



FRHACK 1st edition
Besançon, France
September 8th, 2009

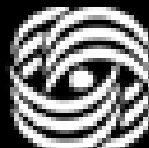
MASSIVE MALICIOUS ACTIVITIES

Insight via simulation

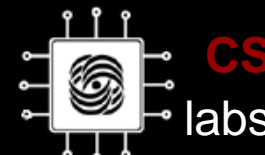
**Global
Network
Hybrid
Simulation**



**Moscow
State
University**



**Calc. Math &
Cybernetics
Department**



**CS
labs**



Some intro

- Alexei Kachalin
 - Moscow State University
 - Simulation: systems efficiency estimation
 - Security: networks and malware
- The project
 - Started in 2006 succeeding the research of malware outbreaks models
 - Team: students of network security seminar of CS labs/CMC dept.
 - Goal: useful simulation framework



Global Network Hybrid Simulation

Analysis of a network security systems operation impact on a network performance and malware, considering:

- Large-scale network
 - Countrywide network analysis
 - Worldwide network impact
- Security-related issues and impact
 - Malware population and it's behavior
 - Network performance effects
- Requirements to simulation
 - Computation feasibility
 - Simulation setup data availability



Massive malicious activities overview

■ Abuses

- Viral spreading: Network/mail worms
- Attacks: DoS/DDoS
- Malicious cooperation: Botnets
- Misc abuses: SPAM

■ Consequences

- Services/Defenses down
- Large-scale incidents
- Network infrastructure failure, network instability

AFFECTS
NETWORK
TRAFFIC



Questions to answer: Malware

- 0-day population
 - Number
 - Placement
- Spreading mechanisms
 - Target selection
 - Intensity
- Payload
 - Network activity type
 - Intensity



Network services

- Horsepower
 - Additional & backup servers
 - Alternative servers locations
- Anti-DoS service configuration
 - Restrictions/traffic drop policies
 - Switching to light (static/stateless) version
- Integrity violation and malware detection:
rate of scanning
- Patching delay



Questions: Network Security Systems

- Could be considered a network service
- Traffic collection loss on high speed channels – could it be tolerated
- Delays and reaction speed – system productivity (algorithm complexity)
- Memory demands – statefull or stateless?
- Analysis errors – acceptable or not?



Acting parties

- Malware
 - Spreading
 - Performing attacks/misuse
- Network Services
 - Provides content
 - Network Security Systems: Collecting & Analyzing, Filtering
- Network
 - Maintaining operation
 - Providing service

Framework purpose: getting insight into the processes relations



Models and simulation

■ Simulation

- Object abstraction
- Key characteristics and dependencies
- Assumptions and approximation

■ Simulation model complexity

- Object entities
- Events

“I should have tried it on
a simulator first.”
Robert Morris



Obstacles to overcome

- Calculation and memory complexity
 - Network hosts # 10^5 up to 10^8
 - Network traffic packets - sending and receiving simulation events # (for every network hop) \gg host #
- Getting too abstract to overcome the complexity
 - Network-behavior critical traffic
 - Network critical points

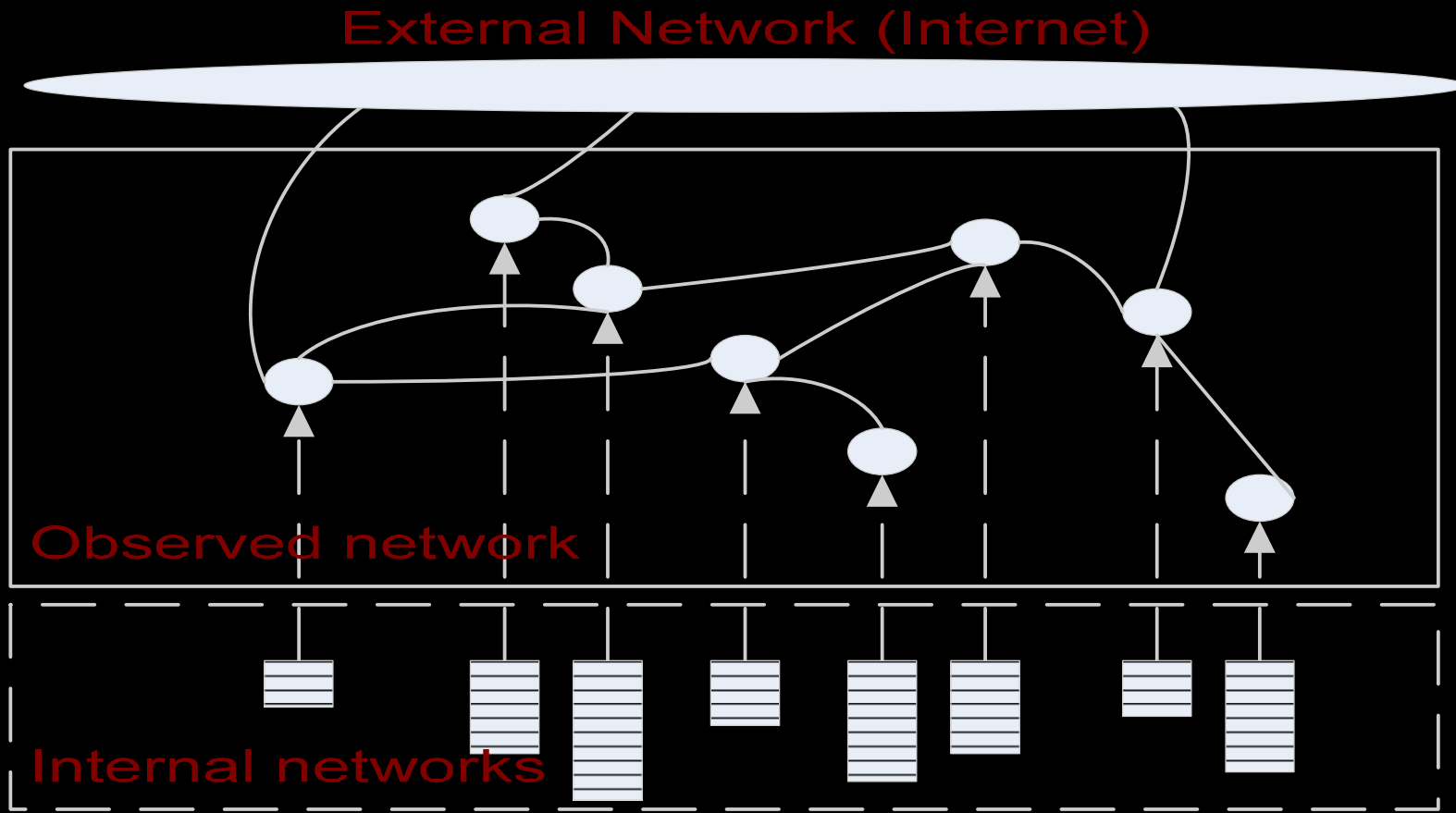


The path

- Use malware/attacks/security system experience
 - Types of malware/activities
- Focus on traffic loads
- Network representation abstraction levels
 - AS level – observed network segment with underlying internal networks models
 - External network segment
- Scenarios
 - Long-term (days, weeks)
 - Human reactions (i.e. patches distribution, network administration actions)



Network model:





Network sub-models (2): Internal network of AS

■ Properties

- Internal AS network: star or specified topology
- Domains (state vectors)
 - Domain hosts (ip address space, # active hosts, etc.)
 - Networking programs for domain (legitimate software, # active malware agents)

■ Provides

- Connection points to security systems models
- Outbound traffic for observed network



Network sub-models (3): external network – the rest of the world

■ Properties

- # hosts/IPs
- # malware agents
- Rate of legitimate traffic generation

■ Mechanisms

- Malware population growth model
 - Security systems could be included in this models
- Malware traffic calculation

■ Provides

- Traffic load for observed network model (both legitimate and malicious)

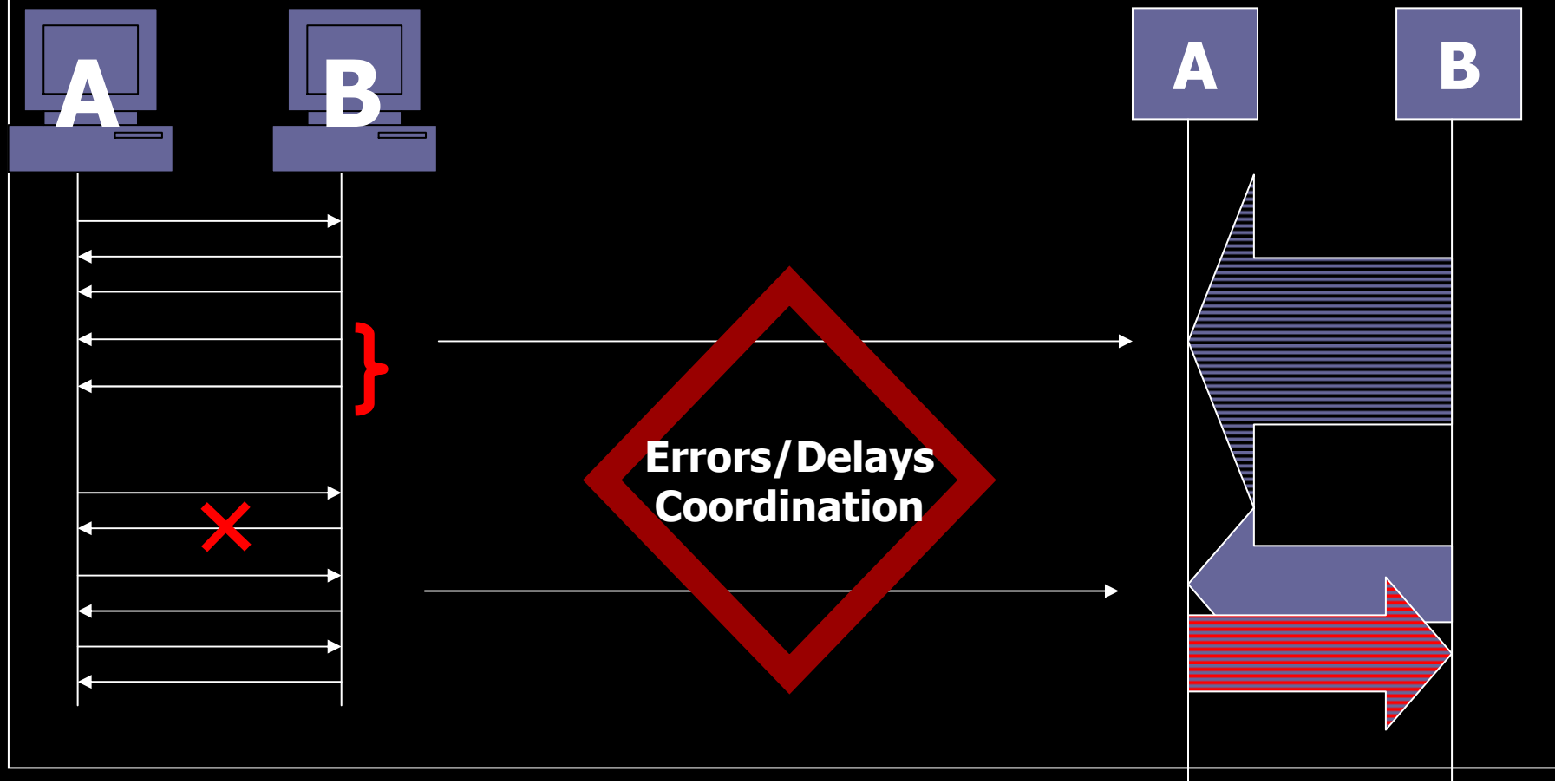


Traffic model summary

- Few levels of abstraction are present simultaneously
 - Traffic flow (traffic load - that is what matters)
 - Packet level simulation
- Technically
 - Time-stepped flow calculation
 - Traffic types (protocol + application)
 - Routing: weights to route flows to interfaces depending on traffic type
 - Routing updates: Interface weights are updated according to routing tables, services state, etc.

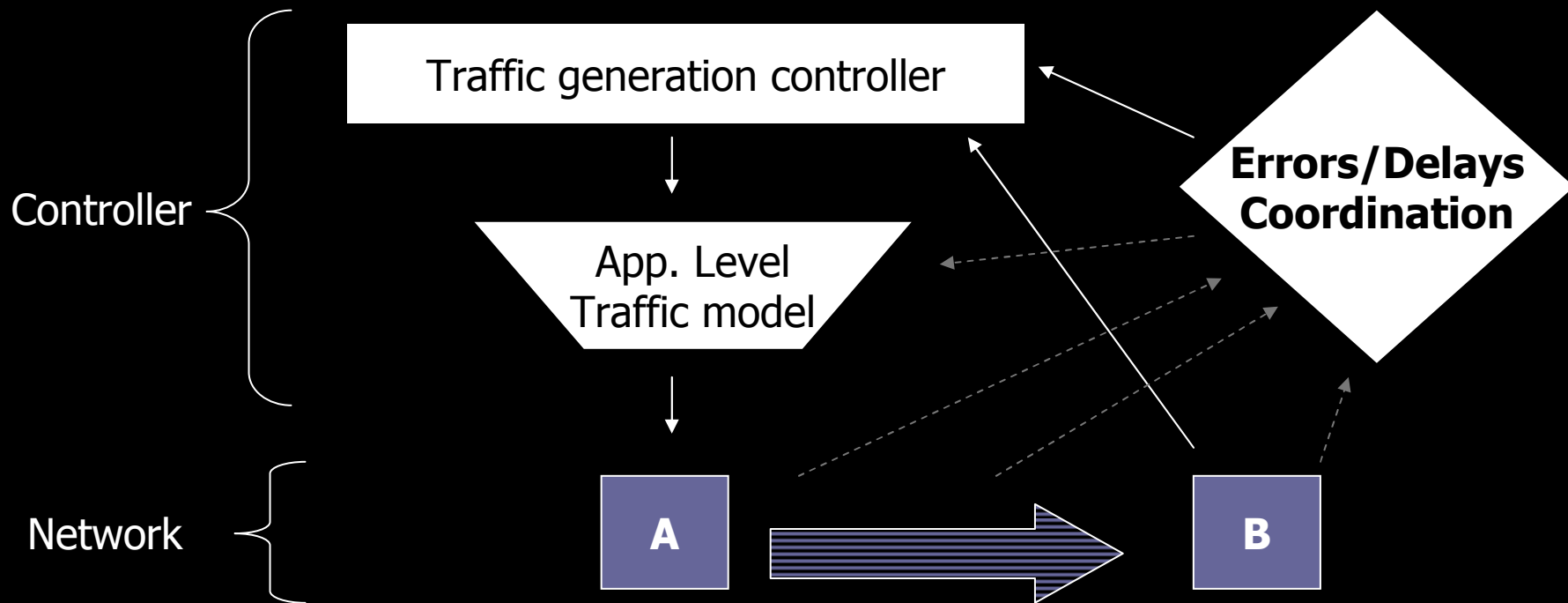


Getting above packets level: loss and delay coordination





Model controllers



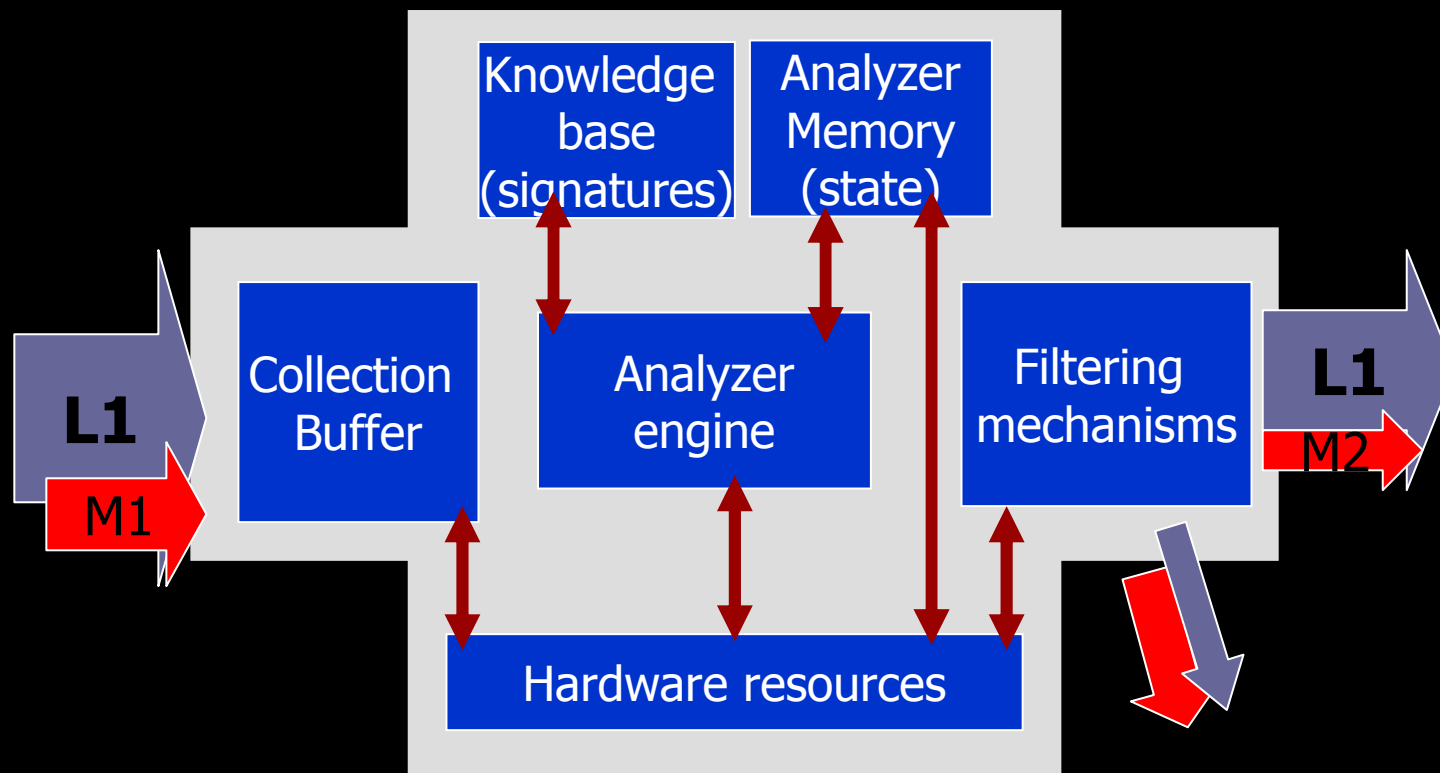


Malware 2-part model: malicious traffic generators

- MW.Ext
 - # of malware agents in external network
 - Malware population dynamics model
 - Malware traffic generation
- MW.Obs
 - Distribution and # of malware on domains
 - Malware traffic generation based on resources available
 - Infectious Ratio (Successful attempts/All attempts)
 - Targeting mechanisms
 - Untargeted/Multitargeted (spreading)
 - Targeted (DoS/DDoS)



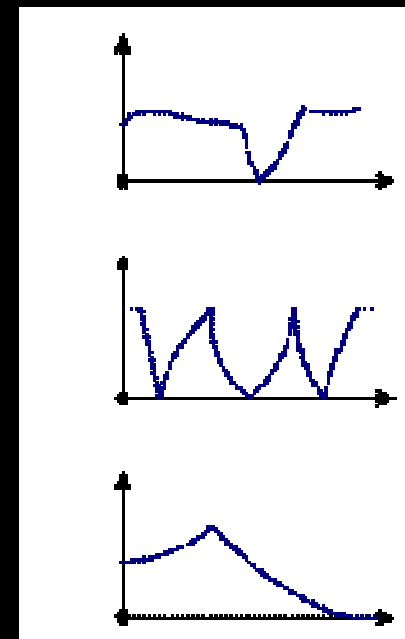
Network Security system model





Efficiency meltdown: it's never 100%

- Overload and hang-ups
- Downtime, upgrades, backups
- Correctness degradation: delay of updates, malware modification
- Multiply security systems
“cooperation” $1+1 < 2$:
 - Same knowledge, twice delay
 - Same true positives, different false positives



**Malfunction
profiles**

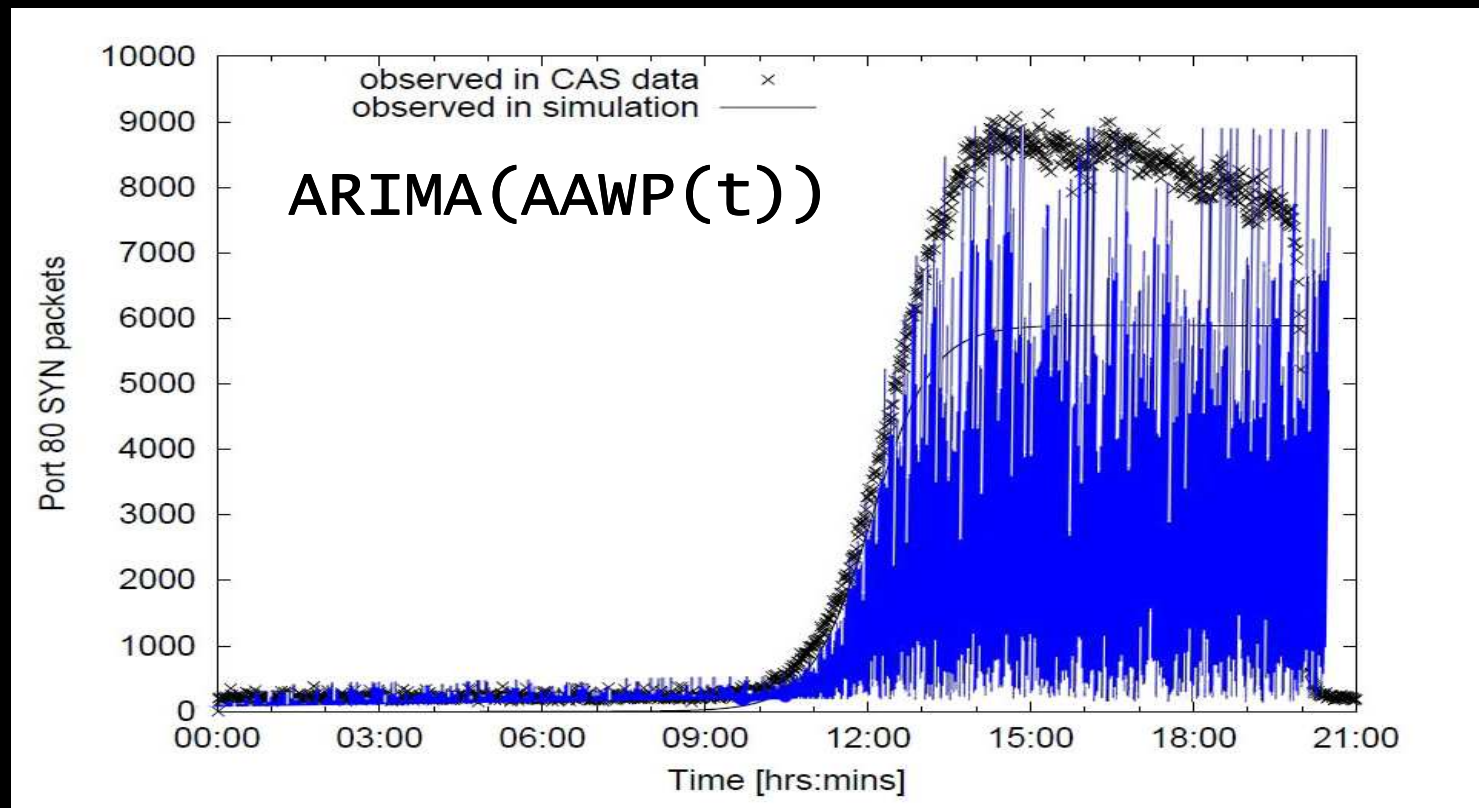


Efficiency metrics

Malware	Malware population dynamics $m(t)$ Malware traffic generation $T(m(t))$
Security systems performance and correctness	% of resources utilization, # of analyzed obj/sec, % of true positive, % true negatives
Security system (network point of view)	Reduce of malicious traffic Legitimate traffic loss (false positives) Traffic delays to perform analysis
Network performance	Traffic loss, delay, jitter % of active/disconnected hosts

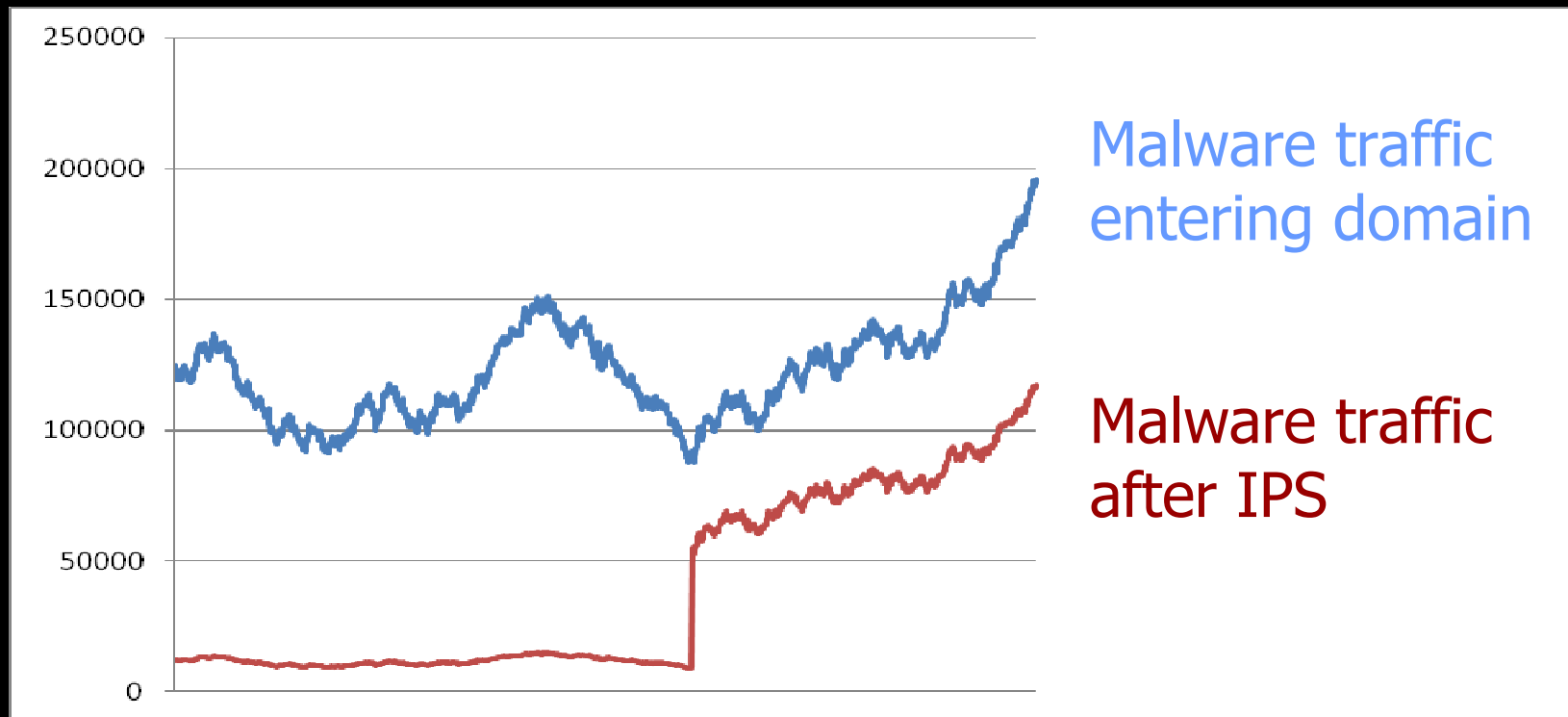


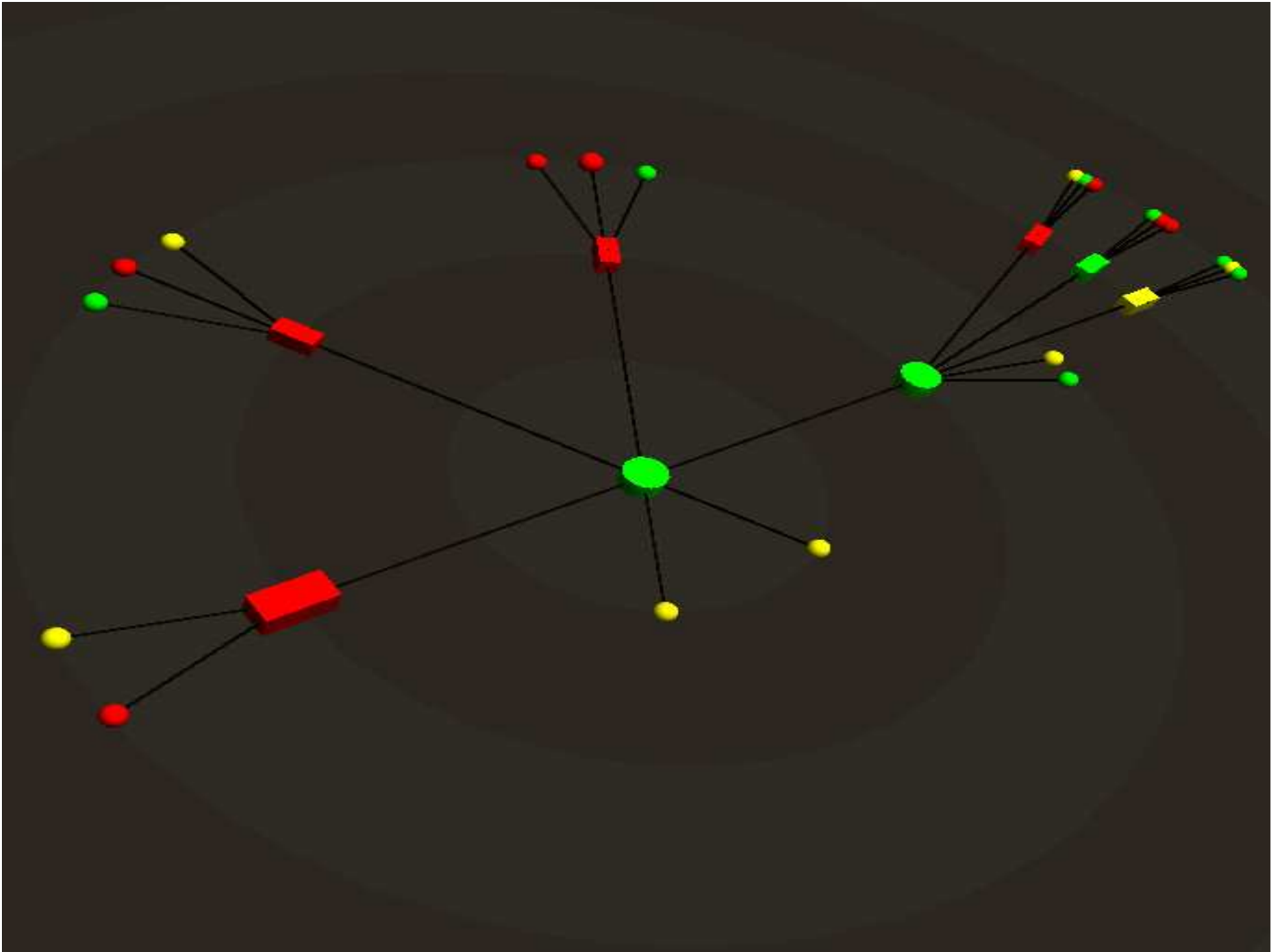
Simulation Example: External network Code Red malicious traffic

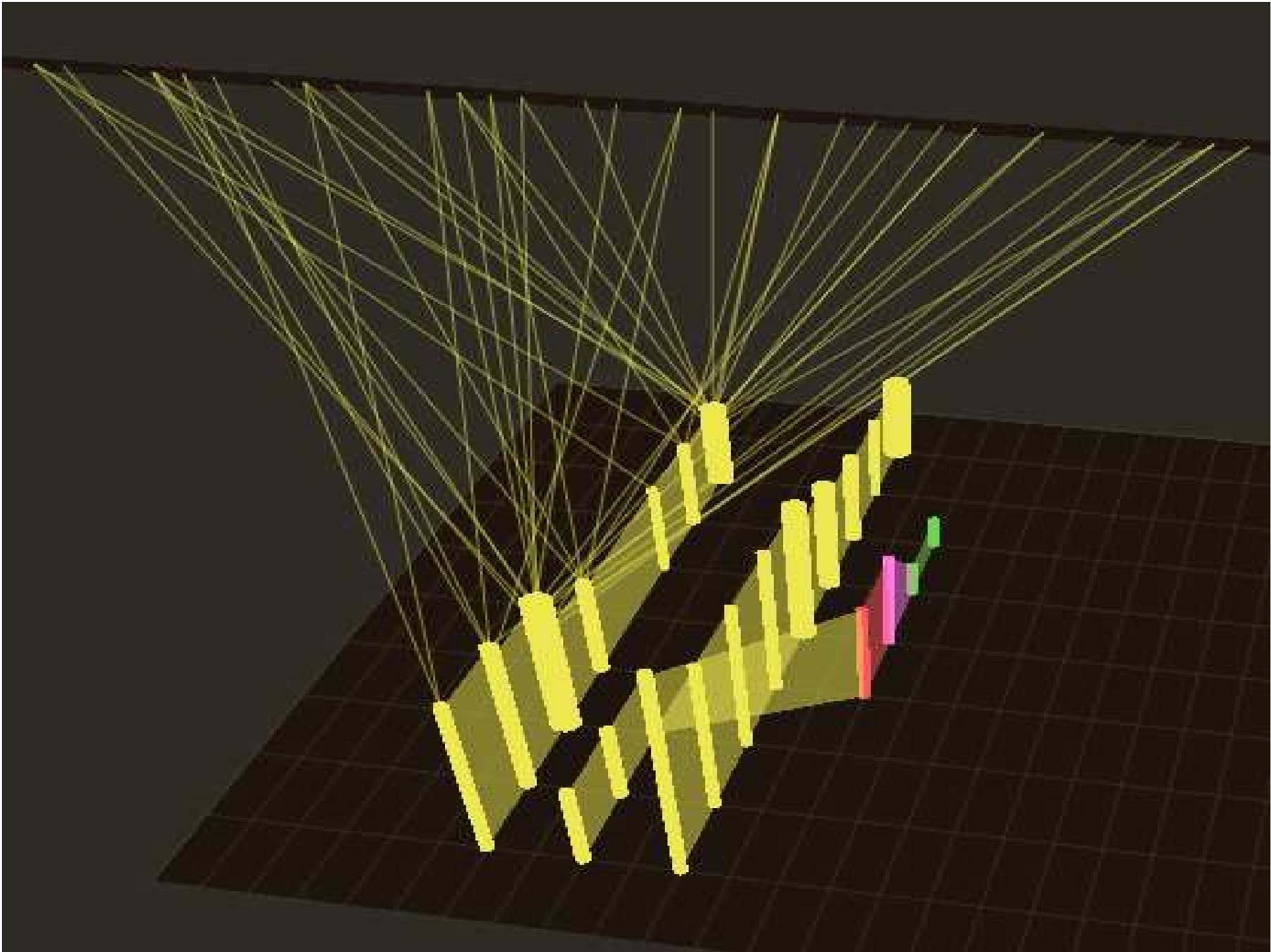




Simulation Example: Malfunction effects









GloNeHyS use cases

- Impact (positive/negative) vs. price analysis of security systems installation
- The way for innovative distributed security systems and procedures testing
- Network security systems on-site efficiency metrics development and measurement
- Network configuration stability and survivability analysis



Simulation scenarios

- Malware rampage
 - External network originated DDoS
 - Malware epidemics
- All your base...
 - Attacks on infrastructure (routing and routers)
 - Security efficiency decrease WCA due to being the subject of attack, zero-day malware etc.
- Wrong time, wrong place
 - Infrastructure down + malware activity



Plans

- Components integration – autumn 2009
- Releases
 - Testruns videos - december 2009
 - Public access to project's TRAC/git – 2010
- Discuss&Cooperation
 - Open to scenario ideas
 - Summer school – Moscow 2010



References/Keywords

- **Malware population dynamics models**

SI, SIS, SISD, Kermack–McKendrick, AAWP, PSIDR, Zou Gong two-factor worm model, CAIDA

- **Traffic flow generator models**

Wavelet traffic model, self-similarity traffic models, ARIMA, fractional brownian motion, SRD/LRD self similarity, PPBP, BMAP, MMPP, N-dMMPP, Arrowsmith/Barenco, Clegg/Dodson, PSST, Wang, On/Off process

- **Related research efforts and projects**

*NS-2, PRIME SSF, SSF.WORM, mixed abstraction level simulation, fluid traffic model, large scale network simulation, network survivability, **bonesi***



Questions?

Alexei «Sadman» Kachalin
a.kachalin@gmail.com

