



# Modeling and Analysis of Worm Interactions (War of the Worms)



Sapon Tanachaiwiwat\* and Ahmed Helmy\*\*

\*Ming Hsieh Department of Electrical Engineering  
University of Southern California  
tanachai@usc.edu

\*\*Computer and Information Science and Engineering  
University of Florida  
helmy@ufl.edu

Web site: <http://nile.cise.ufl.edu>



# Outline

- Motivation
- Related work
- Worm Interaction Model
- Simulation results and metrics
- Factors





# Motivation

- Since 1988, the worm epidemics become major problems for the Internet users.
- Slammer worms infected > 65 k hosts in less than 10 minutes
- What can counter such an extreme attack?
- **Some worms try to stop opposing worms' propagation → "War of the Worms"**
  - Propagate to the same targeted vulnerable hosts to terminate/patch the opposing worms
  - Example: Welchia terminates Blaster, Code Green terminates Code Red, NetSky terminates MyDoom
- **Goal: Mathematically understand the dynamic of worm interactions and derive the *necessary condition(s)* to stop the worm outbreak**





# Related work

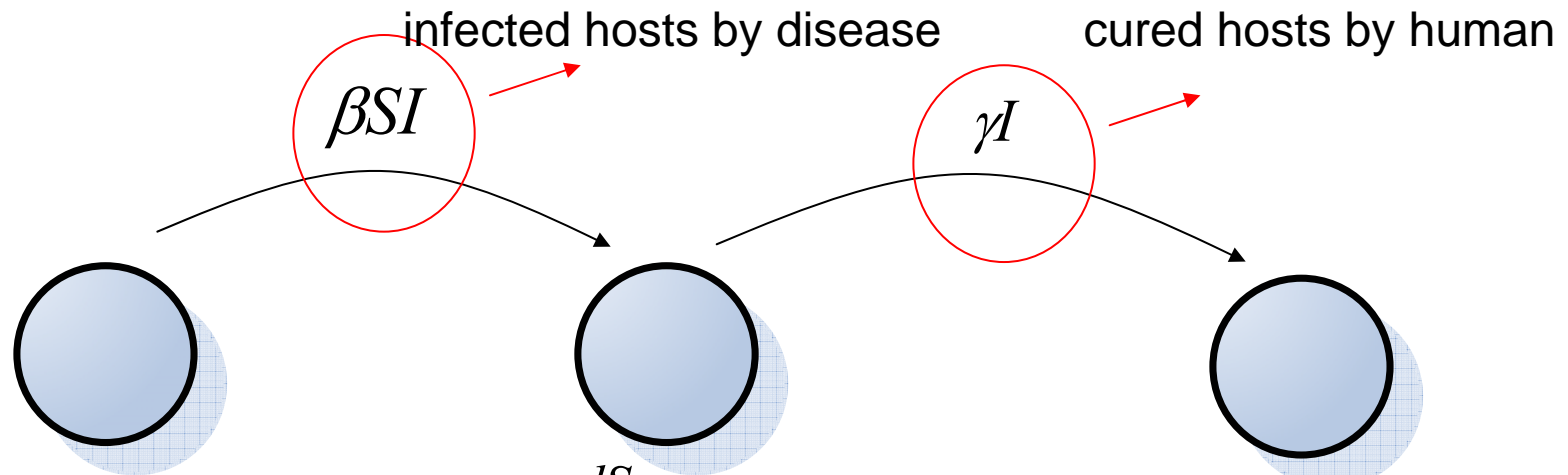
- SIR model [Frauenthal,88 ]
  - Mathematical model to explain contagious disease
  - (+) Extendable to complex interaction
- Worm propagation model
  - Code Red [Zou, ACM CCS 02], Slammer [Weaver, ACM WORM 04]
  - Future worms e.g. Flash worm [Staniford, ACM WORM 04], Adaptive worm [Zhao, SSS 06]
- Automated worm generation [Castaneda, ACM WORM 04]
  - Worm reverse-engineering with basic protocols.
  - (+) Fundamental framework for active response
  - (-) Static protocol

**None of these work focus on understanding the worm interactions**





# BASIC: SIR Model



$$\frac{dS}{dt} = -\beta SI$$

$$\frac{dI}{dt} = \beta SI - \gamma I$$

$$\frac{dR}{dt} = \gamma I$$

$$E_0 = \frac{\beta S}{\gamma}$$

$E_0 < 1 \rightarrow$  no outbreak

Plaque, Cholera  
in fixed population

Where  $S=S(t)$ =Susceptible hosts at time  $t$

$I = I(t)$  =Infected hosts at time  $t$

$R = R(t)$  = Removed (cured) hosts at time  $t$

$\beta$ = Contact rate

$\gamma$ = Removal rate

$E_0$  = Epidemiological Threshold

**Powerful mathematical model extendable to our worm interaction models**





# Descriptions: Worm Interactions

- One-sided Interaction
  - Aggressive Interaction
    - Similar to Welchia/Blaster, Automated beneficial worm generation
    - Predator terminates/patches prey and patches (vaccinate) susceptible hosts

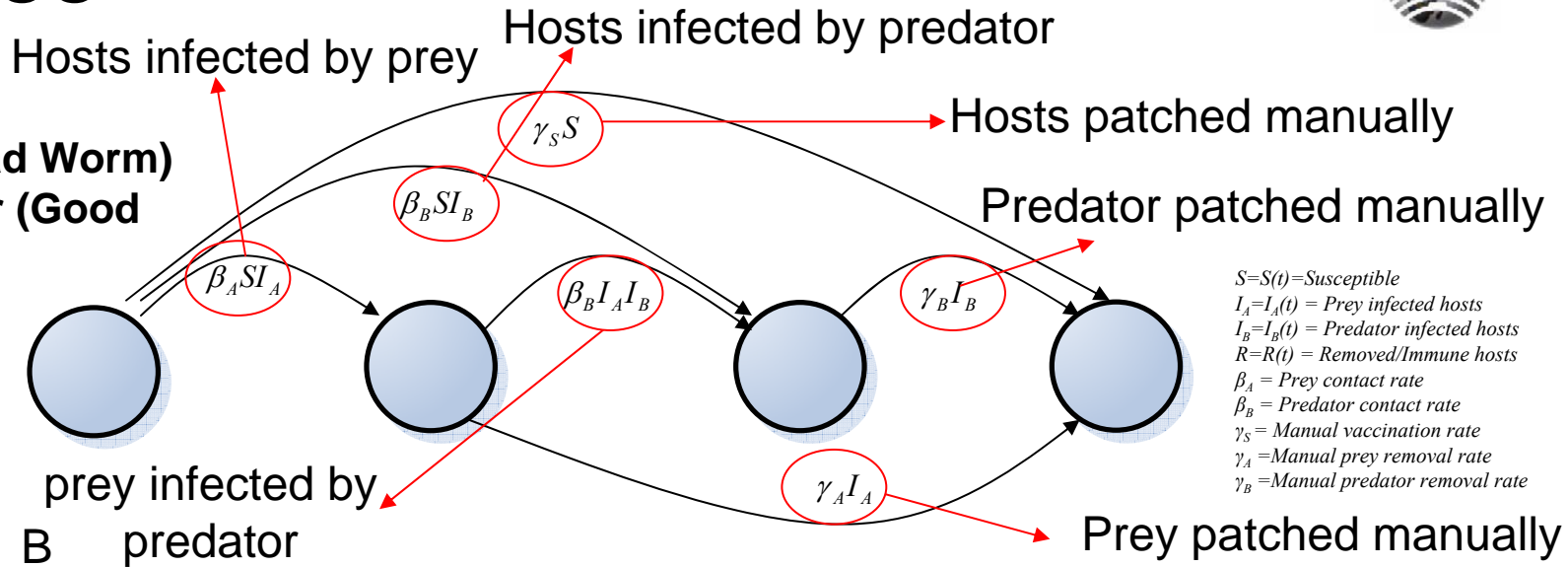
Note: All worms share the same set of vulnerable hosts



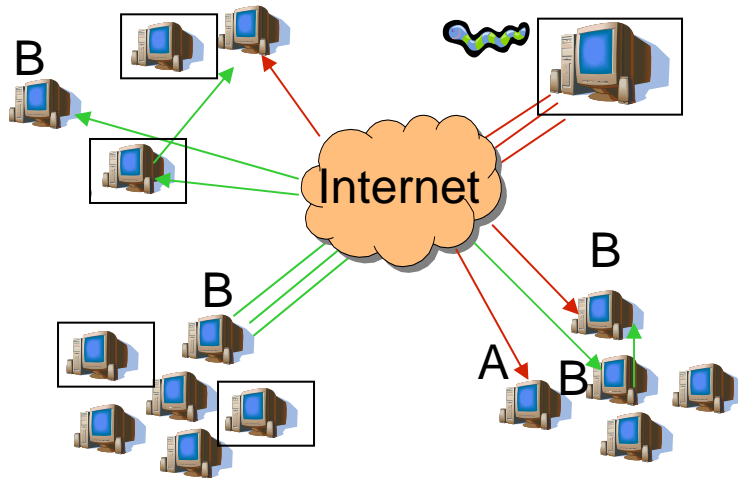
# Aggressive One-sided Interaction



**A = Prey (Bad Worm)**  
**B = Predator (Good Worm)**



$S=S(t)$  = Susceptible  
 $I_A=I_A(t)$  = Prey infected hosts  
 $I_B=I_B(t)$  = Predator infected hosts  
 $R=R(t)$  = Removed/Immune hosts  
 $\beta_A$  = Prey contact rate  
 $\beta_B$  = Predator contact rate  
 $\gamma_S$  = Manual vaccination rate  
 $\gamma_A$  = Manual prey removal rate  
 $\gamma_B$  = Manual predator removal rate



$$\frac{dS}{dt} = -\beta_A S I_A - \beta_B S I_B - \gamma_S S$$

$$\frac{dI_A}{dt} = \beta_A S I_A - \beta_B I_A I_B - \gamma_A I_A$$

$$\frac{dI_B}{dt} = \beta_B S I_B + \beta_B I_A I_B - \gamma_B I_B$$

$$\frac{dR}{dt} = \gamma_S S + \gamma_A I_A + \gamma_B I_B$$

**Prey infection rate derived for Epidemiological Threshold for Prey's outbreak**



# Tunable Parameters



- Scan rate ( $r$ ):
  - Rate at which a worm probes other hosts
- Contact rate ( $\beta$ ):
  - Rate at which a worm replication reaches other hosts ( $F(r)$ )
- Scan Rate Ratio ( $X$ ):
  - Ratio of scan rate between predator and prey
- Initial Infective Ratio ( $Y$ ):
  - Ratio of initial infected hosts between predator and prey

**Needed for predator performance prediction**

S. Tanachaiwiwat USC/ A. Helmy UF



# Aggressive One-sided Interaction



- Epidemiological Threshold for prey

$$E_A = \frac{\beta_A S I_A}{\beta_B I_A I_B + \gamma_A I_A} = \frac{\beta_A S}{\beta_B I_B + \gamma_A}$$

We want  $E_A < 1$  Hence

$$\gamma_A = 0 \rightarrow \frac{\beta_B}{\beta_A} = X > \frac{S(0)}{I_B(0)} = \frac{S(0)}{Y I_A(0)}$$

$X$  = scan rate ratio  
 $Y$  = initial infective ratio

$$Y > \frac{S(0)}{X I_A(0)}$$

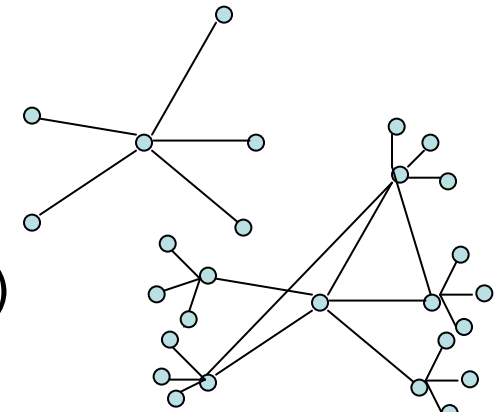
**Prey outbreak does not occur if  $XY > S(0)/I_A(0)$**



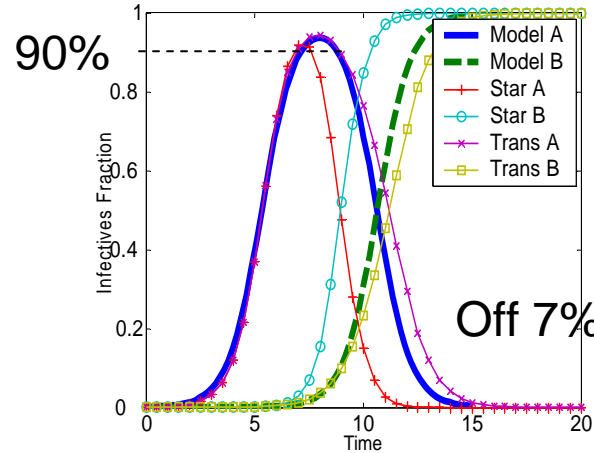
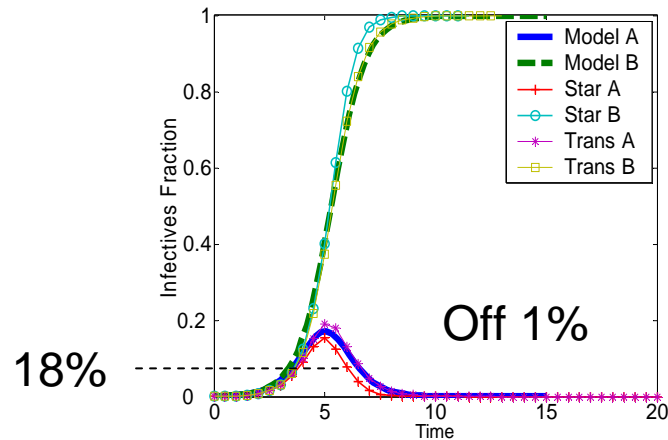


# Simulation

- Network-level simulation (ns-2)
  - 1000 nodes
  - UDP worms (bandwidth limited)
  - Topologies
    - Star topology (512 Kbps, delay 1 ms)
    - Transit-Stub topology (2-level topology)
      - Internet level, AS level
      - 3 outbound bandwidths from local network: 512 Kbps, 1 Mbps, 2 Mbps, average prop. delay 1.5 ms
      - local network bandwidth 10 Mbps, prop. delay 1 ms
  - Scan rate (from 1/sec – 500/sec)



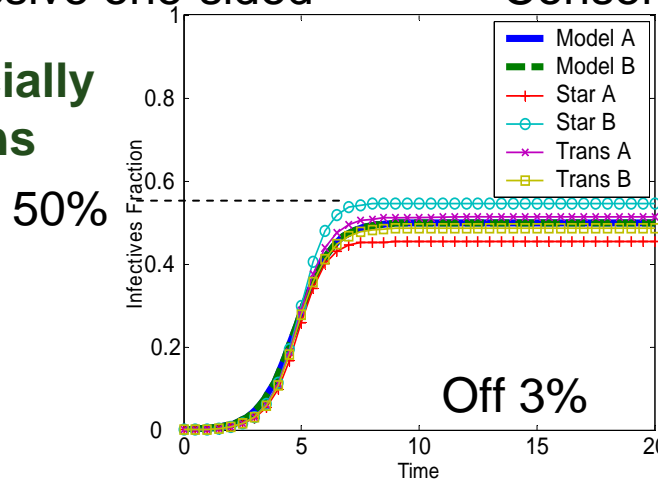
# Model Accuracy



Aggressive one-sided

Conservative one-sided

**Close estimation especially to all type of interactions**



Two-sided

**Maximum prey's infected hosts in different interaction types can be different as much as 500%**





# Metrics

- Effectiveness of predator can be measured (quantified) by prey's
  - Total infectives

$$T = \int_{t=0}^{\infty} \beta_A S I_A dt$$

How many hosts have been infected by prey at least once?

- Individual life span

$$L = \frac{\sum W_t * (1/(\beta_B I_B))}{T}$$

How long does a prey infective live (per host)?

$$W_t = (\Delta \beta_B I_A I_B) - \Delta I_A$$

**Need to minimize total infectives and individual life span as much as possible**





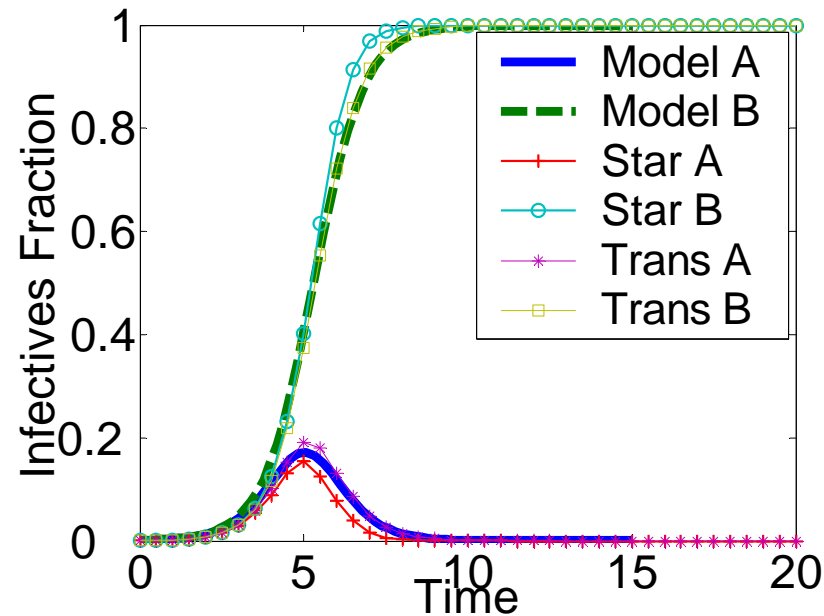
# Factors

- Topology
- Worm replication size and bandwidth between routers
- Scanning Strategies
- Reaction Time



# Factors

- Topology

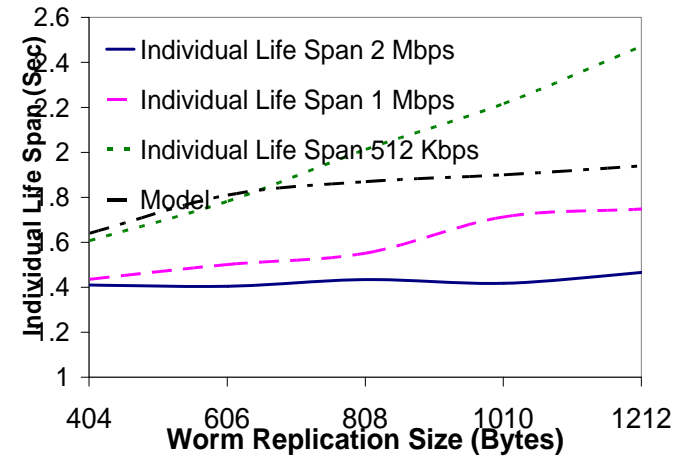
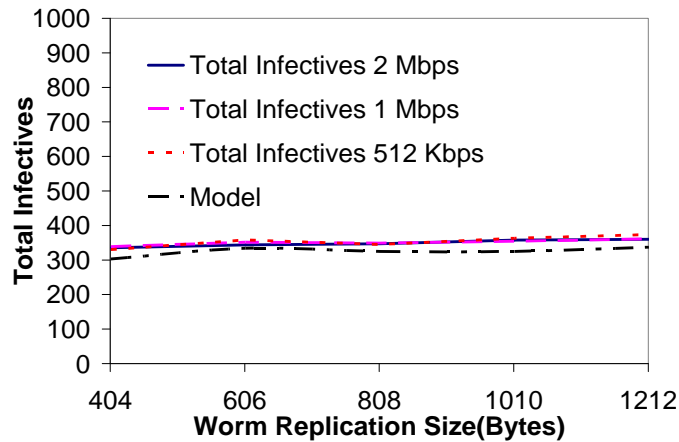


Diff topologies → Diff network delay factor → Diff effectiveness



# Factors

- Worm replication size and bandwidth



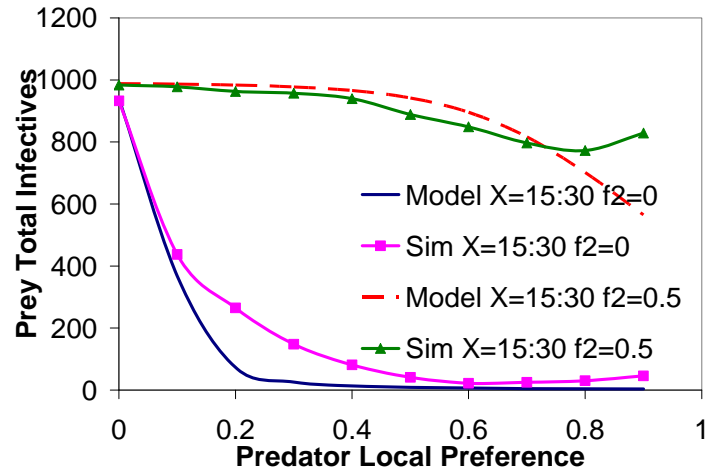
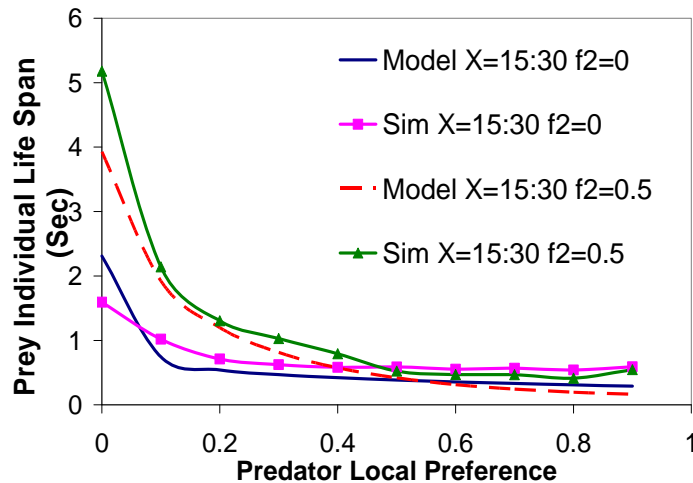
Significant impact on individual lifespan (large replication size and small bandwidth is the worst)





# Factors

- Scanning Strategies



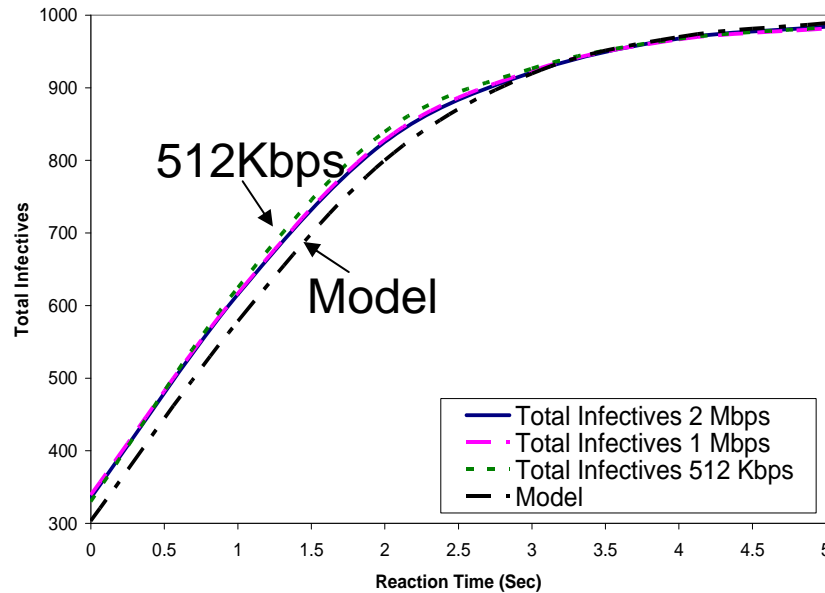
80:20 (local/outside) seems to be the best ratio for chosen scenario



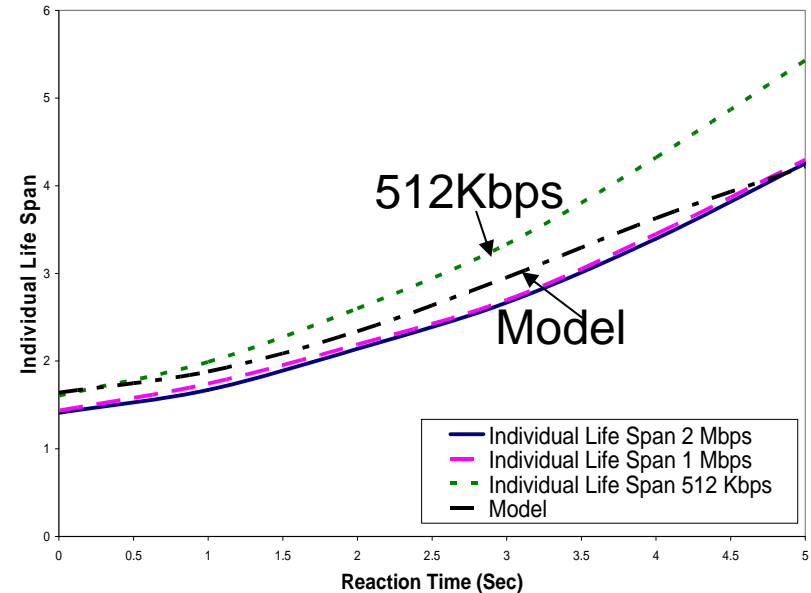


# Factors

- Reaction Time (time after first prey launched)



Off by 4%



Off by 9%

When compared with 512 kbps network

**Growth rate of total infectives down with the increase of reaction time**  
**Growth rate of individual life span up with the increase of reaction time**





# Summary/Contributions

- Network-factor worm interaction models
- Identifying the scan rate ratio/initial host ratio to stop the prey outbreak
- Metrics quantifying effectiveness of beneficial worms
- Future work
  - Worm countermeasure architecture/protocols
  - Worm Interactions in Delay-Tolerant Networks

Link to papers: <http://www-scf.usc.edu/~tanachai>

S. Tanachaiwat USC/ A. Helmy UF

