A Closed-Form Expression for Static Worm-Scanning Strategies

Zesheng Chen

Florida International University

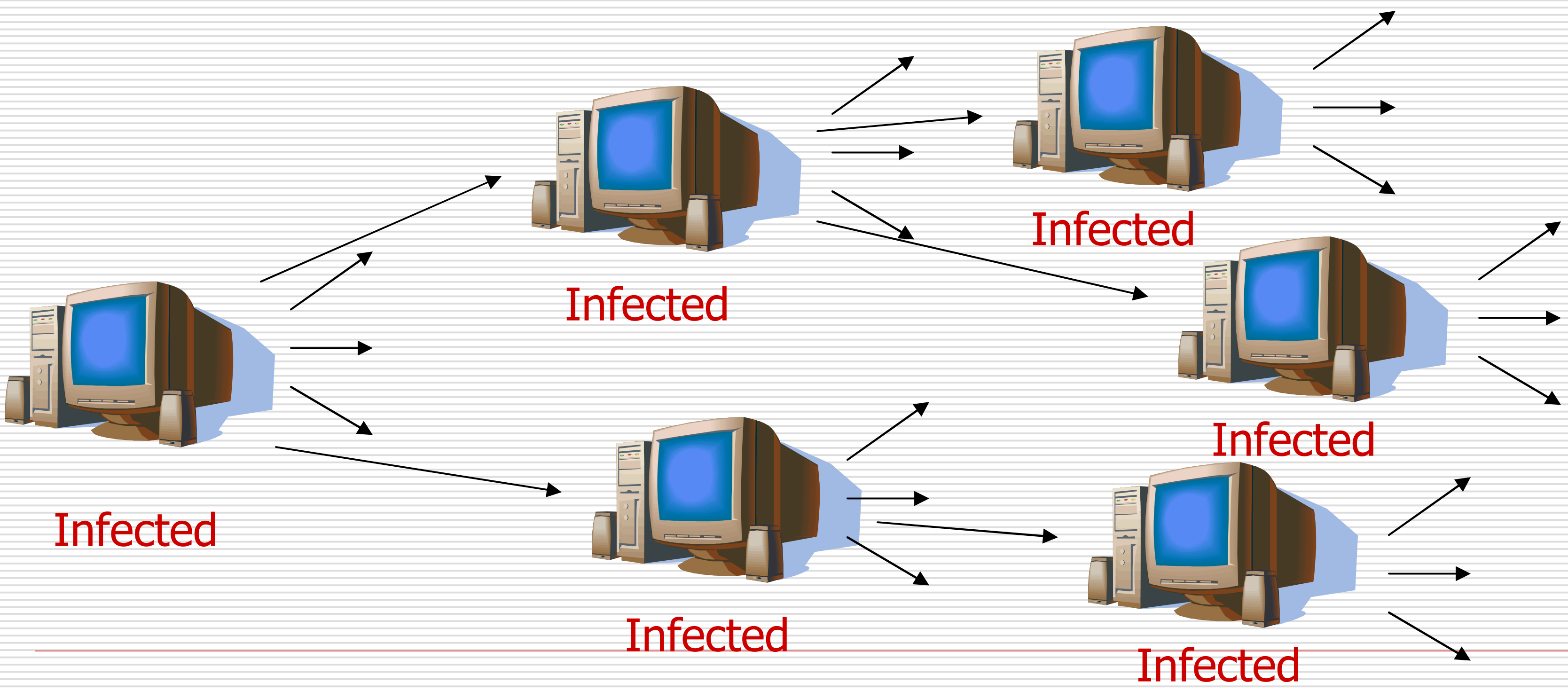
Chao Chen

Indiana University – Purdue University Fort Wayne

IEEE International Conference on Communications (ICC 2008)
May 21, 2008, Beijing, China

Worm Propagation

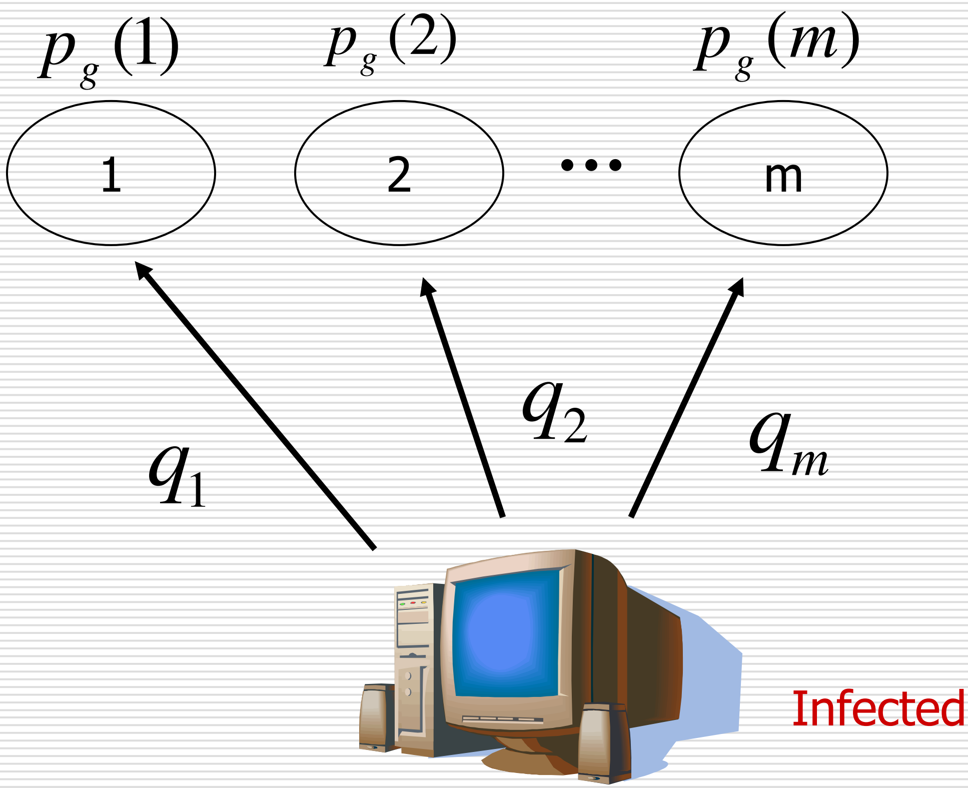
- Worm is a program that self-propagates across Internet by exploiting security flaws



Worm Scanning Methods

- Random scanning
  - Selects target IPv4 addresses at random
  - Code Red v2, Slammer, and Witty worms
- Localized scanning
  - Preferentially searches for targets on “local” address space
  - Code Red II and Nimda worms
- Sequential scanning
  - Scans IP addresses sequentially
  - Blaster worm

Importance Scanning



- $p_g(i)$: group distribution

$$p_g(i) = \frac{N_i}{N}$$

- q_i: group scanning distribution

Importance Scanning

- Has shown to be able to spread worms much faster than random scanning
- Has two types
  - Static importance scanning
    - OPT-STATIC and random scanning
  - Dynamic importance scanning
    - Localized scanning and K-FAIL

In this work, we focus on static importance scanning

Motivations

- Why studying worm-scanning methods is important?
- Worm attacks present a significant threat
- Many applications have used epidemic-style information dissemination
  - Database maintenance
  - Streaming broadcasting
  - Web-service management

M. Vojnovic, V. Gupta, T. Karagiannis, and C. Gkantsidis, "Sampling Strategies for Epidemic-Style Information Dissemination," IEEE INFOCOM, 2008.

Model Worm Propagation

- Stochastic models
  - Capture the variance of worm spreading at the early stage
  - Require extensive computations and focus only on the early stage
- Deterministic models
  - Ignore the variance of worm infection and use dynamic equation
  - Difficult to understand the effects of important parameters
  - Nearly impossible to derive an exact closed-form expression from the dynamic equation

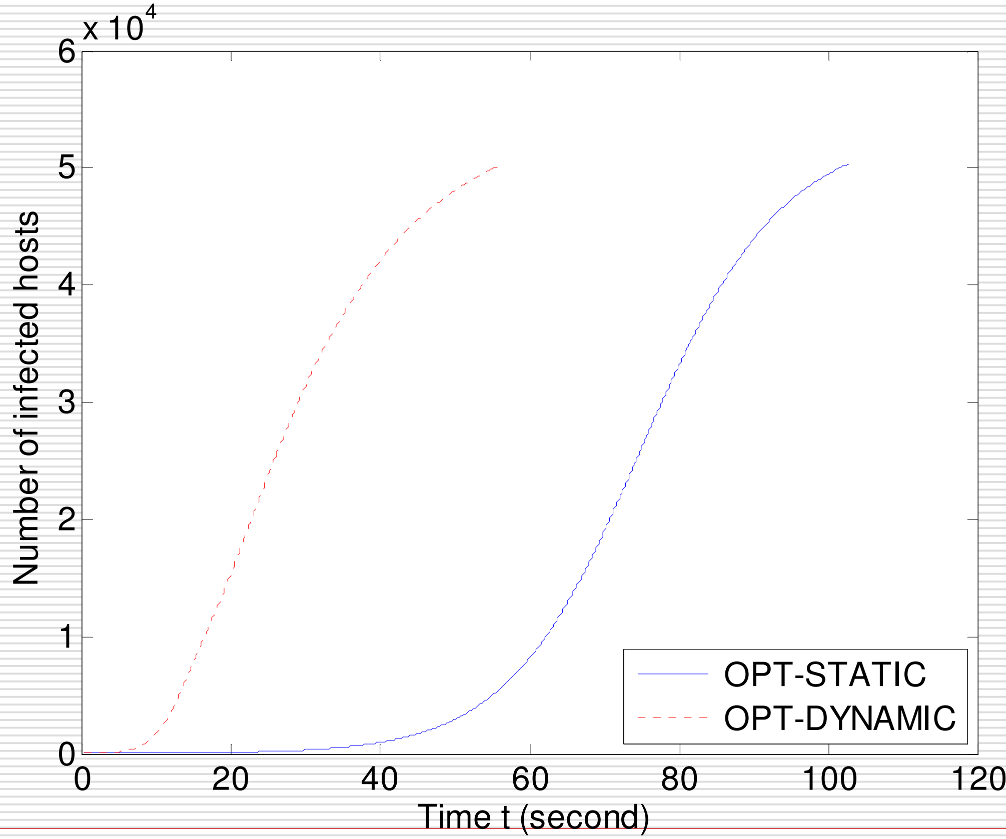
Model Worm Propagation

- Optimization methods
  - Capture parameters' effects
  - Focus on the number of worm scans required to reach a predetermined fraction of vulnerable hosts
  - Cannot characterize the dynamic behavior of worm spreading

In this work, we derive a closed-form expression from the deterministic dynamic equation through a *mean-field* approximation

Why Not *Optimization*

Focus on the number of worm scans required to reach a predetermined fraction of vulnerable hosts



M. Vojnovic, V. Gupta, T. Karagiannis, and C. Gkantsidis, “Sampling Strategies for Epidemic-Style Information Dissemination,” IEEE INFOCOM, 2008.

Mean-Field Approximation

- Gains insight into the behavior of complex systems at a relatively low cost
- Focuses on the average of the system, ignoring fluctuations
- Applies Taylor expansion and focus on the first-order term

Derivation

Dynamic differential equation: $$\frac{dI_i(t)}{dt} = sI(t)q_i \frac{S_i(t)}{\Omega_i}$$

Mean-field approximation: $$I_i(t) = N_i\left[1-\left(1-\frac{1}{\Omega_i}\right)^{q_i u(t)}\right]$$

Taylor expansion (first term): $$\approx u(t)\frac{q_i N_i}{\Omega_i}$$

Close-Form Expression

$$I(t) = \frac{I(0)B}{I(0) + [B - I(0)]e^{-At}}$$

$$A = s\sum_{i=1}^{m} q_i N_i / \Omega_i$$

$\uparrow$

Infection rate

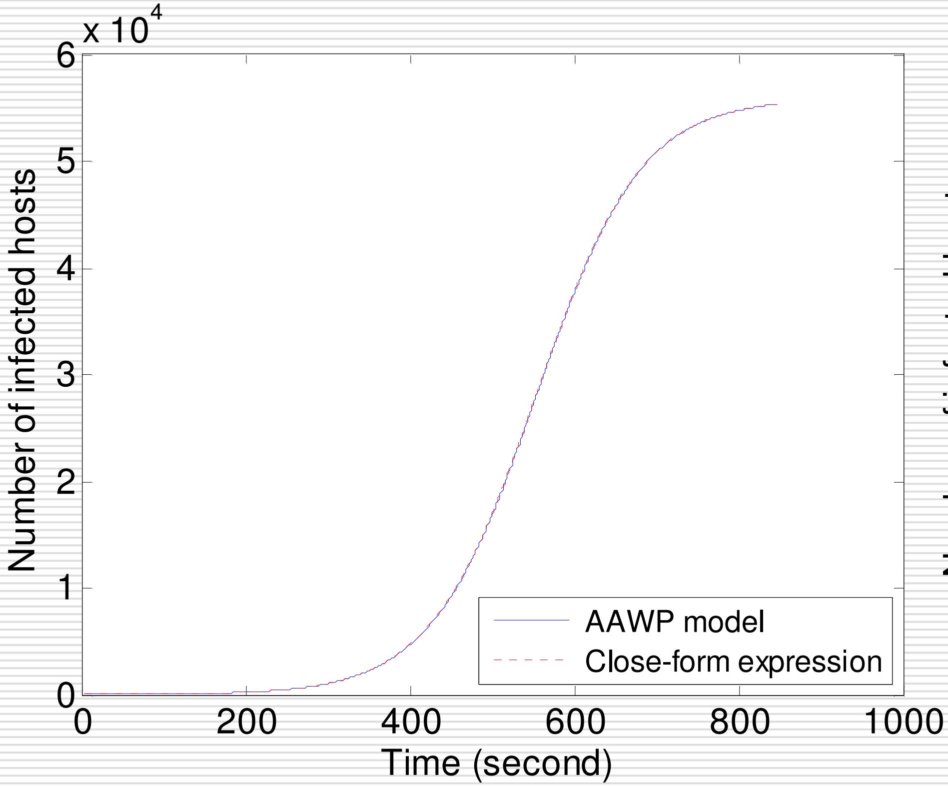
$$B = \frac{\left(\sum_{i=1}^{m} q_i N_i / \Omega_i\right)^2}{\sum_{i=1}^{m} q_i^2 N_i / \Omega_i^2} \le N$$

Performance Evaluation

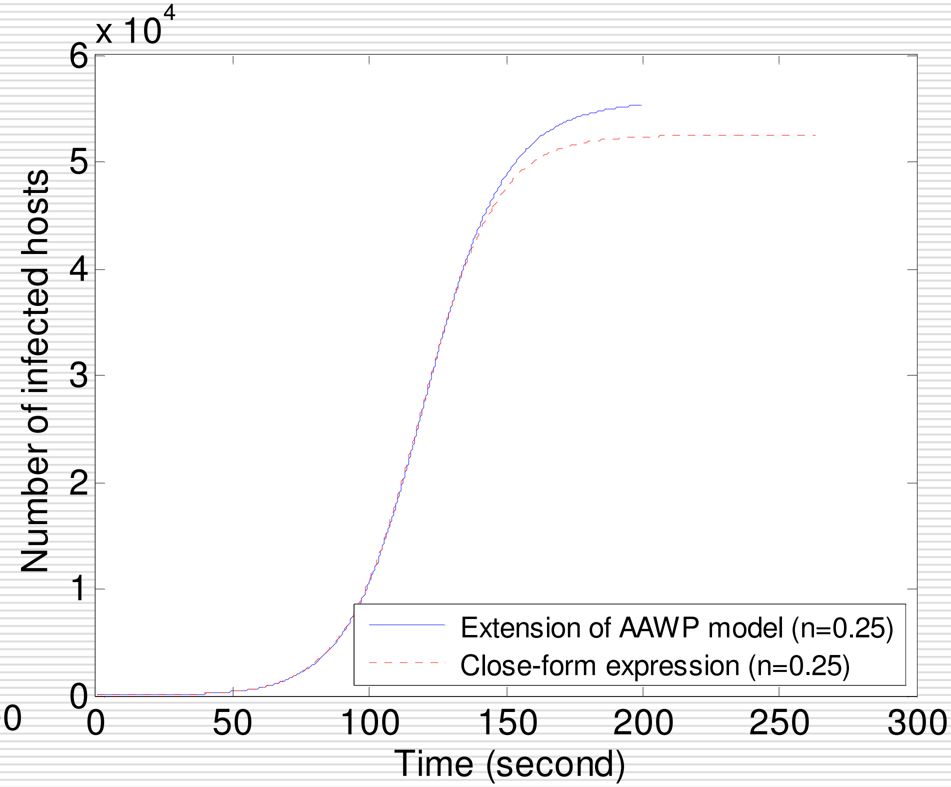
- Simulate the propagation of a Witty worm
  - Vulnerable population N = 55,909
  - Scanning rate s = 1,200 /sec
- Compare with the Analytical Active Worm Propagation (AAWP) model
- Consider a group of static worm-scanning strategies:

$$q_i \propto \left(\frac{N_i}{N}\right)^n$$

Performance Evaluation

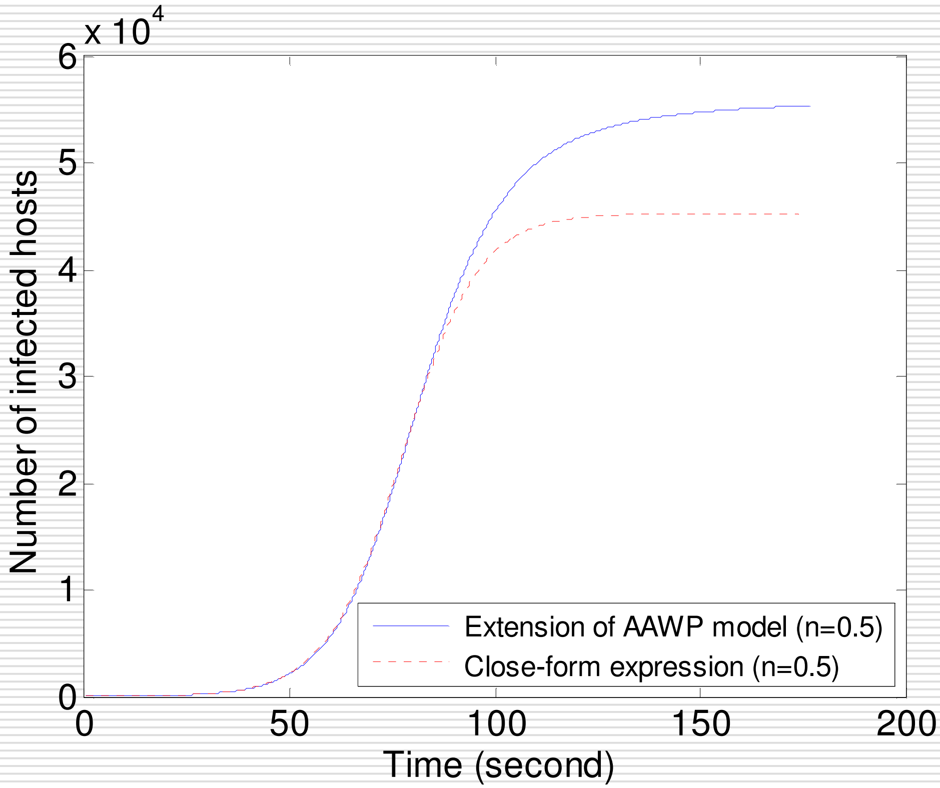


n = 0

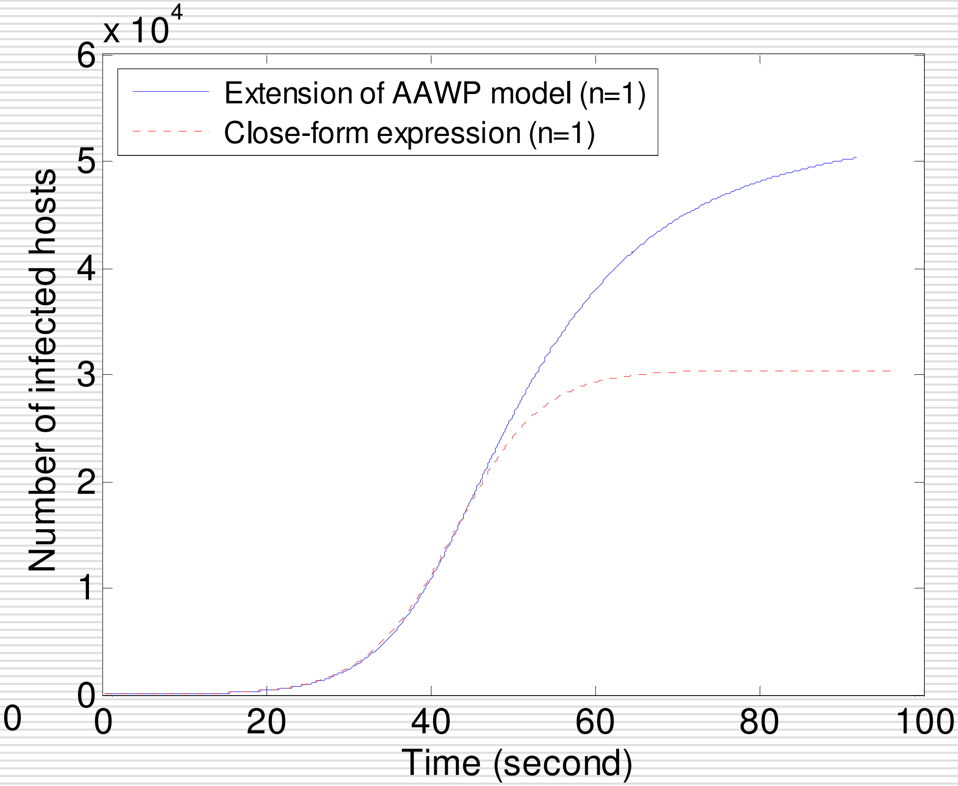


n = 0.25

Performance Evaluation

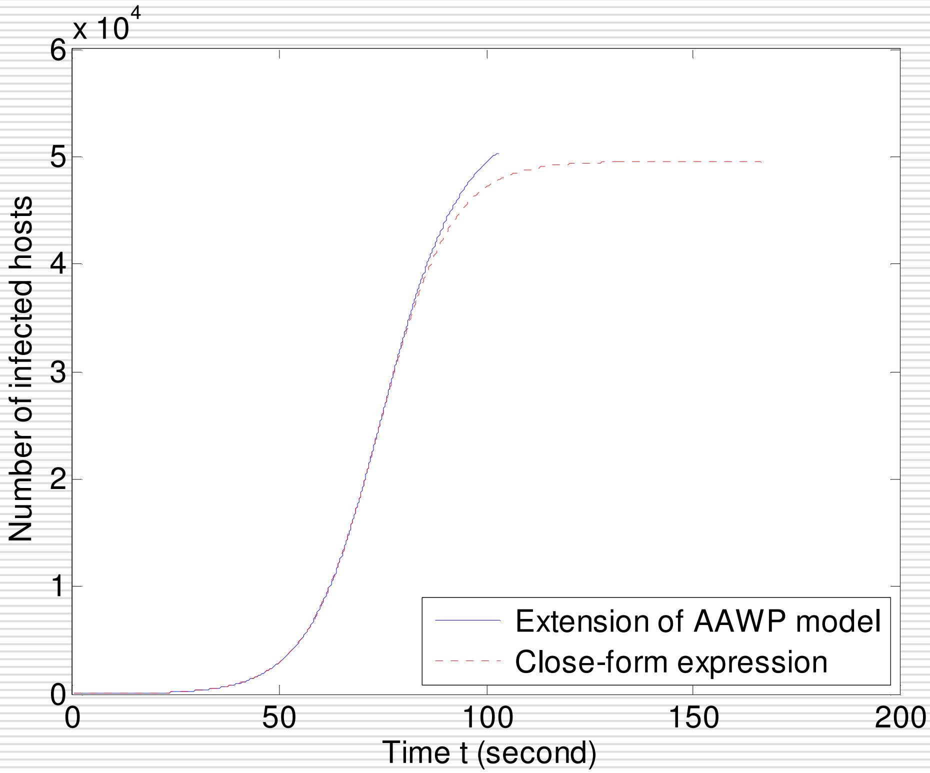


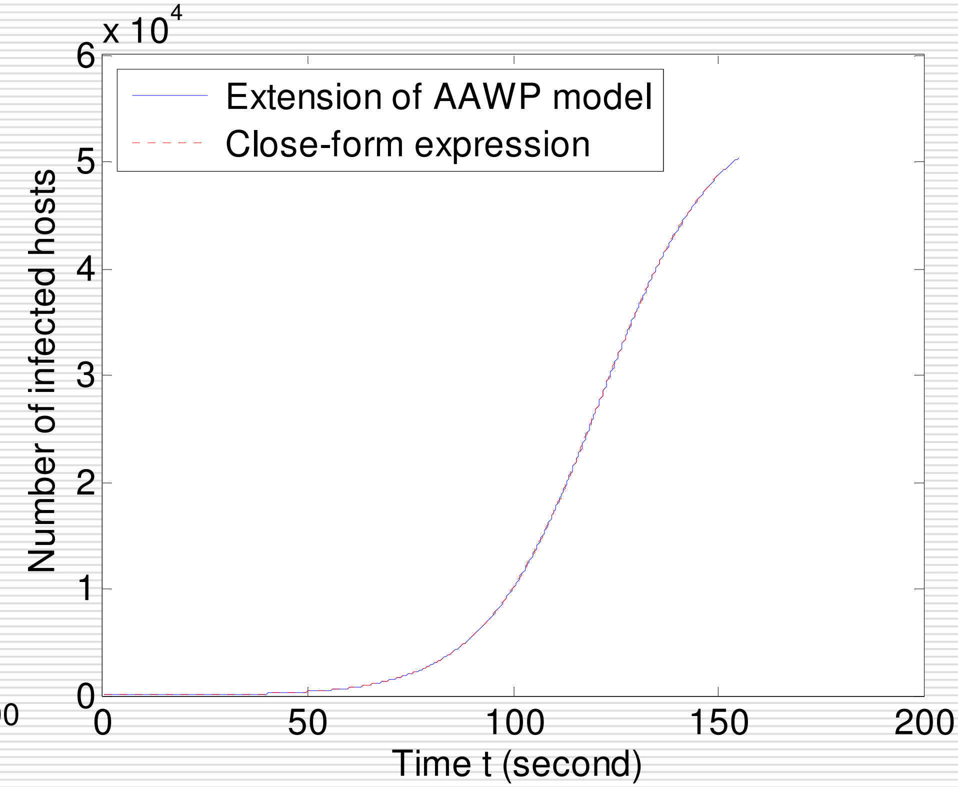
n = 0.5



n = 1

Performance Evaluation





OPT-STATIC

Uniform random sampling
Of a subset of subnets A

M. Vojnovic, V. Gupta, T. Karagiannis, and C. Gkantsidis, "Sampling Strategies for Epidemic-Style Information Dissemination," IEEE INFOCOM, 2008.

Conclusions and Future Work

- Present a closed-form expression
  - Mean-field approximation
- Both accurately characterize worm propagation before the late stage and explicitly capture the effects of the vulnerable-host distribution and the worm-scanning method
- Study the closed-form expression for dynamic worm-scanning methods

Thanks for your attention