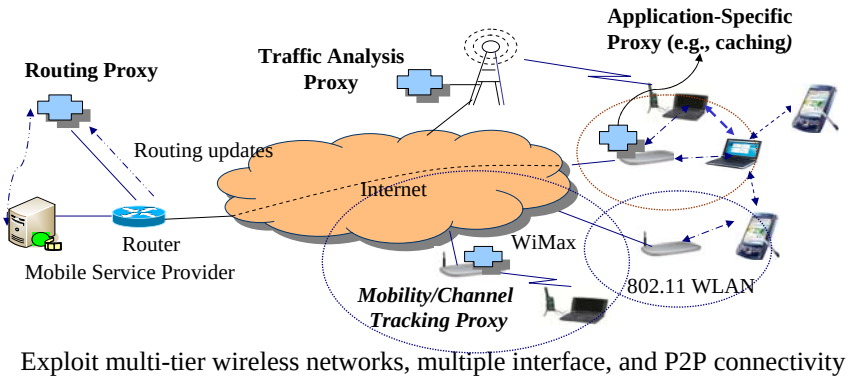
RUBINET

Questions?

- http://www.ece.ucdavis.edu/rubinet

RUBINET

MINESTRONE - Mobile Infrastructure Enablers for Streaming Optimization & New Services

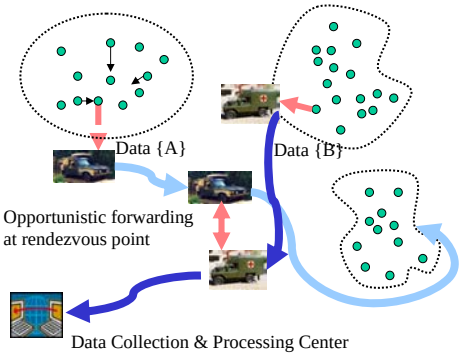


- Exploit multi-tier wireless networks, multiple interface, and P2P connectivity
- Proxy-based approach: monitoring, mobility tracking, persistent data caching, traffic analysis, dynamic service creations
- Target applications: multimedia streaming [PacketVideo'04, JCN'05], gaming, security services
- Sponsors: Hewlett Packard, UC Micro

RUBINET

Vehicular Mesh Networks (VMesh)

- Vehicles as mobile routers, sensors and computing
  - Leverage Dedicated Short Range Communication (DSRC) for inter-vehicle and vehicle-to-roadside communications
  - Opportunistic forwarding between mobile routers
  - Applications: Intelligent transportation system, amber alert, disaster relief
  - *Collaborators:*
    - *Dipak Ghosal (CS)*
    - *Michael Zhang (Civil & Environmental Engineering)*



RUBINET

Some background info …

- Robust & Ubiquitous Networking Research Group
  - ~3 years old
  - PhD Students: R. Keralapura, J. LeBrun, D. Li, J. Mai, L. Yuan
  - MS Students: A. Chen, C. Dana
- Research focus
  - Network measurements and anomaly detection
  - Routing & traffic engineering
  - Overlay networks
  - Multi-layer information exchange, inferences, and optimization
  - Wireless networks (vehicular ad hoc networks, sensor networks)

RUBINET