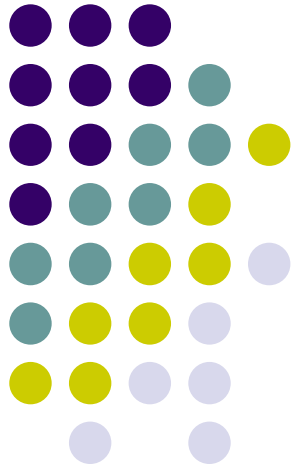
Modeling and Automated Containment of Worms

Sarah Sellke, Ness B. Shroff, and Saurabh Bagchi
School of Electrical and Computer Engineering
Purdue University, West Lafayette, IN 47907
E-mail: {sselke,shroff, sbagchi}@ecn.purdue.edu



PURDUE UNIVERSITY

CWSA

PURDUE UNIVERSITY

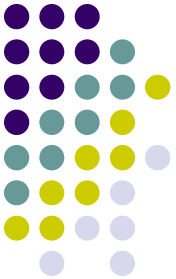
CWSA

Introduction

- Self-Propagating Worms
  - Spreads itself automatically by using a scanning strategy to find vulnerable hosts to infect.
  - Examples: Code Red, SQL Slammer
- Countermeasures:
  - Prevention, treatment, and containment
  - Countermeasures must be taken automatically during the early phase of worm propagation

PURDUE UNIVERSITY

CWSA



Our Contribution

- Provide a means to accurately model the early phase of propagation of uniform scanning worms
- Proposed an automated mechanism for containing worm spreads
  - Effective for both fast and slow worms
  - No need for the worm signature in advance
  - No need to detect the worm
  - Non-intrusive - little impact on legitimate traffic

PURDUE UNIVERSITY

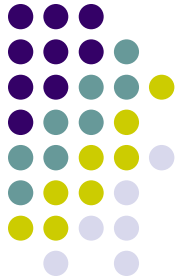
CWSA

Related Work

- Modeling
  - RCS Model - by Staniford et al.
  - Two Factor - Worm Model by Zou et al.
  - AAWP Model - by Chen et al.
- Detection
  - Kalman filter - by Zou et al.
  - DIB:S/TRAFEN - by Liljenstan et al.
- Virus Throttling
  - Restricting scan rate - by M. M. Williamson
- Worm Quarantine:
  - Requirements - by Moore et al.
  - Dynamic Quarantine - by Zou et al.

PURDUE UNIVERSITY

CWSA

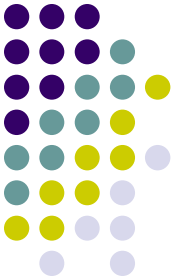


Outline of this Talk

- Modeling
  - Branching Process Model for worms
  - Worm extinction probability
  - Probability distribution of total infections
- Automated Worm Containment Strategy
- Simulation Result
- Conclusion and Future Work

PURDUE UNIVERSITY

CWSA

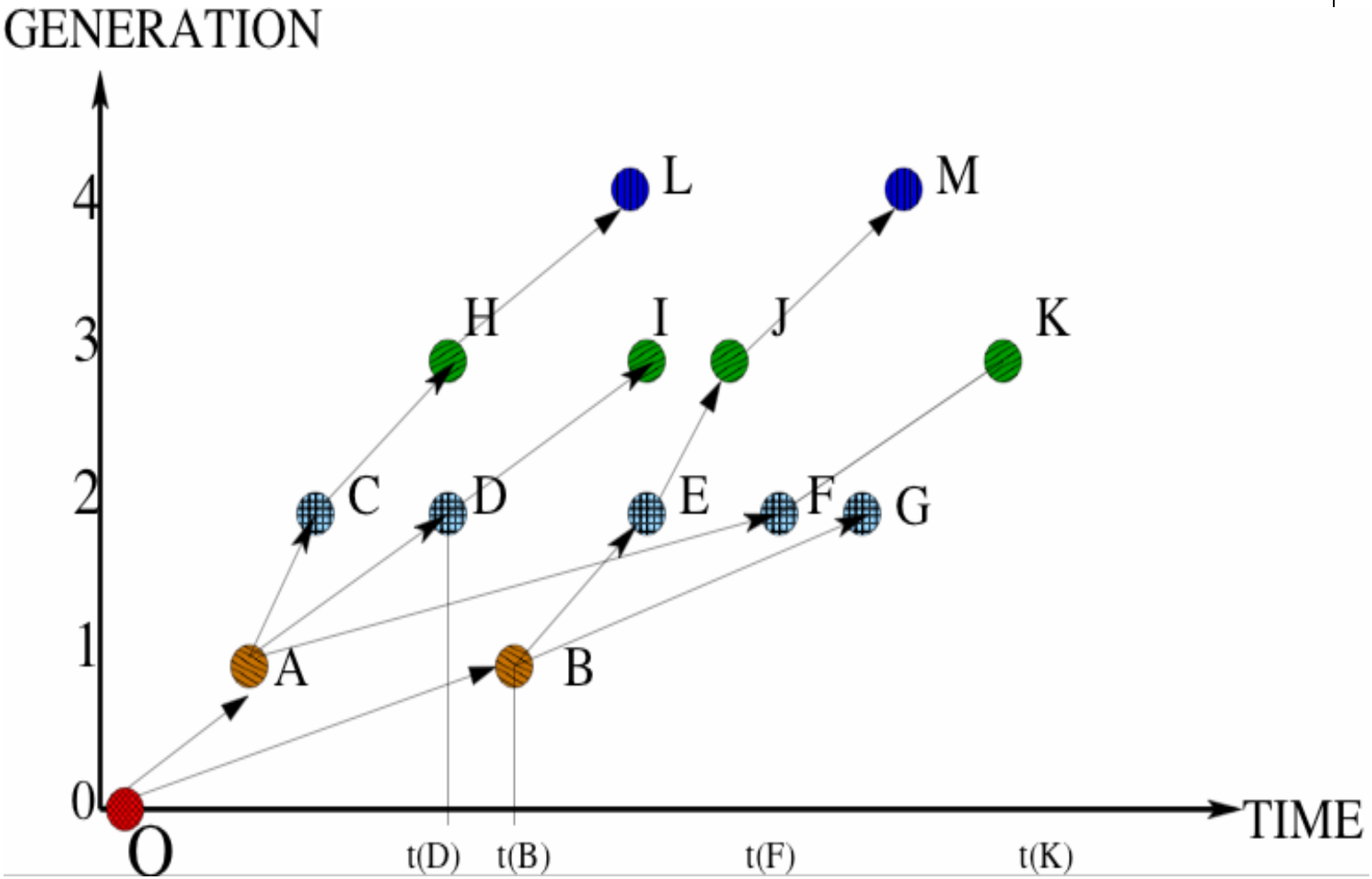


Branching Process Overview

- Branching Process models a population in which each individual in generation ***n*** *independently* produces some random number of individuals (ξ) in generation ***n+1***, according to a *fixed* probability distribution:

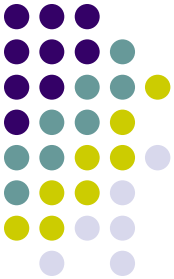
$$P\{\xi = k\} = p_k$$

Generation-wise Evolution of Worms



PURDUE UNIVERSITY

CWSA



Branching Process Model

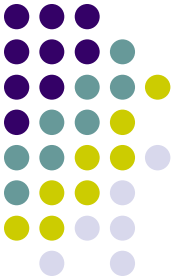
- *p*: the vulnerability density.
- *M:* the total number of scans each infected host may perform.
- ξ: the number of off-springs of one infected host scanning M times.

$$P\{\xi = k\} = \binom{M}{k} p^k (1-p)^{M-k}$$

- During the early stage, the spread of the infected hosts in each generation forms a **branching process.**

PURDUE UNIVERSITY

CWSA



Extinction Probability

- I_n: Number of n^{th} generation infected hosts
- $\xi_k^{(n)}$: Number of offsprings by the k^{th} host of the n^{th} generation

$$I_{n+1} = \sum_{k=0}^{I_n} \xi_k^{(n)}$$

- π : extinction probability

$$\pi = P\{I_n = 0, \quad \text{for some } n\}$$

PURDUE UNIVERSITY

CWSA

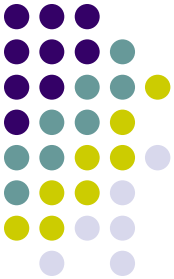
Extinction Probability

- **Branching Process Theorem:**

  The extinction probability π is 1 if and only if the mean number offspring per individual is no more than 1, i.e. $E\{\xi\} \leq 1$.

PURDUE UNIVERSITY

CWSA



Worm Extinction Probability

- **Proposition**: If the density of the vulnerable hosts is ***p***, and the total scans per host is ***M***, Then $\pi=1$ if and only if $M \leq 1/p$.

Recall: $P\{\xi = k\} = \binom{M}{k} p^k (1-p)^{M-k}$

So, $E\{\xi\} = M \times p$

PURDUE UNIVERSITY

CWSA

Practical Implications

- Code Red: V = 360,000
  - $p = 8.5 \times 10^{-5}$
  - Worm extinction probability is 1 iff $M \leq 11930$
- SQL Slammer: V=120,000
  - $p = 2.83 \times 10^{-5}$
  - Worm extinction probability is 1 iff $M \leq 35791$

PURDUE UNIVERSITY

CWSA

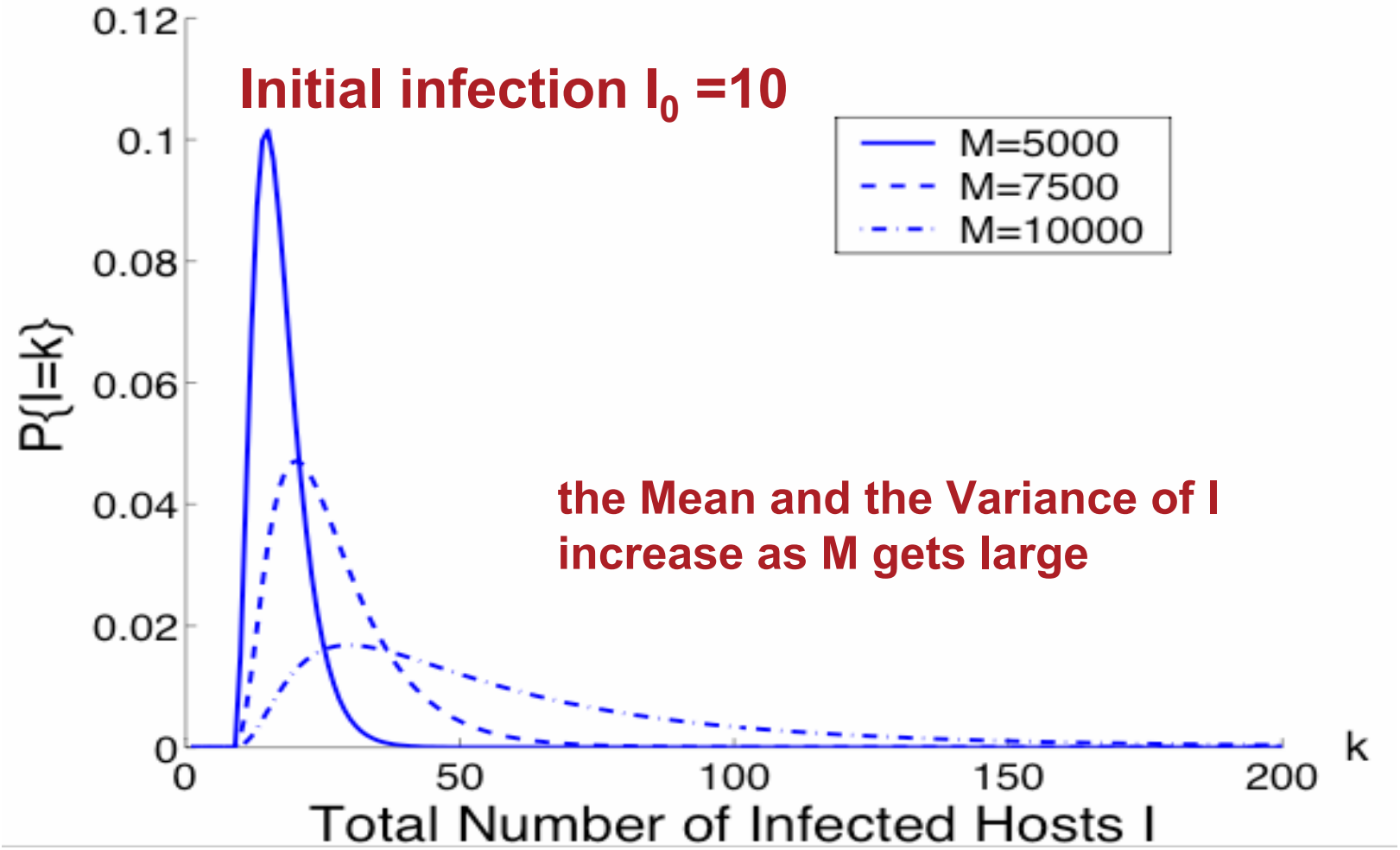
Total Number of Infected Hosts

- The probability distribution of the total number of infected hosts ($I = \sum_{n=0}^{\infty} I_n$) follows the Borel-Tanner Distribution:

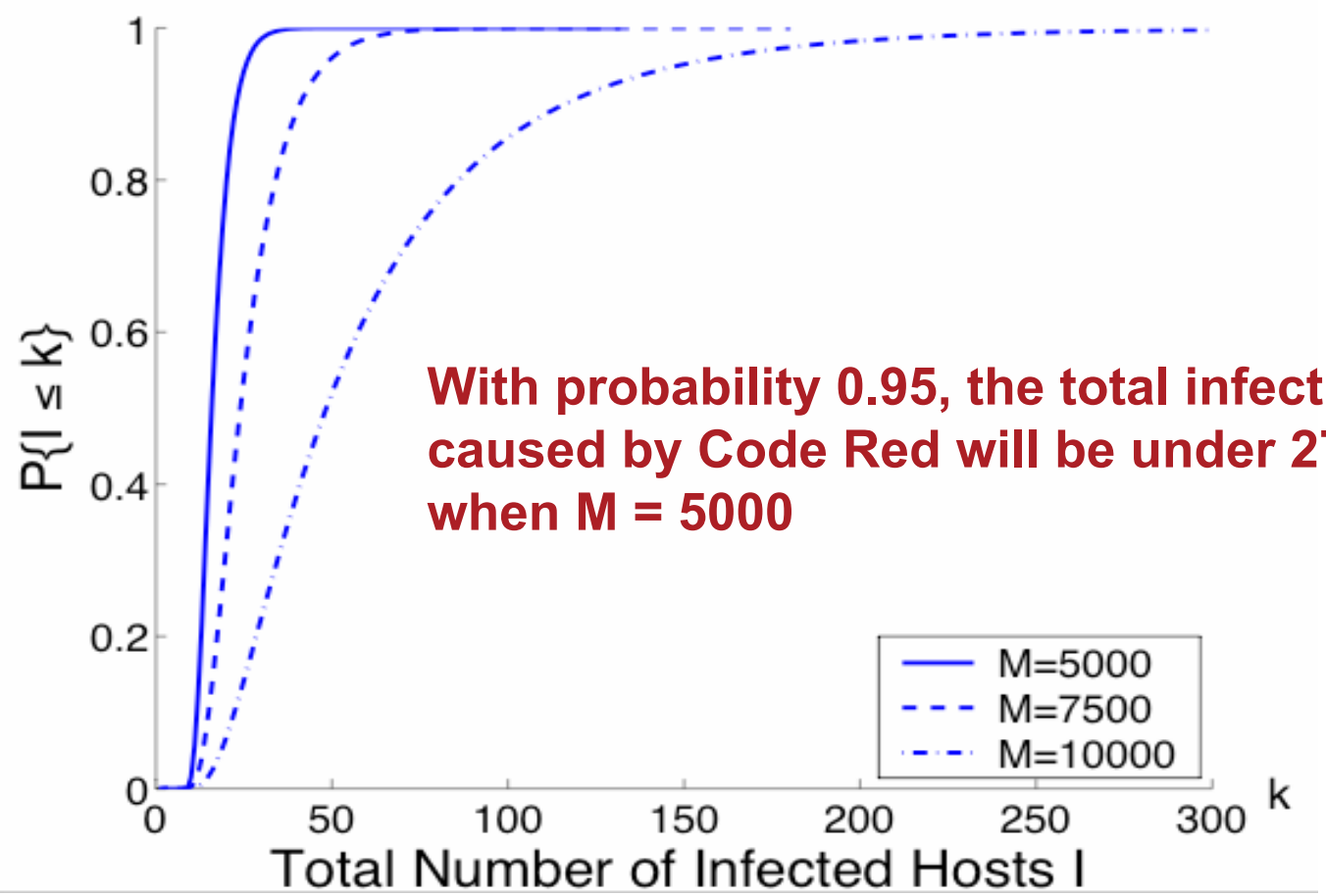
$$P\{I = k\} = \frac{I_0}{k(k-I_0)!}(k\lambda)^{(k-I_0)}e^{-k\lambda},$$
$$k = I_0, I_0 + 1, \cdots$$
$$\text{where } \lambda = Mp$$

$$E(I) = \frac{I_0}{1-\lambda} \qquad VAR(I) = \frac{I_0}{(1-\lambda)^3}$$

Probability Density of I



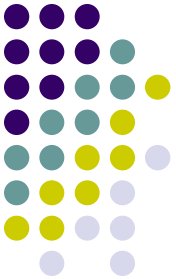
Cumulative Distribution for I



With probability 0.95, the total infections caused by Code Red will be under 27 when M = 5000

PURDUE UNIVERSITY

CWSA



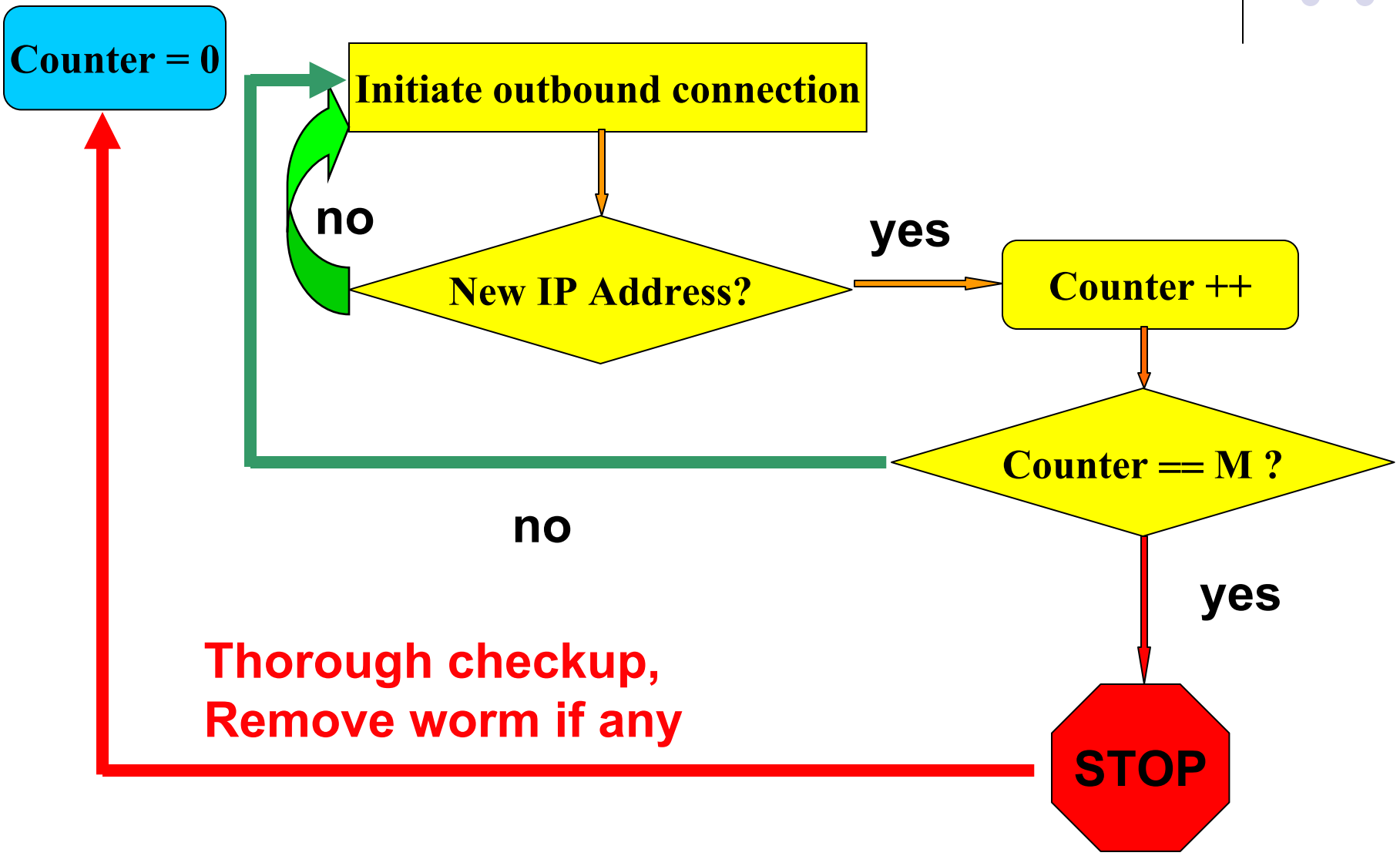
Worm Containment System

- Host based system
- Containment cycle
  - Relative long period of time, on the order of weeks.
  - Can be obtained through a learning process, based on the hosts' normal scanning characteristics.
  - All hosts will be checked for infections at the end of the cycle.
- Policy: Each host is allowed to contact no more than M distinct IP addresses.
- Hosts that reach this maximum will be disconnected from the network and undergo a thorough checkup.

PURDUE UNIVERSITY

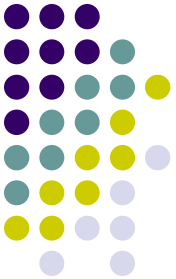
CWSA

Worm Containment System



PURDUE UNIVERSITY

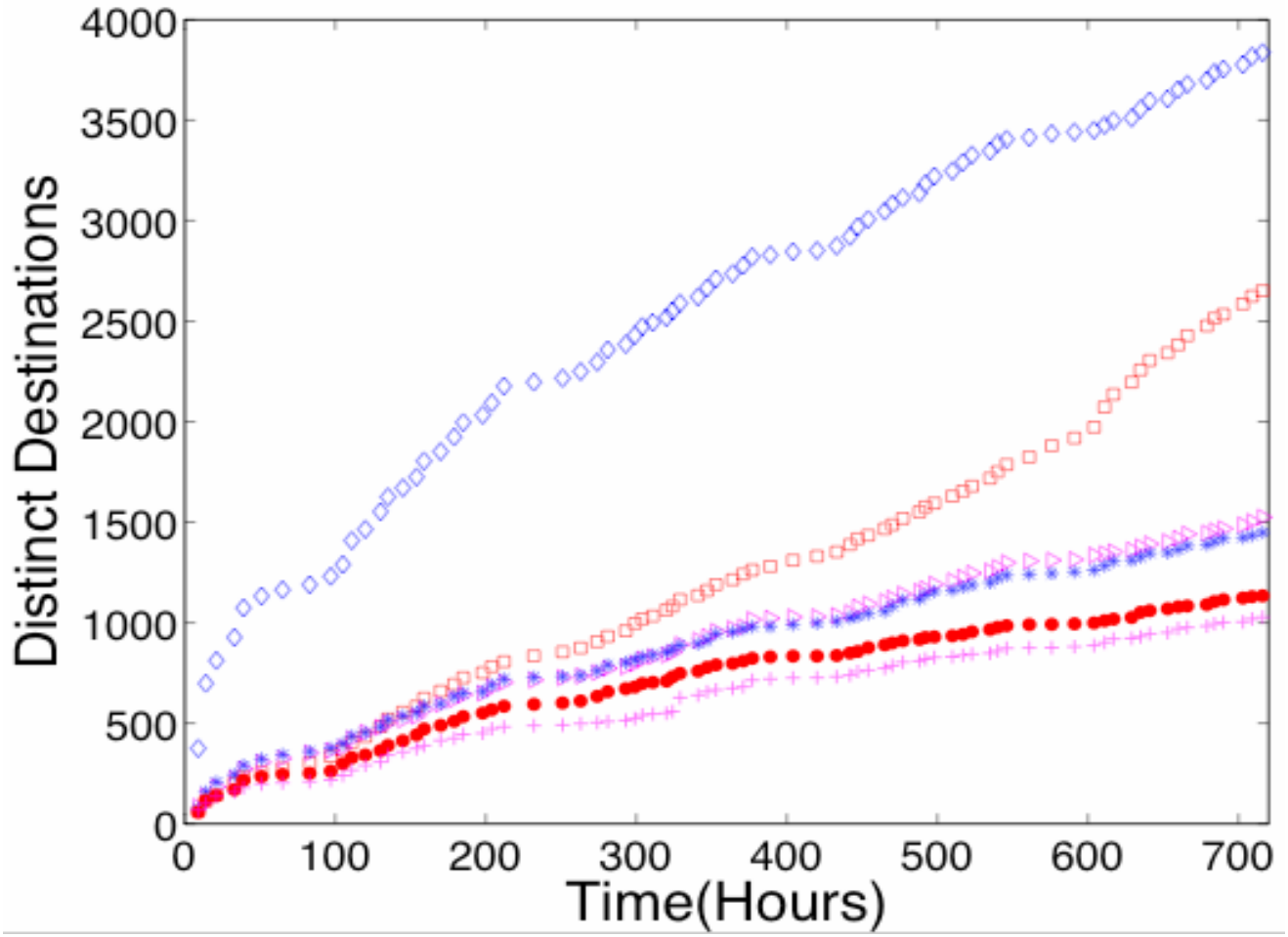
CWSA



Comparison with Virus Throttling

- Virus Throttling:
  - Rate limit of outgoing connections to 1 scans/sec
  - Slow worms will elude detection
- Worm Containment:
  - Limit the *total number* of outgoing connections to a predefined limit M over a *long period of time*
  - Do not need instantaneous rate control, thus less intrusive
  - Slow worms will be contained

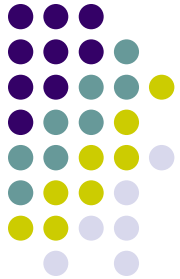
Six Most Active Hosts over 30 days



Source: Thirty Days' Wide Area TCP Connections http://ita.ee.lbl.gov/html/contrib/LBL-CONN-7.html

PURDUE UNIVERSITY

CWSA



Deployment Scenarios

- Host Based
  - Each individual host monitors its outgoing connections to distinct IP addresses
  - Disconnect self from the network when the number of scans exceeds the pre-defined limit M
  - Compared to virus throttling, our scheme is non-intrusive and also effective against slow scan worms
- May be deployed on edge routers
- Not be suitable for deployment at core routers

PURDUE UNIVERSITY

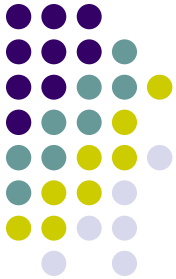
CWSA

Performance (Code Red)

- Our Containment System (M = 7500):
  - Host based
  - With high probability (0.95), the total infections will be less than 50 hosts (0.015%).
- DIB/TRAN Detection:
  - Implemented on a set of carefully chosen routers
  - Detect worm activities when there are 0.03% of total infections(108 infected hosts).

PURDUE UNIVERSITY

CWSA



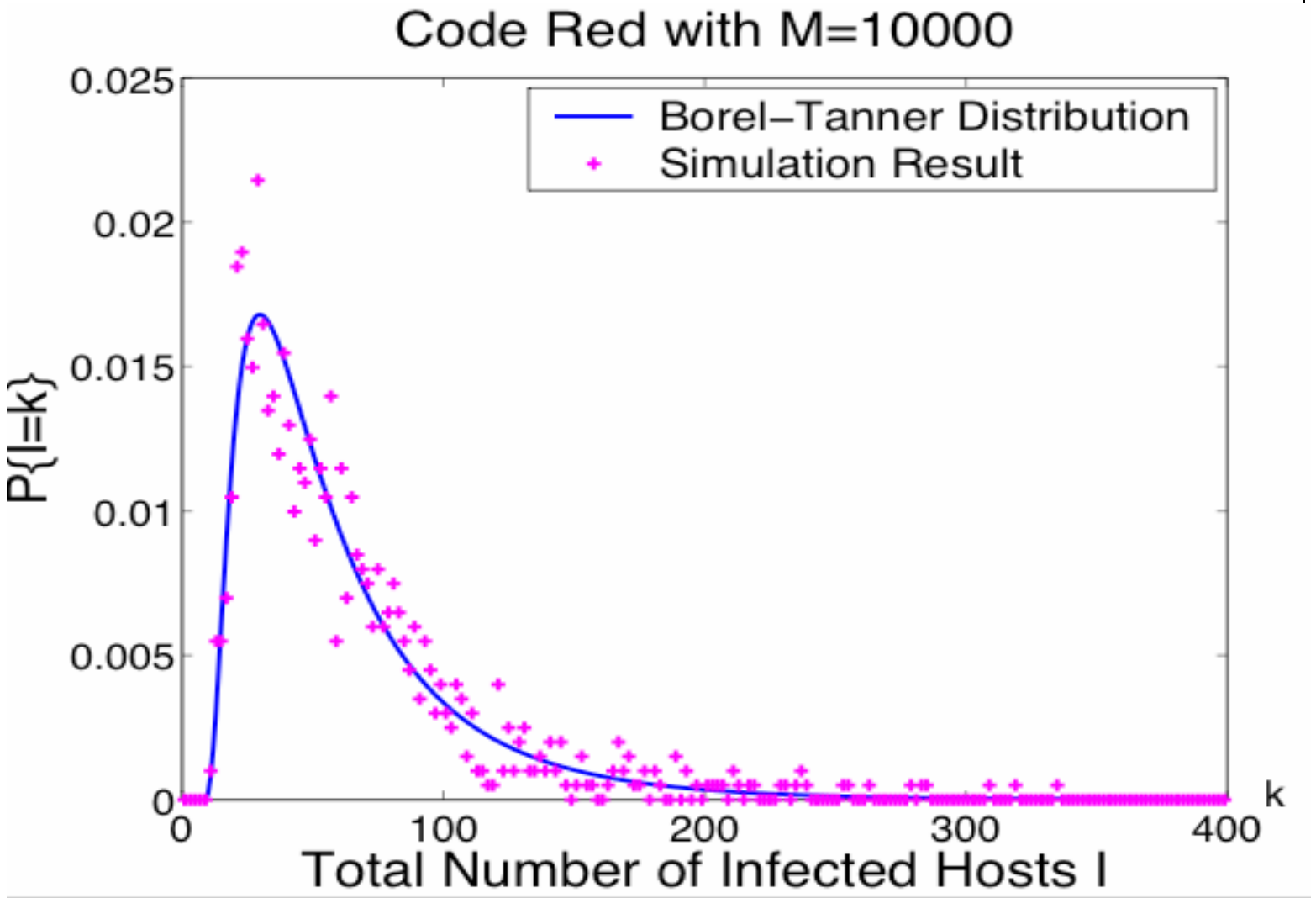
Simulation

- Discrete Event Simulator
  - Input Parameters:
    - V: vulnerable population size
    - I_0: number of initial infected hosts
    - M: maximum number of scans an infected host perform before it is removed.
  - Output Parameters:
    - Total number of infected hosts
    - Number of active infected hosts, removed hosts, accumulated total number of infected hosts.
- Simulations runs: 1000

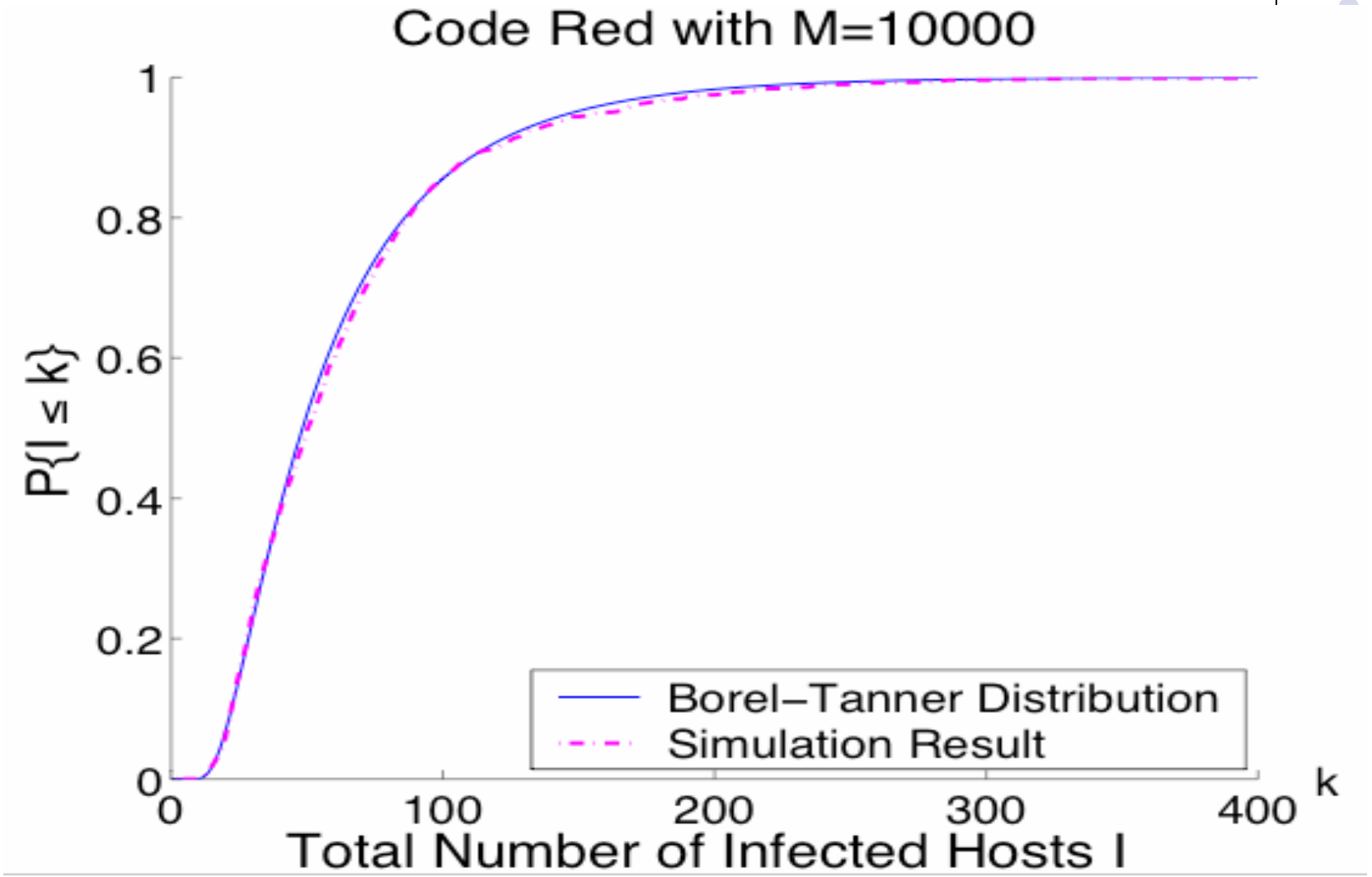
PURDUE UNIVERSITY

CWSA

Simulation Results



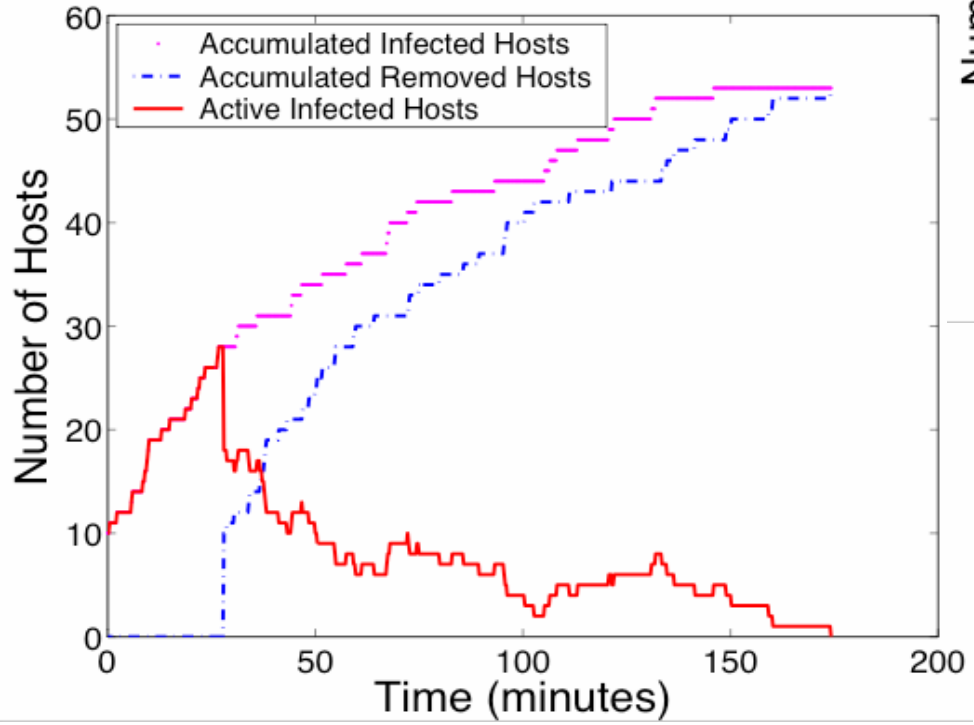
Simulation Results

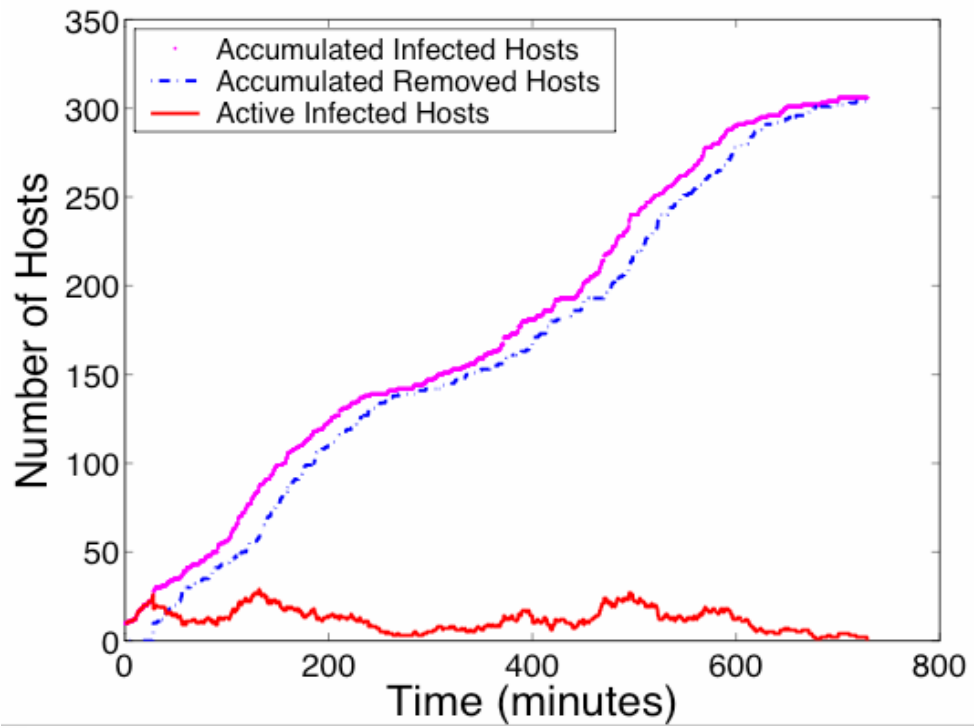


PURDUE UNIVERSITY

CWSA

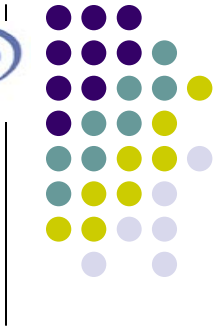
Sample Paths





PURDUE UNIVERSITY

CWSA

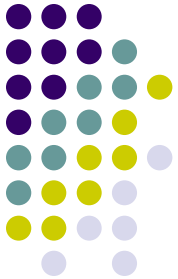


Conclusion

- Developed a branching process model to characterize the early phase propagation of scanning worms
  - Provide a precise bound M on the total number of scans that determines whether the worm will eventually die out.
  - Obtained probability that the total number of hosts that worm infects below a certain level

PURDUE UNIVERSITY

CWSA



Conclusion

- Developed an effective and automatic worm containment strategy.
  - Non-intrusive - legitimate traffic will not be affected.
  - Can contain both fast worms and slow worms
  - No need to know the worm signature in advance
  - No need to explicitly detect the worm

PURDUE
UNIVERSITY

CWSA

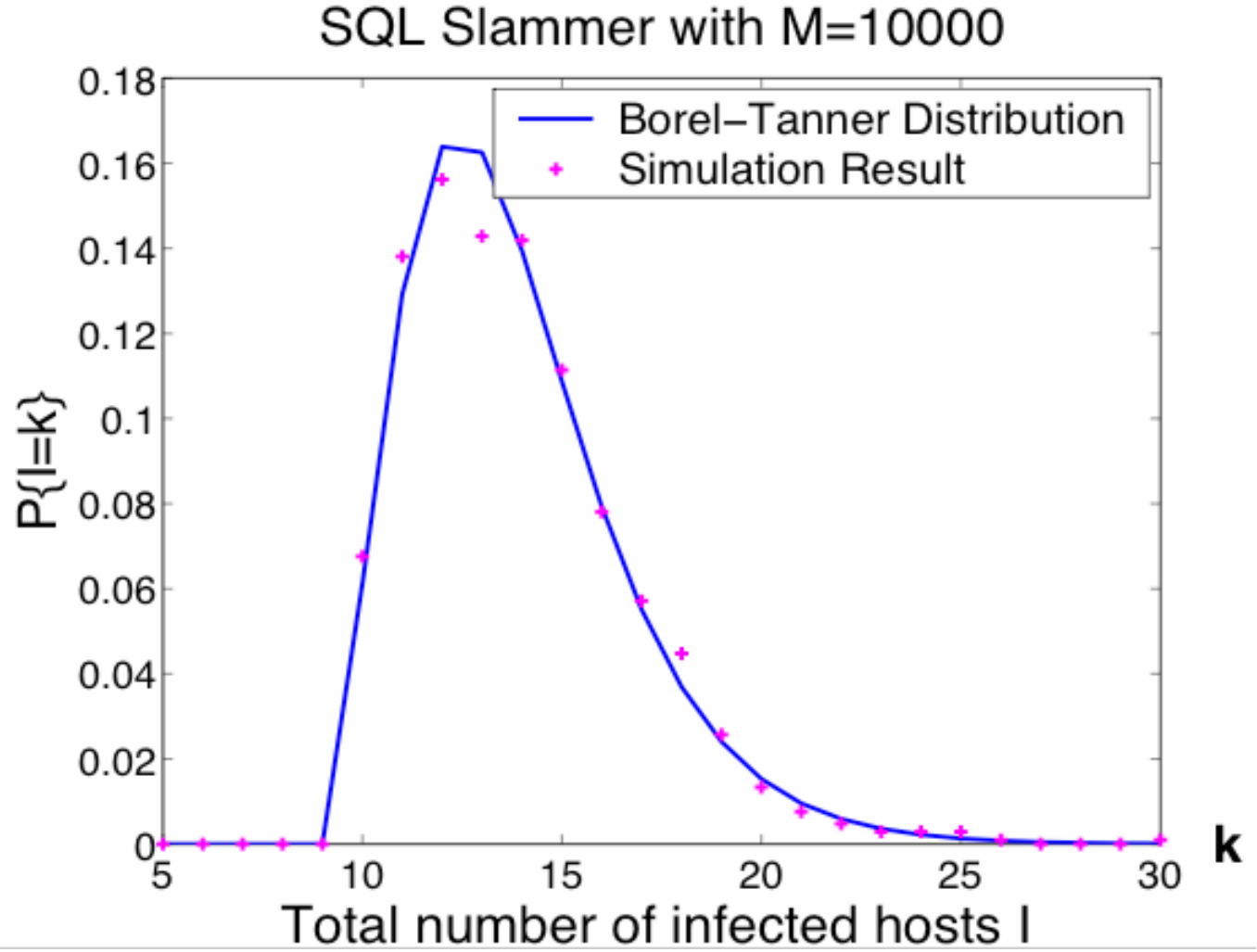
Future Work

- Extend our strategy to model and contain preference scanning worms
- Incremental deployment of the worm containment strategy

PURDUE UNIVERSITY

CWSA

Back Up Slide



PURDUE UNIVERSITY

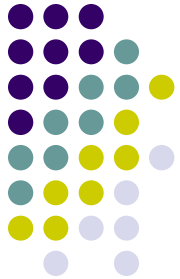
CWSA

Notations for Reference

Symbol	Explanation
V	The size of the vulnerable hosts
p	$p = \frac{V}{2^{32}}$, the density of the vulnerable hosts
M	The total number of scans by each infected host
ξ	Random number of offsprings generated by each infected host
$\xi_k^{(n)}$	Number of offsprings produced by k^{th} host in n^{th} generation
I_0	Number of initial infected hosts
I_n	Number of n^{th} generation infected hosts
I	Total number of all infected hosts $[I = \sum_{n=0}^{\infty} I_n]$
π	Extinction probability
P_n	Extinction probability at n^{th} generation

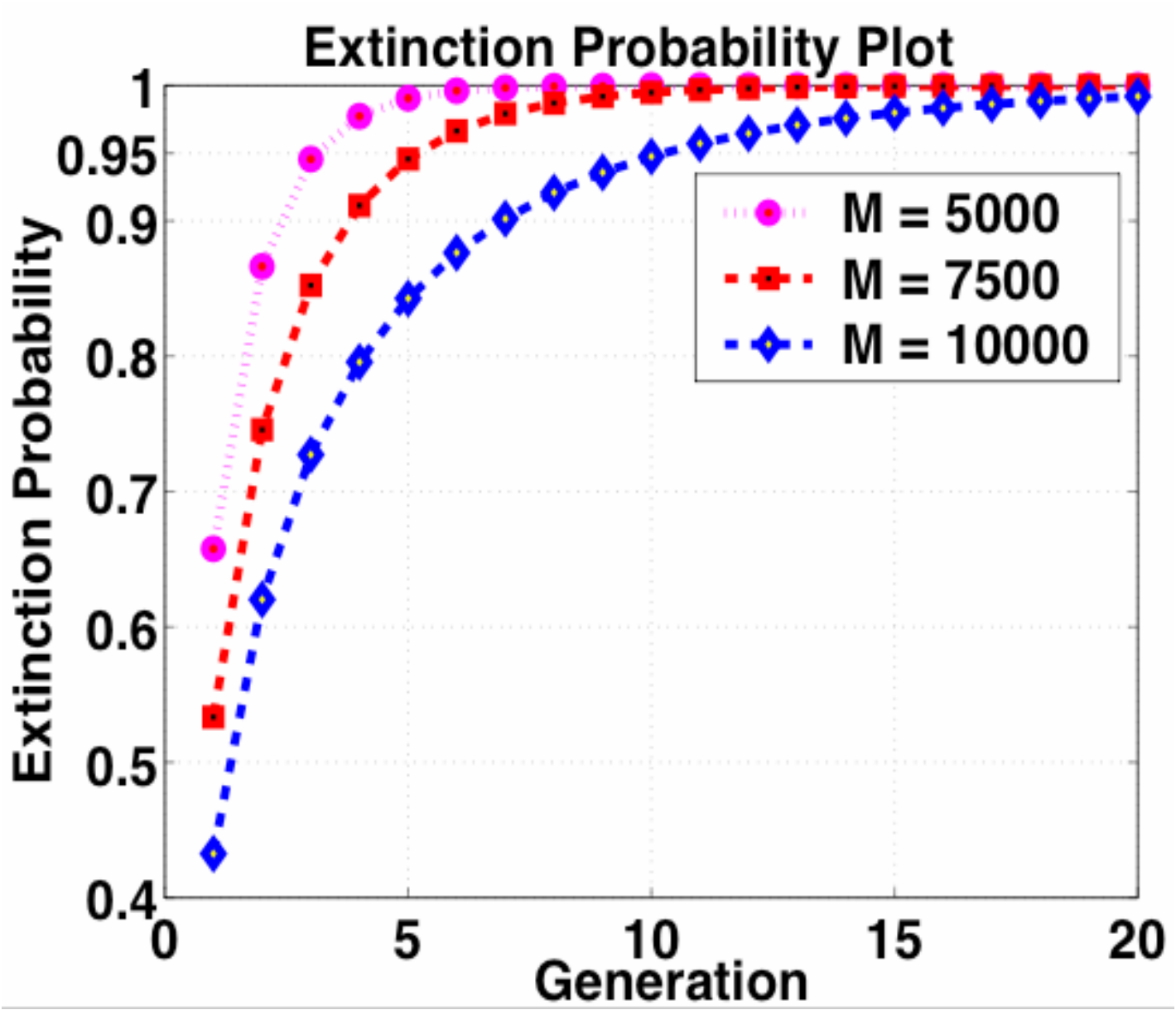
PURDUE UNIVERSITY

CWSA



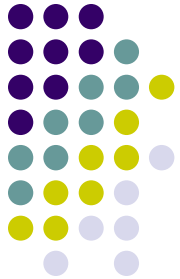
Our Goals

- Develop an accurate model for the early phase of worm propagation
  - Provides insights for controlling the worm spread
  - Existing deterministic models are not adequate
- Develop a robust automatic worm containment strategy
  - Non-intrusive - legitimate traffic not affected
  - Contain both fast scanning worms and slow scanning worms


Extinction Probability Plot
Extinction Probability
Generation
1
0.95
0.9
0.8
0.7
0.6
0.5
0.4
0
5
10
15
20
M = 5000
M = 7500
M = 10000

PURDUE UNIVERSITY

CWSA



Performance (SQL Slammer)

- SQL Slammer with $I_0 = 10$
  - If M = 10,000, with high probability, no more than 10 additional hosts will be infected.
  - If M = 5000, with high probability, no more than 4 additional hosts will be infected
- DIB/TRAN detection: 0.005% (6 infections)