

On the Performance Evaluation of Encounter-based Worm Interactions Based on Node Characteristics



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>

Motivation

- More worms targeting mobile devices especially exposed Bluetooth-enabled phones e.g. Cabir, CommWarrior, Mibir,...
- Centralized approach like Firewall is inapplicable in such networks
- Need decentralized approach
- We propose “Worm Interaction” Approach

Goal

- Model more realistic worm propagation and interactions
 - Most of work assumes fully cooperation, all susceptible and always ON
- Our model focus on effects of cooperation, immunization, and on-off behavior on worm interaction in encounter-based networks

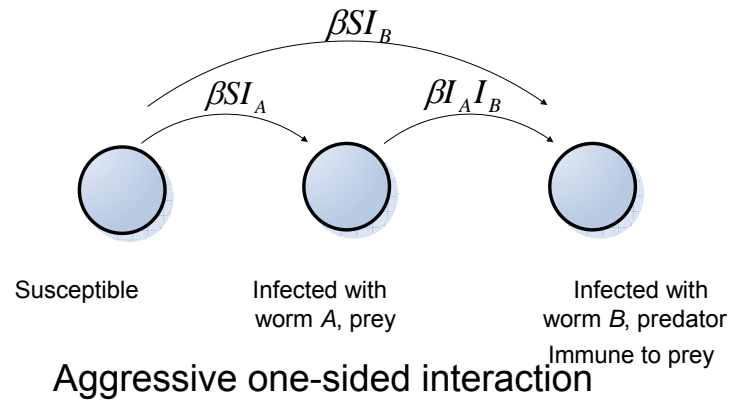
Related work

- Disease spread modeling: *SI, SIS, SIR, SEIR* (*S=Susceptible, I=Infected, R=Recovered, and E= Exposed*)
- Worm propagation models motivated by above models
- Automated security countermeasure
- Epidemic routings in delay tolerant networks

Definitions

- Encounter-based networks
 - Delay-tolerant networks
 - Store-and-forward
 - Rely on human encounter pattern
 - Worms in encounter-based networks = encounter-based worms
- Prey = Bad worm, Predator = Good worm
 - Predator (Good worm) terminates Prey (bad worm)

Worm Interaction Types



$$\frac{dS}{dt} = -\beta S(I_A + I_B)$$

$$\frac{dI_A}{dt} = \beta I_A (S - I_B)$$

$$\frac{dI_B}{dt} = \beta (SI_B + I_A I_B)$$

Basic model with uniform encounter,
fully cooperation, all susceptible and always on

Basic assumptions

- Uniform encounter
- Both predators (good worm) and prey (bad worm) shares the same susceptible nodes
- Human encounter pattern does not change over time
- Simulation setup: Monte-Carlo Encounter-level simulation, 1000 nodes, 1000 rounds of experiment

Metrics

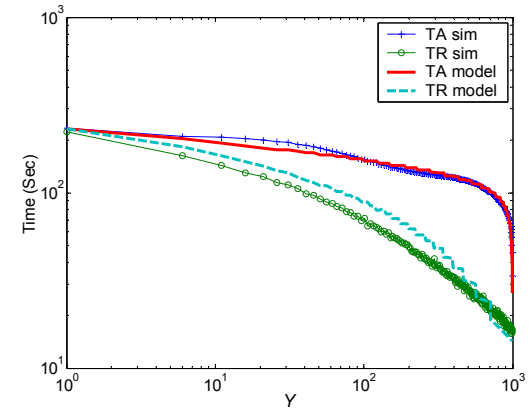
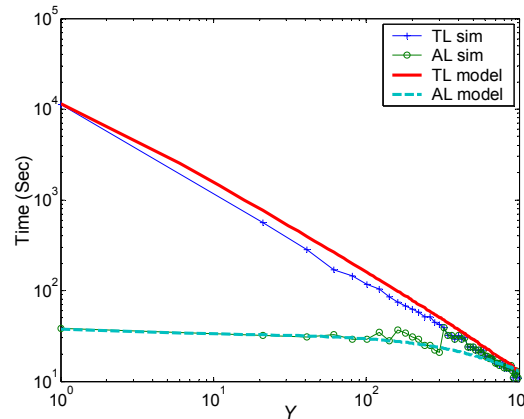
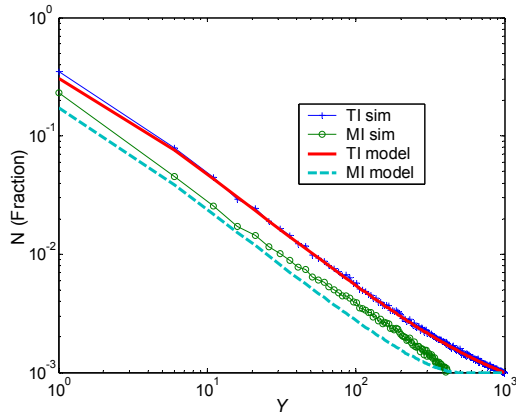
- Total prey infected hosts (TI)
 - Maximum prey infected hosts (MI)
 - Total prey lifespan (TL)
 - Individual prey lifespan (AL)
 - Time to secure all hosts (TA)
 - Time to remove all prey (TR)
- } Damages
 } Weighted Damages
 } Speed of protection

$$TI \geq MI, TL \geq AL \text{ and } TA \geq TR$$

Relationships of Metrics with Host Ratio



$$Y = \text{Initial Infected Host Ratio} = I_B / I_A$$



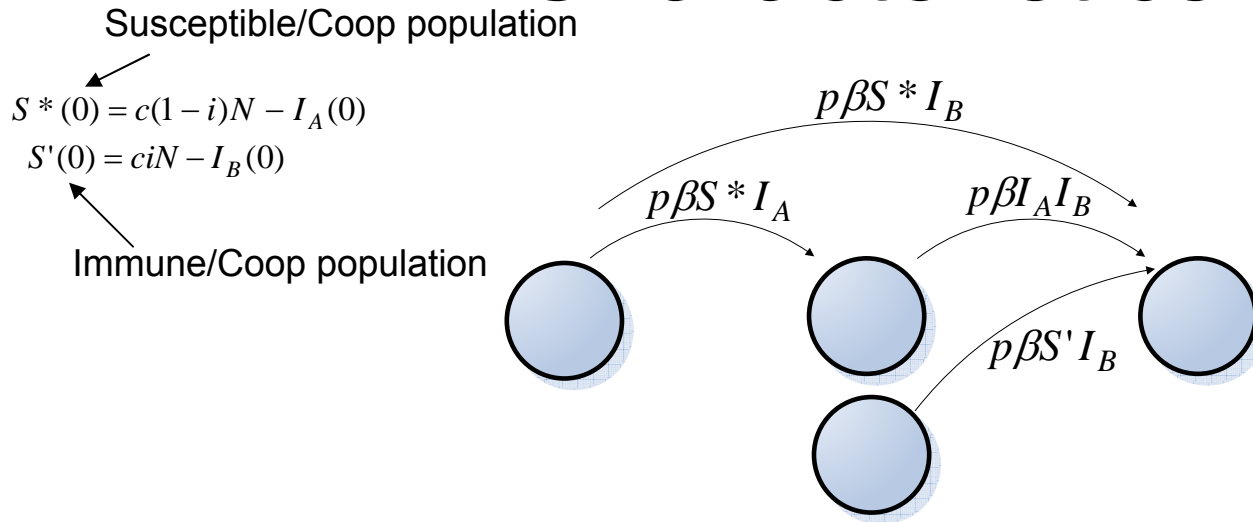
With uniform encounter, fully cooperative, all susceptible and always on
 TI, MI, and TL is exponentially decreasing with increase of Y
 AL and TA is difficult to be reduced

Node Characteristics



- Cooperation
- Immunization
- On-off behavior
- Batch-Arrival

Aggressive One-sided with Node Characteristics



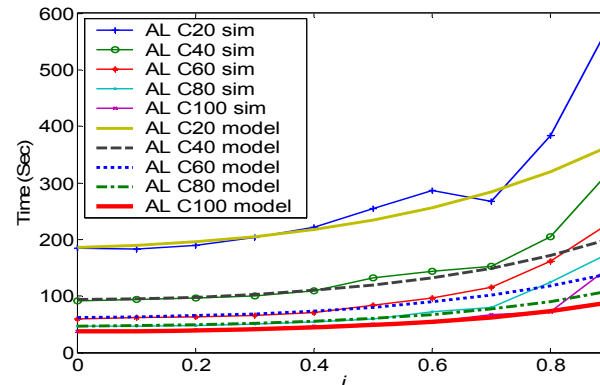
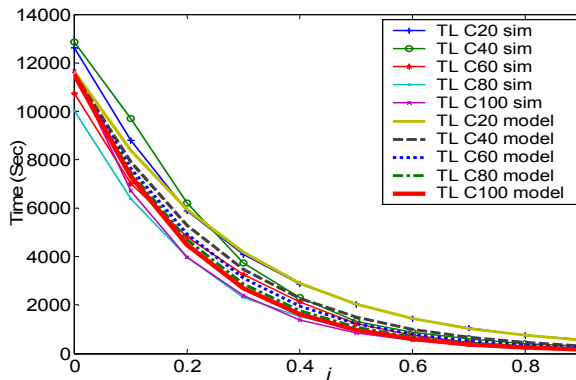
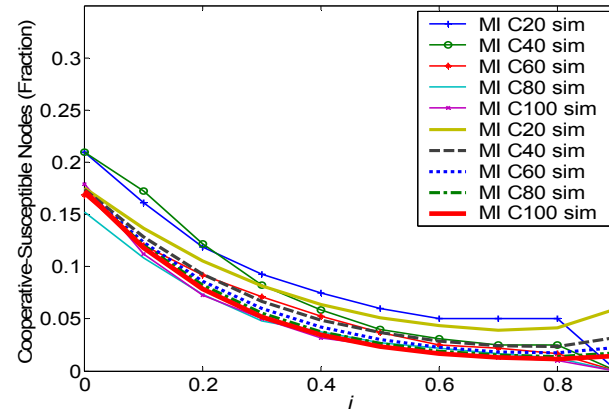
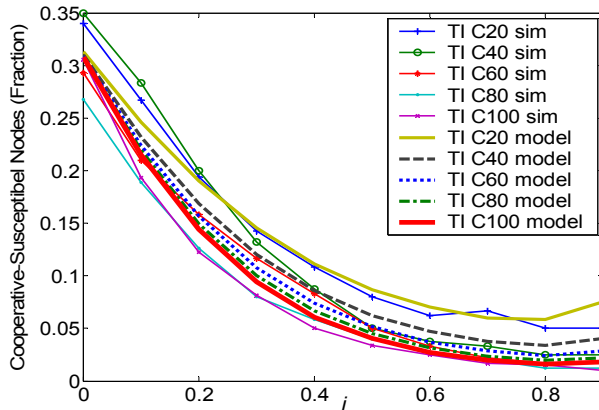
$$\frac{dS^*}{dt} = -p\beta S^*(I_A + I_B)$$

$$\frac{dS'}{dt} = -p\beta S' I_B$$

$$\frac{dI_A}{dt} = p\beta I_A (S^* - I_B)$$

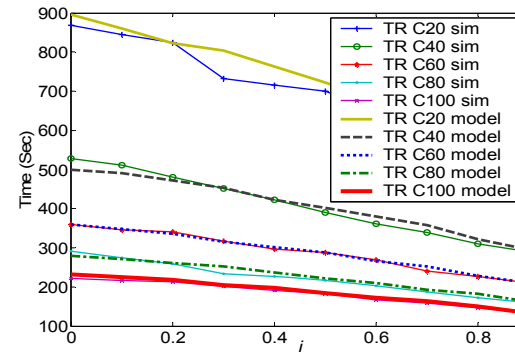
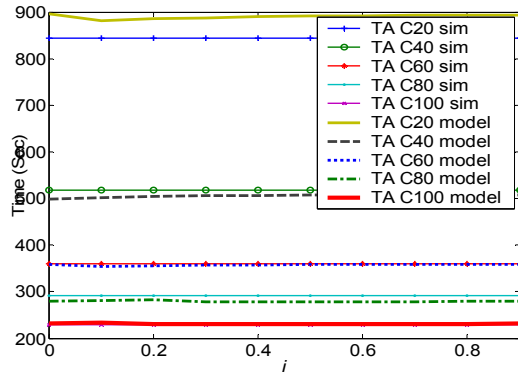
$$\frac{dI_B}{dt} = p\beta ((S^* + S')I_B + I_A I_B)$$

Effect of Cooperation and Immunization



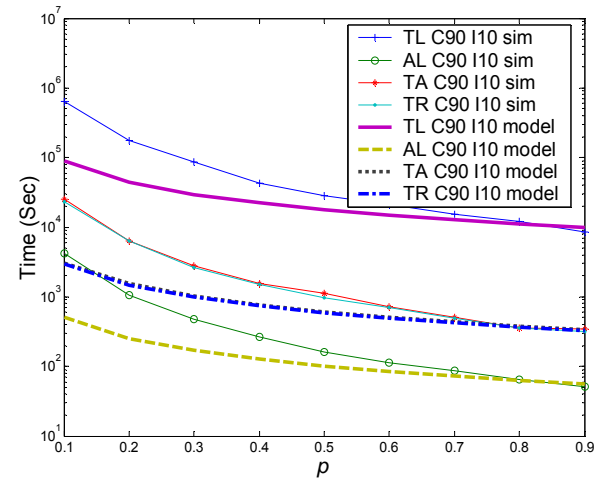
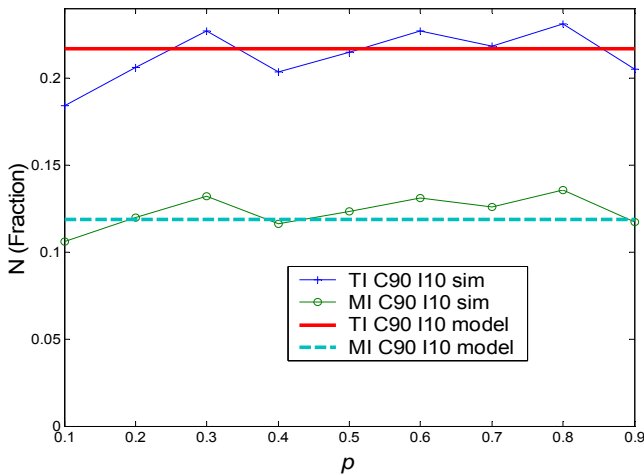
Immunization significantly reduces TI, MI and TL but may increase AL

Effect of Cooperation and Immunization



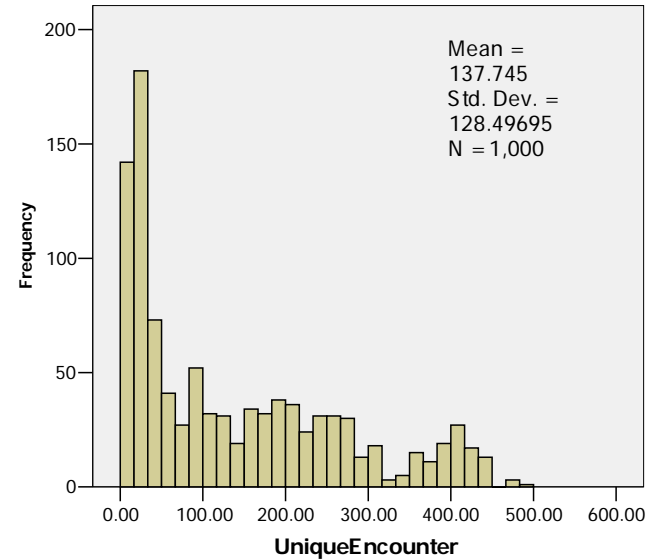
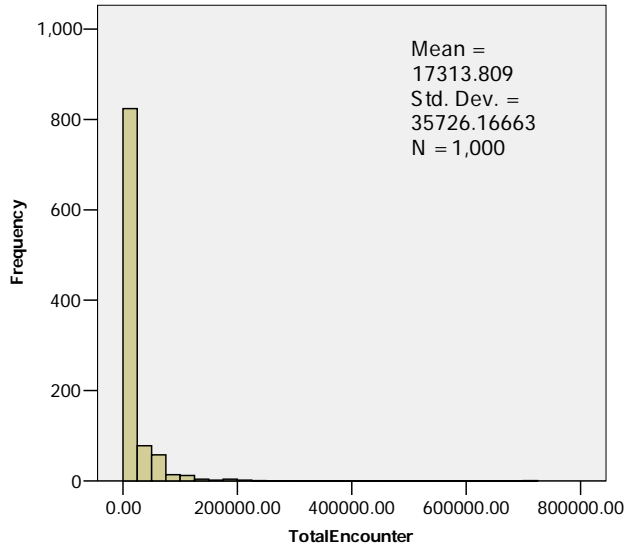
Cooperation significantly reduces AL, TA and TR

Effects of On-Off Behavior



“On-off” behavior does not effect TI and MI
but reduces TL, AL, TA and TR

Realistic encounter patterns

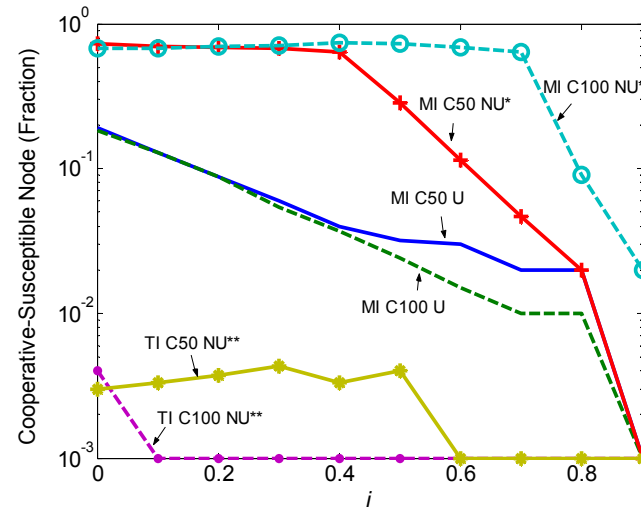
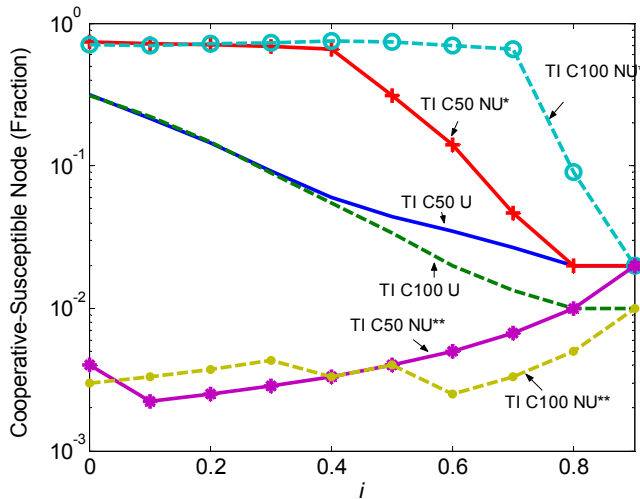


Total encounter = total number of encounters per node

Unique encounter = unique encounters (encountered node ID) per node

Only few nodes have high encounter rate and high unique encounter

Realistic encounter patterns



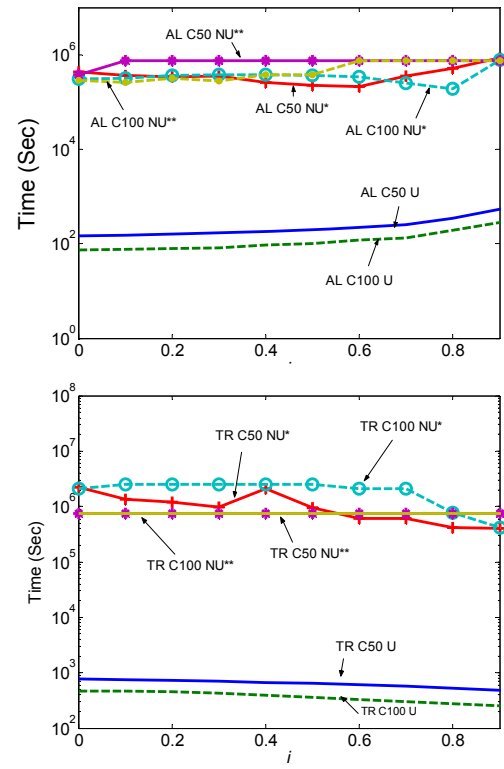
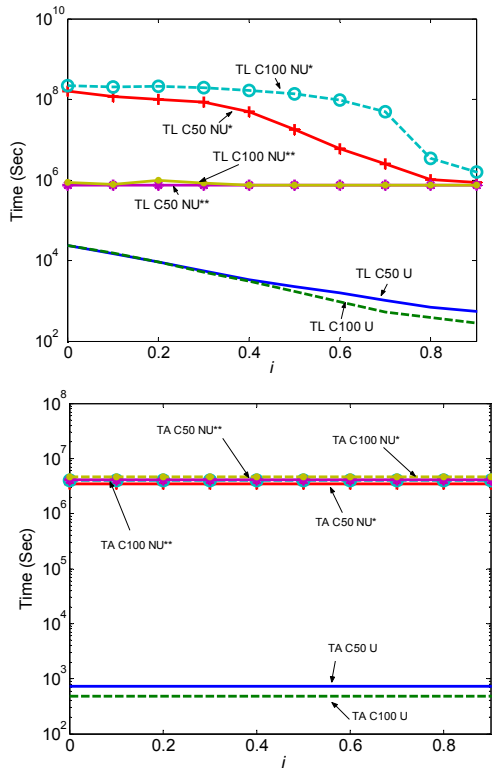
Non-uniform encounters creates advantages/disadvantages to prey and predator from different groups

Slow prey fast predator is the best case scenario

Slow prey = initial prey infected host in slow encounter-rate group

Fast predator = initial predator infected host in fast encounter-rate group

Realistic encounter patterns



Results from uniform encounters are significantly different from results from Realistic encounter patterns
 Arrival patterns matter → delay and batch arrival

Realistic worm interaction using mobile device



- We want to see the worm interactions in action
- We create the Proof-of-concept worm interactions in Bluetooth handheld devices (HP iPAQs)
- See our demo after this talk



Summary

- We introduce node-characteristic aggressive one-sided interaction for encounter-based worms
- Immunization has more impact on worm propagation than cooperation especially in realistic encounter patterns
- Encounter pattern in real-life is significantly far from uniform especially delay and batch arrival patterns
- Non-uniform encounter patterns affects the predator performance significantly when compared with that of uniform encounter patterns