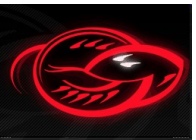
Moscow State University

Global Network Hybrid Simulation

GloNeHyS project

Efficiency Estimation of Network Security Systems of Global Networks

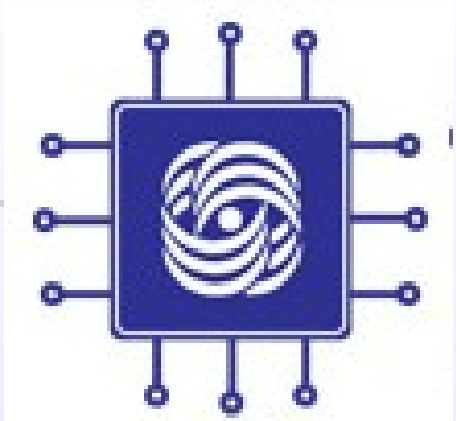
Alexei Kachalin



Confidence 2009, Krakow

GloNeHyS project

CS labs Research timeline



http://lvk.cs.msu.su

- 1980's Models and simulation – network protocols, schedules
  - 2000's Network security systems (IDS) architecture and algorithms development and benchmarking
    - 2005 Malware models and outbreaks simulation

Global network security systems efficiency estimation

Agenda

- Introduction
- Network and Traffic
- Malware and Security systems
- Making it work and getting results

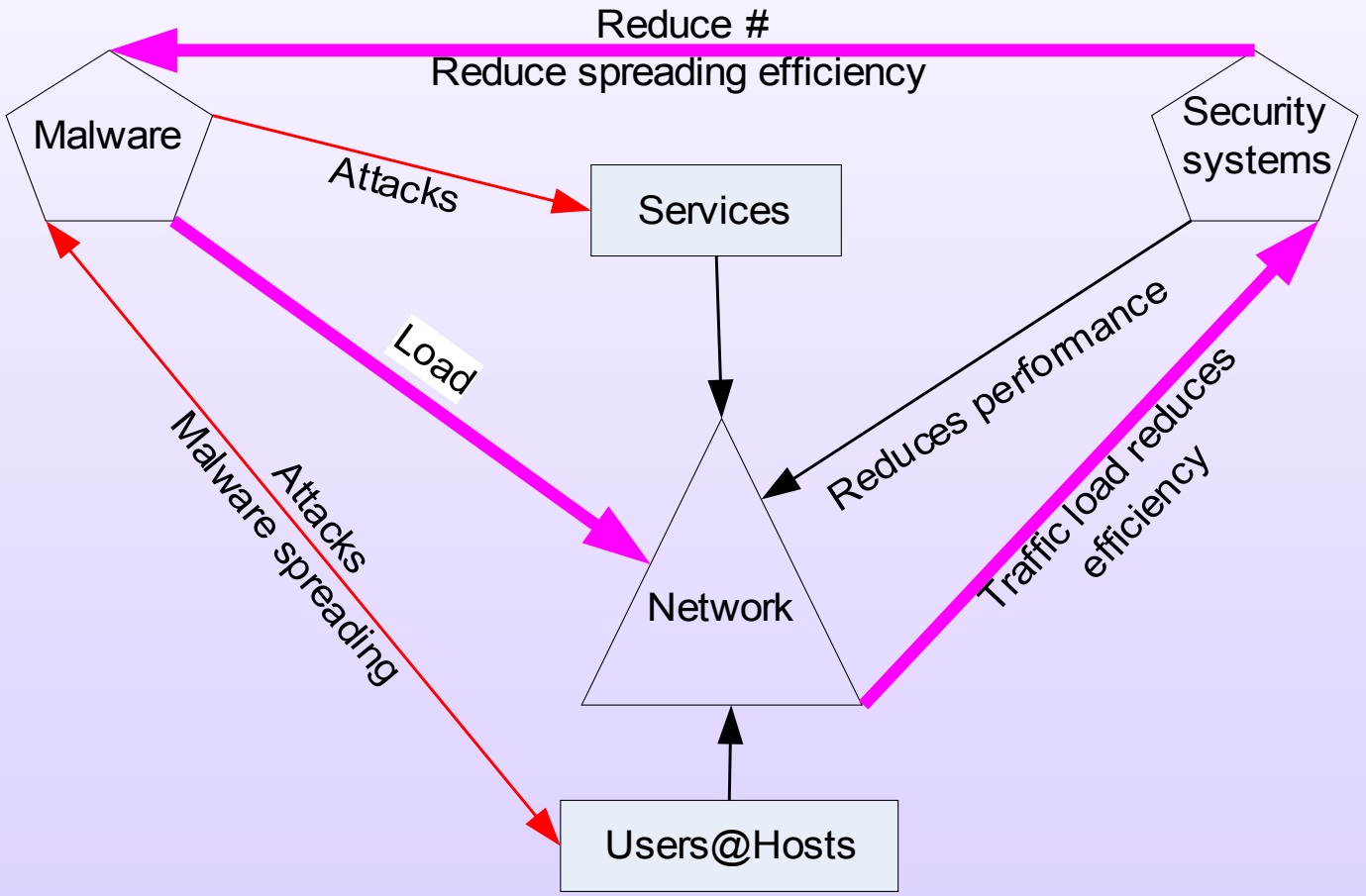
GloNeHyS project

What's this all about

- Network
  - Maintaining operation
  - Providing service
- Network Security Systems
  - Collecting
  - Analyzing
  - Filtering
- Malware
  - Performing attacks/misuse
  - Spreading

Getting insight into the problem by simulation

Dependencies are complex



Models and simulation

- Simulation
  - Object abstraction
  - Key characteristics and dependencies
  - Assumptions and approximation
- Simulation model complexity
  - Object entities
  - Events

GloNeHyS project

The Goal of Global Network Hybrid Simulation project

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
  - Network performance effects
- Requirements to simulation
  - Computation feasibility
  - Simulation setup data availability

GloNeHyS project

Disclaimer: few words about going straightforward

- Straightforward approach is good
  - Network=graph or its dynamics etc.
- Forward and backward compatibility
  - Model configuration identical to the object
  - Results are directly applicable to the object
- Programs are ready-to-use models already

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) >> host #
- Getting too abstract to overcome the complexity
  - Network-behavior critical traffic
  - Network critical points

GloNeHyS project

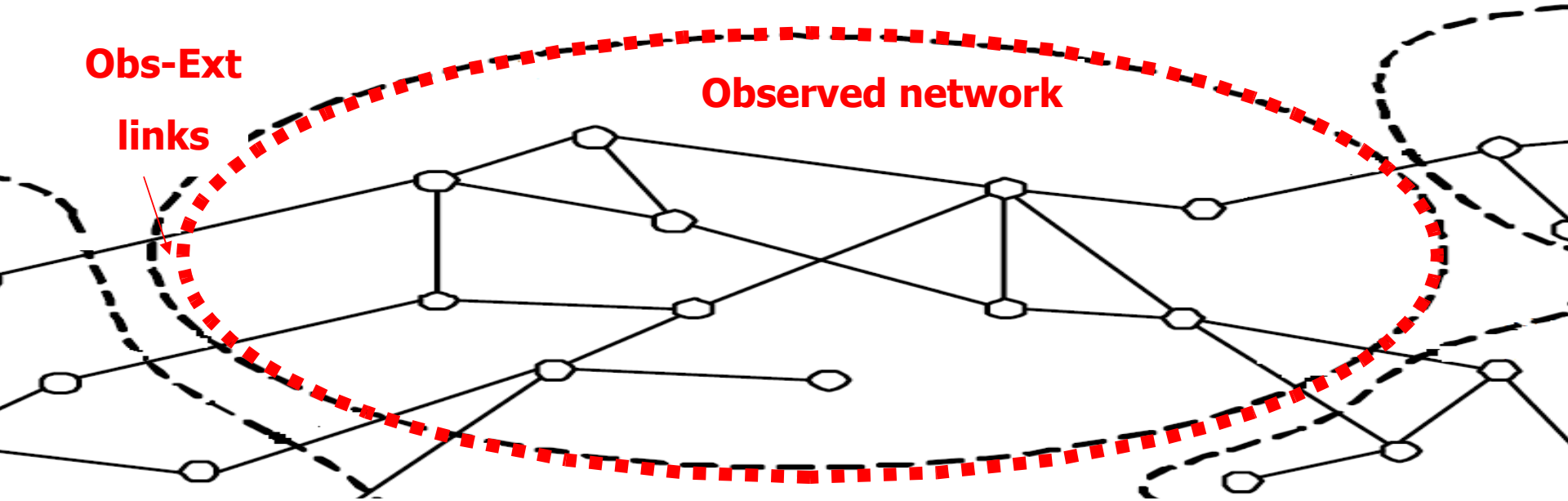
Agenda

- Introduction
- Network and Traffic
- Malware and Security systems
- Making it work and getting results

GloNeHyS project

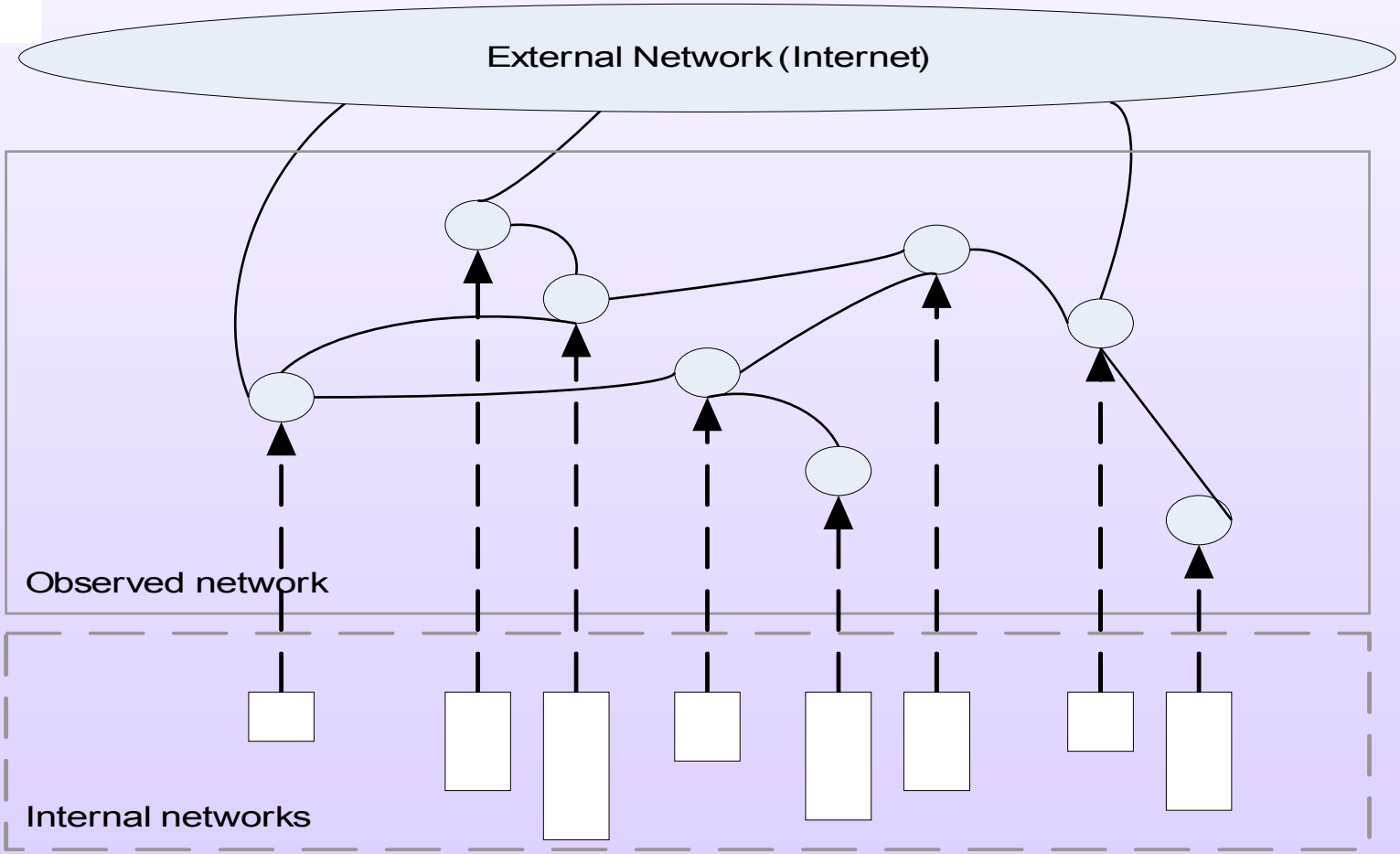
GloNeHyS network model overview (1)

- Divide network on Autonomous Systems level:
  - Observed network – simulation POI
  - External network - provides traffic load



GloNeHyS project

GloNeHyS network model overview (2)



GloNeHyS project

Network sub-models (1): Observed AS network

- Properties
  - Autonomous systems
  - Links between ASes
  - Links to external network
- Provides traffic handling
  - AS to AS traffic routing
  - AS2domains/domains2AS traffic splitter/summer

GloNeHyS project

Network sub-models (2): Internal AS network

- 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

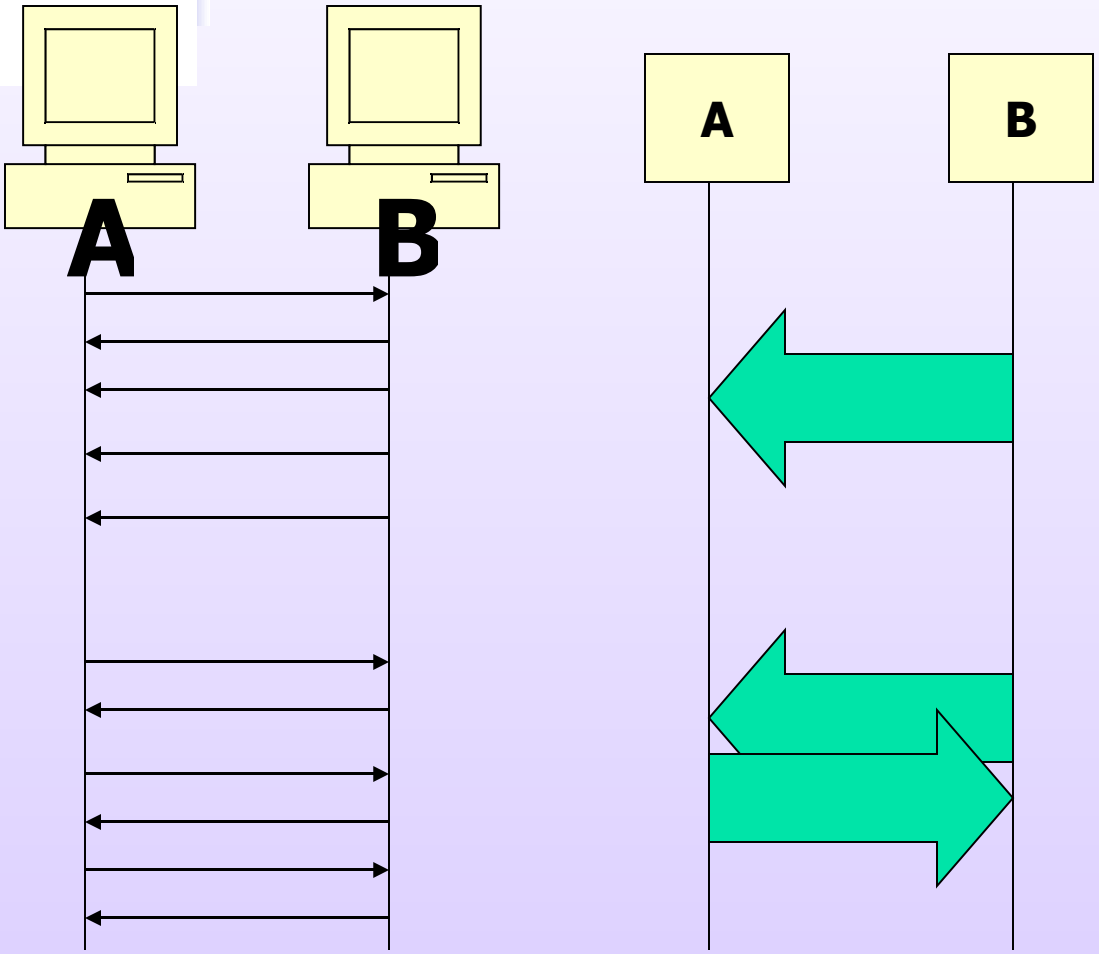
- Properties
  - # hosts/IPs
  - # malware agents
  - Rate of legitimate traffic generation
- Mechanisms
  - Malware population growth model
    - Security systems could be included in this models
  - Malware traffic calculation
- Provides
  - Traffic load for observed network model (both legitimate and malicious)

Traffic model: Network traffic abstraction levels

Abstraction level/ Network size	Packet level	Session/Traffic flows	System dynamics (analytical model)
LAN	+	+	Unstable
WAN	Massive distributed simulation	+	+
Global (Internet)	Computationally Infeasible	Massive distributed simulation	+

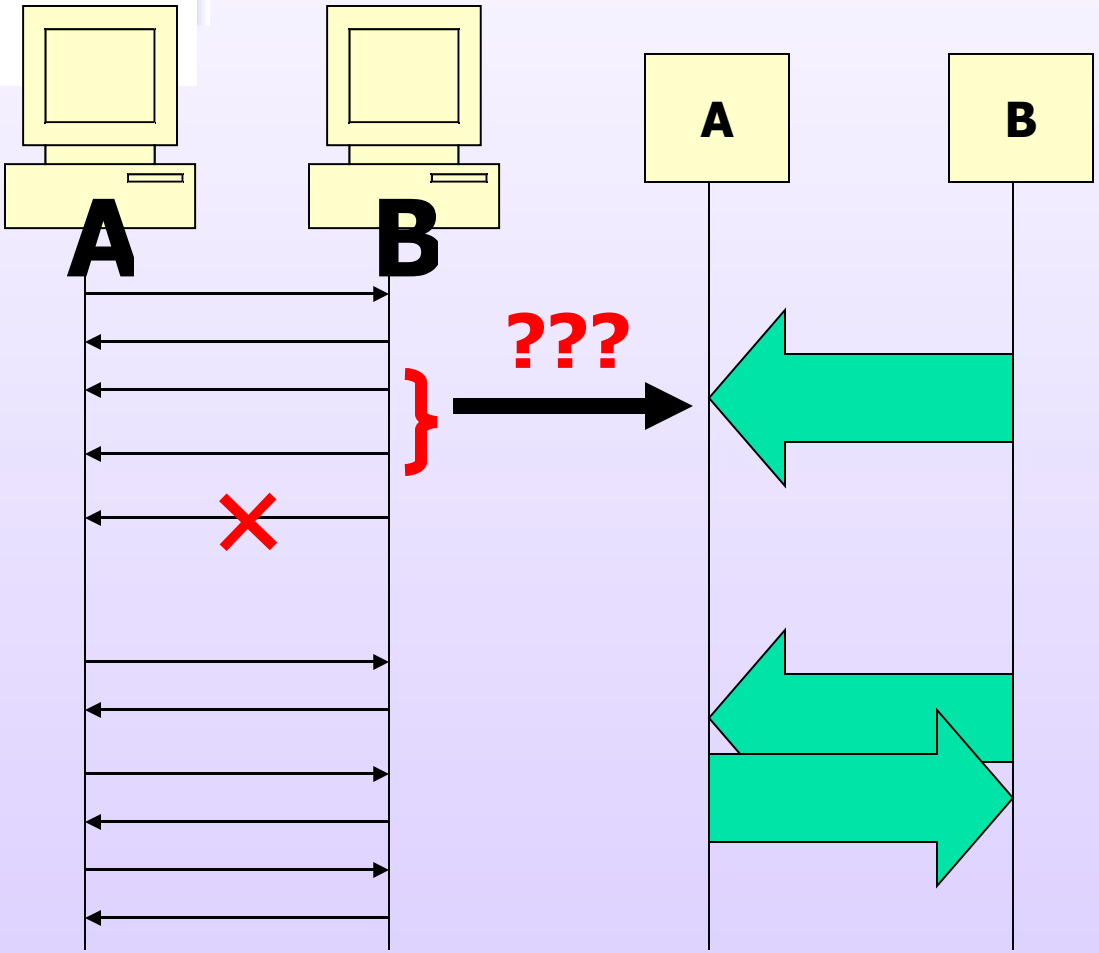
GloNeHyS project

Getting simulation above packets level (1)



GloNeHyS project

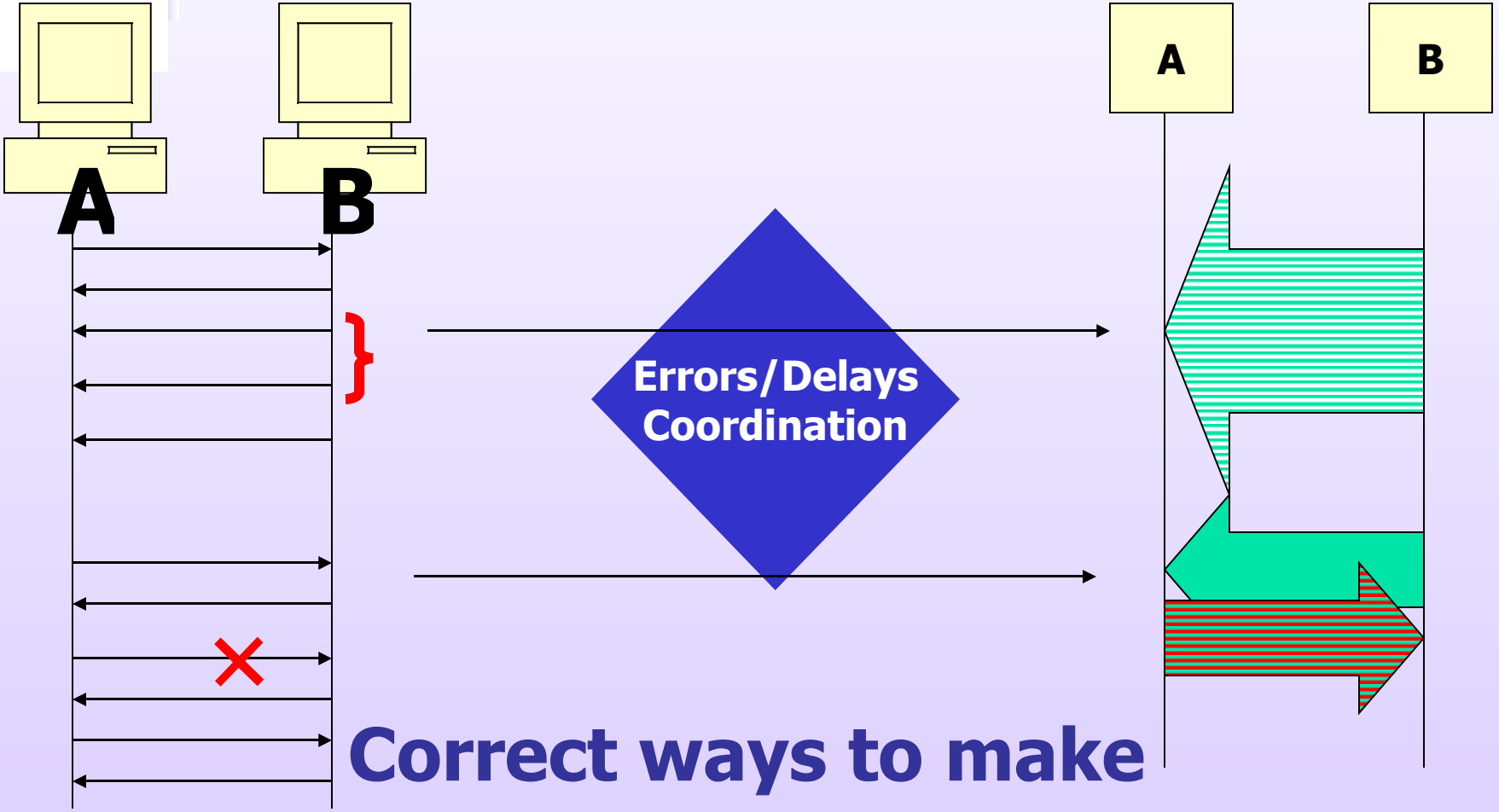
Getting simulation above packets level (2)



} Delays

✕ Packet drop

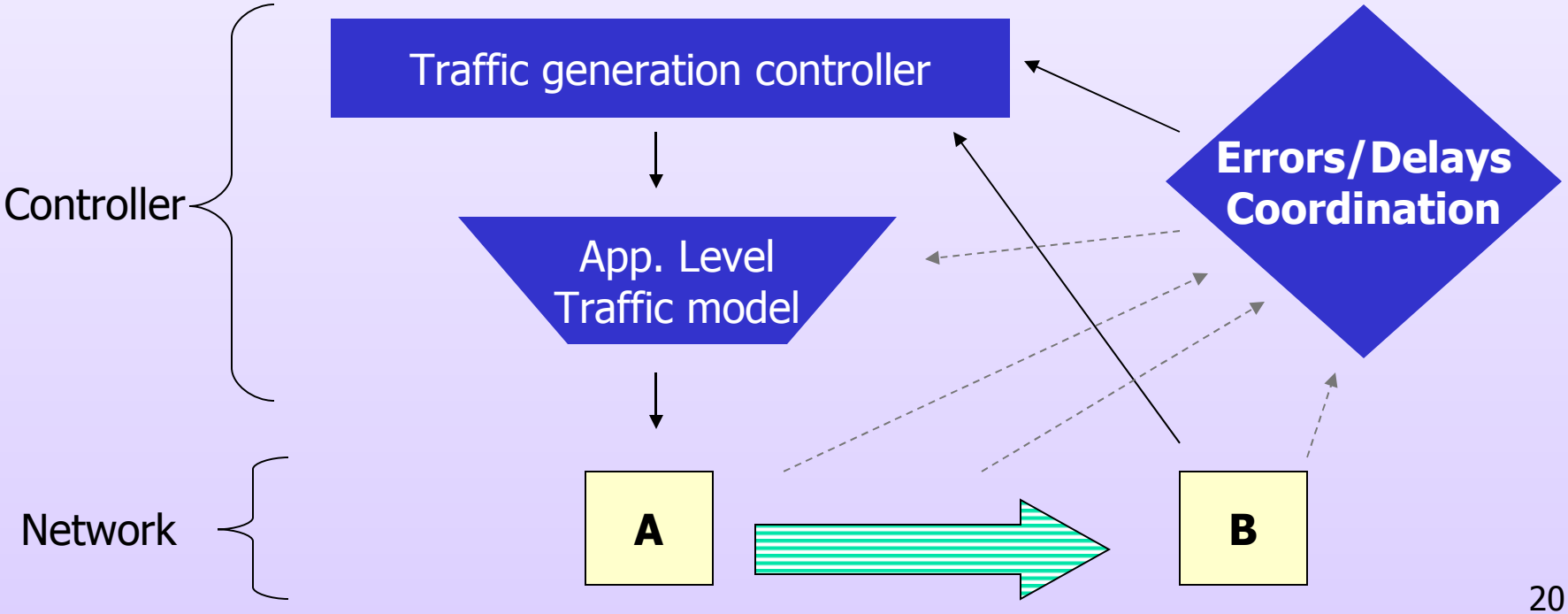
Getting simulation above packets level (3)
Packet-to-flow loss and delay coordination



Correct ways to make things go wrong?

Model controllers

- Traffic generation controller
- Application level traffic models
  - Web, p2p, video and malware



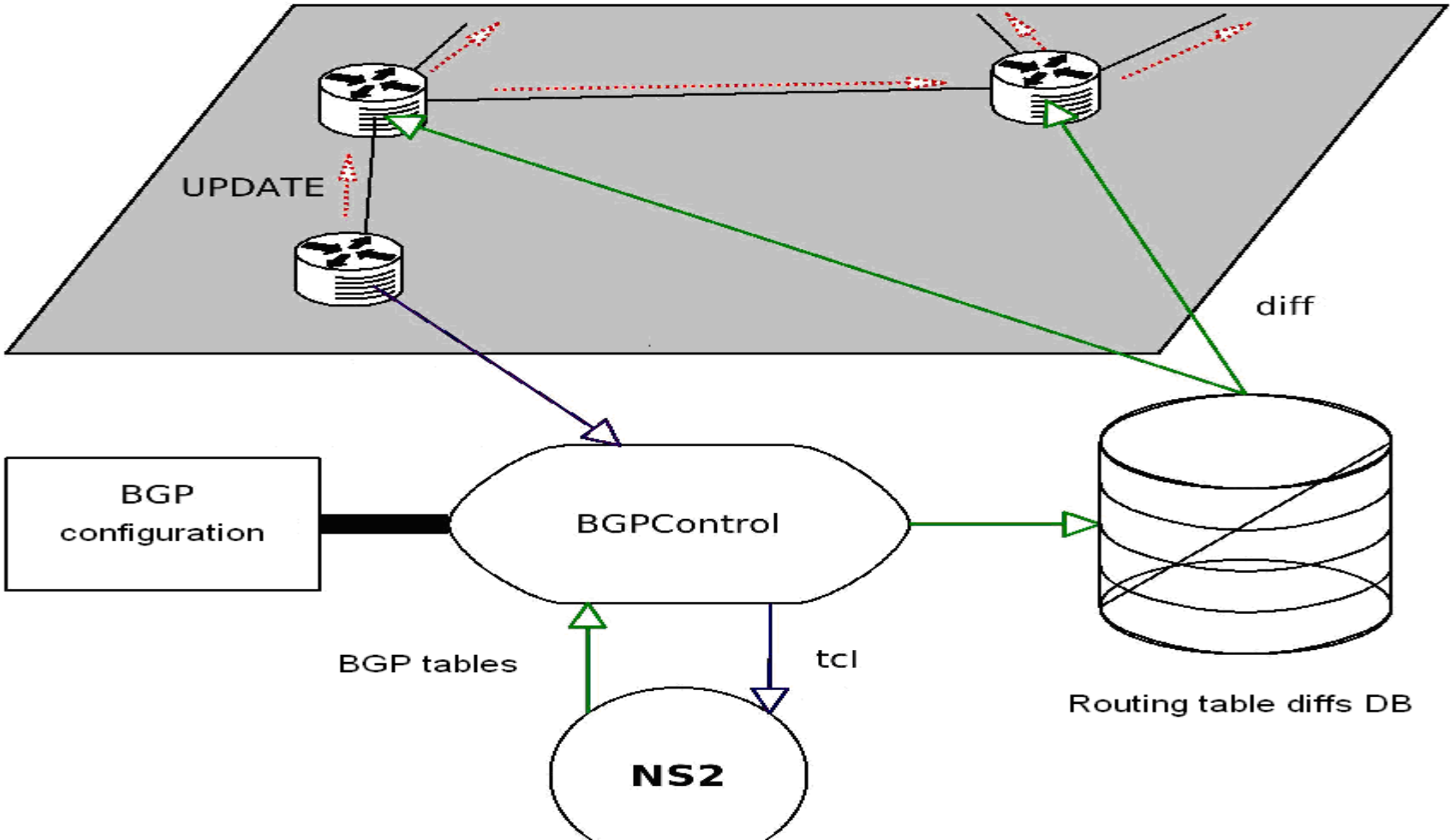
GloNeHyS project

GloNeHyS 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
  - Routing: weights to route flows to interfaces depending on traffic type
  - Interface weights are updated according to routing tables and services state

GloNeHyS project

Why keeping packet level?



Agenda

- Introduction
- Network and Traffic
- Malware and Security systems
- Making it work and getting results

Malware 2-part model

- MW.Ext
  - # of malware agents in external
  - 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)

Malware traffic models sample: ARIMA(AAWP(t))

ARIMA(p,d,q)

$$\Phi(L)(1-L)^d X_t = \Theta(L)\varepsilon_t$$
$$\Phi(L) = 1 - \varphi_1 L - \varphi_2 L^2 - \ldots - \varphi_p L^p$$
$$\Theta(L) = \theta_0 + \theta_1 L + \theta_2 L^2 + \ldots + \theta_q L^q$$

X_t - traffic, L - latency operator $X_{t-1} = LX_t$.

ε_t - white noise

$\varphi_1, \varphi_2, \ldots, \varphi_p$, $\theta_0, \theta_1, \ldots, \theta_q$ - calibrated parameters

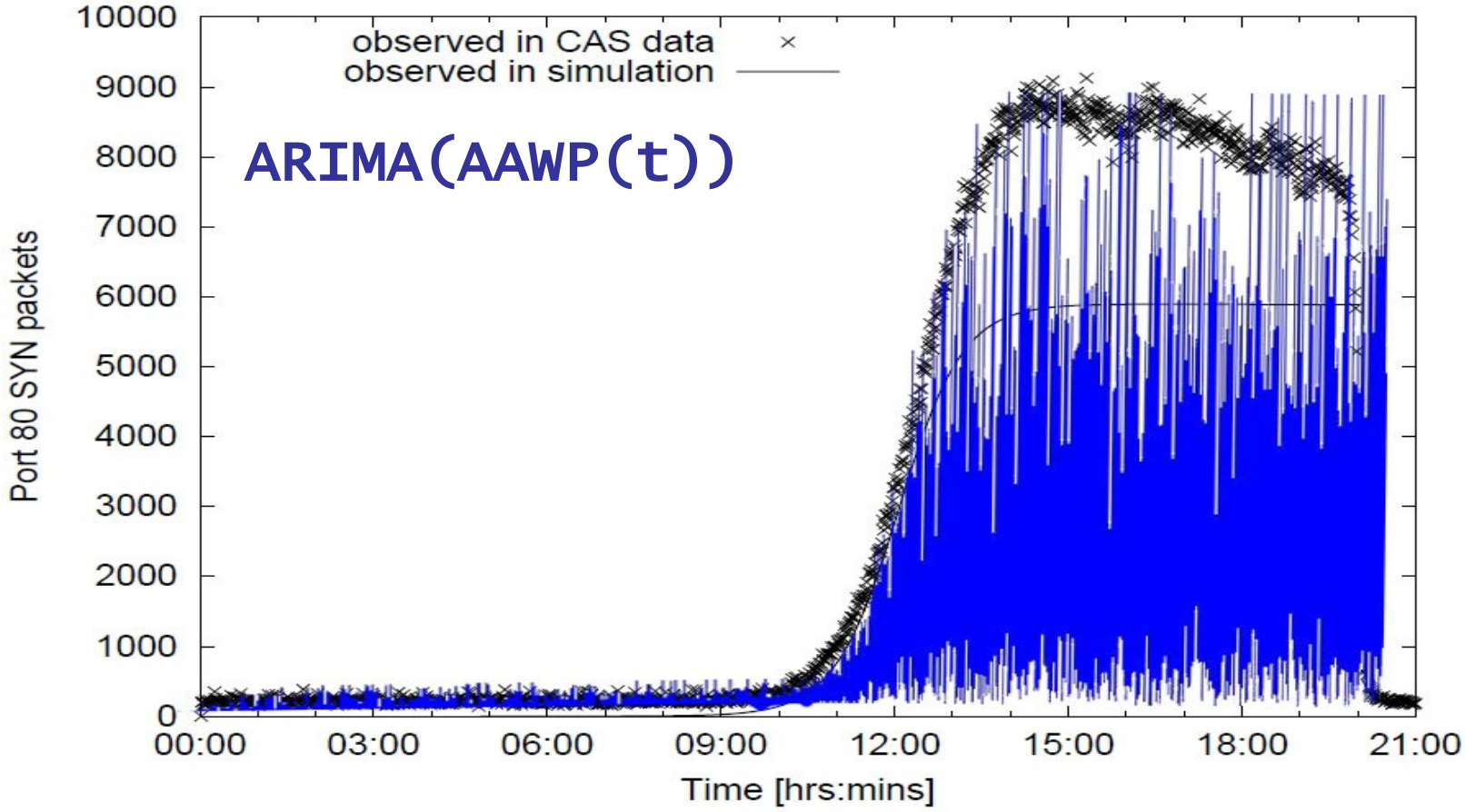
AAWP(n_i)

$$n_{i+1} = (1-d)n_i + (N-n_i)\left[1-\left(1-\frac{1}{2^{32}}\right)\right]^{sn_i}$$

N – susceptible hosts, n_i – number of infected hosts

s – scanning, d – healing rates

Simulation Example: External network Code Red malicious traffic

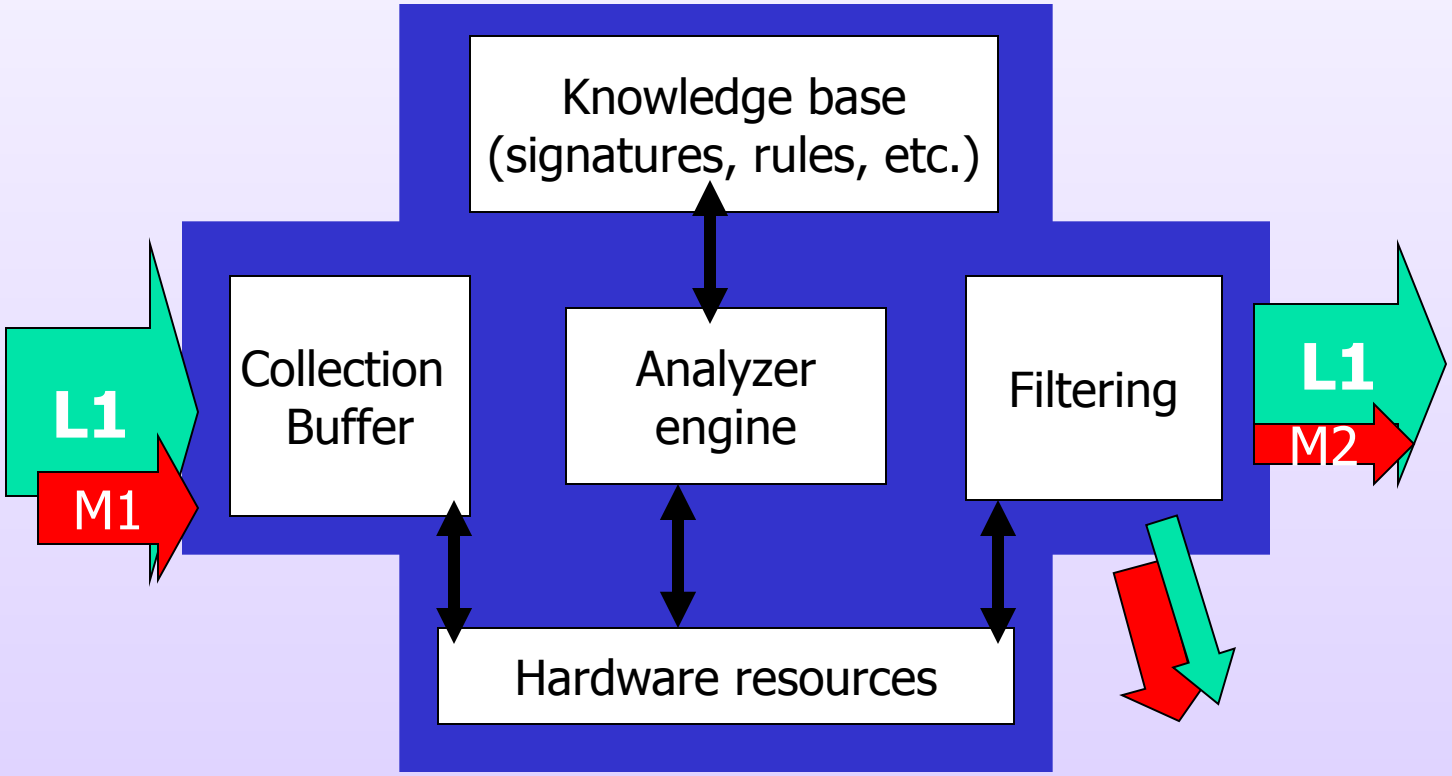


GloNeHyS project

What's efficiency of a security system? (benchmark/test bed)

- Performance
  - % of resources utilization to perform
  - # of analyzed objects per time slot
- Correctness
  - % of true positive
  - % of true negatives

Network security system model



Traffic types matrix for network security systems

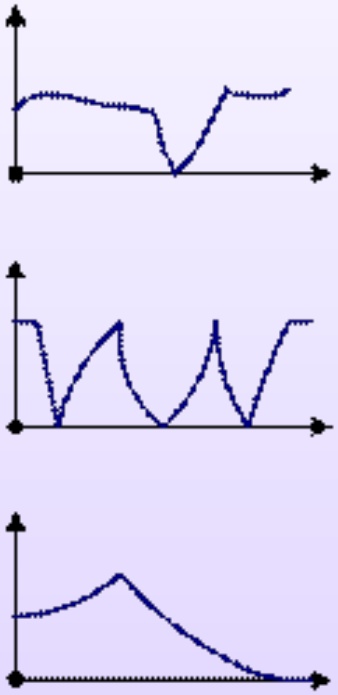
100% performance	NSS1	NSS2	NSS3
L1	0.9998 L1	1.0 L1	1.0 L1
L2	0.9999 L2	0.9999 L2	1.0 L2
M1	0.9999 M1	0.01 M2	0.002 M3
M2	0.9999 M2	1.0 M2	0.9 M3
M3	1.0 M3	1.0 M3	1.0 M3

- Purpose: correct traffic flow drop rates for multiply installation points and system types
- Traffic information remaining: traffic load, traffic "color"

GloNeHyS project

Efficiency meltdown: it's never 100%

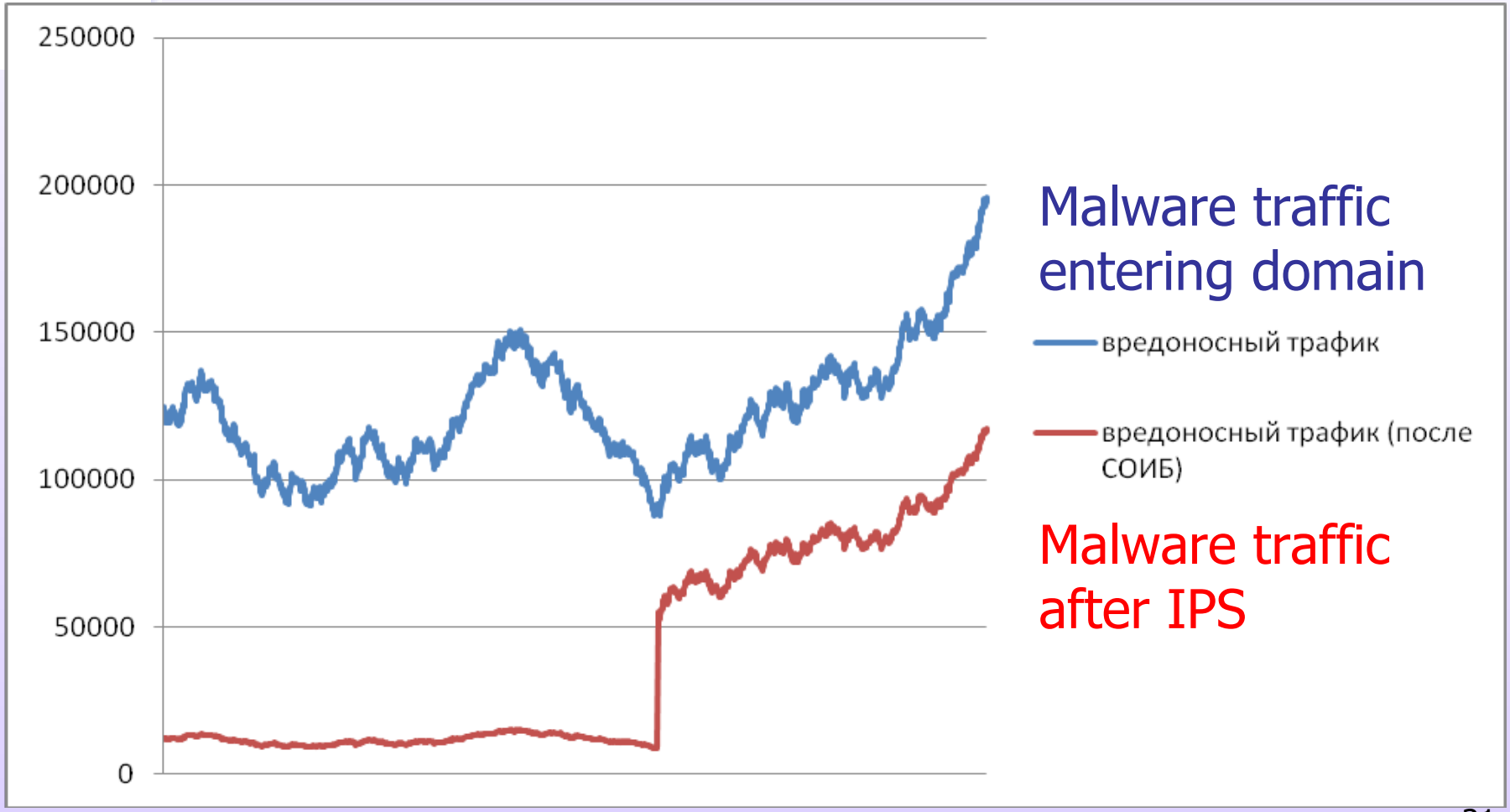
- Overload and hang-ups
- Downtime, upgrades, backups
- Correctness degradation: delay of updates, malware modification
- Multiply security systems "cooperation" 1+1<2:
  - Same knowledge, twice delay
  - Same true positives, different false positives



Malfunction profiles

GloNeHyS project

Simulation Example: Malfunction effects



Agenda

- Introduction
- Network and Traffic
- Malware and Security systems
- Making it work and getting results

Efficiency of a security system from the network point of view

- Positive impact
  - Reduce malicious traffic
- Negative impact – network performance decrease
  - Traffic delayed to perform analysis
  - Legitimate traffic loss (false positives)

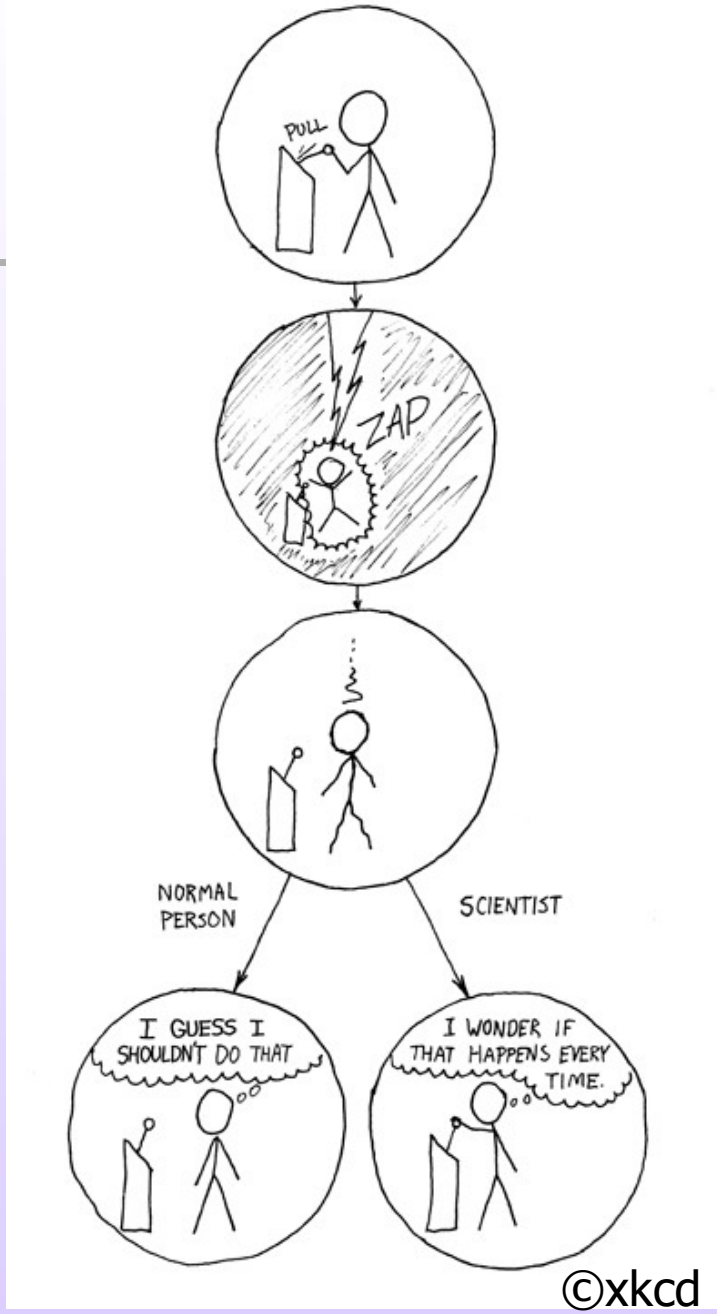
Network Security Systems on-site efficiency

- Network performance
  - Traffic loss
  - Traffic delay
  - Traffic jitter
- Malware
  - Malware population
  - Malware activity (traffic)

GloNeHyS project

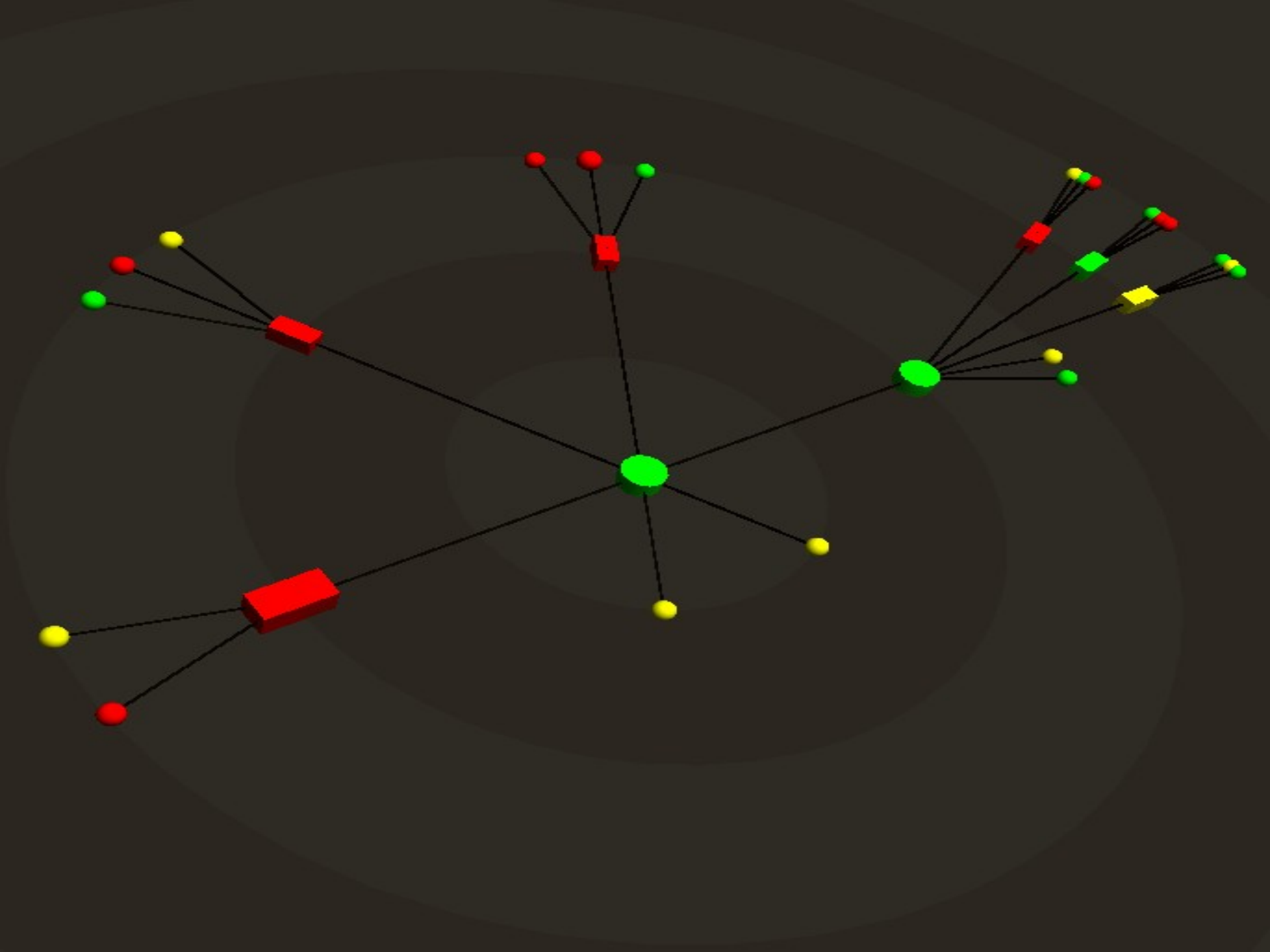
Experiment cookbook

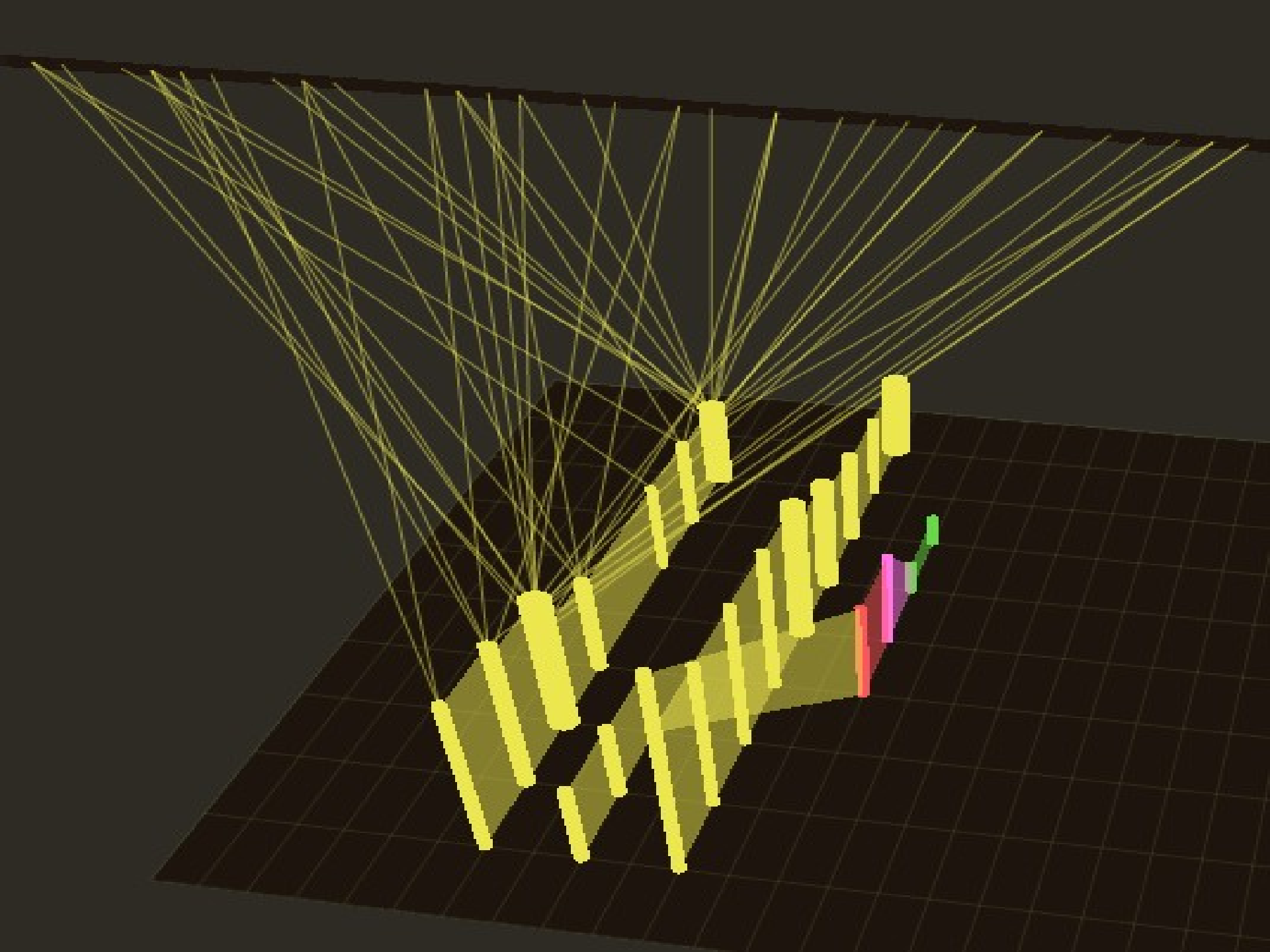
- Network configuration
- Pick and setup traffic models
  - Legitimate traffic – services+consumers
  - Malware models
- Pick and place security systems models
- Simulate (scientist's way)



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





GloNeHyS project

GloNeHyS use cases

- Security systems efficiency estimations. How secure? At what price?
- Network security systems on-site efficiency metrics development and measurement
- Network configuration stability and survivability analysis
- Security response/business continuity plans validation
- Cheap way for innovative distributed security systems algorithms testing

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*

Thanks!

GloNeHyS project

Questions?

CS labs

Alexei Kachalin

ak@lvk.cs.msu.su

Calc. Math & Cybernetics Department

Moscow State University