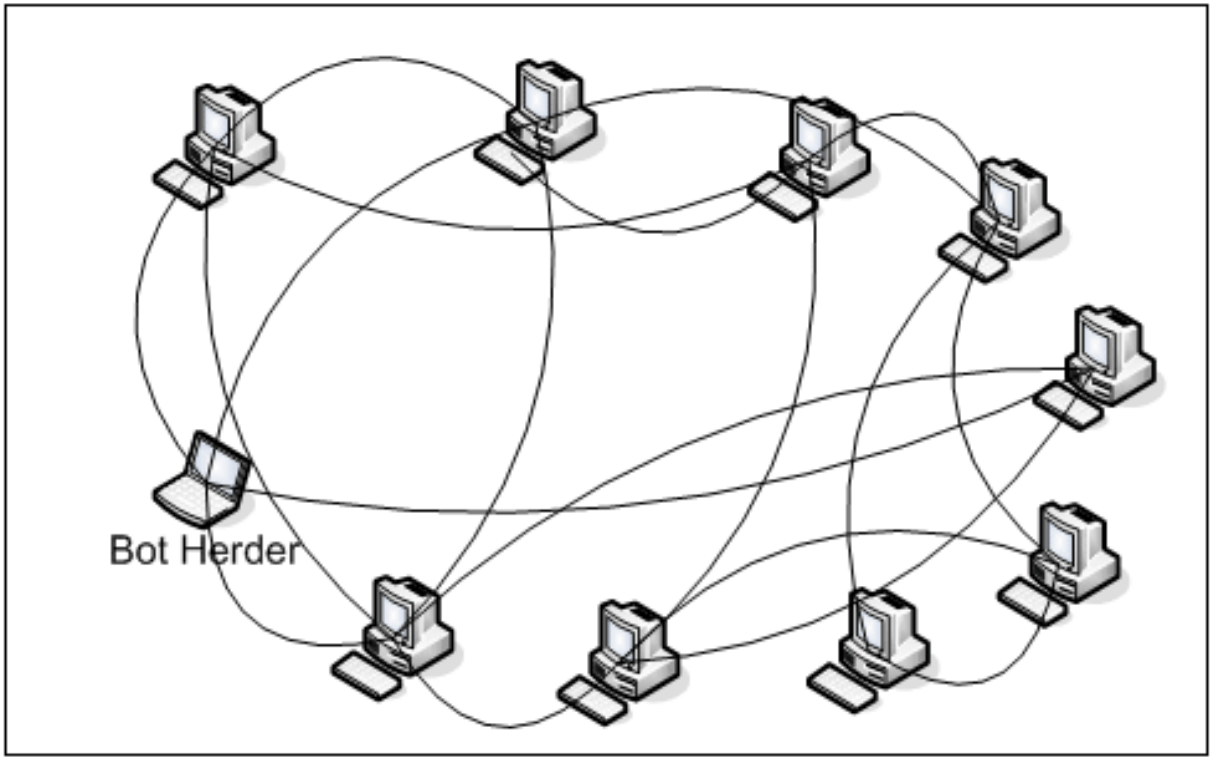
Mean Field analysis of Botnet behavior.

Anna Kolesnichenko
DACS, University of Twente
27.03.2011

Typical Peer-To-Peer Botnet



- Uncentralized
- Spreads fast
- Has no target
- Hard to dismantle

Motivation

QEST 2008, Elizabeth Van Ruitenbeek and William H. Sanders, *Modelling Peer-to-Peer Botnets*.

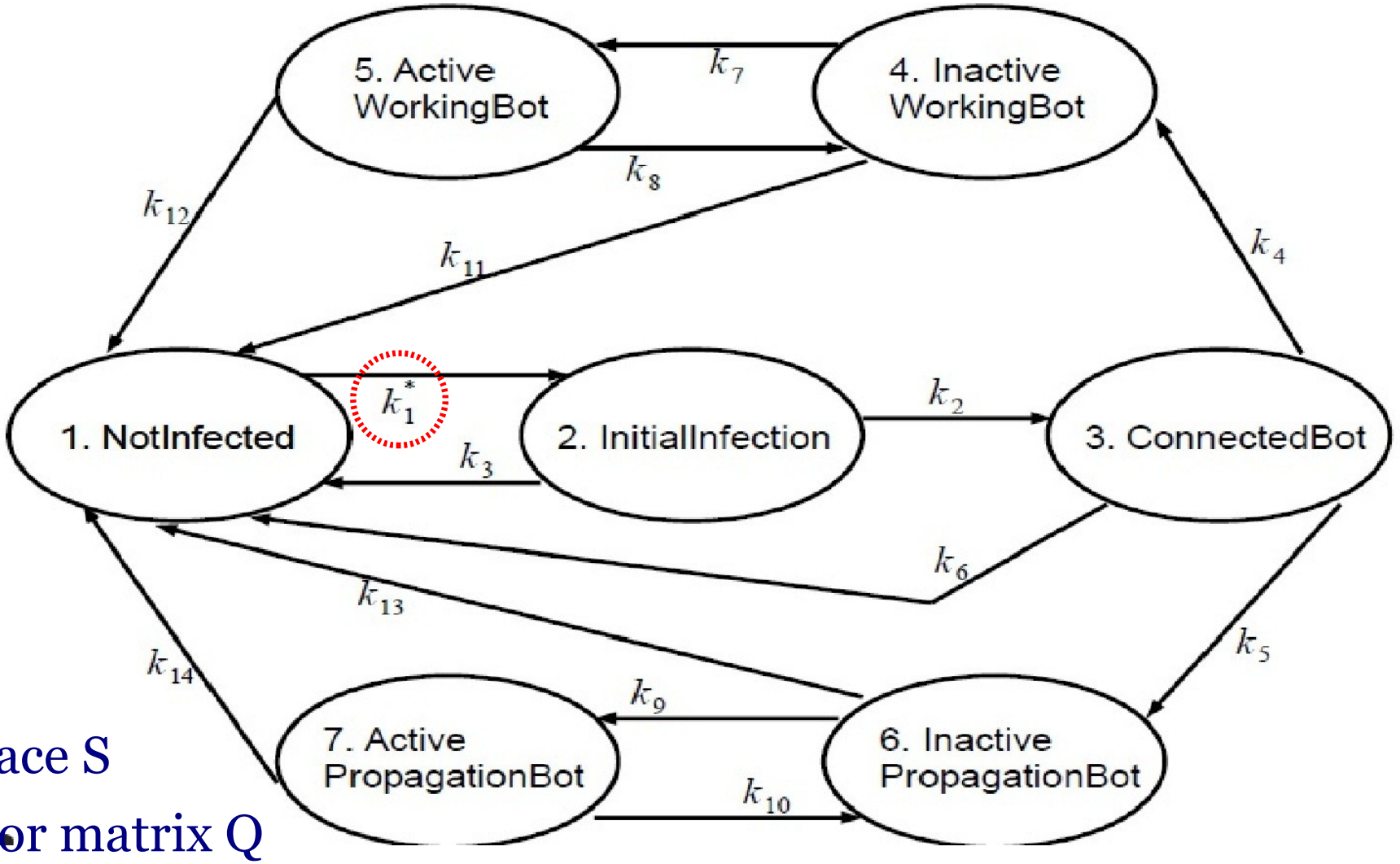
QEST 2009, R. Bakhshi, L. Cloth, W. Fokkink and B. Haverkort. *Mean-field analysis for the evaluation of gossip protocols*.

Other large scale methods

Outline

- Mean-Field model for Peer-to-Peer Botnet
- Simulation vs Mean-Field
- The use of speed up
- Related work
- Conclusions

CTMC Model for one computer



State space S

Generator matrix Q

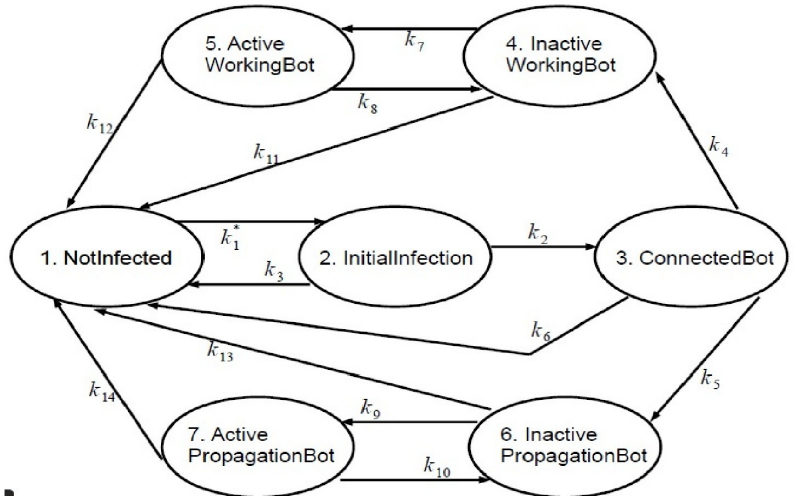
Mean-Field Approximation

Overal CTMC, N computers

$|S^N|$ — identity → $\underline{M}(t) = (\underline{M}_1(t), \underline{M}_2(t), \ldots, \underline{M}_{|S|}(t))$

Generator matrix Q(M(t))

$$k_1^* = \frac{k_1 \cdot M_7(t)}{M_1(t)}$$



Mean-Field Approximation

Dependency on N

$$\underline{m_s}(t) = \underline{M_s}(t)/N$$

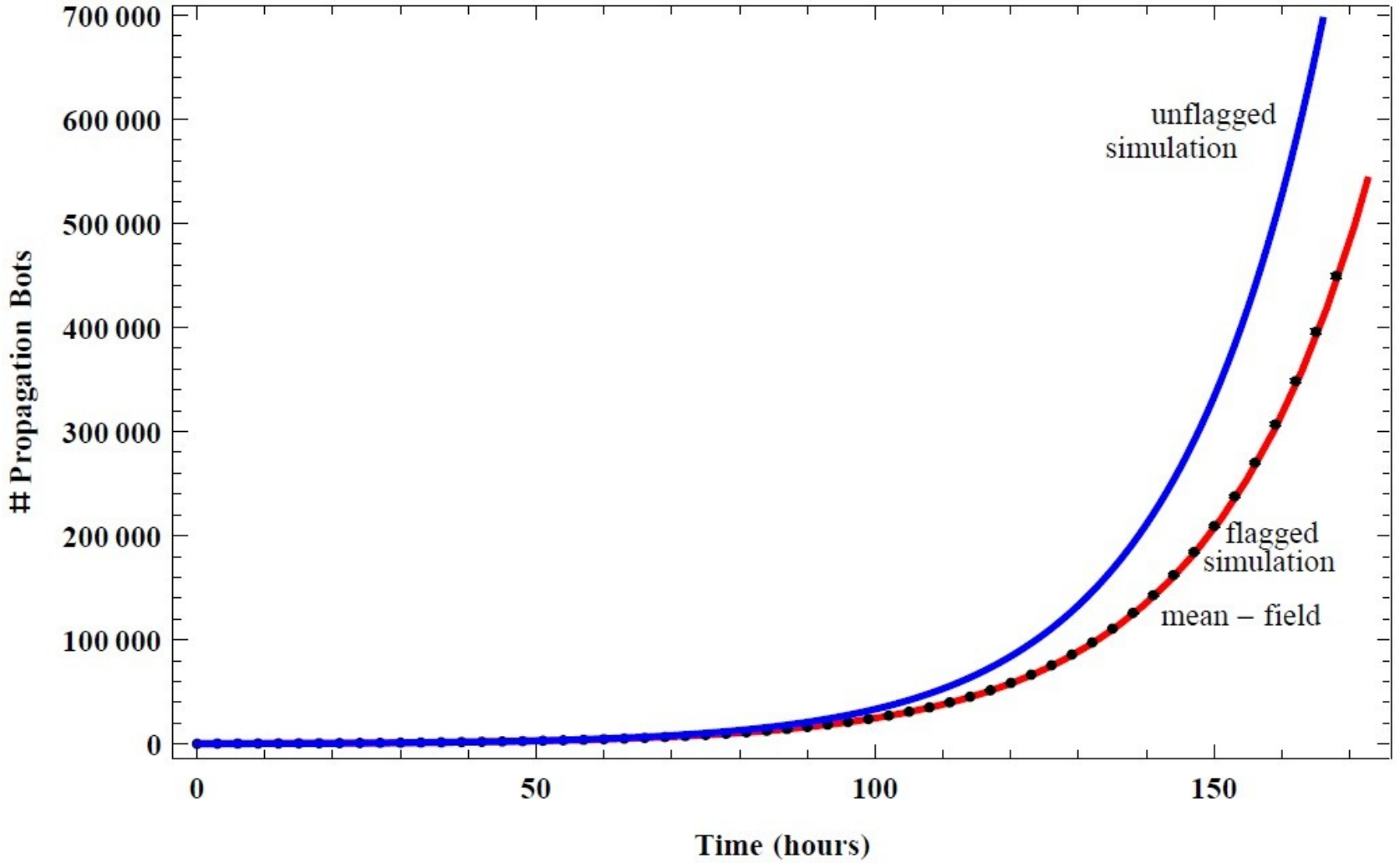
Mean-Field approximation, N → inf

$$\frac{d\,\underline{m}(t)}{dt} = \underline{m}(t)\cdot Q\left(\underline{m}(t)\right)$$

Mean-Field limit, large N

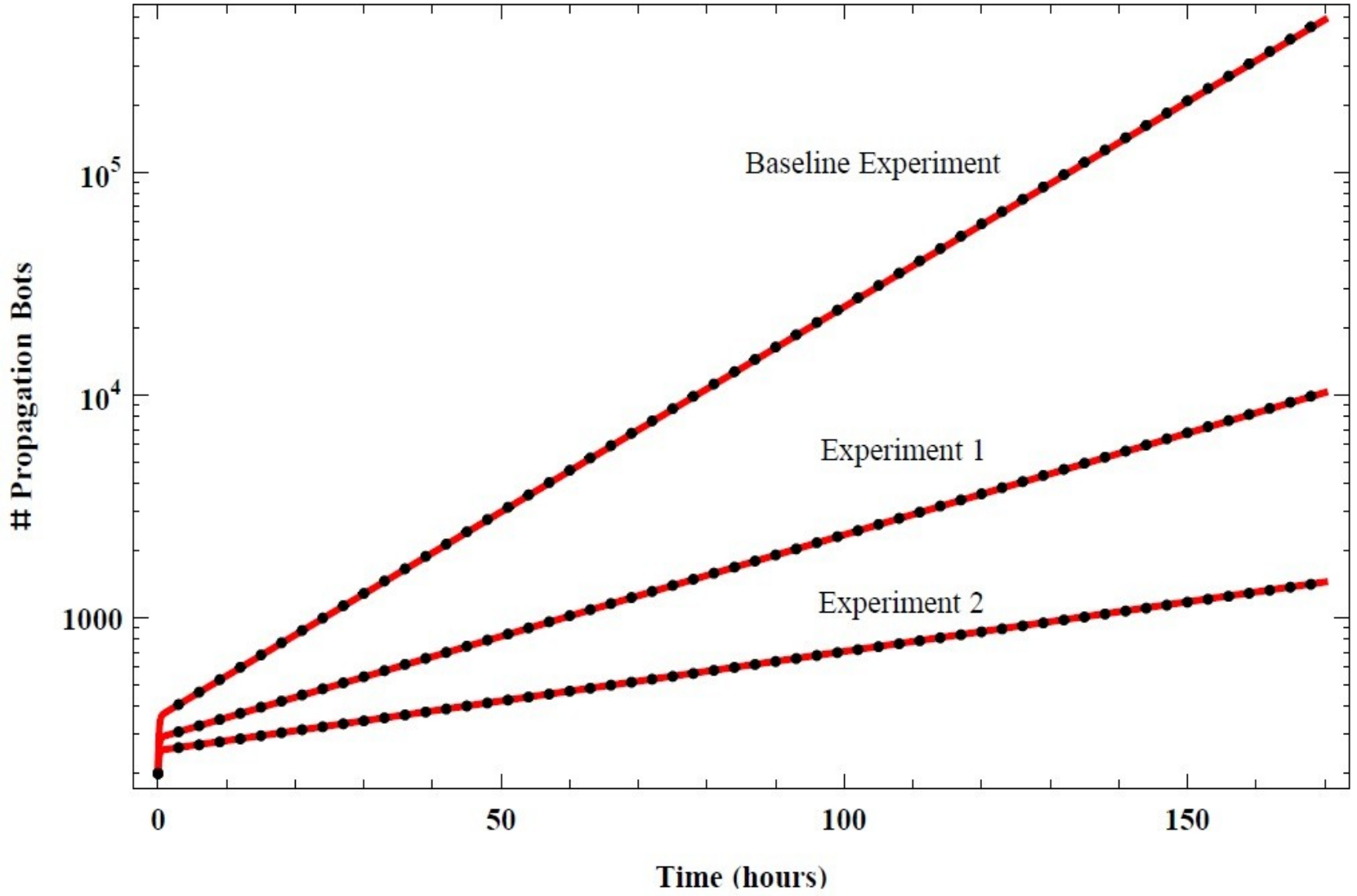
$$\frac{dE\left(m_i(t)\right)}{dt} \approx \sum_{j\in S} E\left(m_j(t)\right)\cdot Q_{ij}\left(\underline{m}(t)\right), i\in S$$

Mean-Field vs Simulation



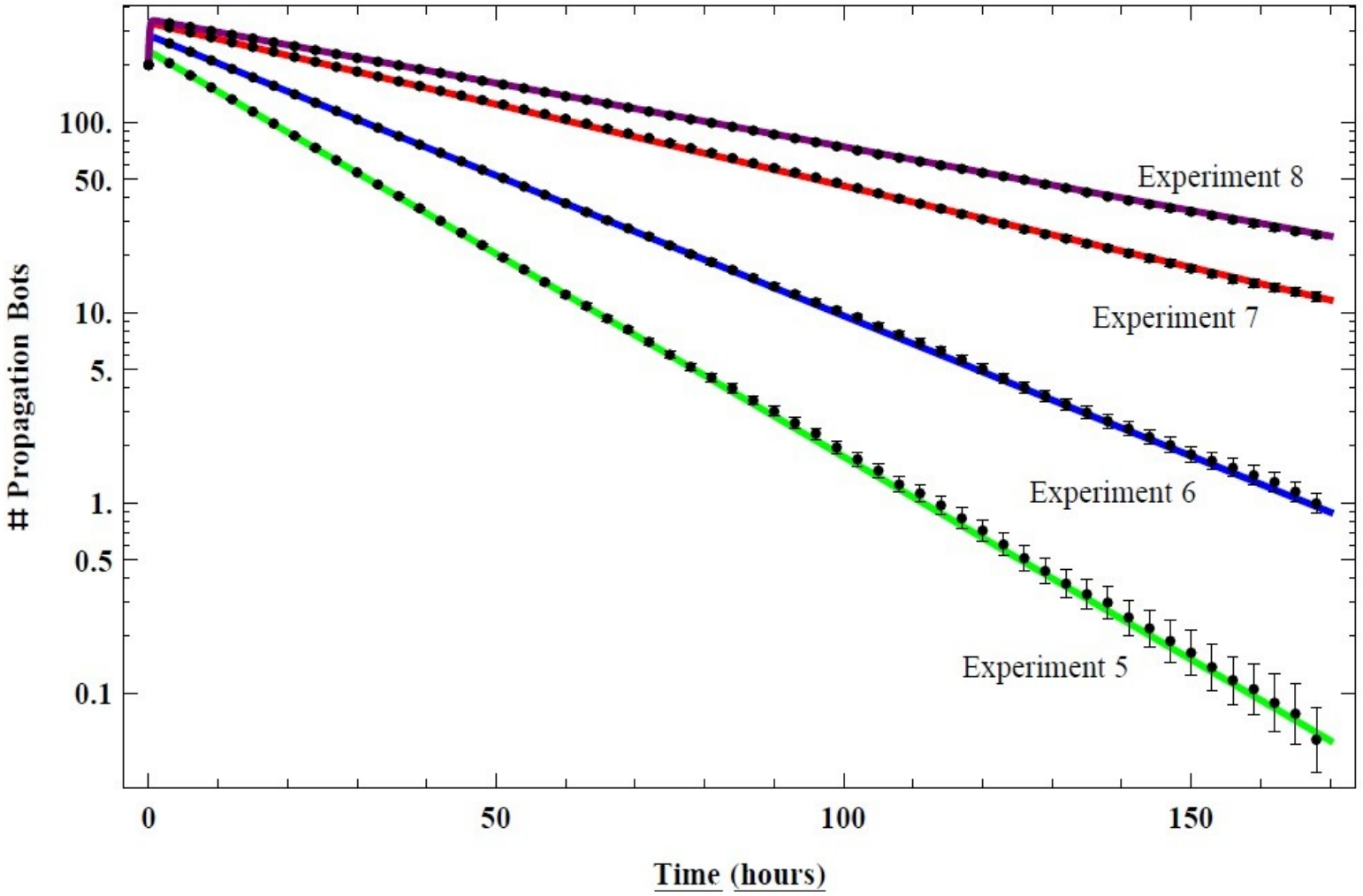
t=0 200 Active Propagation Bots

The “user factor”



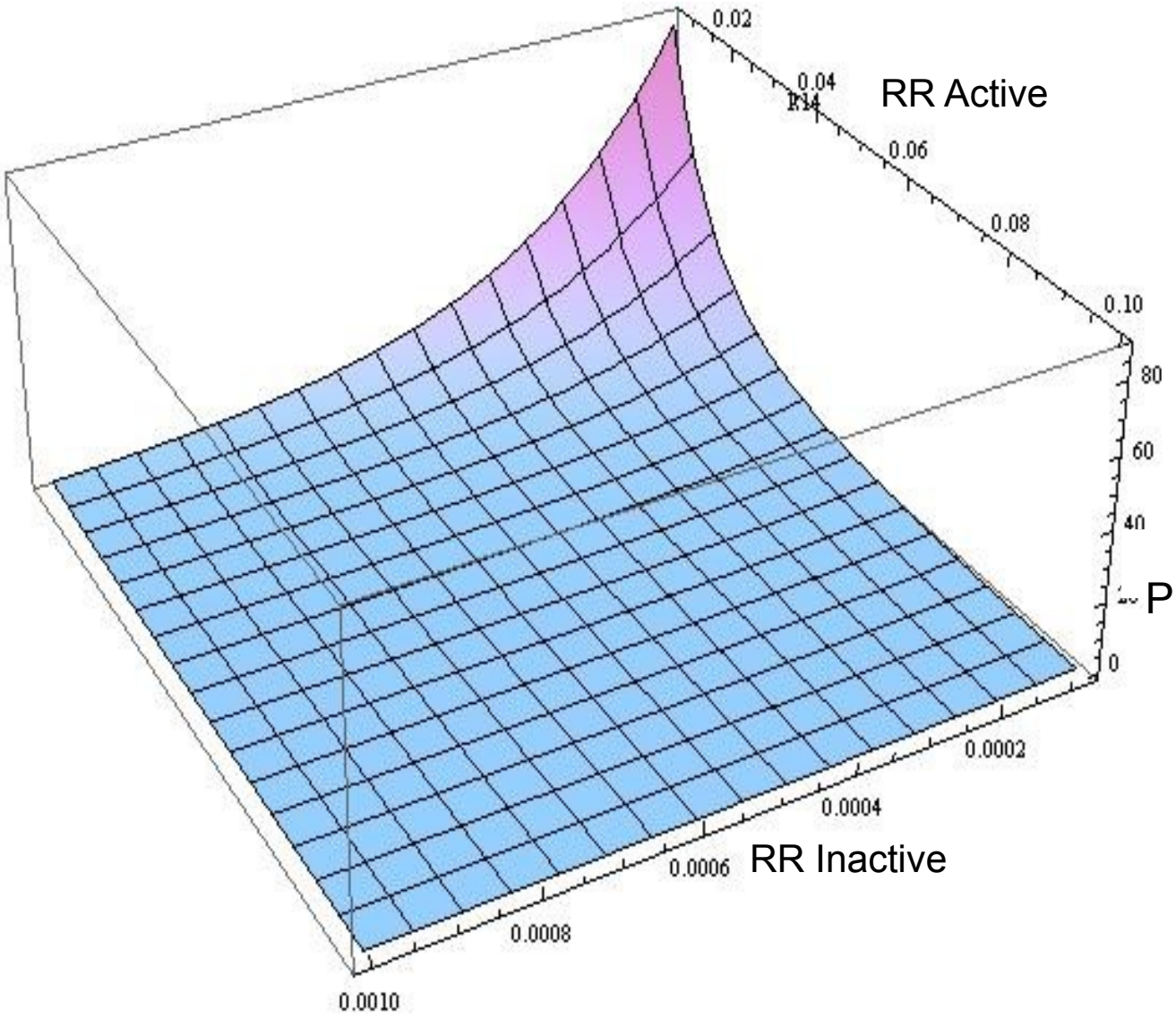
Probability of initial infection is reduced by 60% and 40%

Antivirus performance



Removal rates are increased by 70%, 40%, 20% and 15%

Speed up and quality up



COST concept

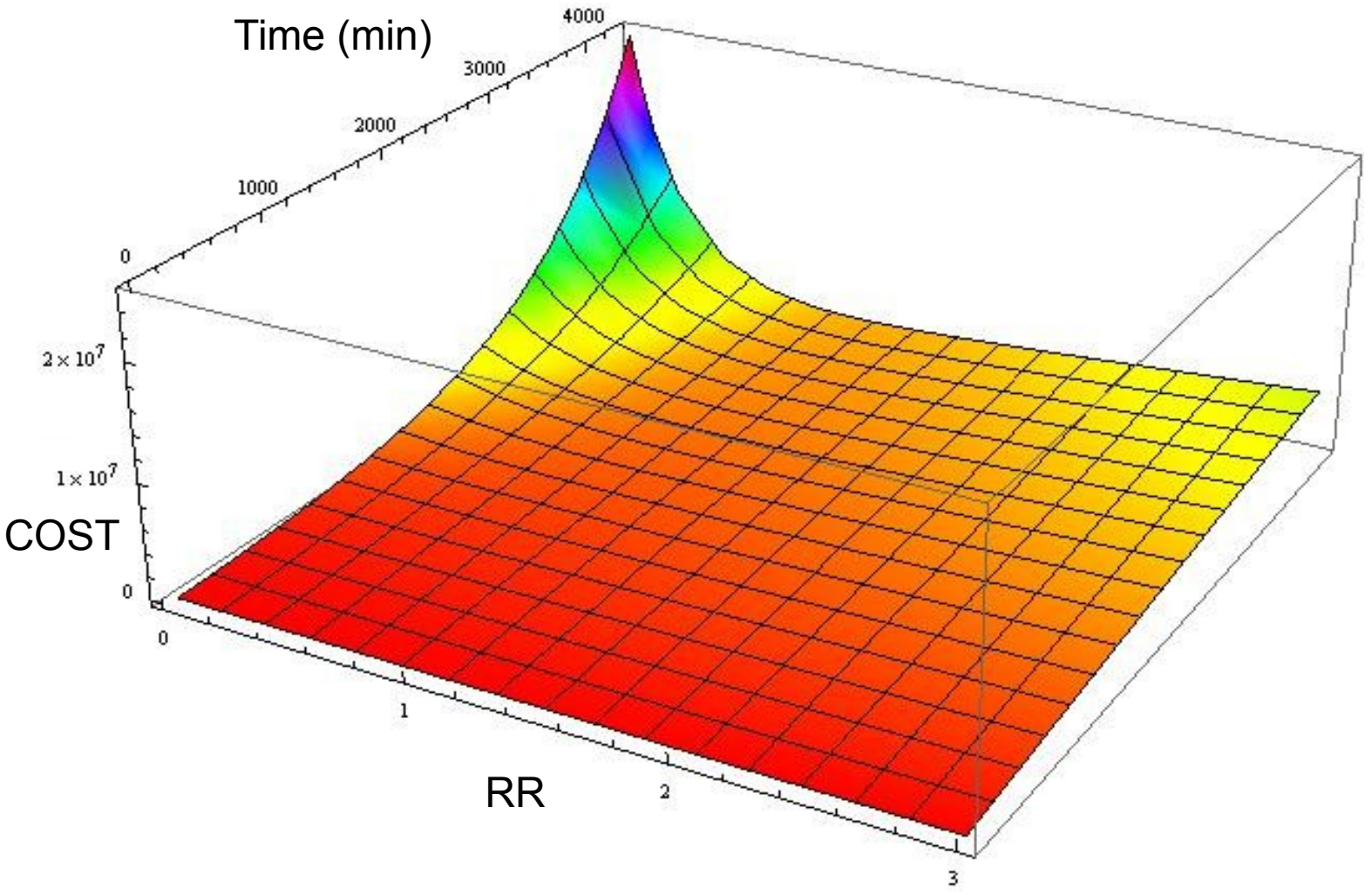
COST= Infected computers + Checking with antivirus

Infected=InfectedComputers*D1

Checking=AllComputers*RR*D2

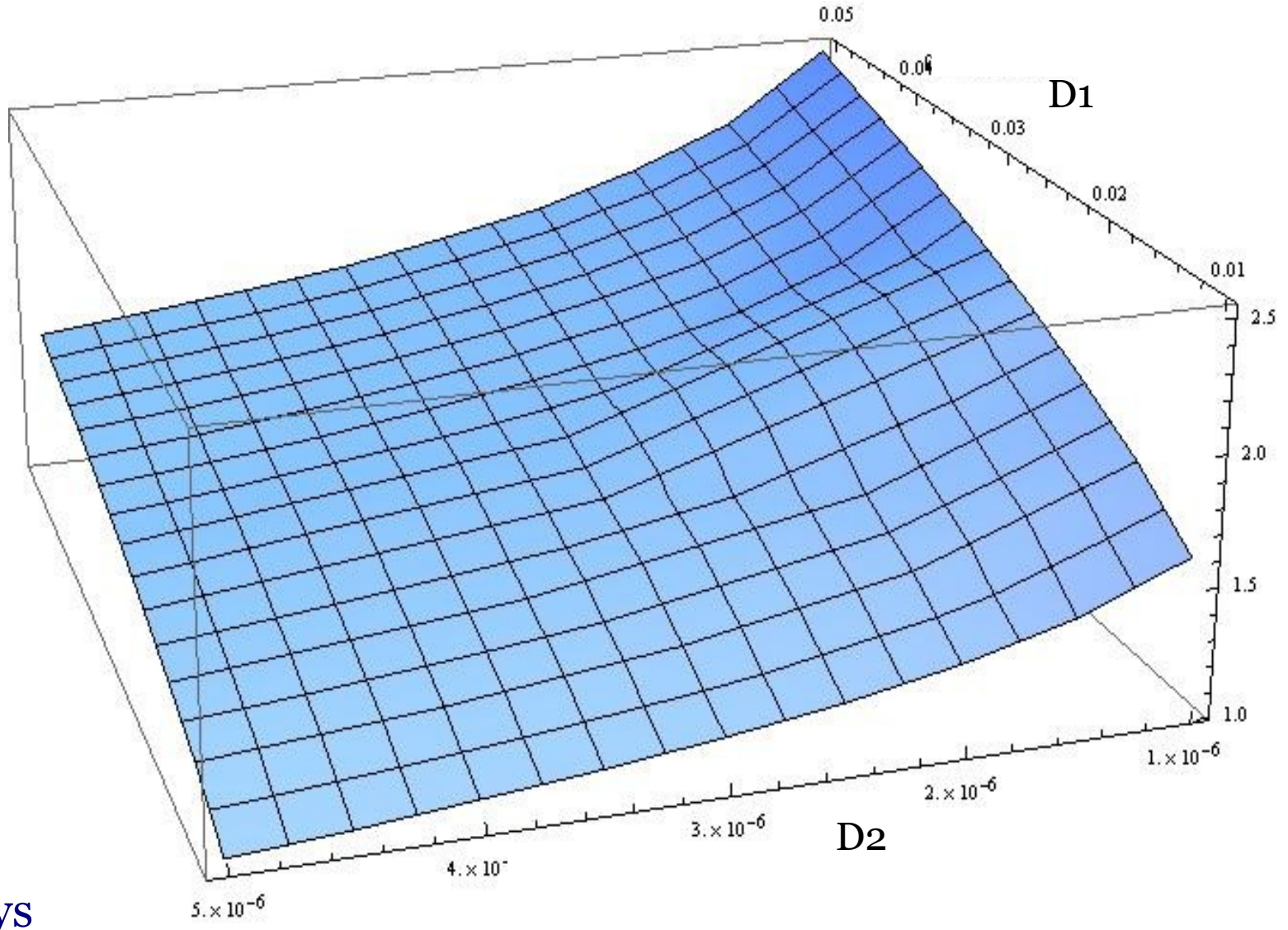
$$CumulativeCOST = \int_{t_0}^{t_1} \left(D_1 \cdot Inf\left(t\right) + D_2 \cdot RR \cdot All \right) dt$$

Cumulative cost



D1=0.01
D2=10^ -6

Optimal Removal Rate



T=3 days

Related work

- Discrete time: DTMC.

- ODE

CMSB 2005, M. Calder, S. Gilmore, and J. Hillston, *Automatically deriving ODEs from process algebra models of signalling pathways*

Conclusions

- Acuracy of the method
- Speed up is clear
- Other methods are similar

Thank you for your attention.