



M O S E S

M o d e l i n g O f S E c u r i t y a n d S y s t e m s

Multiscale Modeling and Simulation of Worm Effects on the Internet Routing Infrastructure

David M. Nicol

Michael Liljenstam

Jason Liu

Coordinated Science Laboratory

University of Illinois at Urbana-Champaign

First Things First : The Global Internet

The Global Internet is a confederation of *Autonomous Systems*

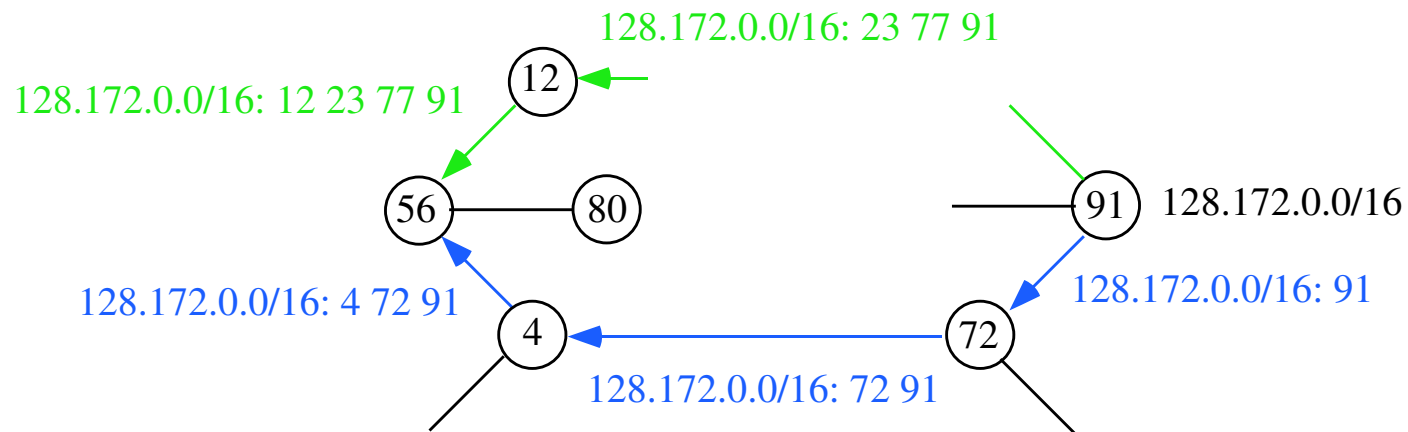
- e.g. AT&T, Sprint, WorldComm, ...
- Traffic is routed within an AS any way the owner pleases

Global connectivity achieved through agreements to *share traffic*

- the *Border Gateway Protocol* is the inter-AS protocol used by all
- Traffic between ASes pass through *BGP speakers*

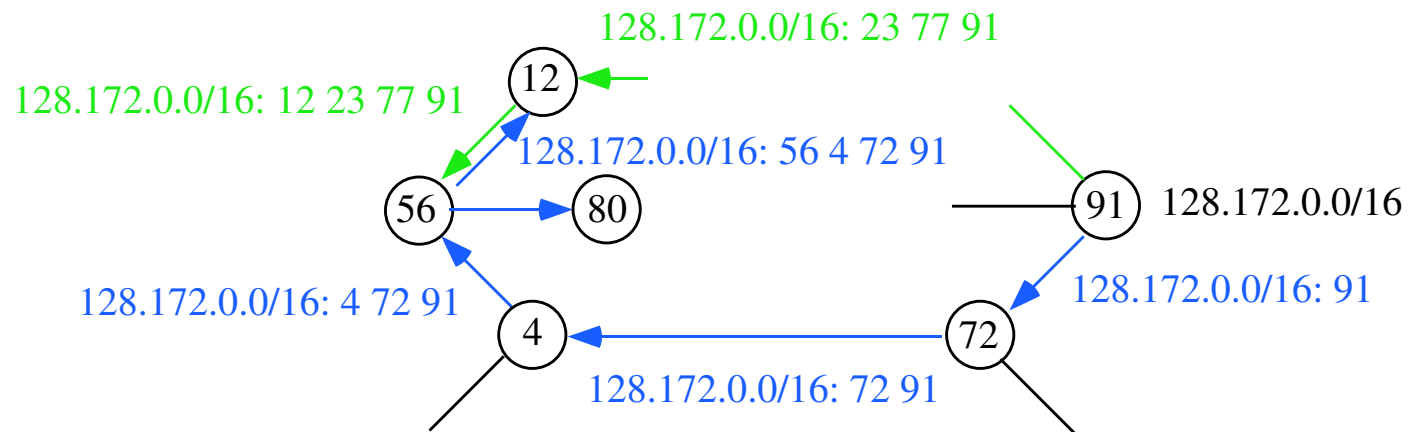
BGP Primer

- Each BGP speaker in principle can route to every *advertised prefix* (destination)
- Each speaker *advertises* to its *peers* the entire AS route it intends, for every advertised prefix it sees
 - A speaker chooses a route as a function of routes advertised to it, by its peers



BGP Primer

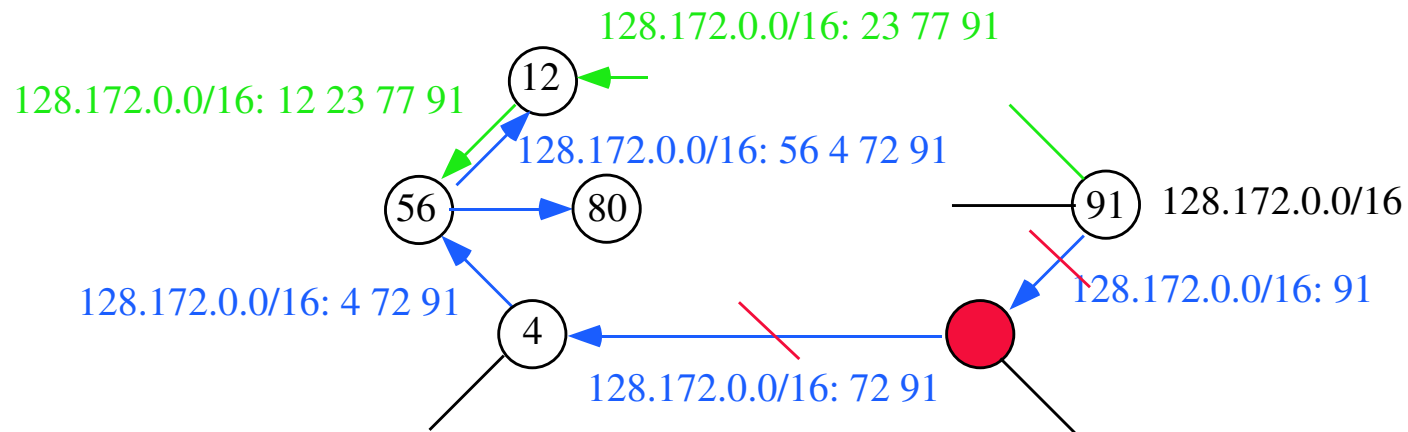
- Each BGP speaker in principle can route to every *advertised prefix* (destination)
- Each speaker *advertises* to its *peers* the entire AS route it intends, for every advertised prefix it sees
 - A speaker chooses a route as a function of routes advertised to it, by its peers



BGP Announcements

Every announcement is rooted in a session state change

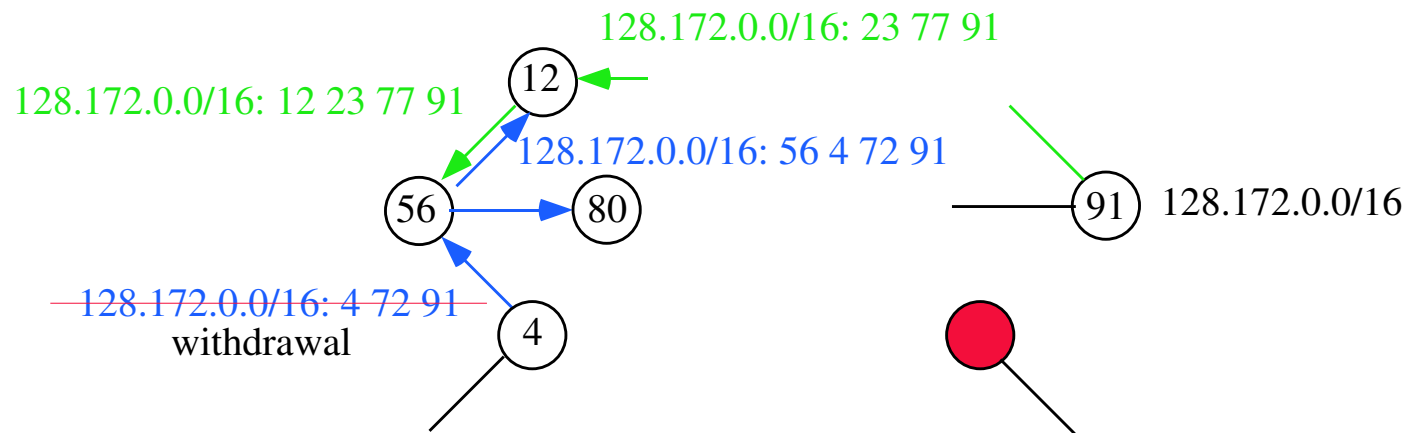
- a router reboots, and announces all prefixes owned by its AS
- a previously existing session times out



BGP Announcements

Every announcement is rooted in a session state change

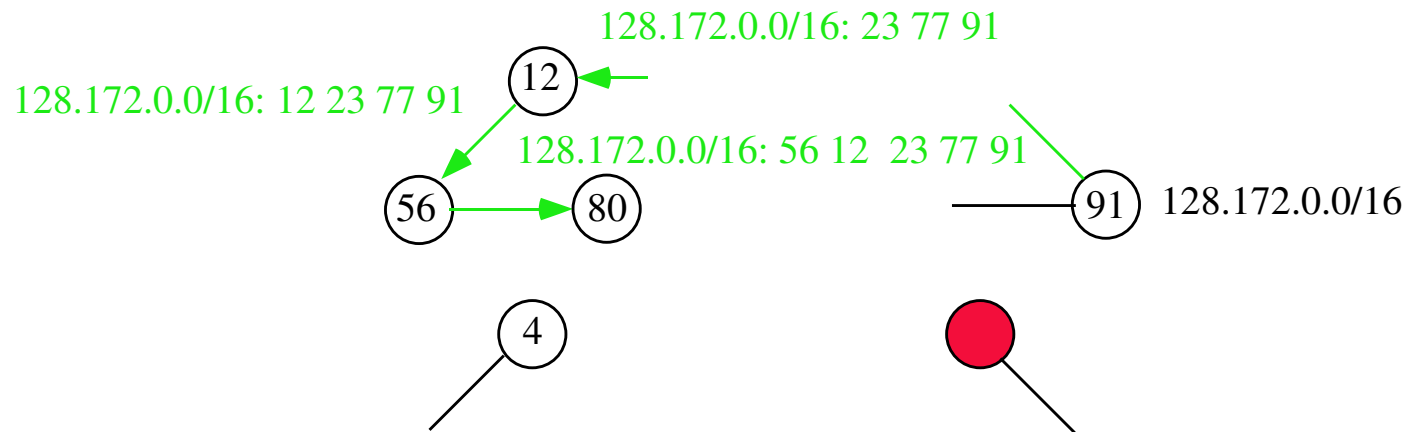
- a router reboots, and announces all prefixes owned by its AS
- a previously existing session times out



BGP Announcements

Every announcement is rooted in a session state change

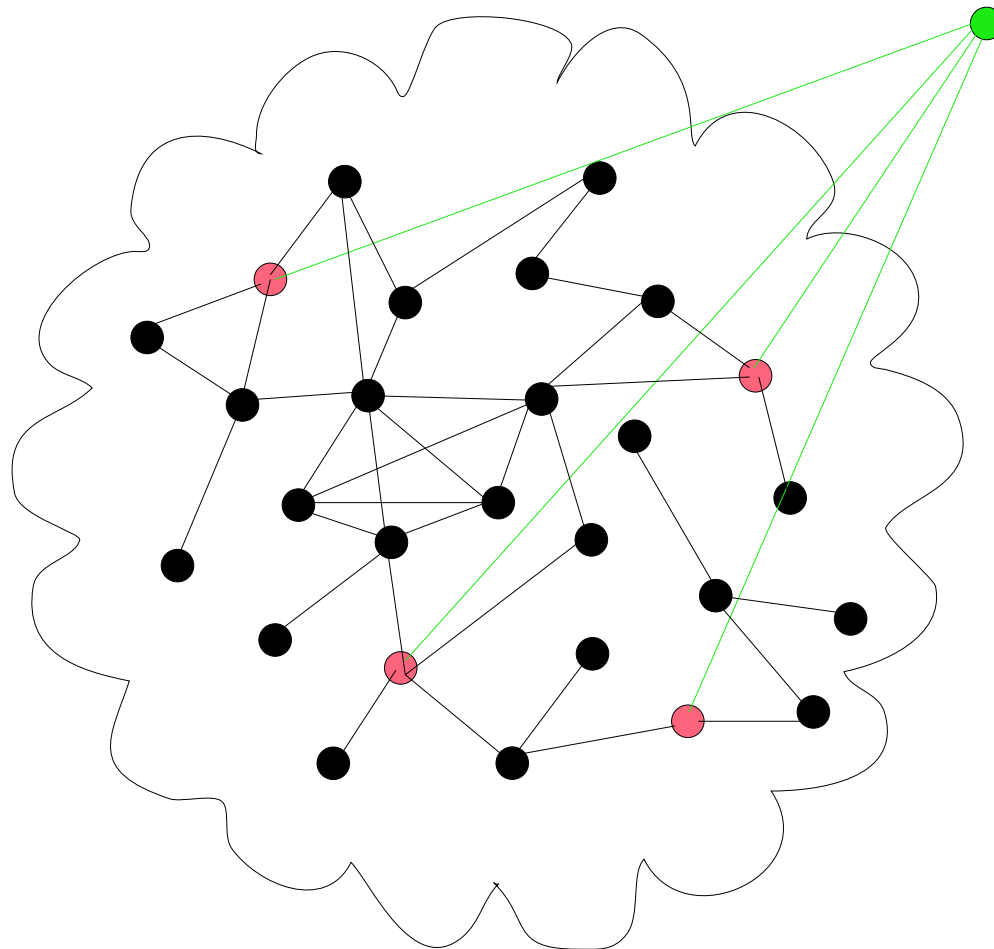
- a router reboots, and announces all prefixes owned by its AS
- a previously existing session times out



Global View of BGP Behavior

Monitor speakers peer with working speakers throughout the Internet

- A monitor gets a global perspective on activity



The World of Worms

A *worm* is malware that, without human interaction, propagates copies of itself to vulnerable hosts

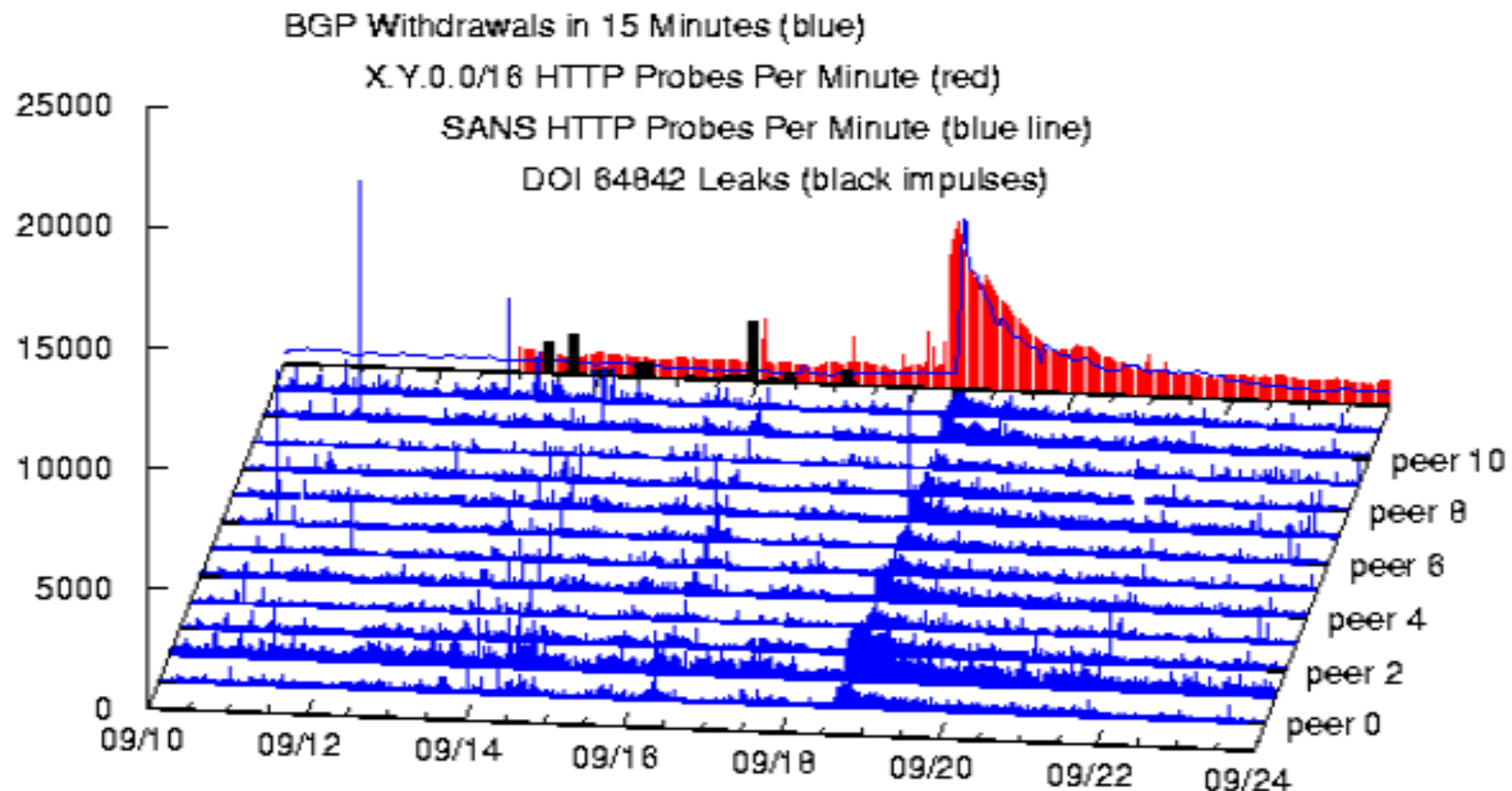
- e.g. Morris worm (1988), Code Red (2001), nimble (2001), Slammer (2003), Blaster (2003)

Common characteristics:

- Exploits vulnerabilities that allow executable access
- Executing worm uses multiple threads to *scan* the Internet for other infectable hosts
 - A scan probe typically is a packet or connection attempt with a randomly chosen target

Worms and Routing

In 2001 colleagues at Renesys noticed interesting correlations between announcement intensity and Code Red II and nimbda worm scans (graph courtesy of Renesys Corporation)



So What?

- Higher rates of BGP announcements—especially withdrawals—signal instability
- Withdrawals signal disconnectivity
- Disconnectivity causes lack of functionality

An increasing amount of economic activity depends on Internet availability

The Questions

How does scan traffic affect BGP speakers?

- Fast movers (e.g. Slammer) traffic overwhelm bottlenecks in routing infrastructure

The Questions

How does scan traffic affect BGP speakers?

- Fast movers (e.g. Slammer) traffic overwhelm bottlenecks in routing infrastructure
- The issue was more subtle with Code Red and nimba—it was not traffic volume
- Principle suspected causes
 - (outgoing) Prefix-to port caching
 - (incoming) probe destination **prefix** is legitimate, but address is not. Forces Address Resolution Protocol (ARP) action

The Questions

How does scan traffic affect BGP speakers?

- Fast movers (e.g. Slammer) traffic overwhelm bottlenecks in routing infrastructure
- The issue was more subtle with Code Red and nimba—it was not traffic volume
- Principle suspected causes
 - (outgoing) Prefix-to port caching
 - (incoming) probe destination **prefix** is legitimate, but address is not. Forces Address Resolution Protocol (ARP) action

What impact on Internet functionality?

The Modeling Challenge

Model, simulate, and validate

- the spread of worms on large-scale networks
- the effects on BGP behaviour of worm traffic
- the effects of BGP instability on
 - global network connectivity
 - critical application traffic

The Multiscale Challenge

Critical phenomena occur at *different time scales*

- packet transit in μ -secs
- Worm propagation in seconds (slow)
- BGP dynamics in minutes

and at *different spatial resolutions*

- per-thread per-host worm behavior
- router dynamics (packet and BGP)
- worm impact on LANs
- AS infection behavior
- Internet-scale infection behavior

Modeling Worm Spread

Look to macroscopic epidemiological models

$\{s(t), i(t), r(t)\}$ # {susceptible,infected,removed} at time t

β pairwise infection rate

γ removal rate

$$\frac{ds(t)}{dt} = -\beta s(t)i(t)$$

$$\frac{di(t)}{dt} = \beta s(t)i(t) - \gamma i(t)$$

$$\frac{dr(t)}{dt} = \gamma i(t)$$

Time-stepped solution very efficient

Problems with Epidemiological Models

Basic assumptions of

- Homogeneous population
- “equal access probability” between any infected/uninfected pair
- Deterministic model smooths over high variance in early stages of propagation

Two solution approaches

- Spatial decomposition, with lags
- Stochastic sampling

Discrete Model

$p_{hit} = 2^{-32} p_{inft}$	ρ per worm scan rate
Δt coarse time-step	$X_t \text{ Binomial}(s(t), p_{hit}i(t)\rho\Delta t)$
$Y_t \text{ Binomial}(i(t), p_{rem})$	

$$s(t + \Delta t) = s(t) - X_t$$

$$i(t + \Delta t) = i(t) - X_t - Y_t$$

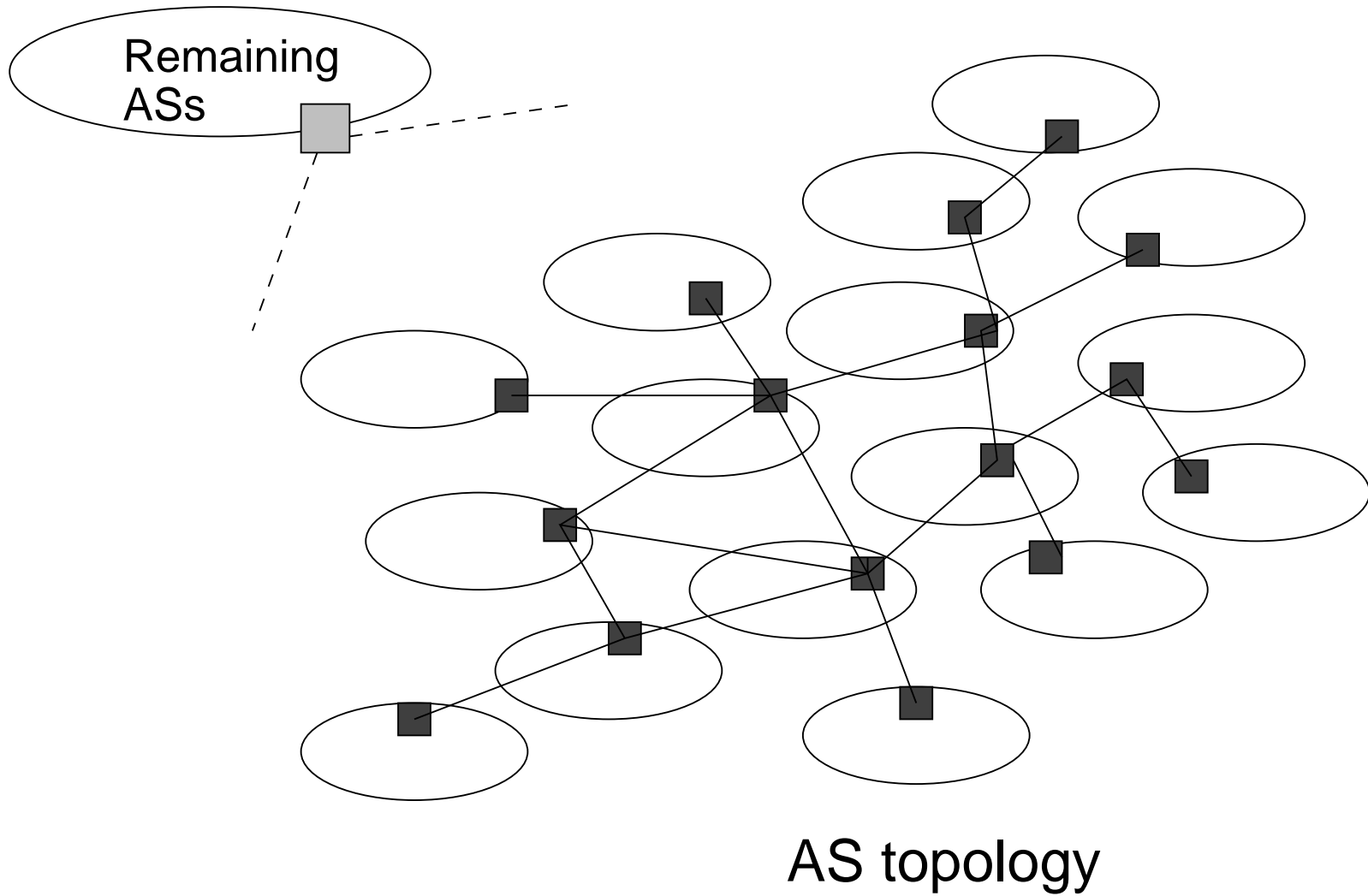
$$r(t + \Delta t) = r(t)Y_t$$

Note that

$$E[X_t] = s(t)i(t) p_{hit}\rho\Delta t$$

deterministic model reflects average behavior

Spatial Decomposition



Epidemiological Spatial Decomposition

- model each AS separately to better capture worm traffic at AS level

$$\frac{ds_j(t)}{dt} = -s_j(t) \left(\sum_k \beta_{kj} i_k(t - d_{kj}) \right)$$

$$\frac{di_j(t)}{dt} = s_j(t) \left(\sum_k \beta_{kj} i_k(t - d_{kj}) \right) - \gamma_j i_j(t)$$

$$\frac{dr(t)}{dt} = \gamma_j i_j(t)$$

Estimation of β_{kj} based on uniform scan model

$$\beta_{kj} = \beta_j = \beta \frac{ip(A_j)}{ip_{total}}$$

Discrete Spatial Sampling

AS_j scan generation rate $\rho_j^{gen} = i_j(t)\rho$

AS_j targeted scan rate $\rho_j^{dest} = i(t)\rho \frac{ip(A_j)}{2^{32}}$

egress scans $\rho_j^{egr}(t) = \rho_j^{gen}(t) \left(1 - \frac{ip(A_j)}{2^{32}}\right)$

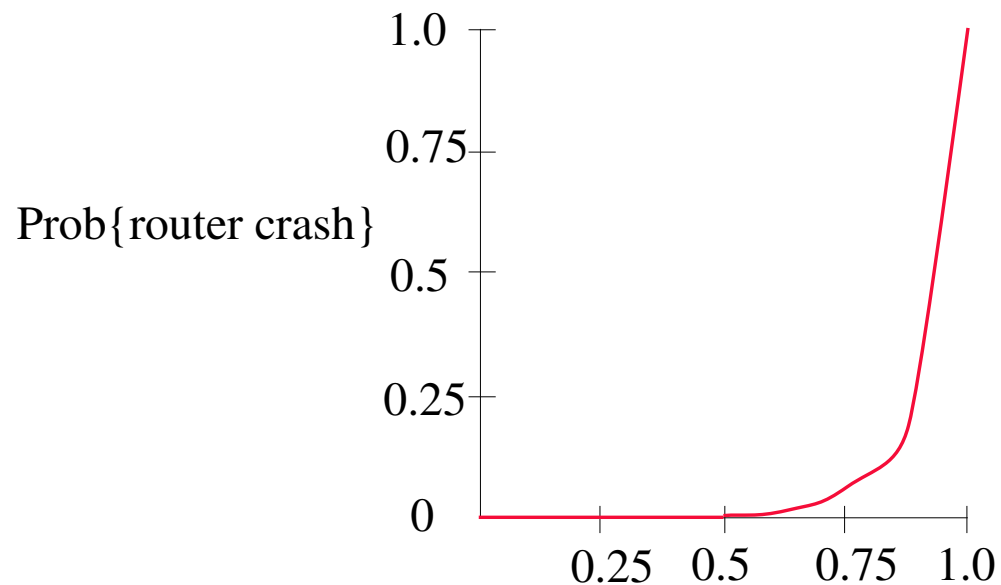
ingress scans $\rho_j^{ingrs}(t) = \rho_j^{dest}(t) - \rho_j^{gen}(t) \frac{ip(A_j)}{2^{32}}$

This is a simple model

- appropriate for Δt on the scale of lag time
- modification needed to handle selective disconnectivity

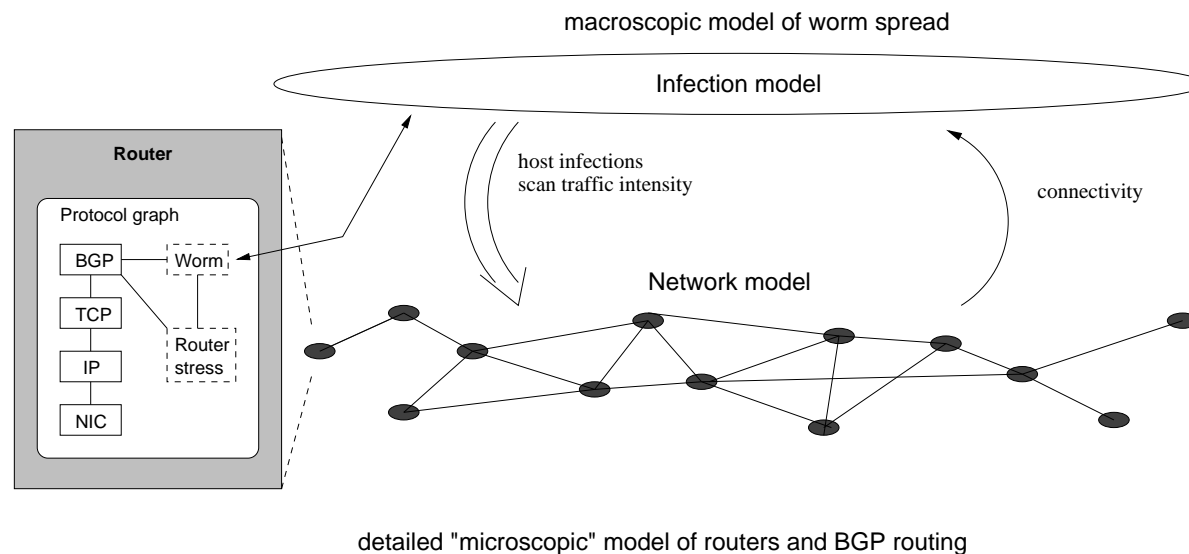
Router Stress Model

- Estimate router CPU & memory utilization as a function of exponentially weighted average scan traffic intensity (time-scale 10s)
- High {CPU,memory} utilization stresses routers
- Associate discrete hazard-rate functions of router failure with CPU and memory utilization



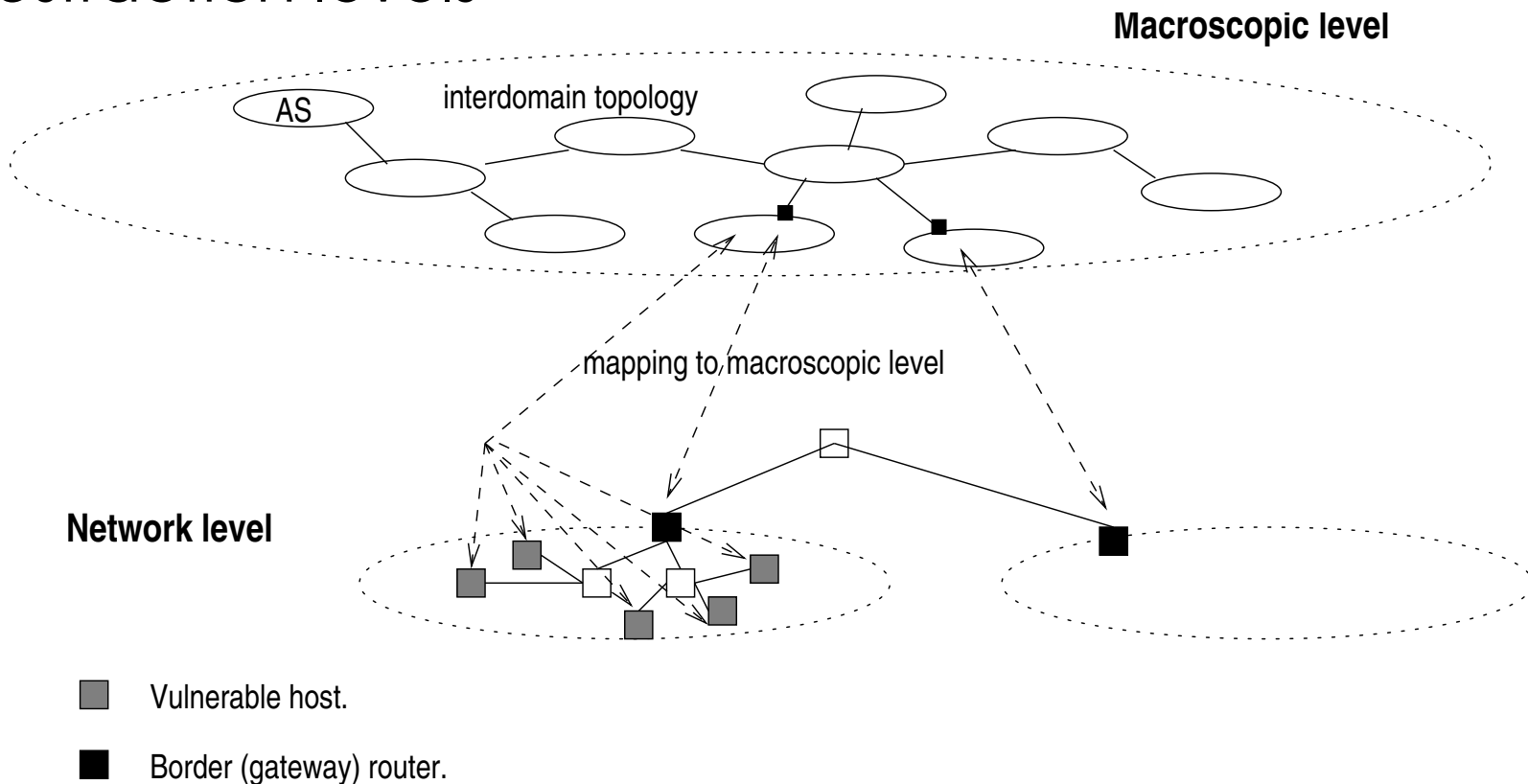
Integrating Routers

- Use outgoing and incoming scan traffic intensities in *stress model*
- Use highly detailed model of BGP protocol from SSFNet



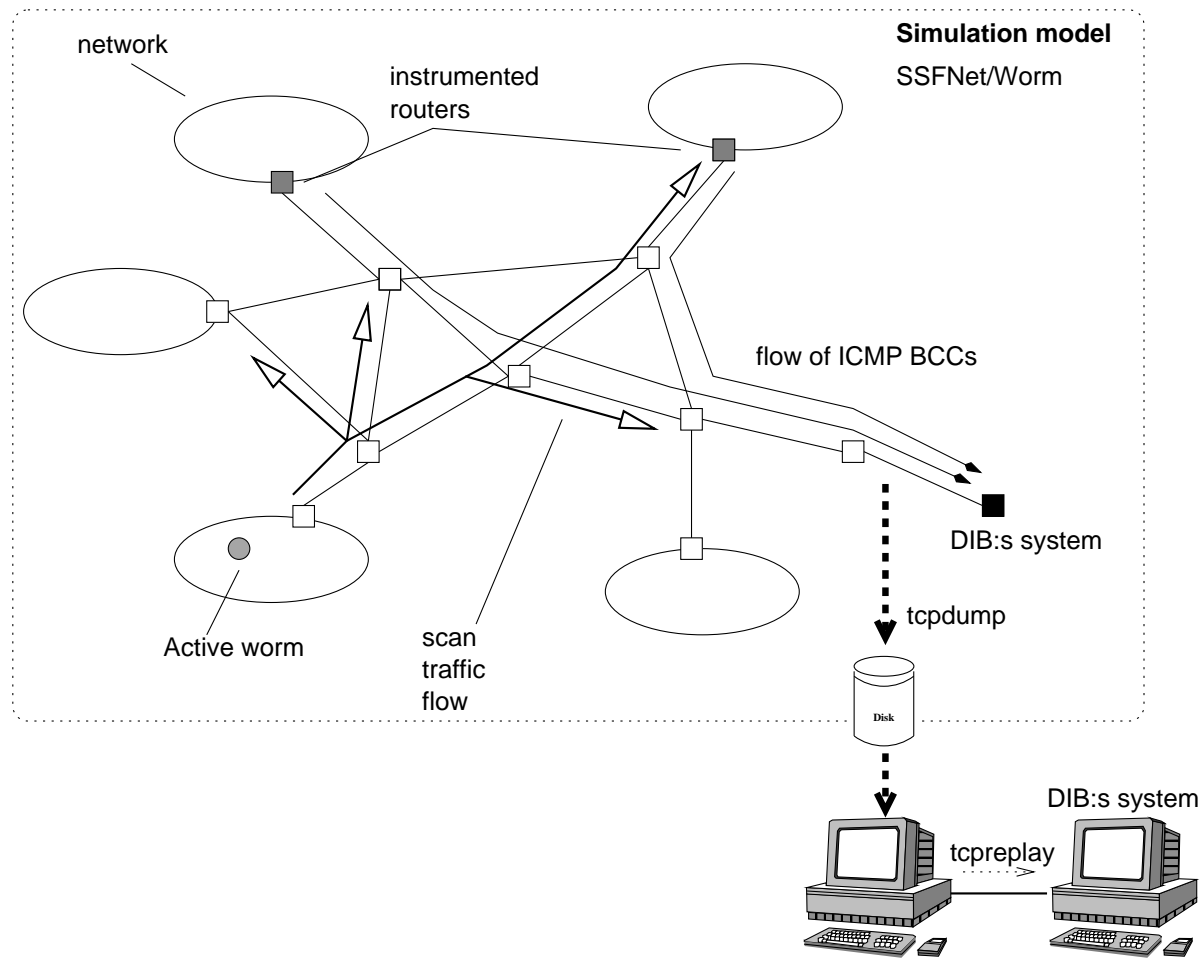
Integrating LANs

Effects of BGP connectivity changes and worm traffic on LANs are integrated through mapping between abstraction levels



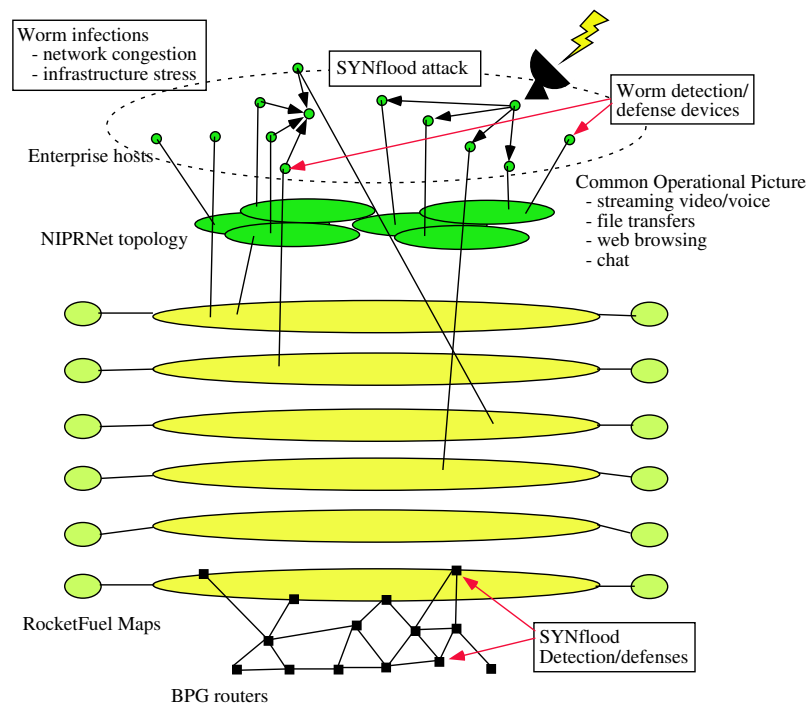
Testing Worm Detection

System is used to generate realistic worm traffic to test Internet monitoring system



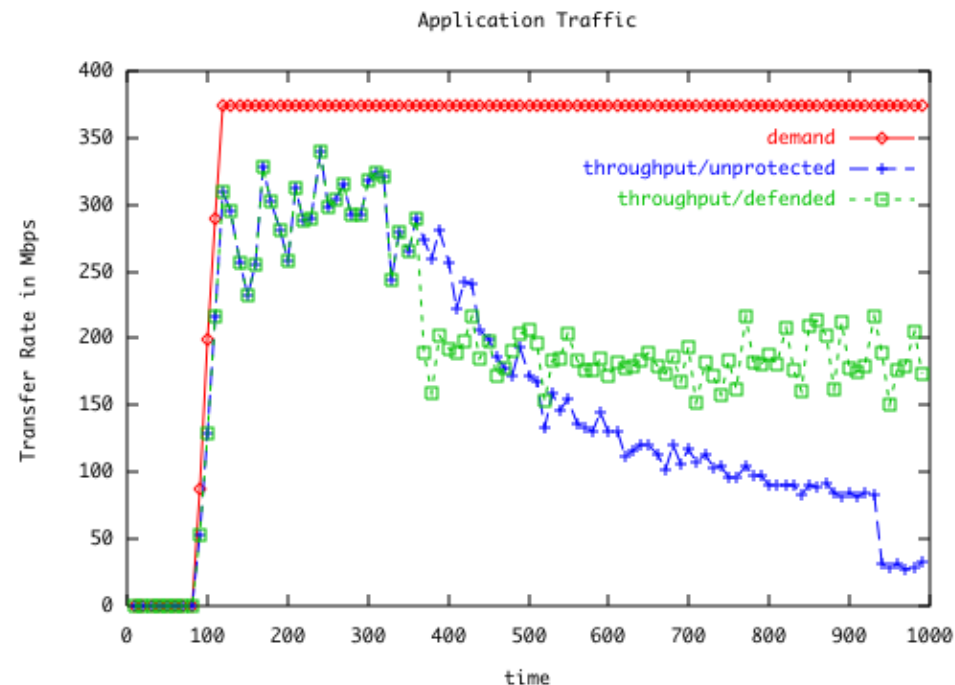
QoS Evaluation of COP Applications

- fast worm attack on large enterprise network (100K devices, 1k routers, 1M flows)
- evaluates connectivity/latency/throughput applications



QoS Evaluation of COP Applications

- fast worm attack on large enterprise network (100K devices, 1k routers, 1M flows)
- evaluates connectivity/latency/throughput applications



Conclusions

- Pressing issues in analysis of security of large-scale systems calls for modeling at vastly different spatial and time scales
- Powerful analysis tools can be—have been—constructed, using models with composite scales
- Outstanding challenges
 - validation/verification
 - memory demands of BGP modeling