WAIL Internet Sinks

Internet Sink Deployments:
On the Design and Use of Internet Sinks for Network Abuse Monitoring

IEPG Meeting, Vienna, 13 July 2003

- **University of Wisconsin-Madison: Wisconsin Advanced Internet Lab (WAIL)**
  http://wail.cs.wisc.edu
  - **Dave Plonka <plonka@doit.wisc.edu>**
  - **Paul Barford**
  - **Vinod Yegneswaran**

iSink Overview

- Definitions, Approach
- Architecture
- Performance
- Real World Observations
- Performance Evaluation
- Active Responses, Tarpit Effectiveness
- Results, Discussion
- Future Work

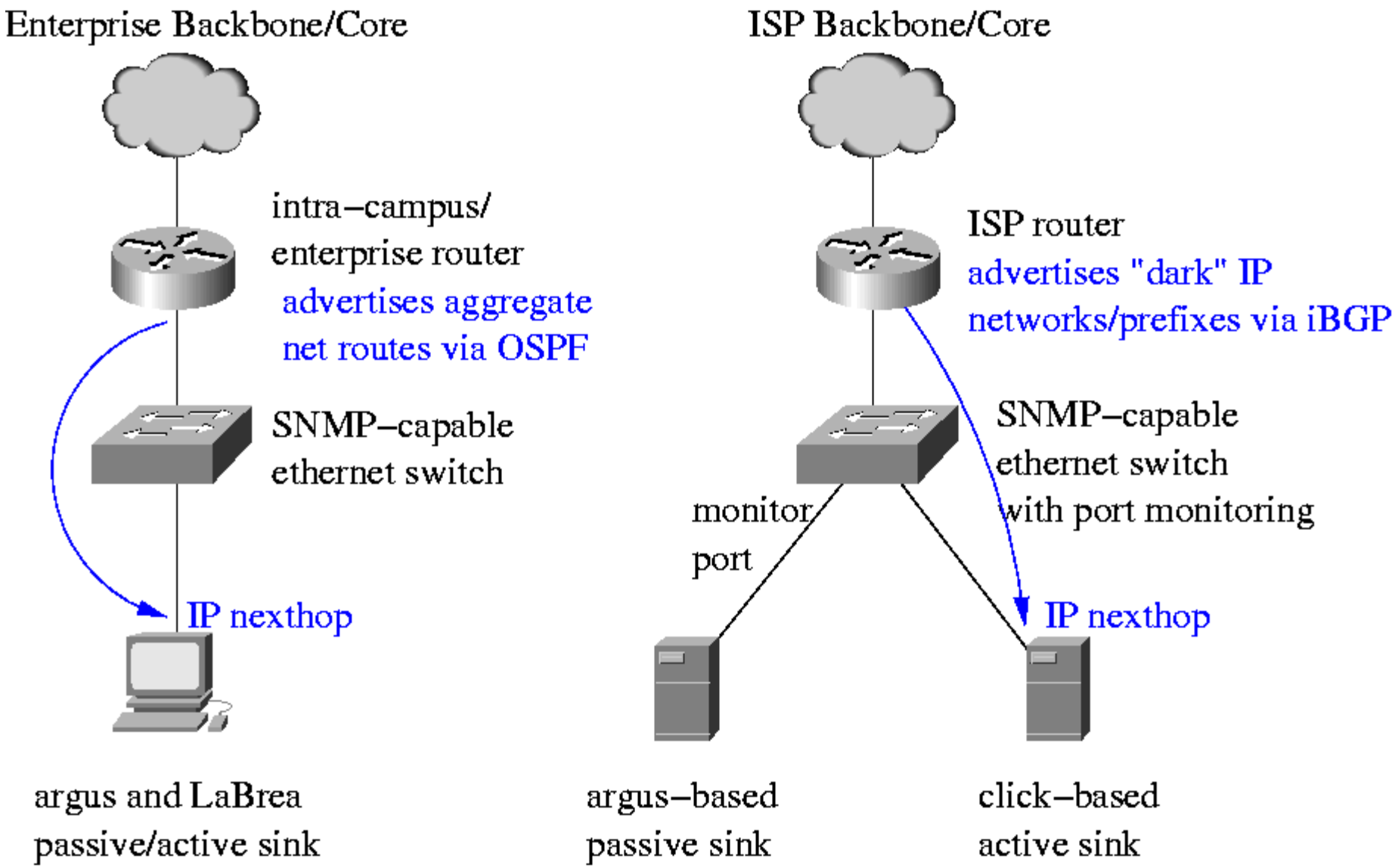
iSink Definitions

- Internet Sink:
  - A system, either passive or active, to which IP traffic is diverted
  - Includes blackhole/sinkhole routers, tarpits
- Network Abuse:
  - Notion is broadly defined,ultimately determined by local policies
  - We focus on intrusion attempts and attack activity

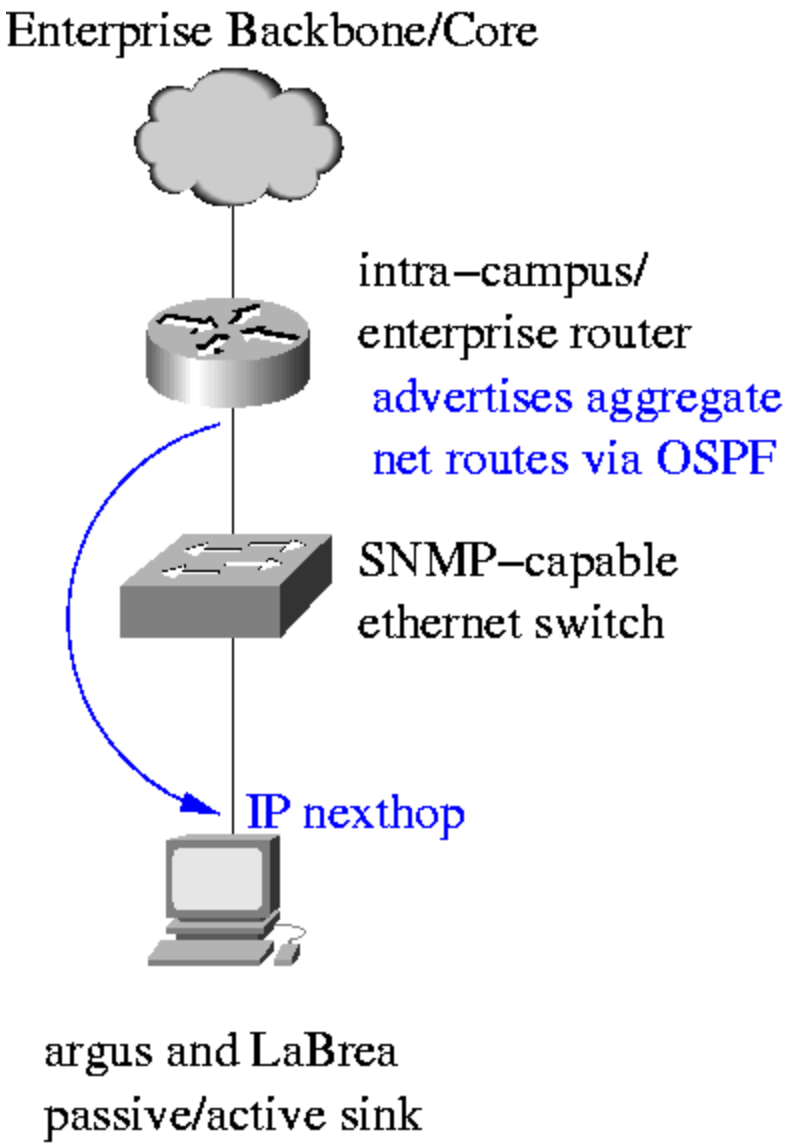
iSink Approach

- Monitor activity of "unused" IP addresses or transport endpoints:
  - This traffic is not often monitored
  - Limited false positives:
    - misconfigurations
    - typos
  - System may be configured to respond without interfering with existing services, ie. an active sink
  - Lower traffic rates
    - sampling not necessarily required
  - Anomalies are unobscured by production traffic

iSink Architecture



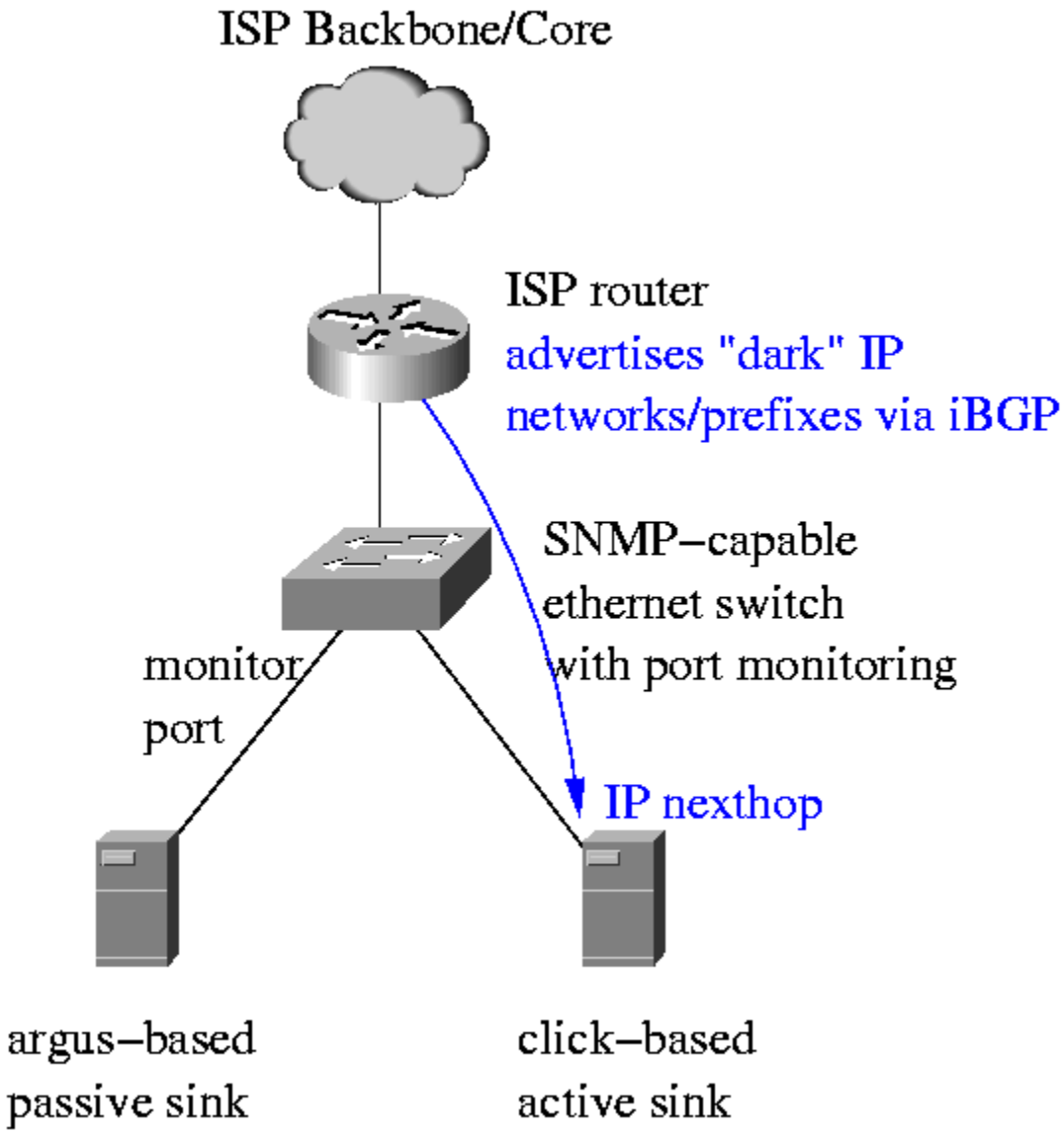
Enterprise iSink Architecture



- Receives traffic destined for ~100,000 IP addresses across four class B networks
  - In /25 - /22 blocks
  - These are the "holes" between campus subnets
- Actively responds using the LaBrea tarpit software

ISP iSink Architecture

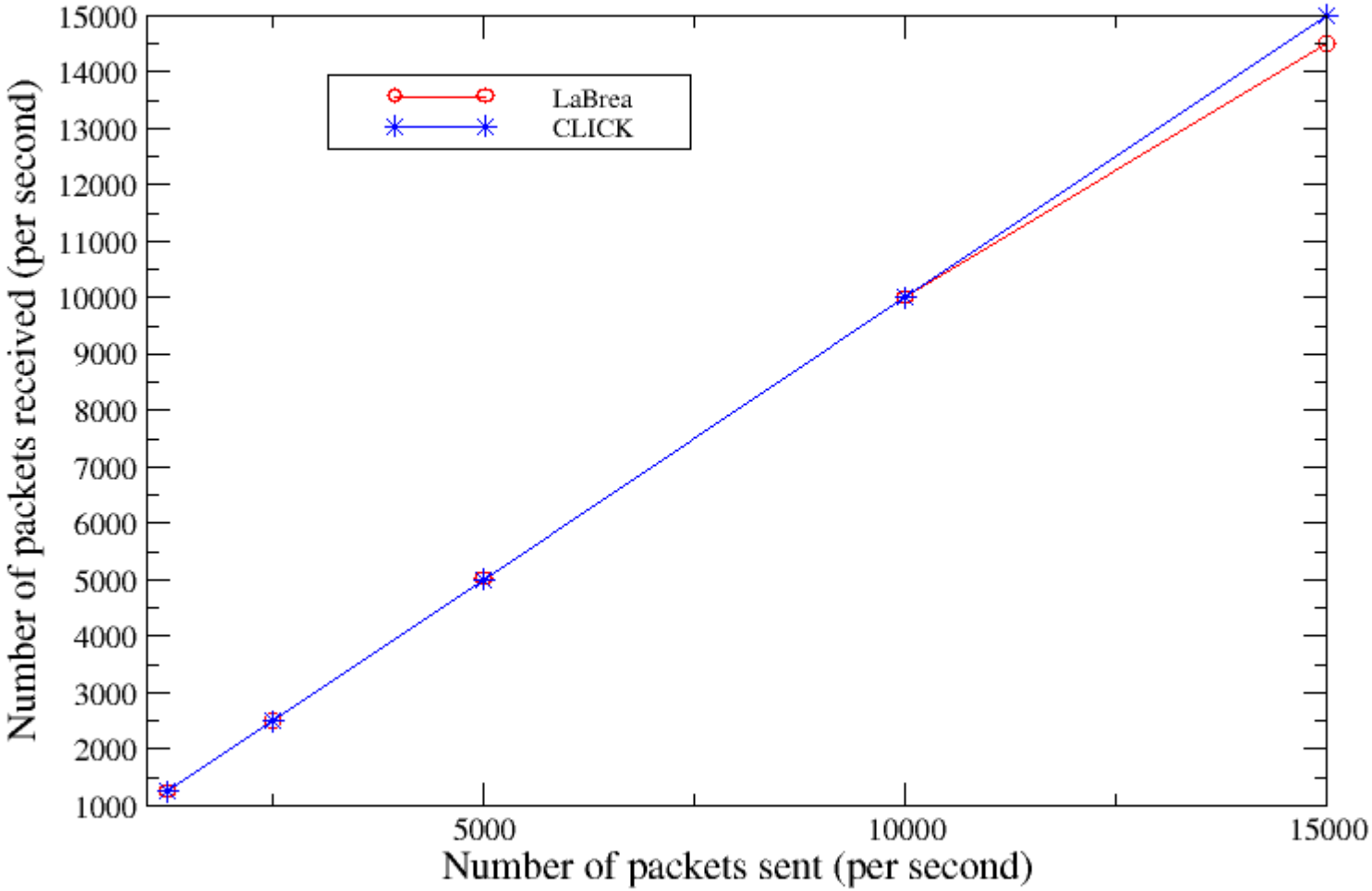
- Receives unsolicited traffic for 16 million IP addresses, one entire class A network
- Actively responds in some subnets:
  - SYNACKer
  - Linux
  - Windows
  - Solaris



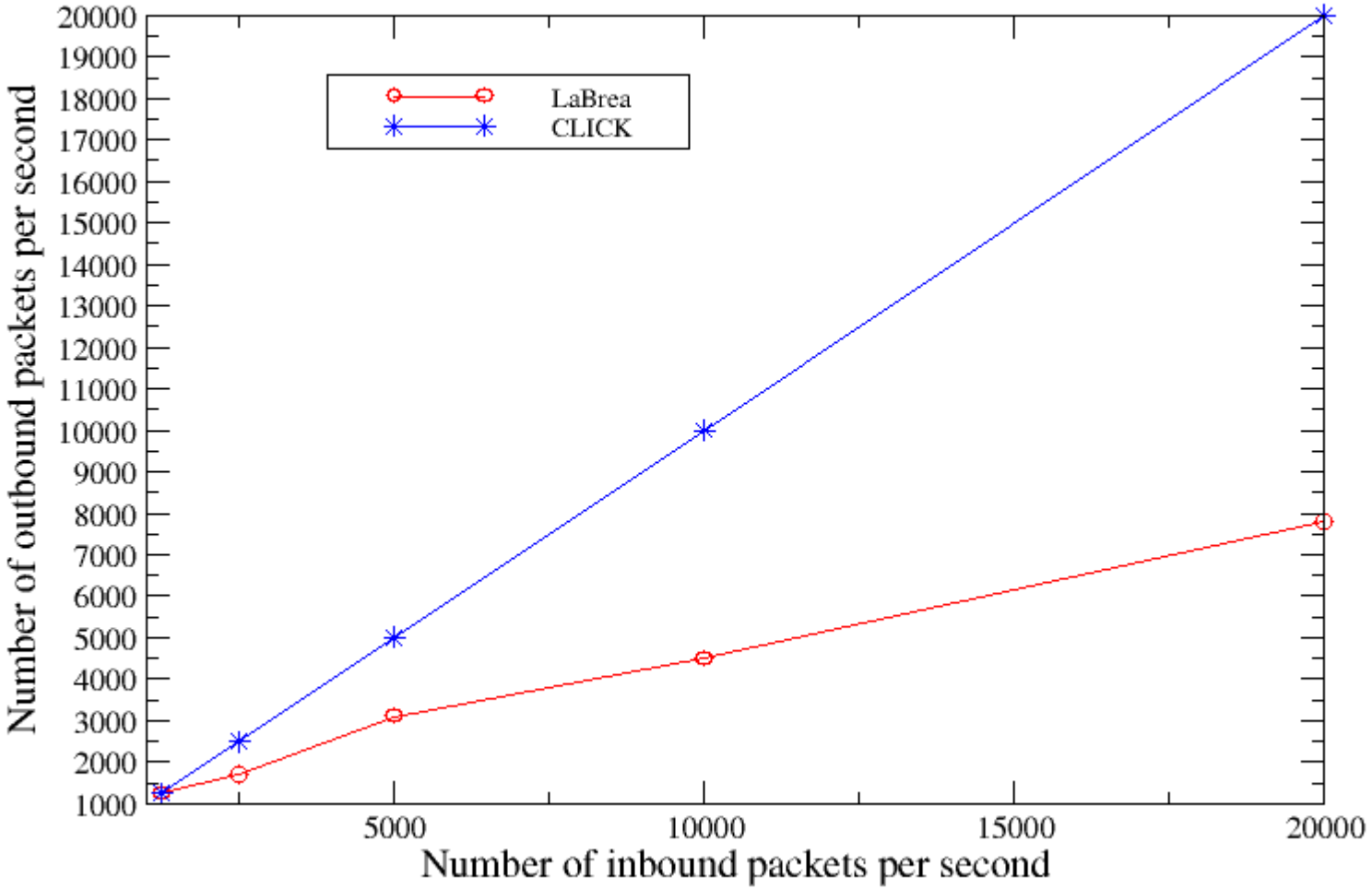
iSink Performance

- We Considered Extensibility and Scalability
- Compare LaBrea and click-based implementations on Pentium 4 machines:
  - determine TCP and UDP response capacity
  - ARP
- Click handled 20k TCP SYNs per second
- LaBrea handled 2k TCP SYNs per second
- Both can handle ~15k UDP packets per second

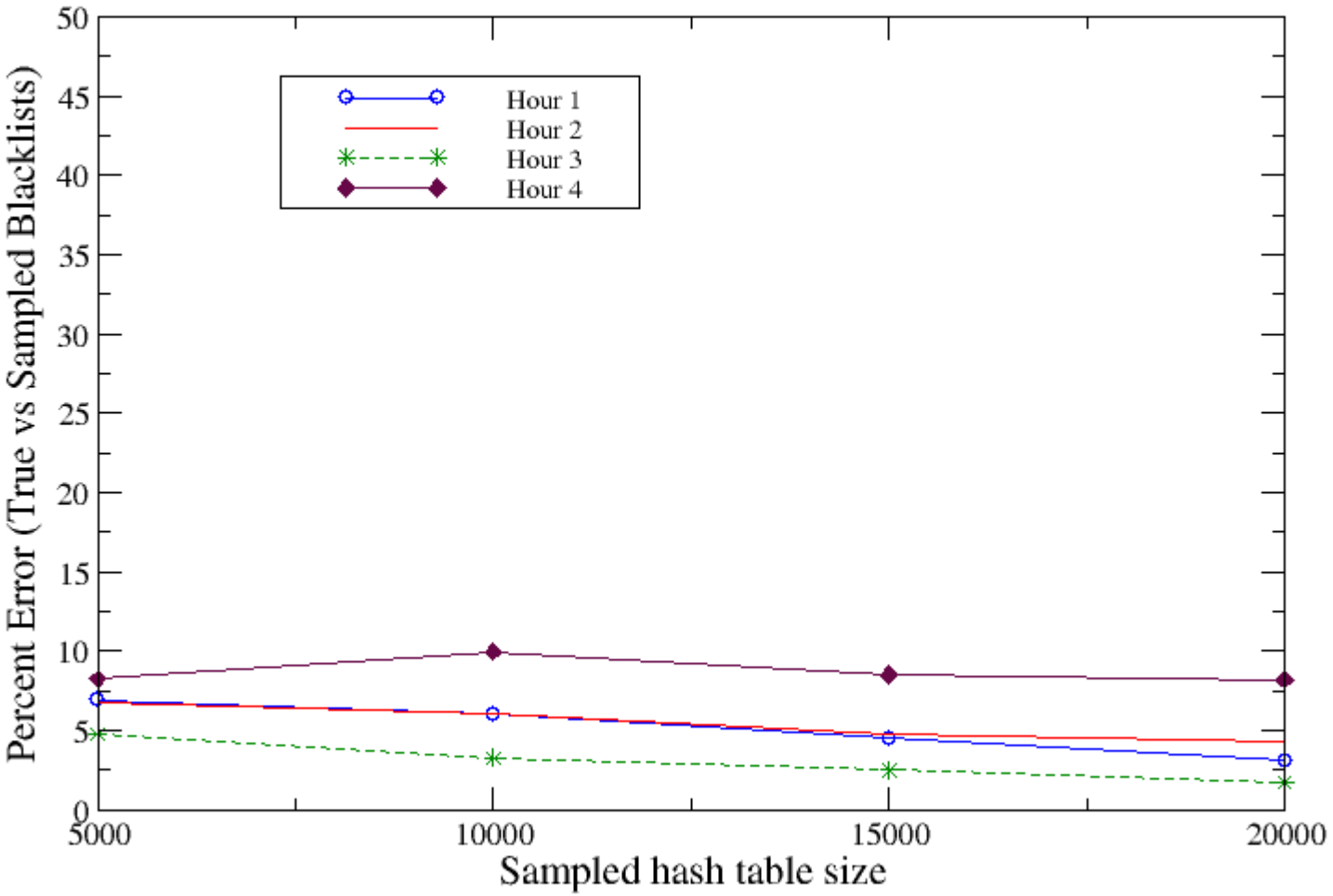
iSink UDP Performance



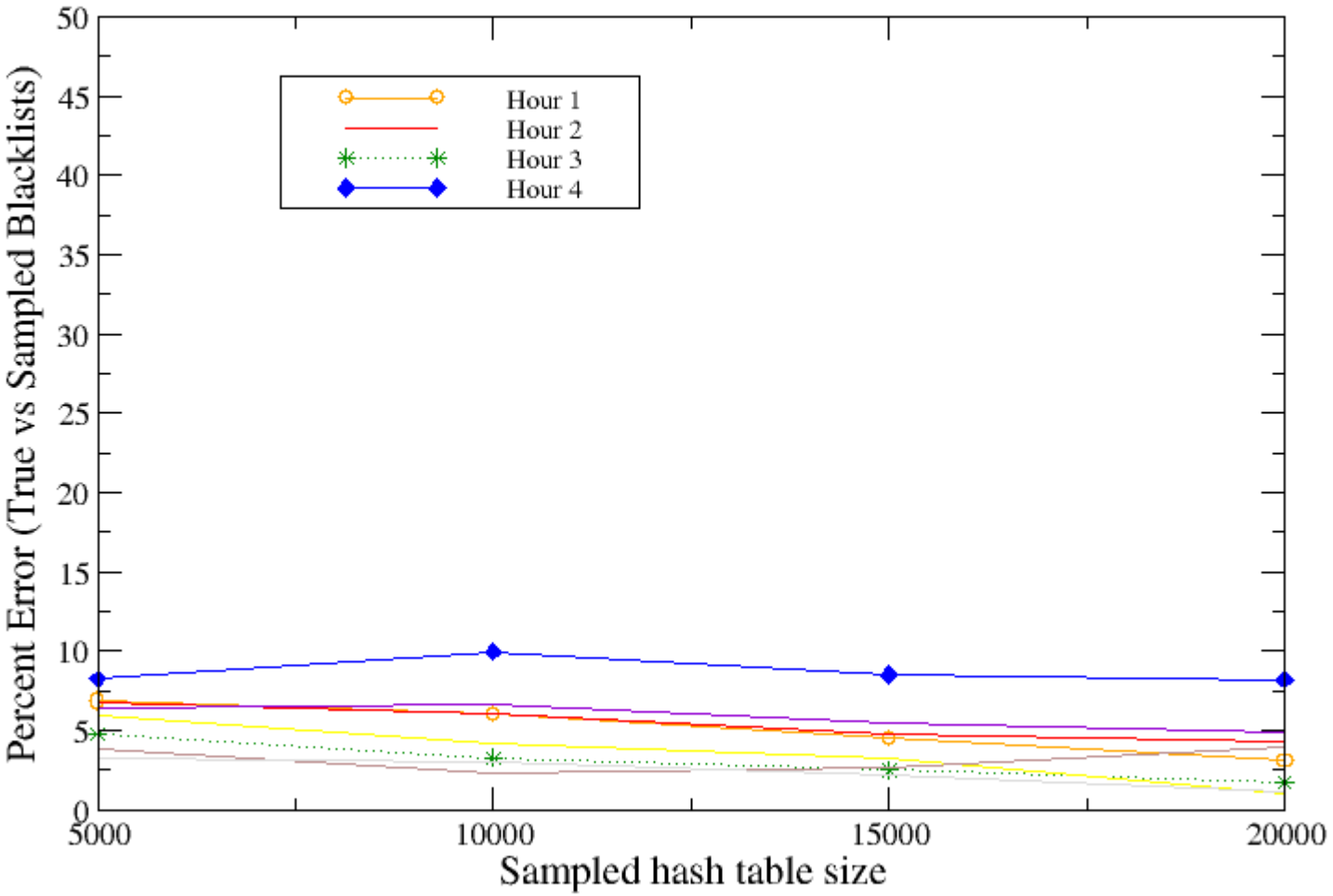
iSink TCP Performance



iSink Sampling 1/300



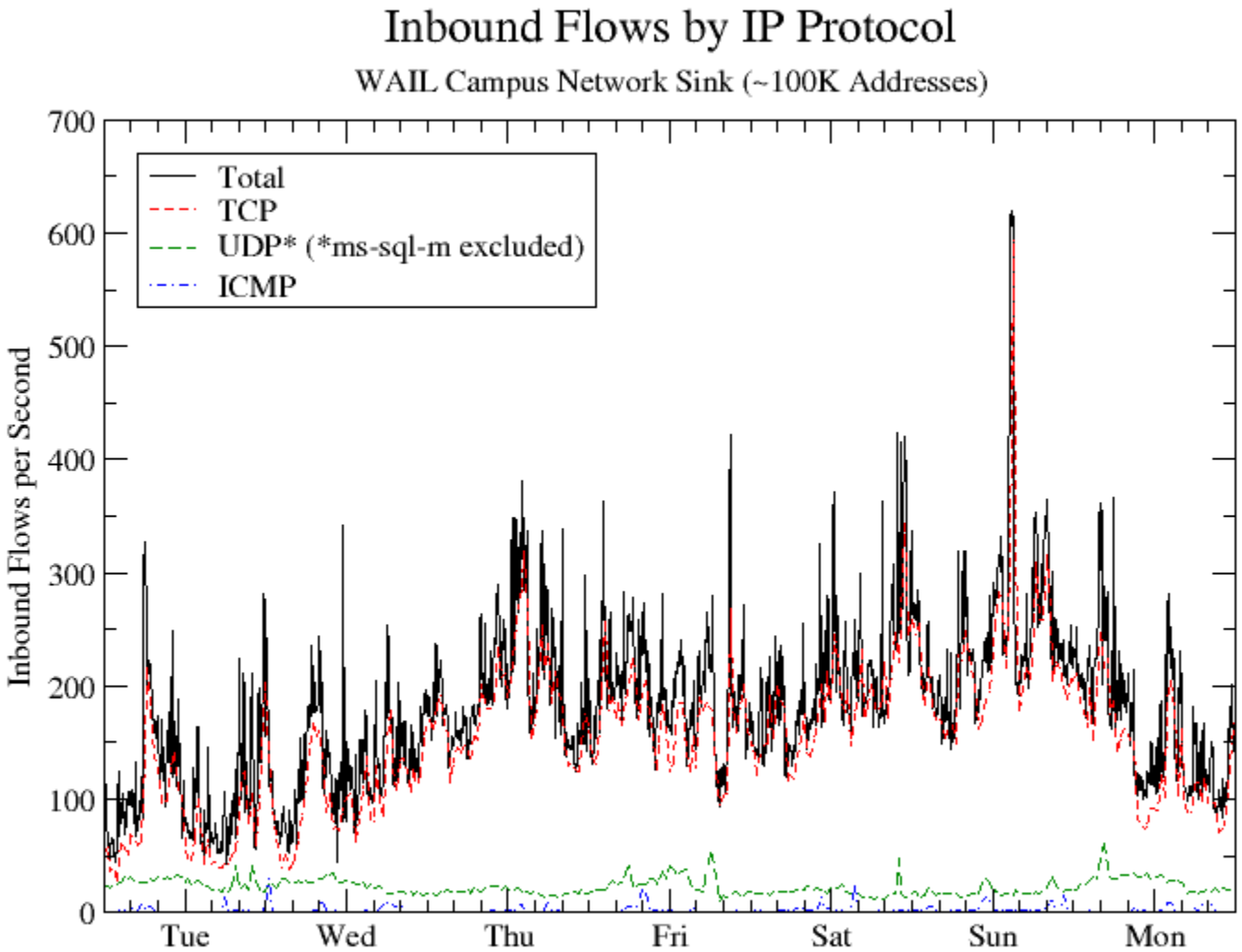
iSink Sampling 1/100



iSink Observations

- Campus iSink received:
  - Traffic from local Network Management Systems such as ping and SNMP query attempts
  - Traffic from misconfigured campus hosts, such as DNS queries to addresses which where presumably DNS servers at some time
    - the IP address space's history matters
  - Traffic from malicious probes or worms with an affinity for the local network or presumed subnet

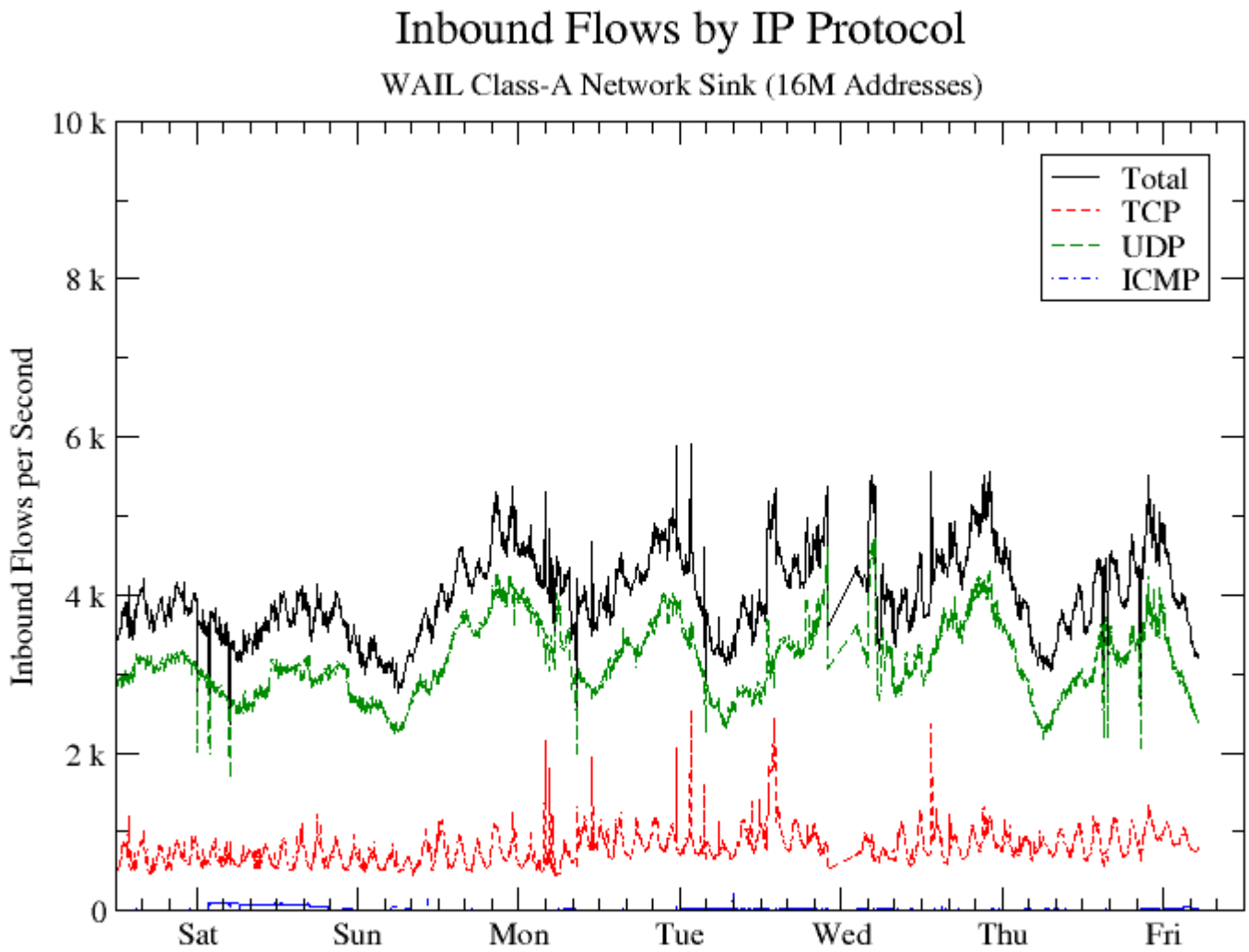
iSink Observations



iSink Observations

- Service-Provider iSink observed:
  - Average inbound rates of 5k packets per second and over 5Mbits per second
  - Not all networks respected more-specific routes in the global BGP, local policies sometimes prevent traffic from routing to iSinks
  - Unsolicited traffic dominated by UDP, due to popular probed services at the time
  - Significant amount of backscatter: traffic from Internet hosts presumed to be under attack from malicious parties forging the source IP address

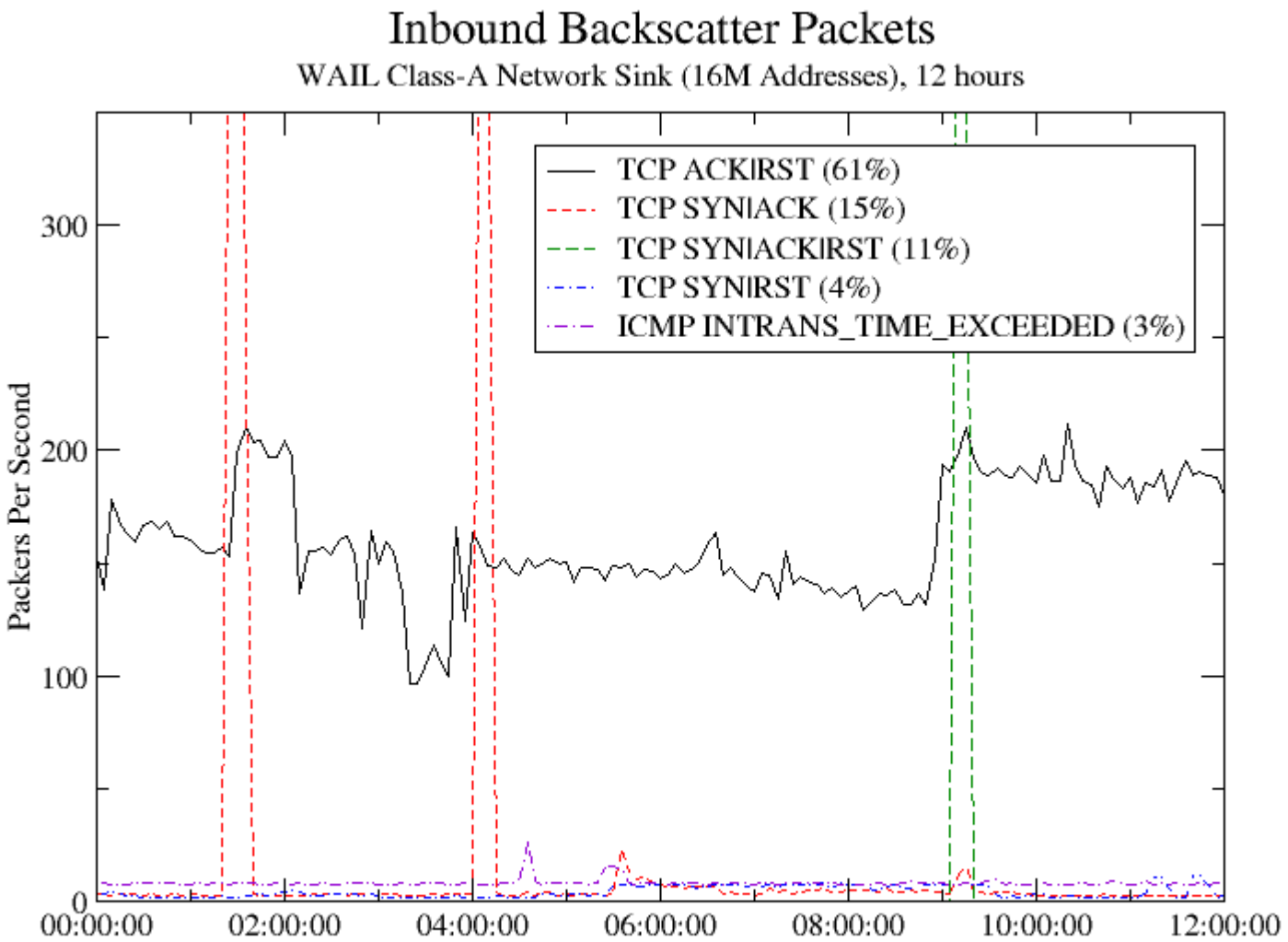
iSink Observations



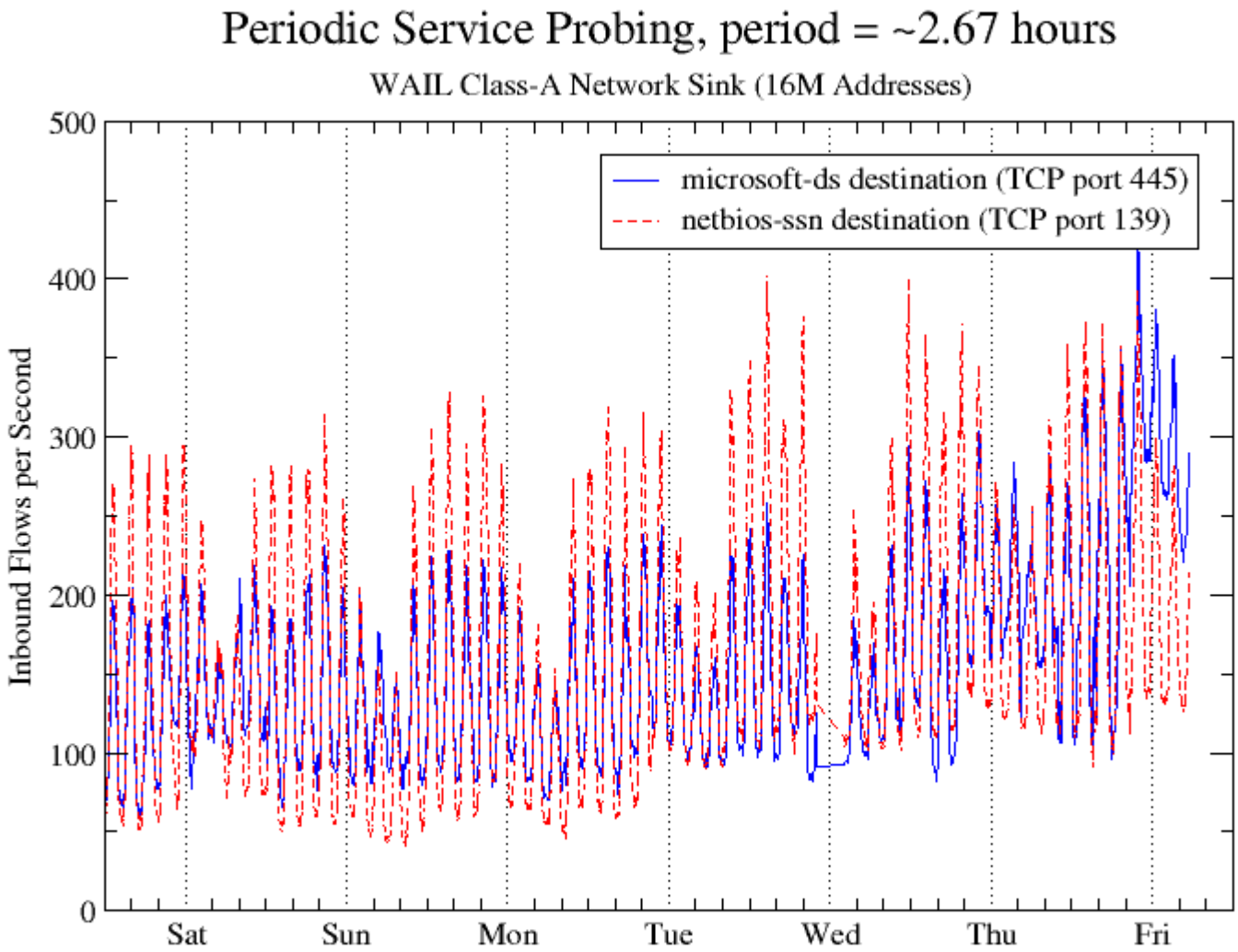
iSink Top Services

Service	Inbound flows per second
UDP netbios- ns destination	1932
UDP ms- sql- m destionation	1187
http destination	197
netbios- ssn destination	133
microsoft- ds destination	115
smtp destination	67
http source	44
http destination	11
ms- sql- s destination	10
telnet destination	2

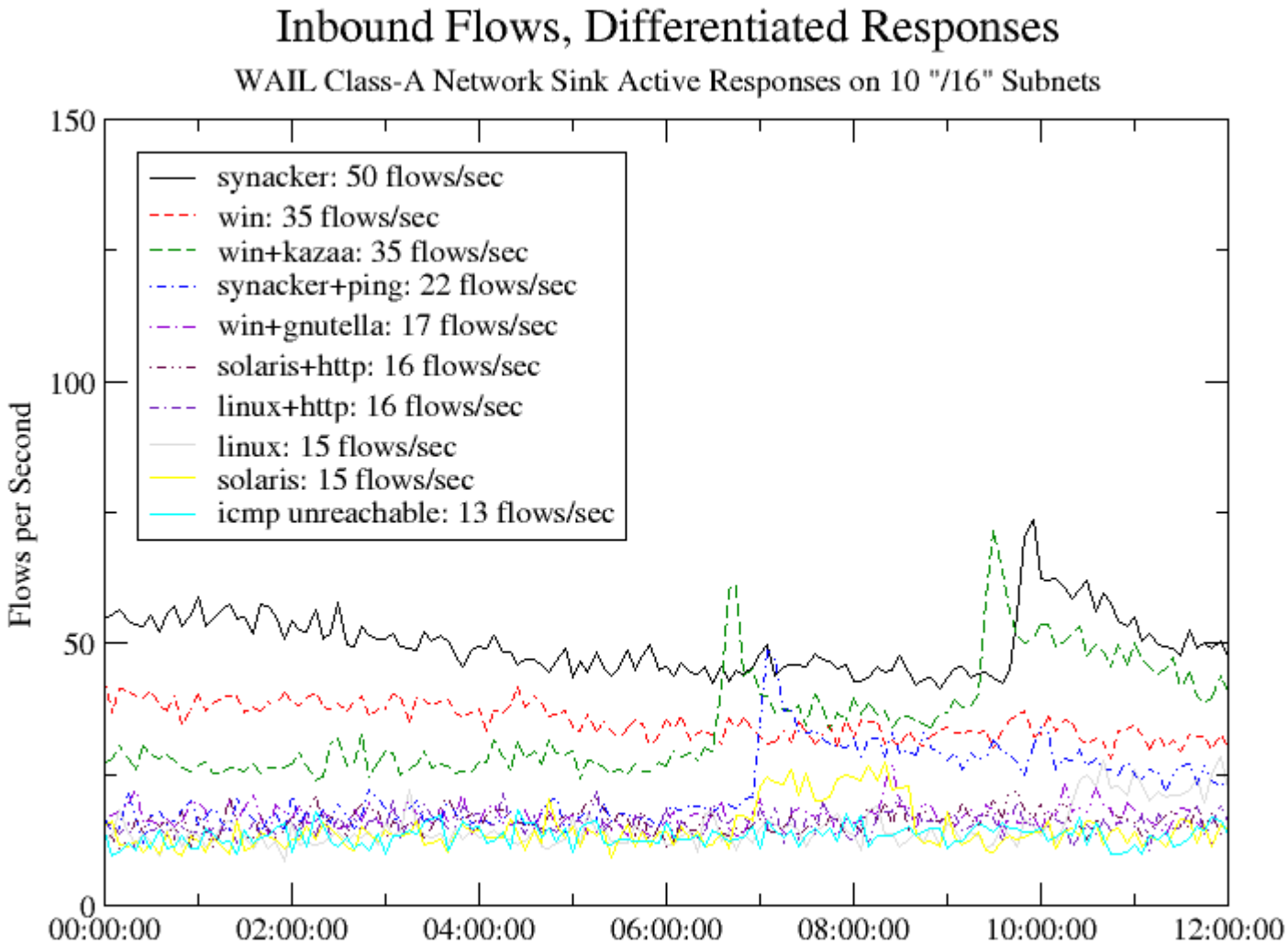
iSink Observations



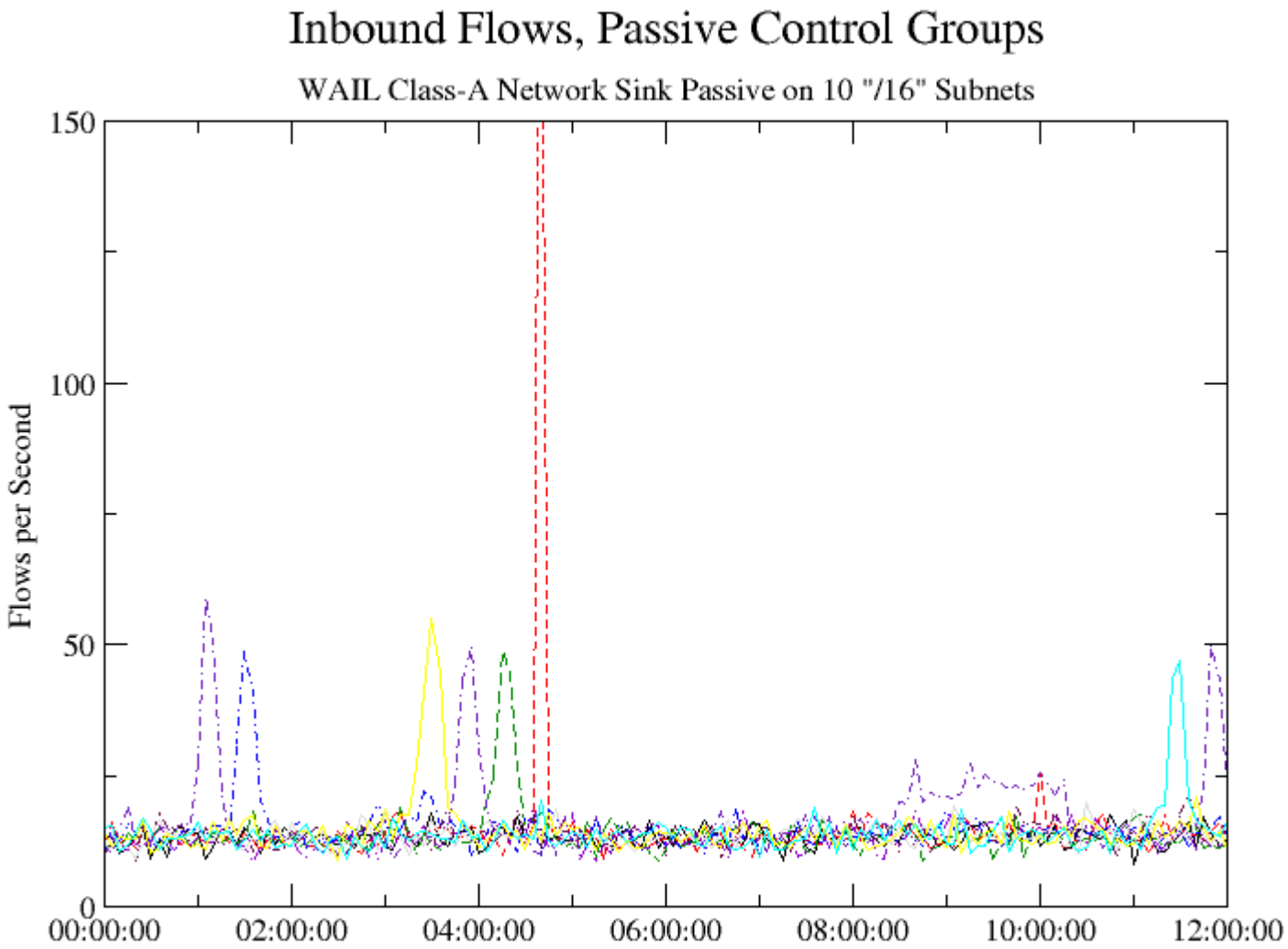
iSink Observations



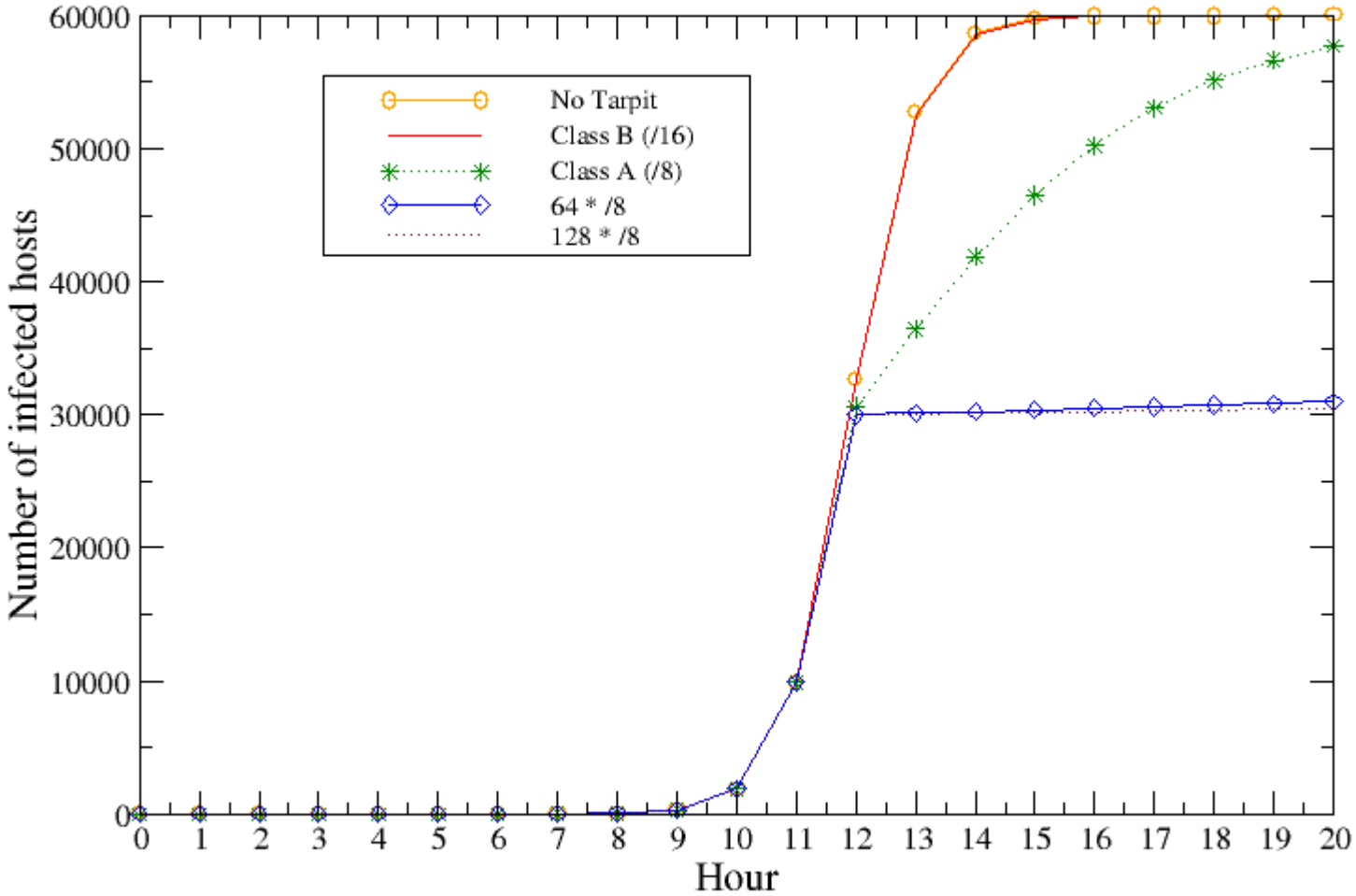
iSink Active Responses



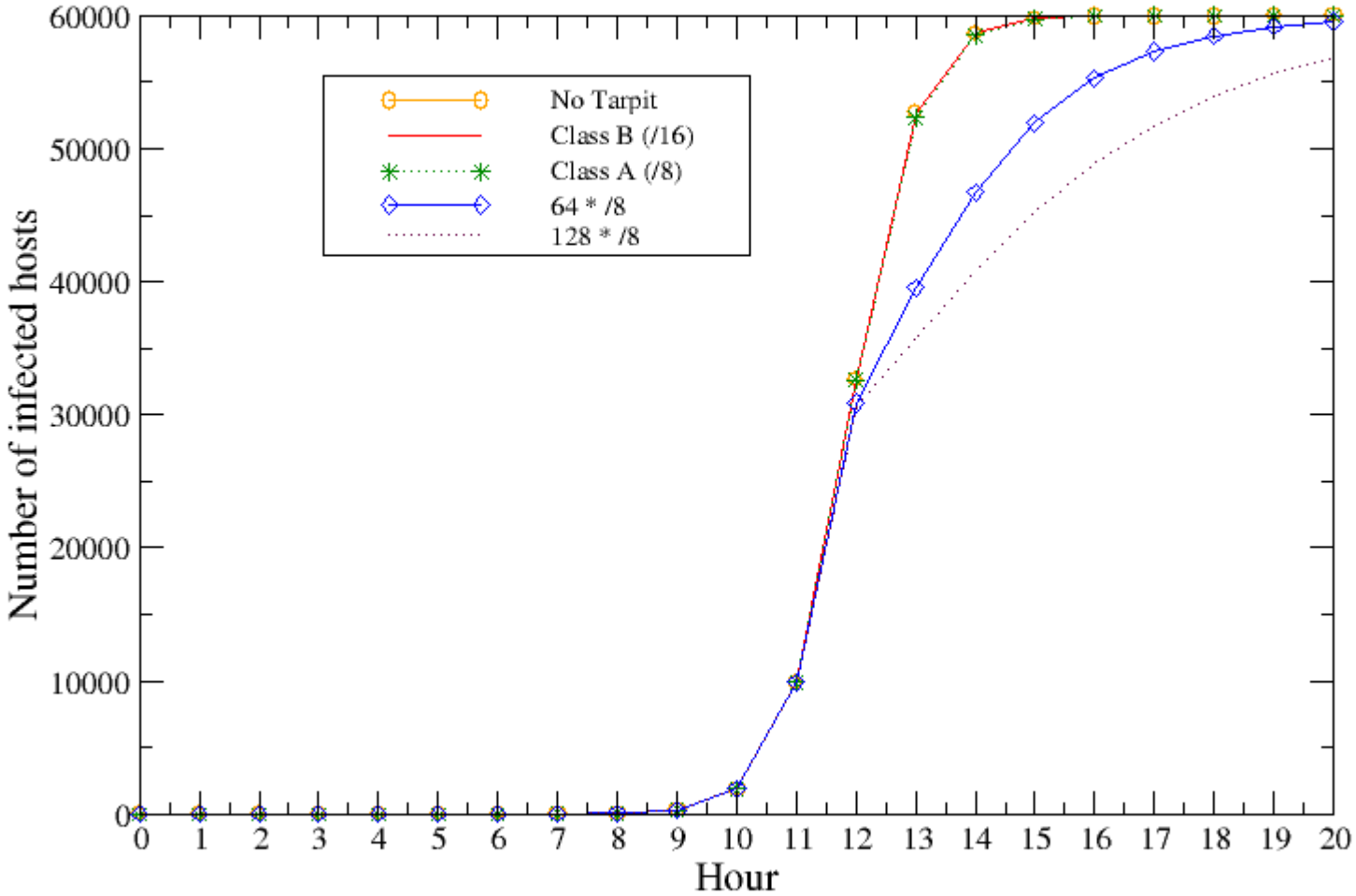
iSink Active Responses



iSink Tarpit Effectiveness



iSink Tarpit Effectiveness



iSink Results

- Our iSinks are a novel application of the Click modular router and argus flow-based measurement tool.
- iSinks based on commodity PCs can handle ~20,000 connection attempts per second, well over the average amount of unsolicited traffic received by an "unused" class A network.
- Packet sampling can be used to effectively produce a list of the "top talker" sources.

iSink Discussion

- How stealthy must an iSink be to get valid results? Is the iSink vulnerable to obfuscation?
- Legal Issues?
- What about IPv6?
  - much larger, much more sparsely populated space
- Enhance the global BGP to supported advertising short-cut routes to deliver unwanted traffic to iSinks? (eg. Barry Greene on advertising dark IP)
- Can Internet appliances and middleboxes act as a sink for unused transport endpoints? (eg. a tarpitting PAT router)

iSink Future Work

- Expand monitoring to other networks
  - Are our results portable to other prefixes?
- Add NIDS-like signature recognition and alert capability
- Explore the efficacy of packet sampling
  - Can packet-sampling iSinks detect rare events?