UNIVERSITY OF
SOUTHERN CALIFORNIA

VACCINE: War of the Worms in Wired and Wireless Networks

Sapon Tanachaiwiwat, Ahmed Helmy

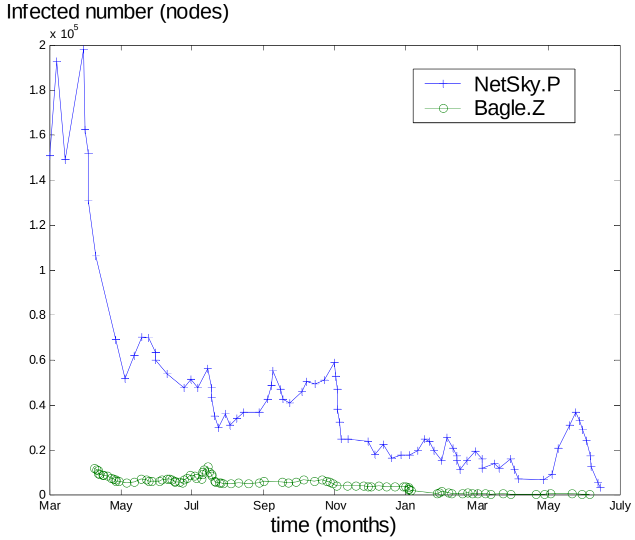
Department of Electrical Engineering

University of Southern California

{tanachai,helmy}@usc.edu

Introduction and Motivation

- Worm is significant threat to wired/wireless computer users
- Worm is self-replicated, usually combined with Trojan, Virus, Backdoor, etc.
- Worm spread **FAST** (even with random scan) usually outpaces human responses, we need something **FASTER!!**
- Worm can be terminated by other opposing worm type e.g. NetSky terminates Bagle (Email worms), CodeGreen terminates CodeRed (Network worms)
- Our work investigates this phenomena by building the model and simulating the scenarios.



Definitions

- Worm Interaction
  - Termination among multiple worm types
    - Indirect interaction
    - One-sided interaction
    - Two-sided interaction
- Scan Rate
  - Rate of worm issuing packet to target or possible susceptible hosts
- Effective Contact Rate
  - Rate of contact between worm and susceptible hosts causing susceptible hosts to be infected by worm (= scan rate / total hosts)
- Infection Rate
  - Rate of change of infected hosts per time unit
- Removed/Recovered Rate
  - Rate of infected hosts being vaccinated or crashed (by the worm) and will not be re-infected per time unit.
- Predator
  - Worm terminating other worm type
- Prey
  - Worm being terminated by other worm type

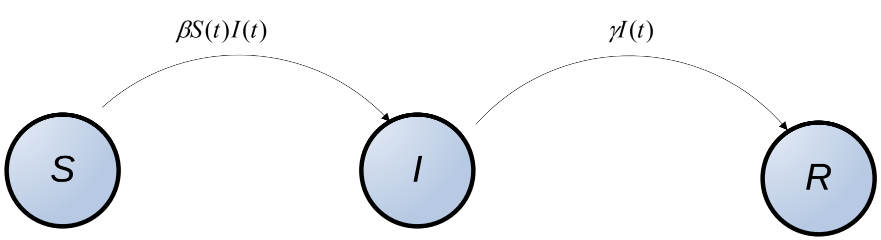
Epidemic Model

- Epidemic Model (SIR)
  - Mathematical model explaining the dynamic of contagious disease (the one we use is SIR or susceptible, infectious, recover model)

$$\frac{dS(t)}{dt} = -\beta I(t)S(t)$$

$$\frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t)$$

$$\frac{dR(t)}{dt} = \gamma I(t)$$



SIR State Transition Diagram

S = Susceptible hosts
I = Infected hosts
R = Recovered/Removed hosts
β = Effective contact rate
γ = Removal rate

Scan Rate Ratio

$$\Gamma_{BA} = \frac{SR_B}{SR_A}$$

- SR_B scan rates of worm type B
- SR_A scan rates of worm type A

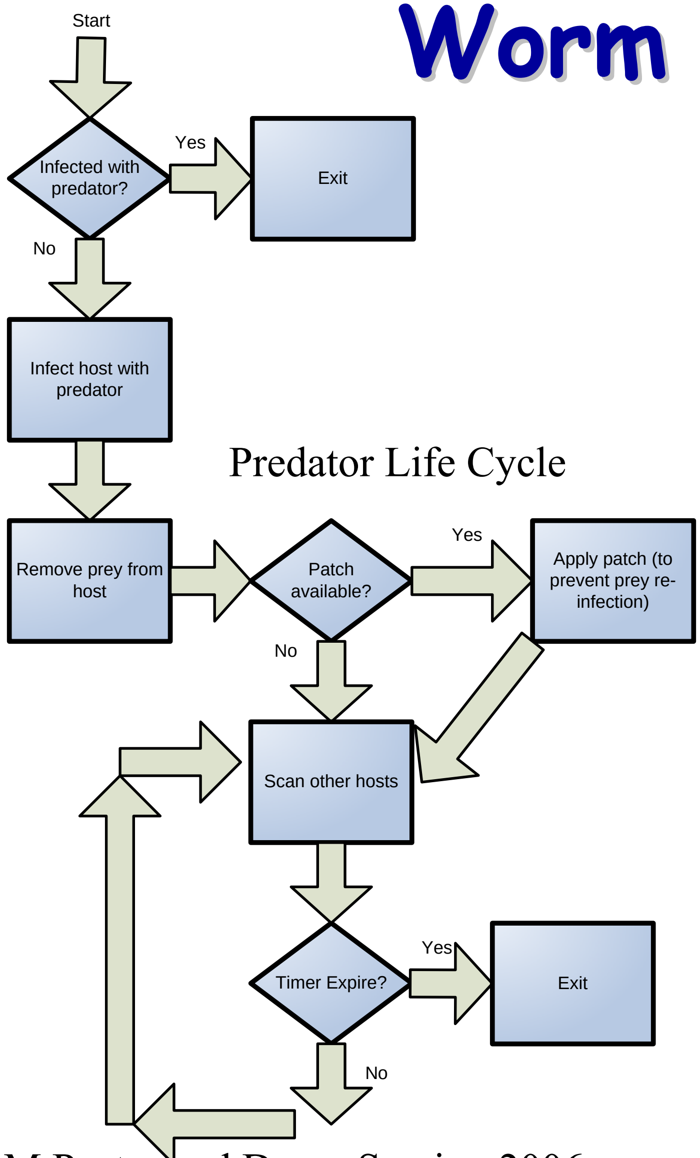
Initial Host Ratio

$$\Lambda_{BA} = \frac{I_{B(0)}}{I_{A(0)}}$$

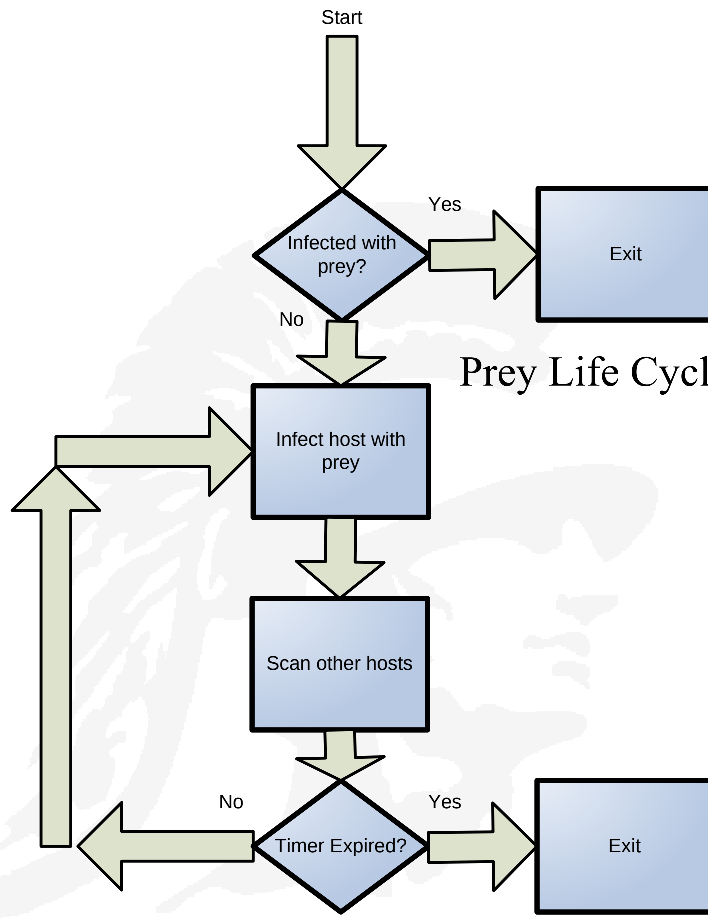
- $I_{B(0)}$ initial hosts of worm type B
- $I_{A(0)}$ initial hosts of worm type A

We use these parameters to predict pandemic of prey and predator

Worm Life Cycle



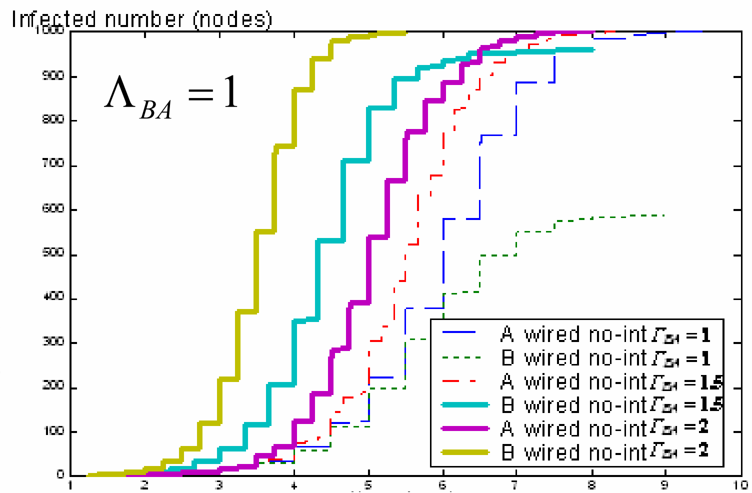
Predator Life Cycle

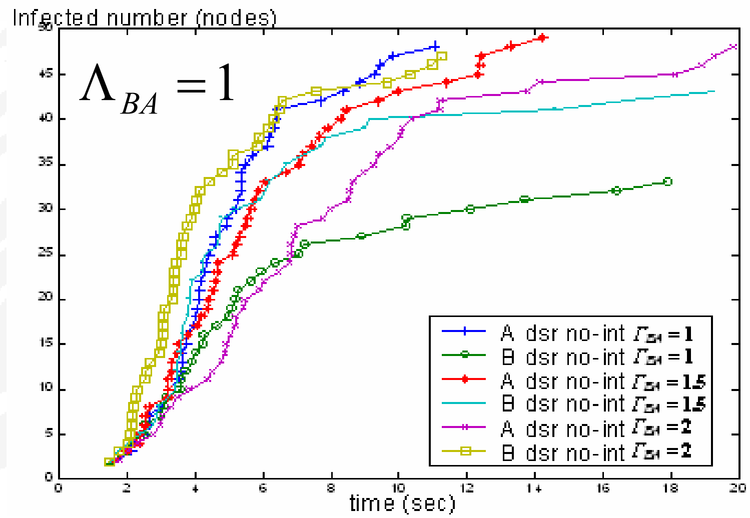


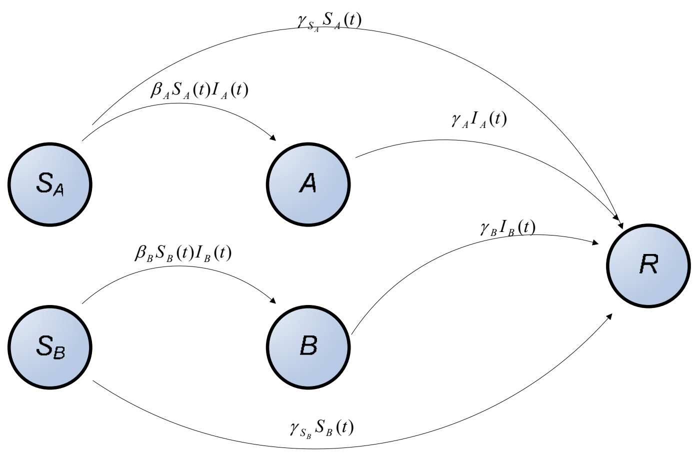
Prey Life Cycle

Indirect Interaction

- No predator/prey
- Two worm types simply coexist and compete for available resources (network, CPU)
- Simply adding worm type to epidemic model (SIR model)



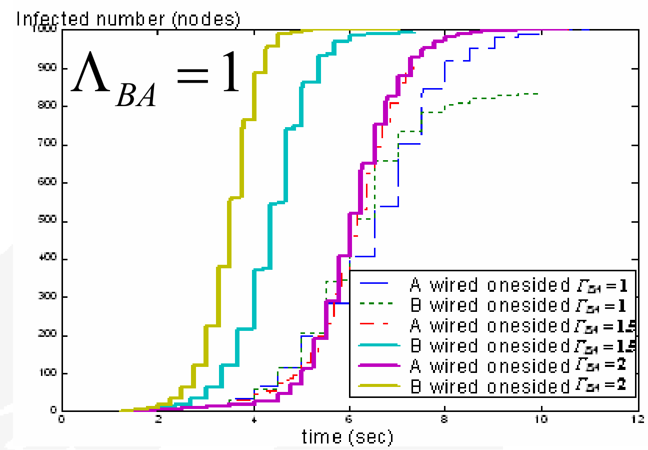


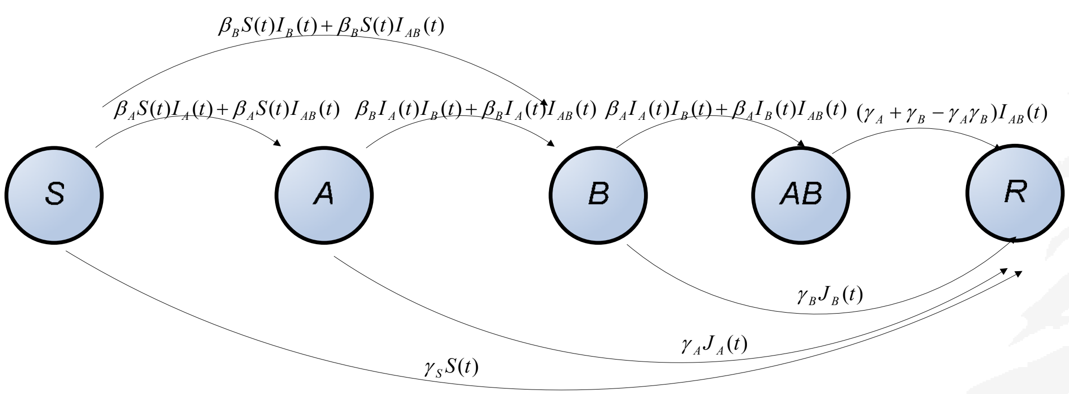


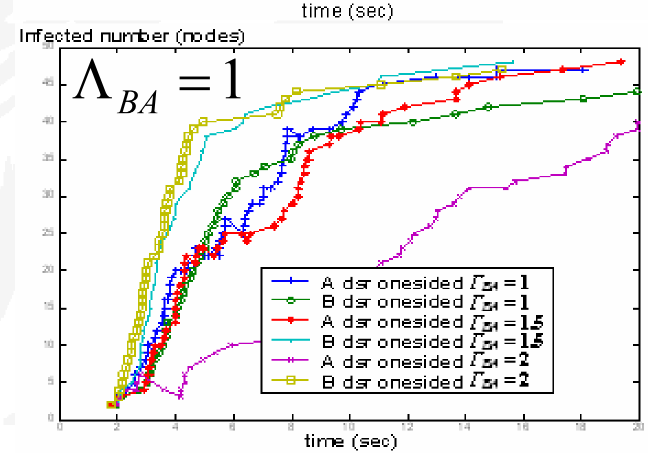
A = Predator
B = Prey

One-sided Interaction

- There is one predator and one prey
- One-sided interaction can be patched or un-patched
- Patching (or false signature) by predator prevents re-infection from prey
- Example is CodeGreen&CodeRed (they both use the same exploit and code green patchs the hosts after it infect the host)





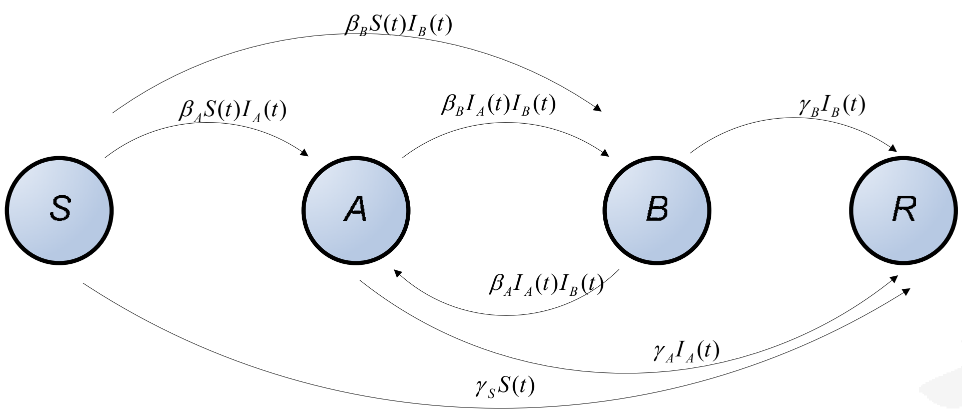


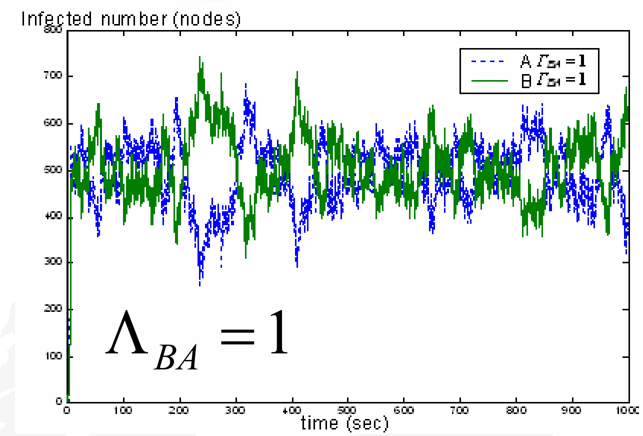
A = Predator
B = Prey

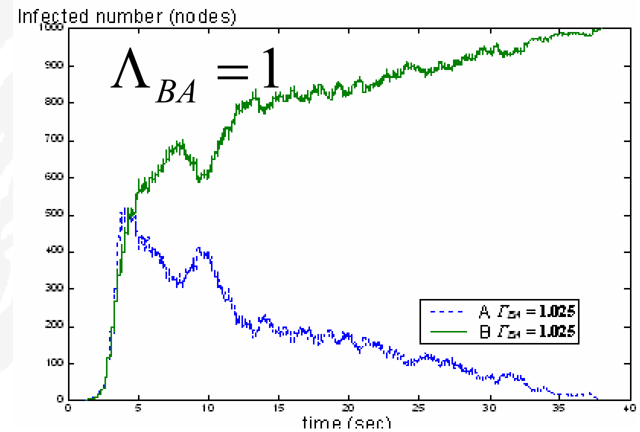
Two-sided Interaction

Predator 1 Predator 2

- There is two predators which can terminate each other
- Two-sided interaction can also be patched or un-patched
- Example is NetSky terminates Bagle and vice versa (with different sub type)
- Equilabrium with equal scan rate (both types have equal infectives)



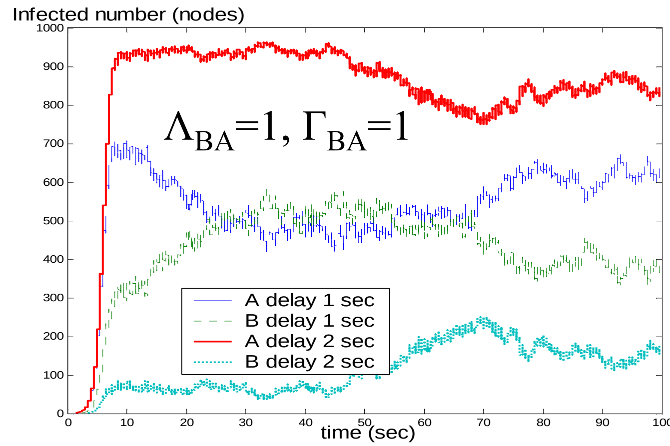




A = Predator
B = Prey

VACCINE Framework

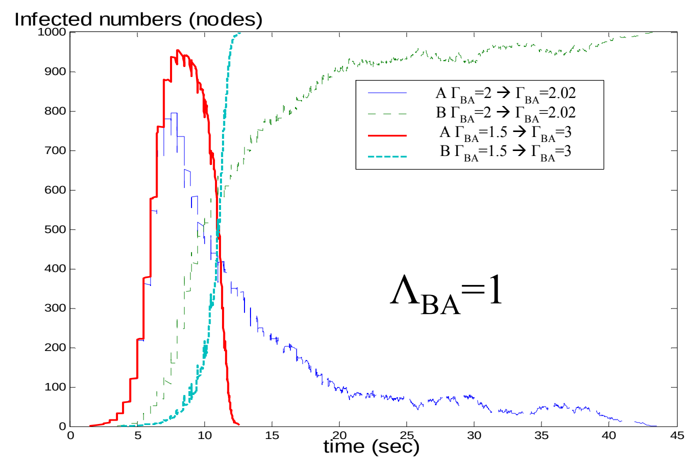
- Using good worms to terminate bad worms
- Need to know the bad worms scan rate (as well as bad worm strategy)
- Delay after bad worms launching has significant impact on effectiveness
- Can be reactive (increase scan rate after detect bad worms) or active (always using highest scan rate possible or increase scan rate without bad worm detection)



Static scan rate

VACCINE Procedure

STEP 1: Infect susceptible hosts with same strategy as of targeted worms
STEP 2: After successfully infecting the host, check whether targeted worm has already infected the host.
STEP 3: If infected, adjust initial scan rate (based on releasing delay of non-malicious worm and scan rate of malicious worm). Otherwise, continue scan with same scan rate.
STEP 4: Remove targeted worms. If patch is available go to step 5. Otherwise go to step 6.
STEP 5: Apply patch (or false signature of malicious worm).
STEP 6: Wait for K period of time, if there is no additional incoming malicious worms, remove self from host.



2-step scan rate

VACCINE Challenges

- Distinguishing between good and bad worm is not easy.
- Worm scan rate can be varied based on available network bandwidth or size of email address available (How to make sure that there are available resources for counter worms)
- Need accurate estimation of worm releasing time to minimize the maximum required speed for good worms.
- Good worm can cause undesirable denial of service if heavily scan innocent hosts

SUMMARY/FUTURE WORK

- We identify three types of interactions: indirect interaction, one-sided interaction, and two-sided interaction that show significantly different patterns of propagation.
- We develop a new worm propagation model which is validated through extensive simulations.
- We shall further develop the VACCINE architecture, protocol and evaluate it in a test bed. Worm interactions in different mobility models will be explored.
- More details of worm interaction models and simulation results can be found in “S. Tanachaiwiwat, A. Helmy, "*VACCINE: War of the Worms in Wired and Wireless Networks*", Technical Report CS 05-859, Computer Science Department, USC”