

Sharing Information for Better Network Security

Mark Allman, ICSI(-midwest)

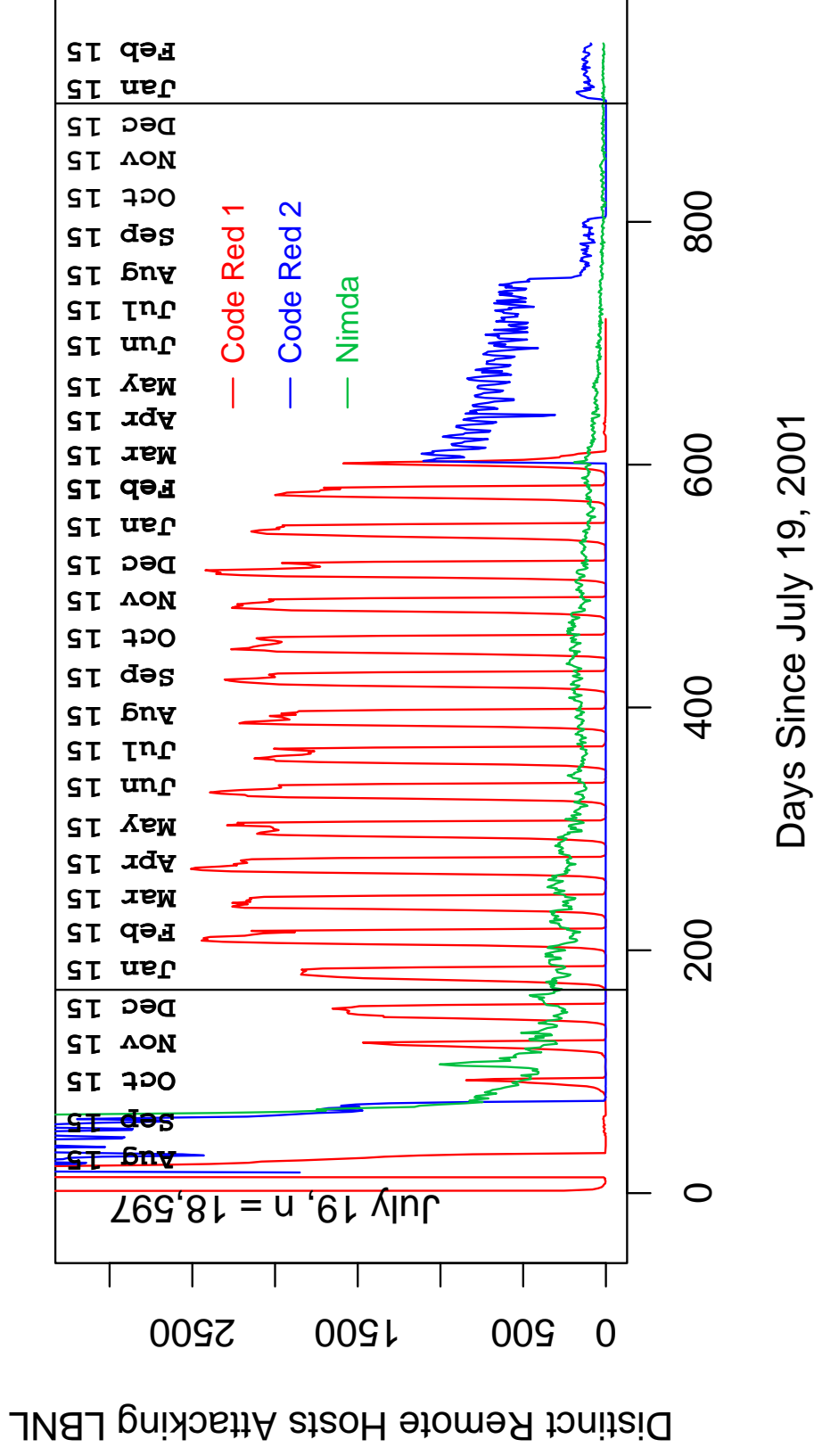
OhioICE Technical Conference
October 2006

*"As we celebrate mediocrity all the boys upstairs want to see,
How much you'll pay for what you used to get for free"*

Background

- Network security is a mess
 - ▶ viruses, worms, spam, phishing, botnets, etc., etc.
- Always a new (and clever) attack
- Also, a multitude of *persistent* attackers
 - ▶ constant "background radiation"

Background (cont.)



(plot from Vern Paxson)

Background (cont.)

- Standard approaches:
 - ▶ firewalls
 - ▶ intrusion detection systems
 - ▶ virtual private networks
 - ▶ NATs
 - ▶ virus scanners
 - ▶ spyware cleansers
- Mostly single point mitigations
 - ▶ *whack-a-mole*

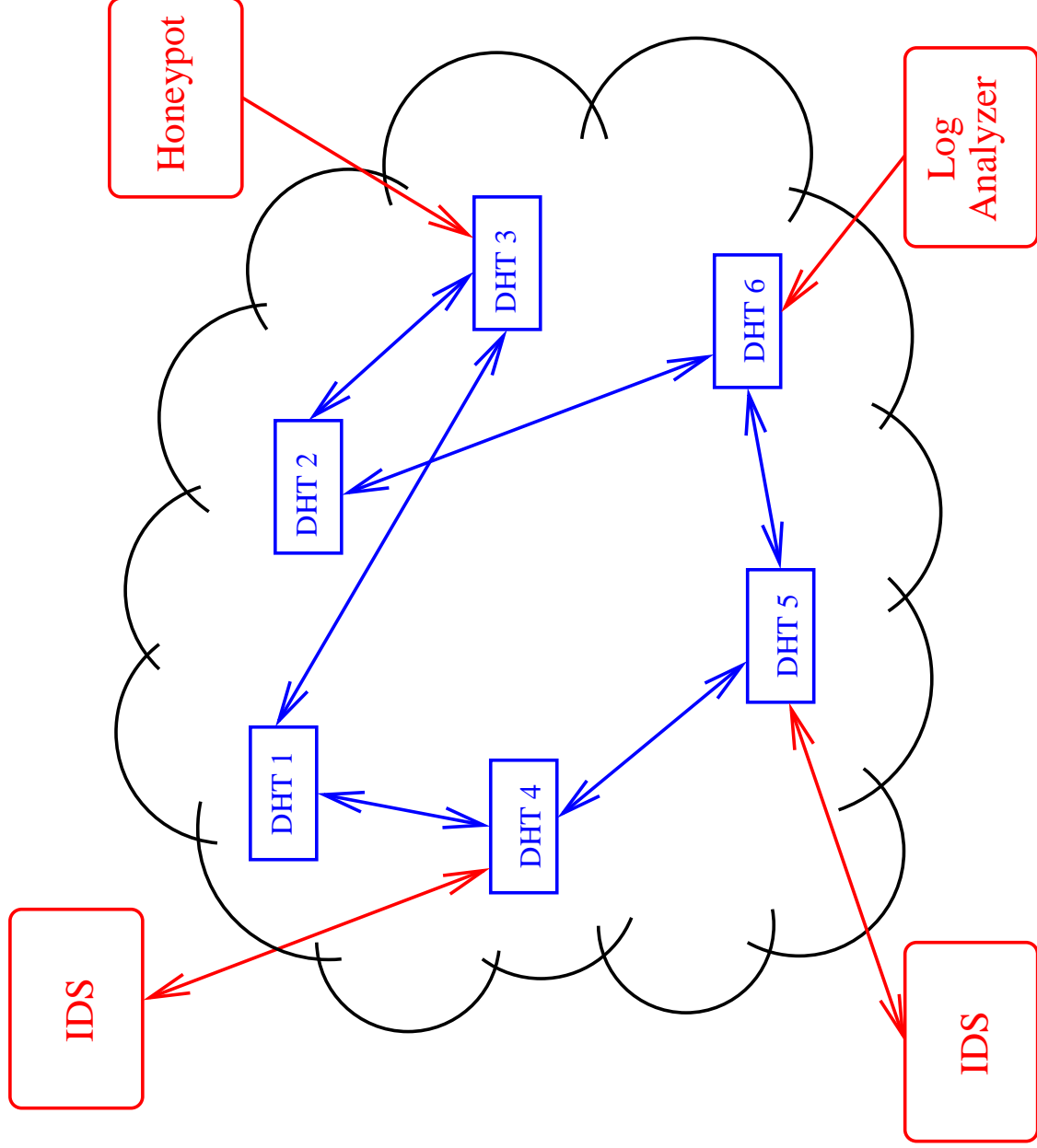
Basic Wonderings

- Can we improve the state of network security by sharing more information across organizations?
- Informal sharing exists -- especially in times of crisis
 - ▶ how much can we automate?
- How can we conduct information sharing in a routine and *practical* way that respects the possible sensitivity of the data?
 - ▶ e.g., due to user's privacy concerns
 - ▶ e.g., due to a provider's competitive concerns

New Approach I

- An open global system for sharing behavioral information about bad actors in the network
 - ▶ many vantage points sharing their view of the network
 - ▶ grass roots

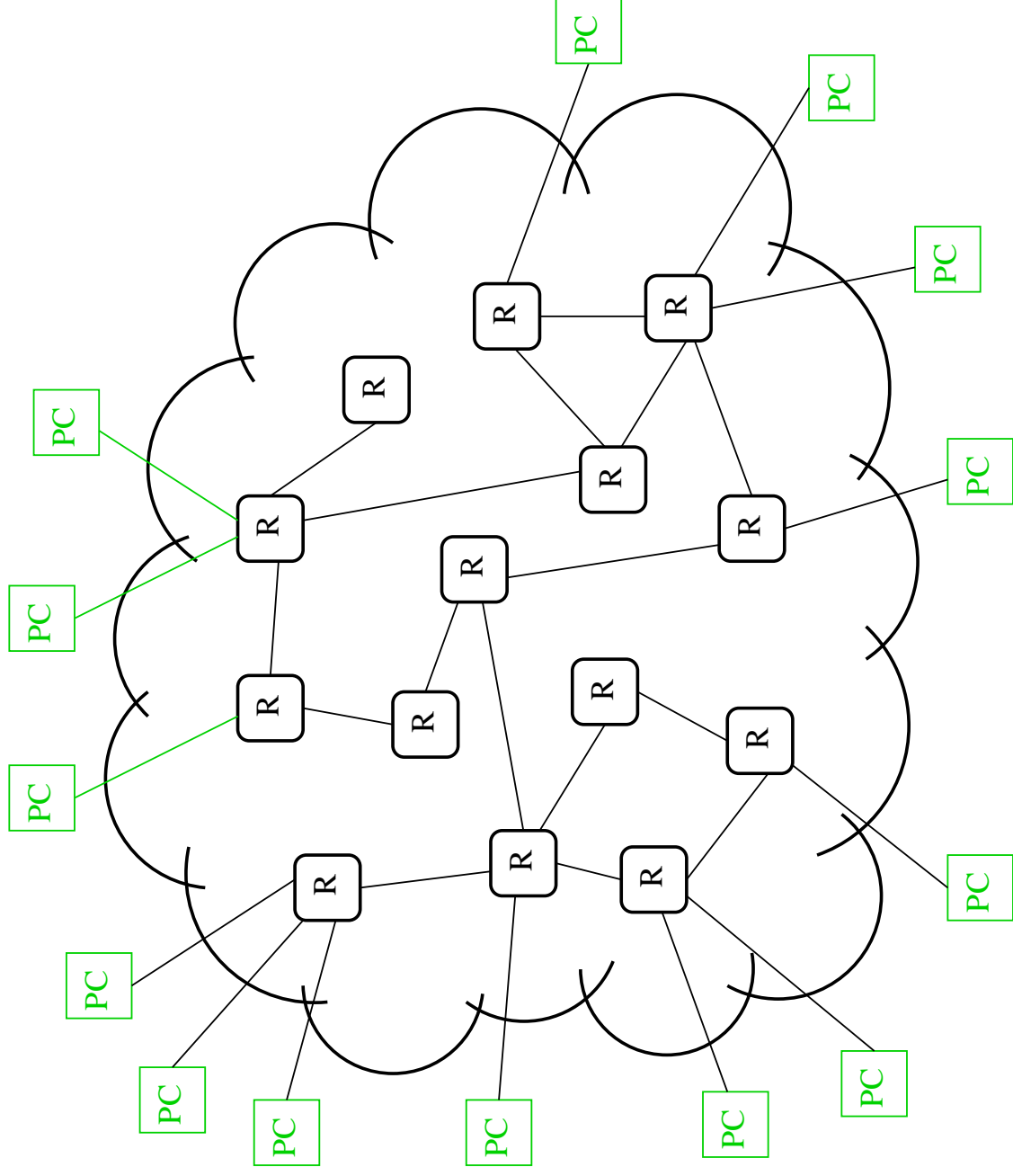
Global Database



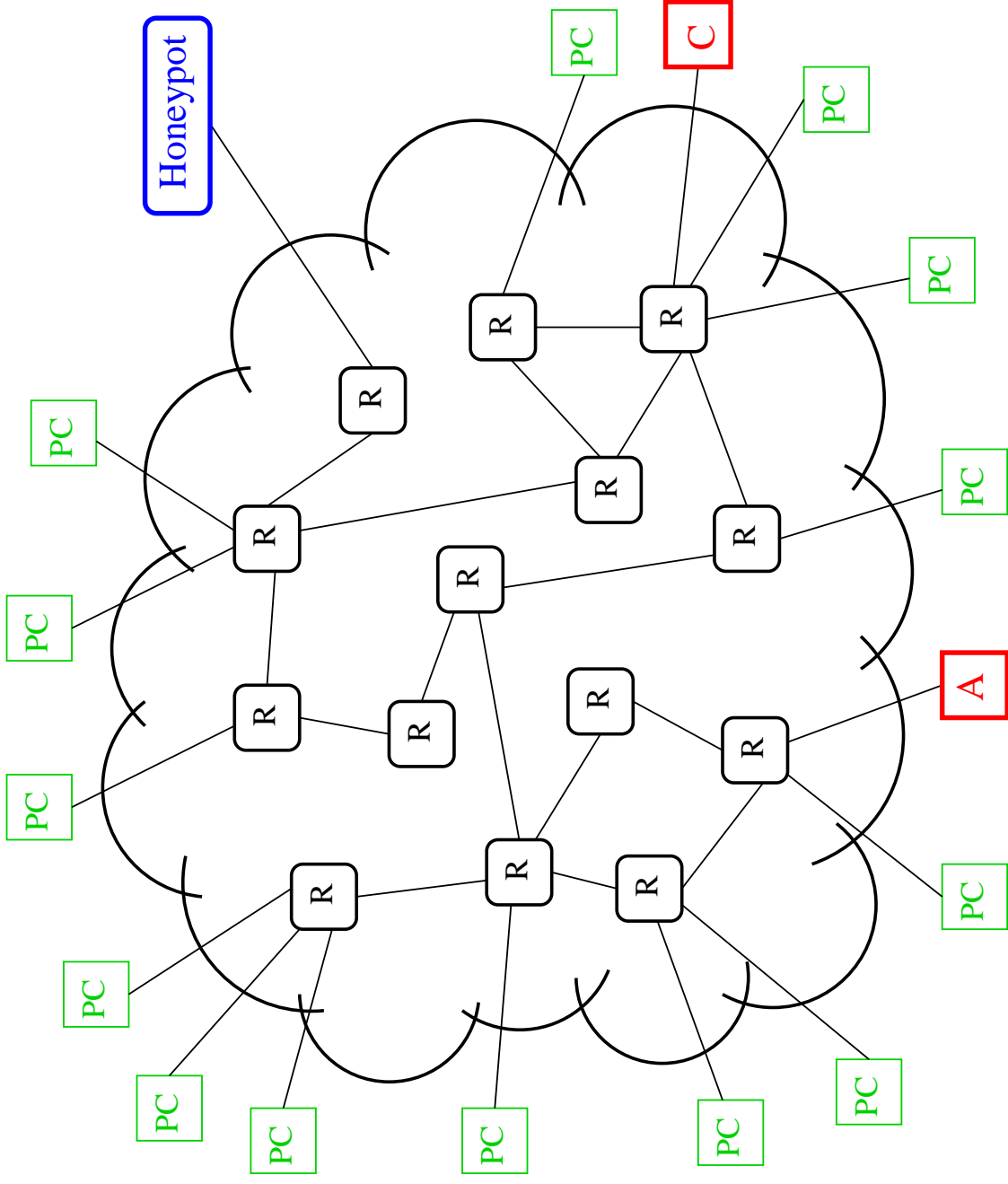
New Approach II

- A problem with simply sharing observations is that the *linkages* between attacks are not taken into account
- ▶ we propose a two-tiered system

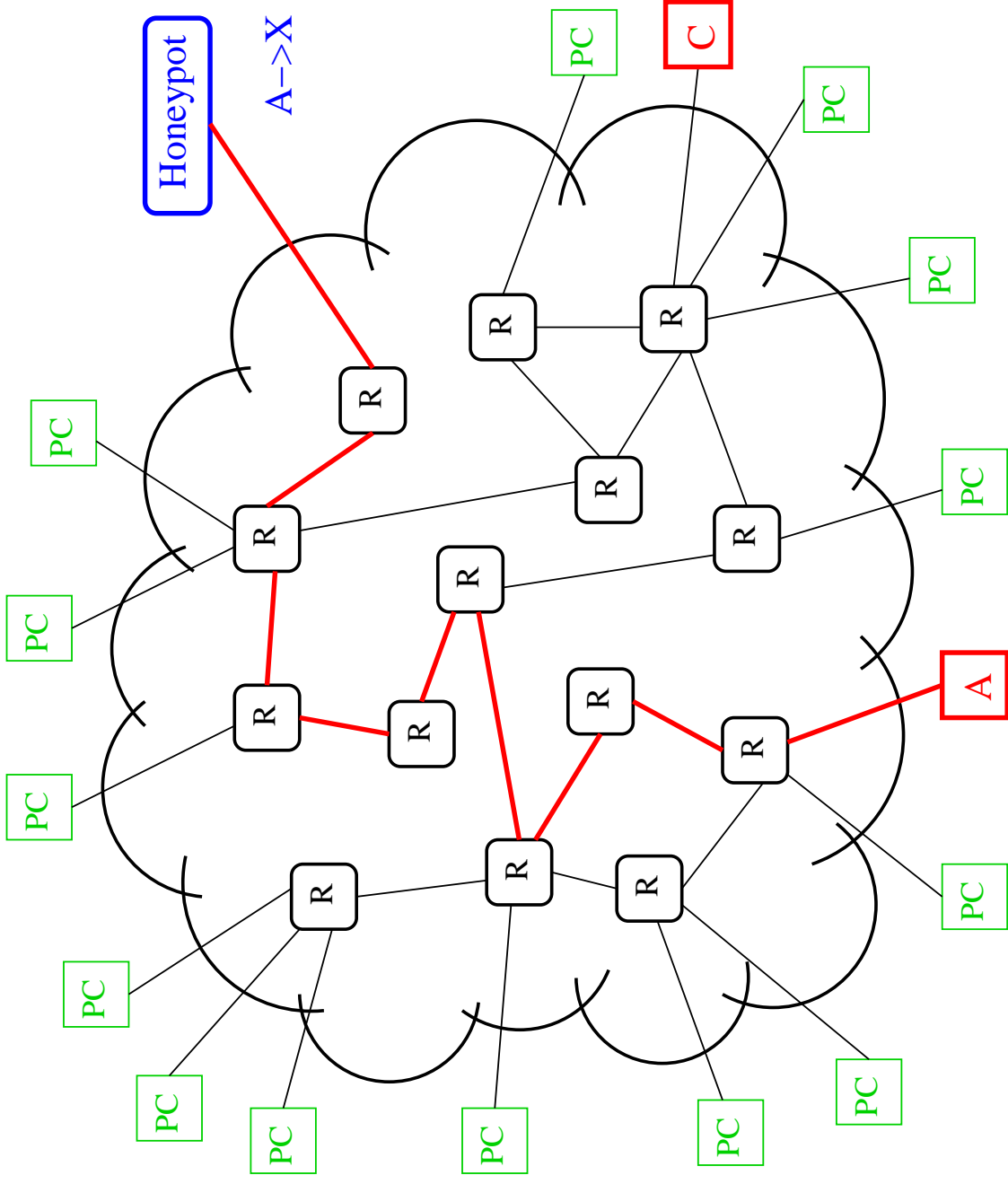
Of Detectives and Witnesses



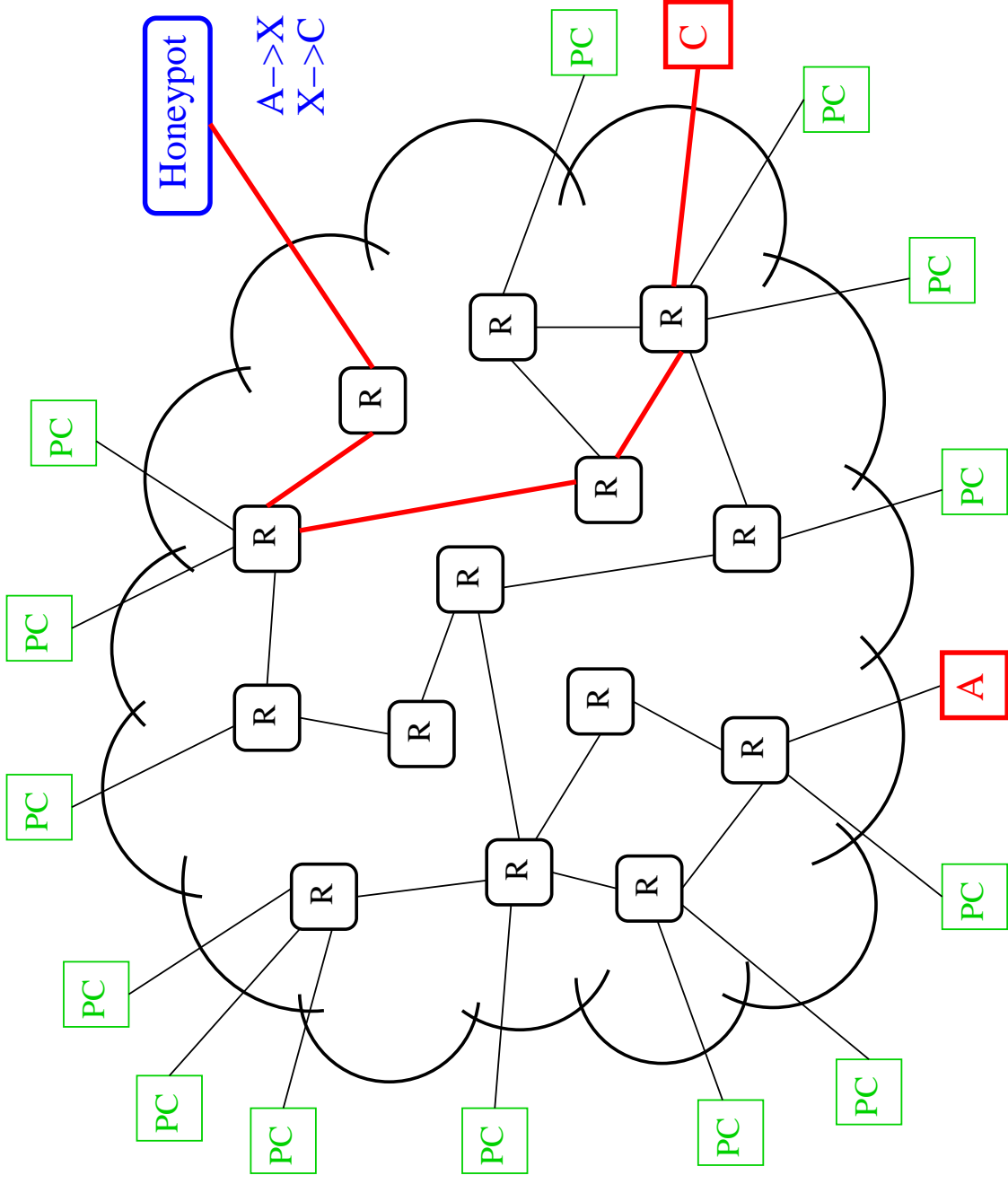
Of Detectives and Witnesses



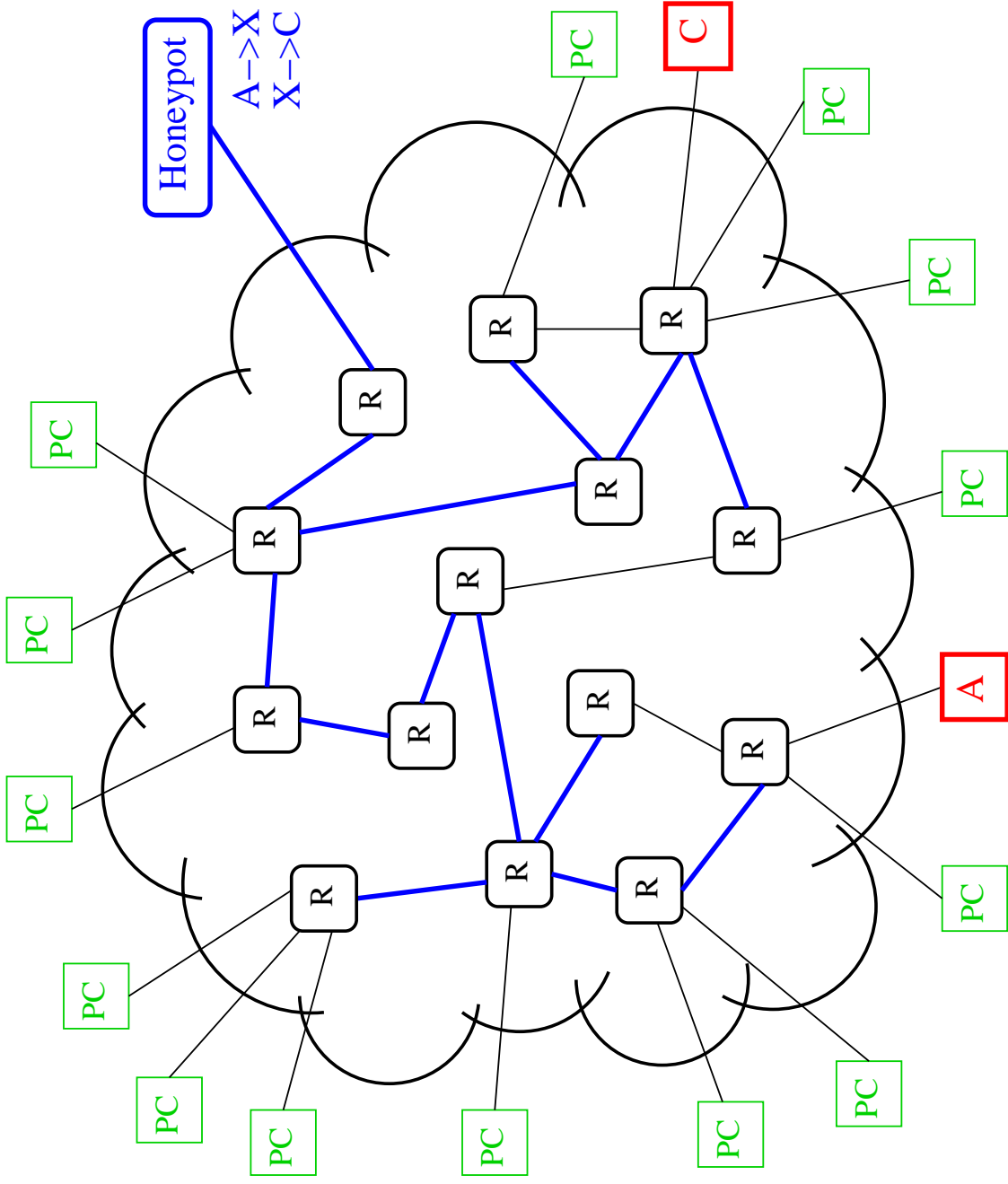
Of Detectives and Witnesses



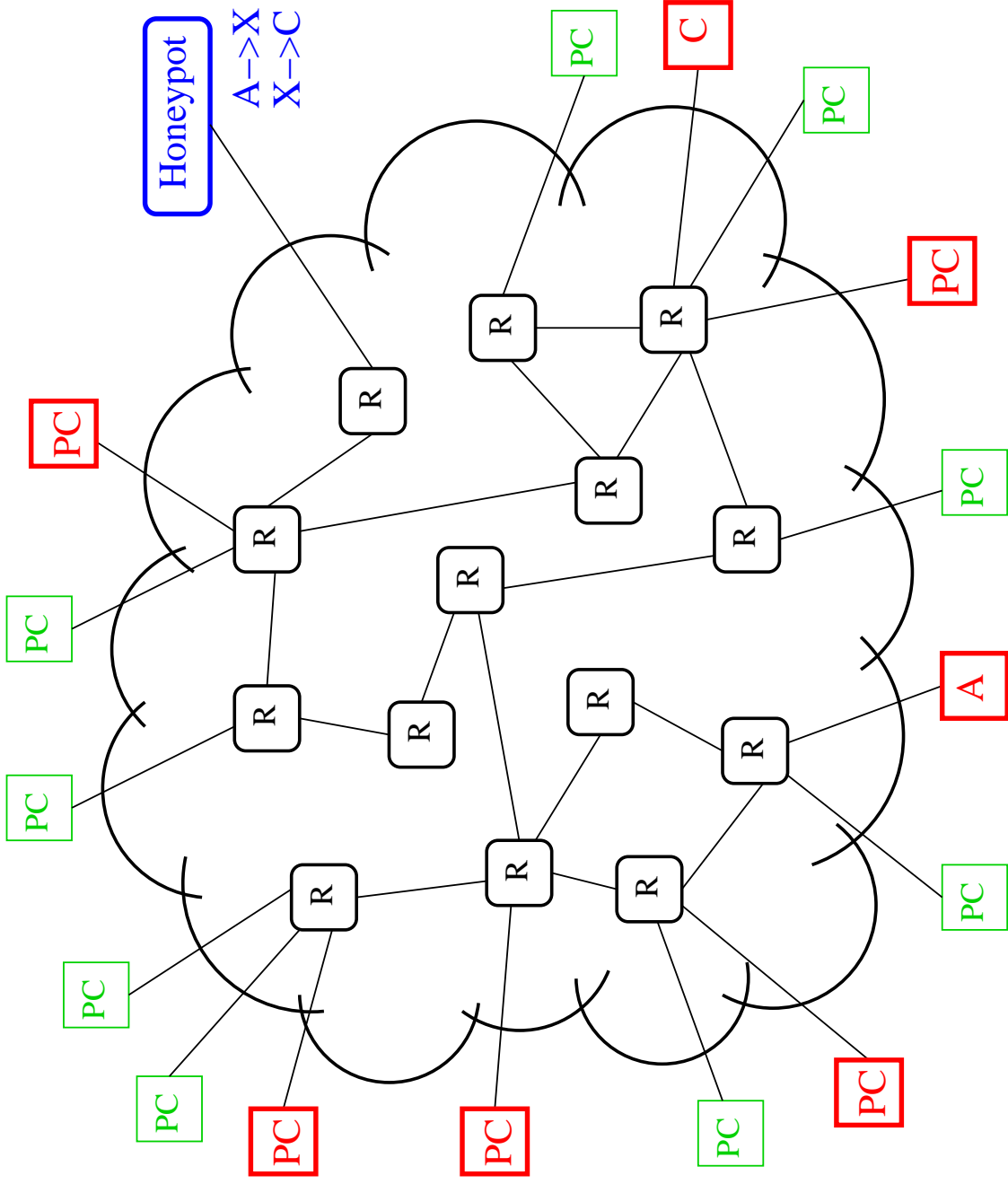
Of Detectives and Witnesses



Of Detectives and Witnesses



Of Detectives and Witnesses



Summary

- Conjecture: Systematic sharing of security information can make for a more secure Internet
- But, can we make it work in the face of numerous challenges?

References

- Mark Allman, Ethan Blanton, Vern Paxson. *An Architecture for Developing Behavioral History*. USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet, July 2005.
- Mark Allman, Ethan Blanton, Vern Paxson, Scott Shenker. *Fighting Coordinated Attackers with Cross-Organizational Information Sharing*. ACM SIGCOMM HotNets, November 2006. To appear.
- Contact:
 mal1man@icir.org
 <http://www.icir.org/mal1man/>