Encounter-based worms: Analysis and Defense

Sapon Tanachaiwiwat
Department of Electrical Engineering
University of Southern California, CA
tanachai@usc.edu

Ahmed Helmy
Department of Computer and Information Science and Engineering
University of Florida, FL
helmy@ufl.edu

Abstract— An encounter-based network is a frequently-disconnected wireless ad-hoc network requiring immediate neighbors to store and forward aggregated data for information disseminations. Using traditional approaches such as gateways or firewalls to deter worm propagation in encounter-based networks is inappropriate. We propose a worm interaction approach that relies upon automated beneficial worm generation to alleviate problems of worm propagations in such networks. To understand the dynamics of worm interactions and their performance, we mathematically model worm interactions based on major worm interaction factors, including worm interaction types, network characteristics, and node characteristics using ordinary differential equations and analyze their effects on our proposed metrics. We validate our proposed model using extensive synthetic and trace-driven simulations. We find that all worm interaction factors significantly affect the pattern of worm propagations. For example, immunization linearly decreases the infection of susceptible nodes, while *on-off* behavior only impacts the duration of infection. Using realistic mobile network measurements, we find that encounters are "bursty", multi-group, and non-uniform. The trends from the trace-driven simulations are consistent with the model, in general. Immunization and timely deployment seem to be most effective in countering worm attacks in such scenarios, while cooperation may help in a specific case. These findings provide insight that we hope would aid in the development of counter-worm protocols in future encounter-based networks.

I. INTRODUCTION

An encounter-based network is a frequently-disconnected wireless ad-hoc network requiring close proximity of neighbors, i.e., encounter, to disseminate information. Hence, we call this the "encounter-based network", which can be considered as a terrestrial delay-and-disruptive-tolerant network. It is an emerging technology that is suitable for applications in highly dynamic wireless networks.

Most previous work on worm propagation has focused on modeling a single worm type in well-connected wired networks. However, many new worms target wireless mobile phones. The characteristics of worms in mobile networks are different from random-scan network worms. Worm propagation in random-scan networks is mainly limited by the network bandwidth, link delay and worm scanning strategies [8]. Worm propagations in mobile networks depend heavily on user encounter patterns. Many of those worms rely on Bluetooth to broadcast their replications to vulnerable phones, e.g., Cabir and

ComWar.M [10, 13]. Since Bluetooth radios have very short ranges of around 10-100 meters, the worms need neighbors in close proximity to spread their replications. Hence, we call these "encounter-based worms". This worm spreading pattern is very similar to the spread of packet replications in delay tolerant networks [15, 17], i.e., flooding the copies of messages to all close neighbors. An earlier study of encounter-based networks actually used the term "*epidemic routing*" [15] to describe the similarity of this routing protocol to disease spreading. Using traditional approaches such as gateways or firewalls to deter worm propagation in encounter-based networks is inappropriate. Because this type of network is highly dynamic and has no specific boundary, a fully distributed counter-worm mechanism is needed. We propose to investigate a worm interaction approach that relies upon automated beneficial worm generation [1]. This approach uses an automatically generated beneficial worm to terminate malicious worms and patch vulnerable nodes.

Our work is motivated by wars of Internet worms such as the war between NetSky, Bagle, and MyDoom [13]. This scenario is described as "worm interactions" in which one or multiple types of worm terminates or patches other types of worms.

In this paper, we mathematically model worm interactions based on three major worm interaction factors, including worm interaction types [11], network characteristics, and node characteristics [12]. Worm interaction types in our model are *aggressive one-sided*, *conservative one-sided*, or *aggressive two-sided*. The variation of these worm interaction types can also be created from our model.

There are many important node characteristics to be considered, but we focus only on a fundamental subset including cooperation, immunization, *on-off* behavior, and delay. We shall show that these are key node characteristics for worm propagation in encounter-based networks. Other characteristics, such as trust between users, battery life, energy consumption, and buffer capacity are subject to further study and are beyond the scope of this paper.

The majority of routing studies in encounter-based networks usually assume ideal node characteristics, including full node cooperation and *always-on* behavior. However, in realistic scenarios, nodes do not always cooperate with others and may be *off* most of the time [5]. In worm propagation studies, many works have also assumed that all nodes are susceptible (i.e., not immune) to worm infection. An *immune* node does not cooperate with infected nodes and is not infected. To investigate more realistic scenarios, we propose to study mobile node characteristics and analyze the impact of cooperation, immunization, and *on-off* behavior on the worm interactions. Cooperation and *on-off* behavior are expected to have an impact on the timing of infection. Intuitively, cooperation makes the network more susceptible to worm attacks. Immunization, however, may help reduce overall infection level. This paper examines the validity of these expectations, using the overall infection level and timing of infection as metrics (see Section III.*C*).

We consider several important network characteristics, including node sizes, contact rate, group behaviors, and batch arrival. Using realistic mobile network measurements, we find that encounters are *"bursty", multi-group, and non-uniform*.

Most worm propagation studies have only focused on the instantaneous number of infected nodes as a metric. We believe that additional systematic metrics are needed to study worm response mechanisms. We utilize new metrics, including total prey-infected nodes, maximum prey-infected nodes, total prey lifespan, average individual prey lifespan, time to secure all nodes, and time to remove all preys to quantify the effectiveness of worm interaction.

In this paper, we attempt to answer the following questions: How can we model this *war of the worms* systemically based on worm interaction factors including worm interaction types, node characteristics, and network characteristics? What type of worm interaction, conditions of network, and node characteristics can alleviate the level of worm infection? How do worms interact in realistic mobility scenarios? This worm interaction model can be extended to support more complicated current and future worm interactions in encounter-based networks.

Our main contribution in this paper is a new *Worm Interaction Model*, focusing on worm interaction types, network characteristics, and node characteristics in encounter-based networks. We also use new metrics to quantify the effectiveness of worm interactions, and our proposed metrics are applicable to study any worm response mechanism. We also provide the first study of worm propagation based on real mobile measurements.

Following is an outline of the remainder of the paper. We discuss related work in Section II. In Section III, we explain the basic definitions of our model, the metrics, worm interaction types, network characteristics, node characteristics, and the general model. We then analyze and evaluate worm interactions in both uniform and realistic encounter networks in Section IV. In Section V, we conclude our work and discuss the future work.

II RELATED WORK

Worm-like message propagation or epidemic routing has been studied for delay tolerant network applications [11, 13, 15]. As in worm propagation, a sender in this routing protocol spreads messages to all nodes in close proximity, and those nodes repeatedly spread the copies of messages until the messages reach a destination, similar to generic flooding but without producing redundant messages. Performance modeling for epidemic routing in delay tolerant networks [13] based on ordinary differential equations (ODE) is proposed to evaluate the delivery delay, loss probability, and power consumption. In addition, the concept of the anti-packet is proposed to stop unnecessary overhead from forwarding extra copies of the packets after the destination has received the packets. This can be considered as a special case of non-zero delay of aggressive one-sided interaction (see Section III.*B*), which we consider in our model.

Epidemic models, a set of ODEs, have been used to describe the spread of contagious diseases, including the *SI, SIS, SIR SIRS, SEIR,* and *SEIRS* models [4, 10] in which *S, I, E, R* stand for Susceptible,

Infected, Exposed, and Recovered states, respectively. There is an analogy between computer worm infection and disease spread in that both depend on the node's state and encounter pattern. For Internet worms, several worm propagation models have been investigated in earlier works [2, 6, 8, 18]. Few works [1, 9, 11] have considered worm interaction among different worm types. Our work, in contrast, focuses on understanding how we can systemically categorize and model worm propagation based on worm interaction types, network characteristics, and node characteristics in encounter-based networks.

In [1], the authors suggested modifying existing worms such as Code Red, Slammer, and Blaster to terminate the original worm types. In this paper, we model this as aggressive one-sided worm interaction. Other active defenses, such as automatic patching, were also investigated in [16]. Their work assumed a patch server and overlay network architecture for Internet defense. We provide a mathematical model that can explain the behavior of automatically-generated beneficial worms and automatic patch distribution using one-sided worm interaction in encounter-based networks. The effect of immunization on Internet worms was modeled in [8] based on the *SIR* model.

In our previous work [12] and this paper, we discuss the encounter-based worm problem and show trace-based simulation results compared with the model. However, in [12], we only focused on node characteristics in aggressive one-sided interaction types (one of the worm interaction types). This paper explores all worm interaction factors including different types of worm interactions, network characteristics, and node characteristics. The mathematical model presented in [12] was also very limited, while the mathematical model in this paper elaborates on all worm interaction factors as well as re-susceptible transitions and removed states. The experimental results between the two studies are also drastically different. In [12], we showed preliminary trace-based results and compared it with our simplistic model, and we stated that the model had to be improved by considering realistic factors such as group concept, batch arrival, and delay. Hence, in this paper, we incorporate those factors into the model, and our new and comprehensive model predicts the outcome much more accurately.

III. WORM INTERACTION MODEL

We aim to build a fundamental worm propagation model that captures worm interaction as a key factor in uniform encounter-based networks. Furthermore, our proposed model addresses and analyzes the dynamics of susceptible and infected nodes over the course of time.

Because the constant removal rate in the basic *SIR* model and its variance [7, 14] cannot directly portray the impact of such interactions on multi-type worm propagations, our model builds upon and extends beyond the conventional epidemic model to accommodate the notion of interaction.

The basic operation of a worm is to find susceptible nodes to be infected, and the main goal of attackers is to have their worms infect the largest amount of nodes in the least amount of time, and if possible, remain undetected by antivirus or intrusion detection systems. Our beneficial worm, on the other hand, aims to eliminate opposing worms or limit the scope of the opposing worms' infection. We

want to investigate the worm propagation caused by various types of interactions as well as network characteristics and node characteristics.

A. Definitions

a. Predator-Prey Relationships

For every worm interaction type, there are two basic characters: Predator and Prey. The ***Predator***, in our case the beneficial worm, is a worm that terminates and patches against another worm. The ***Prey***, in our case the malicious worm, is a worm that is terminated or patched by another worm.

A predator can also be a prey at the same time for some other type of worm. A predator can *vaccinate* a susceptible node, i.e., infect the susceptible node (vaccinated nodes become predator-infected nodes) and apply a patch afterwards to prevent the nodes from prey infection. Manual vaccination, however, is performed by a user or an administrator by applying patches to susceptible nodes.

A *termination* refers to the removal of a prey from infected nodes by a predator, and such action causes prey-infected nodes to become predator-infected nodes. The removal by a user or an administrator, however, is referred to as *manual removal.*

We choose to use two generic types of interacting worms, *A* and *B*, as our basis throughout the paper. *A* and *B* can assume the role of predator or prey depending on the type of interactions.

b. Contact Rate

Contact rate is the frequency of encounter for pairs of nodes, where an encounter occurs when the two nodes are within radio range. We assume a uniform contact rate for all pairs of nodes, their encounter behavior does not directly impact each other, and both predator and prey share the same set of susceptible nodes. We assume that in one encounter, the worm is successfully transferred from one node to another.

c. Metrics

To gain insight and better quantify the effectiveness of worm interaction, we propose to use the following metrics:

(1) Total Prey-infected Nodes (*TI*): the number of nodes ever infected by a prey.

(2) Maximum Prey-infected Nodes (*MI*): the peak of the instantaneous number of prey-infected nodes where $I_A(0) \le MI \le TI$.

(3) Total Prey Lifespan (*TL*): the sum of time of individual nodes ever infected by a prey. It can be interpreted as the total damage by a prey.

(4) Average Individual Prey Lifespan (*AL*): the average lifespan of individual prey-infected nodes where $AL \le TL$.

(5) Time to Secure All Nodes (*TA*): the time required for a predator to infect all susceptible and prey nodes. Its inverse can be interpreted as the average predator infection rate.

(6) Time to Remove All Preys (*TR*): the time required for a predator to terminate all preys where $TR \le TA$. Its inverse can be interpreted as the prey termination rate.

TI and *MI* are indicators of the level of prey infection, *TL* and *AL* are the indicators of the duration of prey infection, and *TA* and *TR* are the indicators of protection and recovery rate, respectively. Our goal is to find the conditions to *minimize* these metrics based on worm interaction factors, of which details are discussed next.

B. Worm interaction factors

Our model considers three major factors that can significantly impact the worm interactions: worm interaction types, network characteristics, and node characteristics. A worm can behave differently based on the types of interactions (or their behaviors): aggressive one-sided interaction, conservative one-sided interaction, or aggressive two-sided interaction [11]. In addition, underlying network characteristics including node size, contact rate, group behaviors, and batch arrivals are the keys of worm propagation. Finally, node characteristics, including cooperation, immunization, *on-off* behaviors and delay, can significantly affect the worm interaction patterns. We start by explaining each individual worm interaction factor before we show our model that addresses all of these factors.

a. Worm interaction types

When there is a prey, *A*, and a predator, *B*, we consider this as a one-sided interaction. If both *A* and *B* are predators, it is denoted as a two-sided interaction. For an ideal scenario, the predator wants to terminate its prey as much as possible, as well as prevent its preys from infecting and re-infecting. To satisfy that requirement, the predator requires a patch or a false signature of its prey.

There are three types of interactions considered: aggressive one-sided, conservative one-sided, and aggressive two-sided. They are described below.

(1) Aggressive one-sided interaction: In this interaction type, a beneficial worm, the predator, has the capability to terminate and patch a malicious worm, the prey, as well as vaccinate susceptible nodes. Simplified interaction between the Internet worms, e.g., Welchia and Blaster, can be represented by this model.

(2) Conservative one-sided interaction: In a conservative interaction, a predator has the capability to terminate a prey but does *not* vaccinate susceptible nodes. Hence, the predator-infected nodes changes depend solely on population of the prey-infected nodes.

(3) Aggressive two-sided interaction: In this interaction type, both worms assume the roles of predator and prey simultaneously. We would simply call *A* as *predator A* and *B* as *predator B*. Predator *B* is capable of vaccinating susceptible nodes but is unable to remove a predator *A* from predator *A*'s infected nodes because it is blocked by predator *A*. Both predator A and B block each other. In automated patching systems [16], their worm-like patch distribution falls into this category. The automated patching that assumes that each worm patches its own node to prevent infection from the other worm is closely related to this model.

According to above worm interaction types, *TI, MI, TL, AL, TA,* and *TR in* aggressive one-sided interactions are expected to be the lowest among those of all interaction types. In conservative one-sided

interactions, because only once-infected-by-prey nodes can be infected by a predator, $TA = \infty$. Similarly, for aggressive two-sided interaction, a predator cannot terminate a prey, hence $TL = AL = TA = TR = \infty$.

b. Network characteristics

Network characteristics represent the characteristics of the encounter-based networks. We particularly focus on node sizes, contact rate, group behaviors, and batch arrival. The other related characteristics, including clustering coefficient and average hop counts, are subject to further study.

(1) Contact rate: Contact rate (β) is one of the most important factors to determine the characteristics of worm interaction. We investigate the relationships between β and our proposed metrics in this section. Because contact rate is the frequency of a pair of nodes encountering each other, increasing the contact rate causes every node to encounter each other more frequently, i.e., the time between consecutive encounters will be reduced. Hence, we expect that the metrics relating to times including *TL*, *AL*, *TA,* and *TR* to be reduced. However, because prey and predator share the same contact rate, *TI* and *MI* should not be different even when contact rates are changed. In other words, if the prey infects other susceptible nodes faster, the predator also terminates and patches faster as well.

(2) Node size: With the same number of initial predator and initial prey-infected nodes and fixed β, the change of node size (*N)* causes a decrease of time between consecutive encounters of any node to any node. Similarly, as we expect from the contact rate, varying node sizes can have a significant impact on *TL*, *AL*, *TA,* and *TR.*

(3) Group behavior: Multi-group encounters, of which the group is classified by its encounter patterns and contact rates, are expected in encounter-based networks. For two-group modeling, we need three different contact rates: two intra-contact rates for encounters within each group, and one inter-contact rate for encounters between groups. For *n* groups, we need *n* intra-contact rates and $\binom{n}{2}$ inter-contact rates. The effects of group sizes and contact rates of the individual group and between groups are investigated.

(4) Batch arrival: Nodes may join the networks simultaneously as a "batch arrival". This can be modeled as the "birth" of the population. We assume that those nodes enter the network only as susceptible nodes. Note that infected nodes that temporarily leave and then join the network would not be considered as a batch arrival. We discuss and investigate the effect of realistic batch arrivals in Section IV.

c. Node characteristics

Each node may have different characteristics because of differences in the user's usage strategies, daily-life activities, or level of security technology and awareness. Four important node characteristics corresponding to this worm interaction factor are addressed, including cooperation, immunization, *on-off*

behavior, and delay. We assume these node characteristics are persistent throughout the lifetime of the networks.

(1) Cooperation: Cooperation is the willingness of a node to forward messages (worms) to other nodes. The opposite characteristic is known as selfishness. Intuitively, cooperation may seem to make the network more vulnerable. However, unlike immunization, cooperation is expected to equally slow down both prey and predator propagations. Hence, the effect of cooperation is hard to anticipate. Cooperation and trust are much correlated concepts in the computer security area where trust is the major key to cooperation. For example, highly trusted nodes will not forward the messages to (or accept messages from) un-trusted nodes. In this paper, we assume strong linear relationship between cooperation and trust.

(2) Immunization: Not all nodes are susceptible to the prey, either because of their heterogeneous operating systems or their differences of promptness to remove the vulnerability from their machines. Hence, some nodes can be immune to prey and will slow down the overall prey infection. It is expected to improve the overall targeted metrics mentioned earlier because immune nodes still help forward predators to other nodes. It is expected to have no positive impact on *TA* but reduce *TR* simply because of less number of nodes are to be removed.

(3) *On-off* behavior: A node is able to accept or forward the packet based on its *on-off* characteristics. In reality, devices are "*on*" or active only a fraction of the time. Activity may be related to mobility. For instance, a mobile phone is usually *on*, while a laptop is unlikely to be mobile while *on*[1]. We model the transition from *on* to *off*, and vice versa, probabilistically. The probability is determined at the beginning of each time interval. Hence, the contact rate is expected to be proportionally reduced according to the probability that the node cannot forward or accept the packets because of the *on-off* status.

(4) Delay: Initial prey-infected nodes and initial predator-infected nodes may start their infections in the networks at different times (depending on prey timers or security architecture of the predator). The gap between those times can be significant. If initial prey-infected nodes start infecting susceptible nodes in the network earlier than initial predator-infected nodes start vaccination and termination, we can expect the increase of *TI, MI, AL*, *TA*, *TL,* and *TR*, and opposite results are expected if the order of their start times is reversed.

C. General Worm Interaction Model

Assume that there are *g* groups in the network. Let β_{nm} be the contact rate between members of group *n* and group *m* (β_{nn} is the contact rate within group *n*), and S_n is the number of susceptible nodes of group *n* (at time *t*) where $1 \le m, n \le g$. Let *c* be the fraction of N_n that is willing to be *cooperative,* where $0 \le c \le 1$ and N_n is the total number of nodes in the networks for group *n*. Let *i* be the fraction of cooperative nodes that are *immune* to the prey, where $0 \le i \le 1$. Let I_{An} and I_{Bn} be the number of prey-

[1] This is observed from measurements [15] and is captured in our study using trace-driven simulations.

infected nodes and predator-infected nodes for group n, respectively. If we assume that the initial predator-infected and initial prey-infected nodes (t=0) are cooperative, then the number of susceptible nodes for both prey and predator is S^*_n, where $S^*_n(0) = c(1-i)N_n - I_{An}(0)$ for group n and the number of susceptible nodes for the predator only is S'_n, where $S'_n(0) = ciN_n - I_{Bn}(0)$ for group n. Note that $N_n = S^*_n + S'_n + I_{An} + I_{Bn}$ and $S_n = S^*_n + S'_n$. We define the probability of "*on*" behavior as p and "*off*" behavior as 1-p, where $0 \le p \le 1$. Hence, the contact rate between group n and m for both predator and prey is $p\beta_{nm}$. Let d be the delay between the initial prey-infected node(s) and the initial predator-infected node(s) (assume that all initial predator-infected (prey-infected) nodes start infection at the same time); then $I_{An}(t) \ge 1$ iif $t \ge 0$ and $I_{Bn}(t) \ge 1$ iif $t \ge d$. For simplicity and brevity, let us assume that the number of groups in the network is 2. Fig.1a shows the state diagram of our model.

Let $K_{S^*_1 I_{A1} I_{A2}}$, $K_{S^*_2 I_{A1} I_{A2}}$, $K_{S^*_1 I_{B1} I_{B2}}$, $K_{S^*_2 I_{B1} I_{B2}}$, $K_{S'_1 I_{B1} I_{B2}}$, $K_{S'_2 I_{B1} I_{B2}}$, $K_{I_{A1} I_{B1} I_{B2}}$ and $K_{I_{A2} I_{B1} I_{B2}}$ be the state transition indicator from S^*_1 to either I_{A1} or I_{A2}, where $K_{S^*_1 I_{A1} I_{A2}} \in \{0,1\}$, from S^*_2 to either I_{A1} or I_{A2} where $K_{S^*_2 I_{A1} I_{A2}} \in \{0,1\}$, from S^*_1 to either I_{B1} or I_{B2} where $K_{S^*_1 I_{B1} I_{B2}} \in \{0,1\}$, from S^*_2 to either I_{B1} or I_{B2} where $K_{S^*_2 I_{B1} I_{B2}} \in \{0,1\}$, from S'_1 to either I_{B1} or I_{B2} where $K_{S'_1 I_{B1} I_{B2}} \in \{0,1\}$, from S'_2 to either I_{B1} or I_{B2} where $K_{S'_2 I_{B1} I_{B2}} \in \{0,1\}$, from I_{A1} to either I_{B1} or I_{B2} where $K_{I_{A1} I_{B1} I_{B2}} \in \{0,1\}$, and from I_{A2} to either I_{B1} or I_{B2} where $K_{I_{A2} I_{B1} I_{B2}} \in \{0,1\}$, respectively. Let α be the rate that prey-infected or predator-infected nodes become susceptible again (α can also be different between prey and predator). The state transition indicators and α are used to identify the types of worm interactions. Let γ be the manual removal rate and γ_S be the manual vaccination rate.

For the aggressive one-sided interaction, $K_{S^*_1 I_{A1} I_{A2}} = K_{S^*_2 I_{A1} I_{A2}} = K_{S^*_1 I_{B1} I_{B2}} = K_{S^*_1 I_{B1} I_{B2}} = K_{S'_1 I_{B1} I_{B2}} = K_{S'_2 I_{B1} I_{B2}} = K_{I_{A1} I_{B1} I_{B2}} = K_{I_{A2} I_{B1} I_{B2}} = 1$ and $\alpha = 0$, for the conservative one-sided interaction, $K_{S^*_1 I_{A1} I_{A2}} = K_{S^*_2 I_{A1} I_{A2}} = K_{I_{A1} I_{B1} I_{B2}} = K_{I_{A2} I_{B1} I_{B2}} = 1$, $K_{S^*_1 I_{B1} I_{B2}} = K_{S^*_1 I_{B1} I_{B2}} = K_{S'_1 I_{B1} I_{B2}} = K_{S'_2 I_{B1} I_{B2}} = 0$ and $\alpha = 0$, for the aggressive two-sided interaction, $K_{S^*_1 I_{A1} I_{A2}} = K_{S^*_2 I_{A1} I_{A2}} = K_{S^*_1 I_{B1} I_{B2}} = K_{S^*_1 I_{B1} I_{B2}} = K_{S'_1 I_{B1} I_{B2}} = K_{S'_2 I_{B1} I_{B2}} = 1$, $K_{I_{A1} I_{B1} I_{B2}} = K_{I_{A2} I_{B1} I_{B2}} = 0$ and $\alpha = 0$.

Let $\lambda_{S^*_1 S^*_2}, \lambda_{S^*_2 S^*_1}, \lambda_{S'_1 S'_2}, \lambda_{S'_2 S'_1}, \lambda_{I_{A1} I_{A2}}, \lambda_{I_{A2} I_{A1}}, \lambda_{I_{B1} I_{B2}}$ and $\lambda_{I_{B2} I_{B1}}$ be the group transition rates from S^*_1 to S^*_2, S^*_2 to S^*_1, S'_1 to S'_2, S'_2 to S'_1, I_{A1} to I_{A2}, I_{A2} to I_{A1}, I_{B1} to I_{B2}, and I_{B2} to I_{B1}, respectively. Let $\Delta_{S^*_1}$, $\Delta_{S^*_2}$, $\Delta_{S'_1}$, and $\Delta_{S'2}$ be the batch arrival rates for S^*_1, S^*_2, S'_1, and S'_2, respectively.

The susceptible nodes' decrease rate is determined by manual vaccination and the contact of susceptible nodes with the prey-infected nodes (from the same or different group) causing the prey infection or with the predator-infected nodes (from the same or different group) causing the vaccination. On the other hand, the re-susceptible (infected nodes become susceptible again[2]) rate causes the increase for susceptible nodes. In addition, the number of susceptible nodes within each group can be changed due to the group transitions and batch arrival. Hence, the susceptible rates of group 1 and 2 are

[2] Some worms only reside in memory, and disappear after restart of the computer

$$\frac{dS^*_1}{dt} = -pS^*_1 (K_{S^*_1 I_{A1} I_{A2}} (\beta_{11} I_{A1} + \beta_{12} I_{A2}) + K_{S^*_1 I_{B1} I_{B2}} (\beta_{11} I_{B1} + \beta_{12} I_{B2})) + (\lambda_{S^*_2 S^*_1} S^*_2 - \lambda_{S^*_1 S^*_2} S^*_1) - \gamma_S S^*_1 + \alpha(I_{A1} + (1-i) I_{B1}) + \Delta_{S^*_1} \quad (2\text{-a})$$

$$\frac{dS^*_2}{dt} = -pS^*_2 (K_{S^*_2 I_{A1} I_{A2}} (\beta_{22} I_{A2} + \beta_{12} I_{A1}) + K_{S^*_2 I_{B1} I_{B2}} (\beta_{22} I_{B2} + \beta_{12} I_{B1})) - (\lambda_{S^*_2 S^*_1} S^*_2 - \lambda_{S^*_1 S^*_2} S^*_1) - \gamma_S S^*_2 + \alpha(I_{A2} + (1-i) I_{B2}) + \Delta_{S^*_2} \quad (2\text{-b})$$

$$\frac{dS'_1}{dt} = -pK_{S'_1 I_{B1} I_{B2}} S'_1 (\beta_{11} I_{B1} + \beta_{12} I_{B2}) + (\lambda_{S'_2 S'_1} S'_2 - \lambda_{S'_1 S'_2} S'_1) - \gamma_S S'_1 + \alpha i I_{B1} + \Delta_{S'_1} \quad (2\text{-c})$$

$$\frac{dS'_2}{dt} = -pK_{S'_2 I_{B1} I_{B2}} S'_2 (\beta_{22} I_{B2} + \beta_{12} I_{B1}) - (\lambda_{S'_2 S'_1} S'_2 - \lambda_{S'_1 S'_2} S'_1) - \gamma_S S'_2 + \alpha i I_{B2} + \Delta_{S'_2} \quad (2\text{-d})$$

Since the prey relies on susceptible nodes to expand its population, the increase of prey infection rate is determined by the contacts of susceptible nodes and prey-infected nodes. The decrease of prey infection rate is determined by prey termination caused by the contacts of prey-infected nodes and predator-infected nodes, the manual removal rate, and the re-susceptible rate. The other factors such as group transition and batch arrival are also applied to the prey infection rate. Hence, the prey infection rates for group 1 and 2 are

$$\frac{dI_{A1}}{dt} = p(K_{S^*_1 I_{A1} I_{A2}} S^*_1 (\beta_{11} I_{A1} + \beta_{12} I_{A2}) - K_{I_{A1} I_{B1} I_{B2}} I_{A1} (\beta_{11} I_{B1} + \beta_{12} I_{B2})) + (\lambda_{I_{A2} I_{A1}} I_{A2} - \lambda_{I_{A1} I_{A2}} I_{A1}) - (\alpha + \gamma) I_{A1} \quad (3\text{-a})$$

$$\frac{dI_{A2}}{dt} = p(K_{S^*_2 I_{A1} I_{A2}} S^*_2 (\beta_{22} I_{A2} + \beta_{12} I_{A1}) - K_{I_{A2} I_{B1} I_{B2}} I_{A2} (\beta_{22} I_{B2} + \beta_{12} I_{B1})) - (\lambda_{I_{A2} I_{A1}} I_{A2} - \lambda_{I_{A1} I_{A2}} I_{A1}) - (\alpha + \gamma) I_{A2} \quad (3\text{-b})$$

Because the predator can terminate its prey as well as vaccinate susceptible nodes, the increase of predator infection rate is determined by the contacts of the predator with either the susceptible nodes or prey-infected nodes. The decreases of prey-infected nodes are caused by manual removal rate and re-susceptible rate. The predator infection rates for group 1 and 2 are

$$\frac{dI_{B1}}{dt} = p(\beta_{11} I_{B1} + \beta_{12} I_{B2})(K_{S^*_1 I_{B1} I_{B2}} S^*_1 + K_{S'_1 I_{B1} I_{B2}} S'_1 + K_{I_{A1} I_{B1} I_{B2}} I_{A1}) + (\lambda_{I_{B2} I_{B1}} I_{B2} - \lambda_{I_{B1} I_{B2}} I_{B1}) - (\alpha + \gamma) I_{B1} \quad (4\text{-a})$$

$$\frac{dI_{B2}}{dt} = p(\beta_{22} I_{B2} + \beta_{12} I_{B1})(K_{S^*_2 I_{B1} I_{B2}} S^*_2 + K_{S'_1 I_{B1} I_{B2}} S'_2 + K_{I_{A2} I_{B1} I_{B2}} I_{A2}) - (\lambda_{I_{B2} I_{B1}} I_{B2} - \lambda_{I_{B1} I_{B2}} I_{B1}) - (\alpha + \gamma) I_{B2} \quad (4\text{-b})$$

Finally, the increase of removed nodes is caused by manual vaccination of susceptible hosts and manual removal of prey-infected and predator-infected nodes.

$$\frac{dR}{dt} = \gamma_S (S^*_1 + S^*_2 + S'_1 + S'_2) + r(I_{A1} + I_{A2} + I_{B1} + I_{B2}) \quad (5)$$

Our model addresses all worm interaction factors and can easily be extended to address other types of worms and a greater number of groups within the network. For example, the basic *SIR* model can also be derived from this model by setting $K_{S^*_1 I_{A1} I_{A2}} = 1$ and $\beta_{11} > 0, S^*_1 > 0, I_{A1} > 0, \gamma > 0$ while setting the other parameters to 0.

IV. EVALUATION

In this paper, we investigate worm interaction and validate our model using three approaches: (1) model analysis, (2) uniform-encounter-based simulation, and (3) trace-driven-encounter-based simulation. Our goal is to observe the relationships between our proposed model and the worm interaction factors. In

the model analysis, we provide basic conditions that can be used to obtain the metrics. In the uniform-encounter-based simulation, we investigate the effect of worm interaction types, network characteristics, and node characteristics on a simple uniform encounter-based network. We then evaluate our model on realistic trace-driven-encounter-based simulations. Let us start by analyzing the proposed model.

***A.* Model Analysis**

For brevity, we assume that there are no transitions between groups, i.e., $\lambda_{S^*_1 S^*_2} = \lambda_{S^*_2 S^*_1} = \lambda_{S'_1 S'_2} = \lambda_{S'_2 S'_1} = \lambda_{I_{A1} I_{A2}} = \lambda_{I_{A2} I_{A1}} = \lambda_{I_{B1} I_{B2}} = \lambda_{I_{B2} I_{B1}} = 0$. We focus our analysis on the aggressive one-sided interaction for two-group encounter-based networks. If we want to suppress the initial infection ($\frac{dI_{A1}}{dt} \le 0$ and $\frac{dI_{A2}}{dt} \le 0$ at t=0), from (3-a) and (3-b), then the required conditions for this are

$$S^*_1(0)(\beta_{11} I_{A1}(0) + \beta_{12} I_{A2}(0)) \le I_{A1}(0)(\beta_{11} I_{B1}(0) + \beta_{12} I_{B2}(0)) \tag{6-a}$$

$$S^*_2(0)(\beta_{22} I_{A2}(0) + \beta_{12} I_{A1}(0)) \le I_{A2}(0)(\beta_{22} I_{B2}(0) + \beta_{12} I_{B1}(0)) \tag{6-b}$$

where $I_{A1}(0), I_{A2}(0), I_{B1}(0), I_{B2}(0)$, $S^*_1(0)$, and $S^*_2(0)$ are the number of prey-infected nodes, predator-infected nodes, and susceptible nodes of group 1 and 2 at t=0, respectively.

From this condition, we obtain

$$TI = MI = I_{A1}(0) + I_{A2}(0),\ I_{A1}(\infty) = I_{A2}(\infty) = 0 \tag{7}$$

where $I_{A1}(\infty)$ and $I_{A2}(\infty)$ are the number of prey-infected nodes of group 1 and 2 at $t = \infty$.

However, we can see from (6-a) and (6-b) that the threshold can only be obtained from such conditions. If those conditions cannot be met, then we can only have a certain acceptable level of infection, and *TI* can be derived from

$$TI = p \int_{t=0}^{\infty} (S^*_2(\beta_{22} I_{A2} + \beta_{12} I_{A1}) + S^*_1(\beta_{11} I_{A1} + \beta_{12} I_{A2}))dt \tag{8}$$

MI can be found from $(I_{A1} + I_{A2})_{\max}$, where $\frac{dI_{A1}}{dt} = \frac{dI_{A2}}{dt} = 0$ at $t > 0$, in which

$$S^*_1(\beta_{11} I_{A1} + \beta_{12} I_{A2}) = I_{A1}(\beta_{11} I_{B1} + \beta_{12} I_{B2}) \tag{9-a}$$

$$S^*_2(\beta_{22} I_{A2} + \beta_{12} I_{A1}(0)) = I_{A2}(\beta_{22} I_{B2} + \beta_{12} I_{B1}) \tag{9-b}$$

Because *TL* is the accumulated life of an individual prey until the last prey has been removed by a predator whose duration indicated by *TR*, we can simply derive *TL* based on the numerical solutions from (3-a) and (3-b) as follows:

$$TL = \sum_{t=o}^{\infty} (I_{A1}(t) + I_{A2}(t))\Delta t \tag{10}$$

Since *AL* is the average lifespan for each node that has been terminated by a predator, which is equal to the number of nodes that are ever infected, *AL* can be derived from (8) and (10) as

$$AL = \frac{TL}{TI}. \tag{11}$$

We can find *TA,* which is derived from *t,* where $\frac{dS^*_1}{dt} = \frac{dS^*_2}{dt} = \frac{dS'_1}{dt} = \frac{dS'_2}{dt}$ $= \frac{dI_{A1}}{dt} = \frac{dI_{A2}}{dt} = \frac{dI_{B1}}{dt} = \frac{dI_{B2}}{dt} = 0$, $S^*_1(0) = I_{B1}(t)$, and $S^*_2(0) = I_{B2}(t)$, while *TR* is derived from *t* where $\frac{dI_{A1}}{dt} = \frac{dI_{A2}}{dt} = 0$, $I_{A1} = I_{A2} = 0$ and $TA \geq TR \geq t_B$ where t_B is the time of last batch arrival.

B. **Uniform-encounter-based simulations**

We use encounter-level simulations to simulate a simple uniform encounter of 1,000 mobile nodes of a uniform encounter-based network with no batch arrivals, and all nodes are susceptible to both prey and predator. Each simulation runs at least 1,000 rounds and we plot the median values for each position. We assume that there is only one group in the network with β = 5x10^{-5} sec^{-1} and two groups in part b.3 with $\beta_{11}, \beta_{12}, \beta_{22}$ between $3x10^{-5}$ to $30x10^{-5}$ sec^{-1}. In addition, we only assume the aggressive one-sided worm interaction in all parts except in part a.

Before discussing our simulation results, we need to define the important parameter, the initial-infected-node ratio, which we use for uniform-encounter-based simulations. Let Y be an initial-infected-node ratio of predator to prey of the whole network,

$$Y \equiv \frac{\sum_{j=1}^{g} I_{Bj(0)}}{\sum_{j=1}^{g} I_{Aj(0)}} \tag{12}$$

where *g* is the number of groups in the network and *j* is the group identification.

Along with the worm interaction factors, *Y* is used to investigate the outcomes of having a number of initial-predator-infected nodes more than the number of initial-prey-infected nodes within the same networks, given that *d* = 0 (non-zero-delay deployment is investigated in b.3).

a. Worm interaction types

As shown in Fig. 2, we can clearly see that the predator in aggressive one-sided interactions is much more effective than the predator in the other two worm interaction types for all metrics. Note that we have not shown *TA* for conservative one-sided and aggressive two-sided worm interaction because $TA = \infty$, and also did not show *TR, TL,* and *AL* for aggressive two-sided worm interaction because $TL = AL = TR = \infty$. Although *TI, MI, TL,* and *AL* in the conservative one-sided interaction is at least one order higher than those of aggressive one-sided interactions, *TR* in the conservative one-sided interaction is only two times higher than that of aggressive one-sided interaction (with the same *Y*). This small difference occurs simply because even with aggressive one-sided interaction, the predator infection rate is slowed down at the later state of the termination/vaccination period. The simplified model for

aggressive one-sided, conservative one-sided, and aggressive two-sided worm interactions are shown in Fig. 1b-d, respectively.

Next, we focus on the effects of large Y on our metrics only with the aggressive one-sided interaction. In Fig. 3a, *TI* and *MI decrease exponentially as Y increases.* We also find that if $S(0):I_B(0):I_A(0)$ is constant, then $MI:N$ and $TI:N$ are also constant even if N changes. From Fig. 3b, *TL decreases exponentially as Y increases. AL,* on the other hand*,* is almost constant for all Y. It is interesting to see that *TL* and *AL* merge at their minimum when $Y = Y_{max}$**. We can see that TL_{min} and AL_{min} do not reach zero at Y_{max} because the next encounter time of a prey-infected node with *any* of initial predator-infected nodes ($I_B(0)$) requires $1/I_B(0)\beta$. Furthermore, from (11), $TL_{min} = TI_{min}AL_{min}$, thus TL_{min} and AL_{min} merge to each other because $TI_{min} = I_A(0) = 1$.

Fig. 3c shows that *TR* decreases much faster than *TA* with an increase of Y. *TR* decreases exponentially as *Y increases*. *TA* begins to be reduced rapidly when $Y \approx Y_{max}$. At $Y_{max,}$ we can see that $TA_{min}=TR_{min}=AL_{min}$, Note that *TA* is also similar to the average time for every node to receive a copy of a message from a random source in an encounter-based network, which can be derived as $(2\ln N + 0.5772)/N\beta$ [3]. (**Y_{max}=1000*)*

b. Network characteristics

We start by examining the relationships of the aggressive one-sided interaction and the network characteristics: node size, contact rate, and group behavior. For contact rate and node size, we simply assume that the network only has one group in order to focus only on the effects of these factors on our metrics. After that, we would look deeper into the group behaviors including group size, contact rate within a group, and the contact rate between groups.

(1) Network size: In Fig. 4a and b, we find that *TI* and *MI* (as the fraction of N) for each Y but different N are saturated at the same fraction of N. This is because the fraction of N that the prey infects susceptible nodes and the fraction of N that the predator terminates/vaccinates are relatively equivalent for all Ns. Surprisingly, in Fig. 4c, *TL* becomes saturated at a certain absolute level and is also independent of N but depends only on Y. This occurs because the encounter rate (δ), which is the rate that a node encounters *any node* (i.e., $\delta = \beta(N-1)$) increases linearly with N (because β is fixed, but the number of pairs *N-1* increases as N increases) and causes a linear reduction of the time between encounter, causing *AL* to be reduced proportionally to N (as shown in Fig. 4d) while *TI is also* increased proportionally to N (as shown in Fig. 4a). The product of these two numbers yields the constant *TL*. In Fig. 4e and f, the impact of N on *TA* and *TR* is quite similar to *AL*. It is interesting to see that for $Y = 1$ (1:1), $TA = TR$ for all N, and hence this implies that the time to remove all preys is simply the time that a predator needs to infect and remove the prey from all nodes (when $Y = 1$). In summary, we can see that N linearly increases *TI* and *MI* and exponentially reduces *AL*, *TA,* and *TR*. The effects of N_n (group size) are further investigated in part c.3.

(2) Contact rate: As shown in Fig. 5a and b, as expected, *TI* and *MI* for each *Y* are relatively constant even with the increase of β (because of the equal change of dI_A/dt and dI_B/dt). Similar to *N,* as the δ increases (fixed number of pairs *N*-1, but β increases*)*, and β exponentially decreases *AL*, *TA,* and *TR*. However, unlike *N*, *TL* is reduced exponentially as β increases*,* simply because *TI* is constant for all β. In addition*,* the lower the *Y,* the greater the impact caused by β will be. The effects of contact rate of multiple groups are examined next.

(3) Group behavior: Earlier, we only assumed single-group behavior in a network; in this part, we will discuss the two-group behavior. Here we look into the effect of group size, the contact rate of one of the two groups, and the contact rate between two groups on the worm interactions.

We begin by investigating the effects of group sizes as the fraction of fixed *N* (1000 nodes) where $\beta_{11} = 6x10^{-5}\ \text{sec}^{-1}, \beta_{22} = 9x10^{-5}\ \text{sec}^{-1}$, and $\beta_{12} = 3x10^{-5}\ \text{sec}^{-1}$. Group 1 and group 2 are called the "slow group" and "fast group", respectively. For the first part (Fig. 6a, b and c), an initial prey-infected node is in the slow group and an initial predator-infected node is in the fast group (slow-prey-fast-predator case). In the second part (Fig. 6d, e and f), an initial prey-infected host is in the fast group and an initial predator-infected node is in the slow group (fast-prey-slow-predator case).

In Fig. 6a and d, we see that as the size of the *fast* group *increases*, *TI*, *MI*, and *TL* linearly *decrease*. This indicates the independence of which group has the initial predator-infected node or the initial prey-infected node. As *TI* and *TL* linearly decrease with the same rate as the increase of the fast-group size, then *AL* is almost constant for all group sizes. *TA* and *TR* increase gradually as the slow-group size increases (and the fast-group size decreases), and drop gradually after reaching their peak value. This occurs because of the low contact rate between groups.

In Fig. 7, we show the impact of the contact rate of the initial-prey-infected-node group where the contact rate of the initial prey group $\beta_{11} = 3$ to $30\text{x}10^{-5}\ \text{sec}^{-1}$, the contact rate of the initial predator group $\beta_{22} = 15\text{x}10^{-5}\ \text{sec}^{-1}$, and the contact rate between group $\beta_{12} = 3\text{x}10^{-5}\ \text{sec}^{-1}$. As expected, *TI*, *MI,* and *TL* increase linearly as β_{11} increases, while *TA* and *TR* decrease exponentially as β_{11} increases. This effect is similar to the increase of contact rate in a single group (fig. 5e-f).

In Fig. 8, we show the impact of the contact between groups where $\beta_{11} = 3\text{x}10^{-5}\ \text{sec}^{-1}$, $\beta_{22} = 15\text{x}10^{-5}\ \text{sec}^{-1}$, and $\beta_{12} = 3$ to $30\text{x}10^{-5}\ \text{sec}^{-1}$. As shown in Fig. 8a-b, as β_{12} increases, the prey in the slow-prey-fast-predator can infect more susceptible nodes and the predator in the fast-prey-slow-predator can terminate more preys and vaccinate more susceptible nodes (as indicated by *TI* and *MI*). Hence, the *contact rate between groups* only helps the *prey or predator in the slower group* to infect relatively more nodes than the one in the faster group (i.e., worms in both groups infect nodes faster, but the one in slower group has higher relative improvement). However, *TL*, *AL*, *TA,* and *TR* decrease as the contact rate between the group increases for all cases (slow-prey-fast-predator and fast-prey-slow-predator cases), and because δ

increases. We evaluate the group characteristics again in trace-driven encounter-based networks (Section C).

c. Node characteristics

We vary the cooperation (c) from 20% to 100%, the immunization (i) from 0% to 90% with 100% "*on*" time for the first part of experiments (Fig. 9a-f), and we vary the "*on*" time from 10% to 90% with 90% cooperation and 10% immunization, for the second part (Fig.9g-h). The first part aims to analyze the impact of cooperation and immunization, whereas the second part aims to analyze the *on-off* behavior on aggressive one-sided worm interaction. In this simulation, again we assume only a single group within the network. Simplified node-characteristic-based aggressive one-sided interaction is shown in Fig. 1e.

(1) Cooperation: In Fig. 9a-f, we find that cooperation surprisingly reduces prey infection for every metric. (Note that cooperation actually increases absolute *TI* and absolute *MI*, but relative *TI* (or TI/N^*) and relative *MI* (or MI/N^*) are decreased where the number of cooperative-susceptible nodes $N^* = c(1-i)N$). *We can observe that cooperation reduces AL, TA,* and *TR significantly* more than it does to *TI*, *MI,* and *TL*.

(2) Immunization: Similarly, for immunization Fig. 9a-f shows that immunization reduces all categories of metrics except *TA* and *AL*. With the increase of immunization, *TI* is reduced much faster than *TL;* thus an increase of immunization increases *AL*. Furthermore, an increase of immunization, as expected, reduces *TR* because of a smaller number of possible prey-infected nodes.

Immunization reduces relative TI, relative MI, and TL more significantly than it does *TR*. With an equal increase (20% to 80%), immunization at cooperation = 100% reduces relative *TI*, relative *MI,* and *TL* approximately 8.8 times, 2.7 times, and 10.6 times, respectively, more than cooperation does at immunization = 0%. On the other hand, cooperation reduces *TR* approximately 3.3 times more than immunization does.

As shown in Fig. 9e, unlike cooperation, immunization *cannot* reduce *TA*.

(3) *On-off* behavior: The impact of *on-off* behavior (p) is clear in Fig. 9g-h. As expected, with varying *"on" time*, relative *TI* and relative *MI do not change*. The ratio of contact rate between predator and prey is an indicator of the fraction of infected nodes irrespective of the contact rate. In this case, the ratio of the contact rate is always 1.0, and hence relative *TI* and relative *MI* are constant. Because of the increase of *"on" time* causing a reduction of time between consecutive encounters between nodes, *TL*, *AL TA,* and *TR exponentially decrease as p increases*.

(4) Delay: As shown in Fig. 9i, the delay *(d)* causes absolute *TI* and absolute *MI* to linearly increase until the number of prey-infected node reaches the *N*. Similarly, in Fig. 9k, *TA* and *TR* also increase linearly as *d* increases. The increase of *TA* and *TR* is simply the delay. In addition, *TA* and *TR* merge after a certain delay. *TL* and *AL* slowly increase as *d* increases (Fig. 9j).

Next, we will apply what we have learned from the simulation of worm interaction in the uniform-encounter-based networks to realistic non-uniform encounter-based networks.

C. Trace-driven encounter-based simulations

We investigate the consistency of the model-based results with those generated using measurement-based real encounters. We drive our encounter-level simulations using the wireless network traces of the University of Southern California from 62 days in the spring 2006 semester [5]. We define an encounter as two nodes sharing the same access point at the same time. We randomly choose 1,000 random nodes from the 5,000 most active nodes based on their online time from the trace. Their median β is 1.27×10^{-6} sec^{-1} and the median number of unique encounter nodes is 94. We use $I_A(0)=1$ and $I_B(d)=1$, where d is the delay between the initial predator-infected node and the initial prey-infected node in the simulation. This delay was introduced as the traced delay between the first arrival of two groups, where the initial predator-infected node and the initial prey-infected node are assumed to be in different groups (and different batch arrivals). The first group and second group account for approximately 90% and 10% of total population, respectively. The first group has an average contact rate $\beta_{11}=3.6 \times 10^{-6}$ sec^{-1}, the second group has an average contact rate $\beta_{22}=3.3 \times 10^{-6}$ sec^{-1}, and the approximate contact rate between the groups $\beta_{12}=4 \times 10^{-7}$ sec^{-1}. When the contact rate of the initial predator-infected node is higher than that of the initial prey-infected node, we call this scenario "*Fast predator*". On the other hand, when the contact rate of the initial predator-infected node is lower than that of the prey, we call this scenario "*Slow predator*". From the trace, the median arrival delay between the initial predator-infected node and the initial prey-infected node is 8.7 days (introduced by the gap between the first and the second batch arrivals). Because the first group is in the first batch, "*Fast predator*" is also the *early* predator and "Slow predator" is also the *late* predator.

We can see the consistent batch arrival pattern in Fig. 7c, where each line represents a different start new-node arrival time into the networks, i.e., day 0, 10, 20, and 30, where day 0 is January 25, 2006. At the beginning of the semester, not all students had returned to campus; hence, the large gap between batch arrivals existed. The smaller gaps (1 day) in other start days were caused by the university's schedule, which has classes either on Tuesday-Thursday or Monday-Wednesday-Friday. *Hence, the batch arrival patterns are likely to occur in any encounter-based networks due to the users' schedules*. In addition, in Fig. 10a-b, we find that a user's encounter in the trace is highly skewed (non-uniform), i.e., the top 20% of a user's total encounter accounts for 72% of all users' encounters, and 70% of users encounter less than 20% of total unique users, which are caused by non-uniform *on-off behavior and location preferences* [5, 6].

We choose to run our trace-driven simulations at day 0 to determine the significance of batch arrival patterns on worm interactions. To validate our model accuracy, we compare the trace-driven simulation results with our aggressive one-sided model with node characteristics and group behavior. We also apply the batch arrival and delay to our model and compare the trace-driven simulation results with our model plot.

In our model, we use $\beta_{11} = 3.6x10^{-6}, \beta_{22} = 3.3x10^{-6}, \beta_{12} = 4x10^{-7}$ with t_1= day 8.7 (second batch arrival, 395 nodes join group 1, 50 nodes join group 2), t_2 = day 8.71 (all predator-infected nodes leaving the networks), t_3 = day 11.57 (predator-infected nodes rejoin the networks), t_4 = day 17.4 (third batch arrival, 50 nodes join group 2), t_4 = day 40.5 (fourth batch arrival, 5 nodes join group 2). These batch arrival patterns are approximated from the observed trace and simulations.

In Fig. 10f-i and l-o, these batch arrival patterns and the delay cause significant additions to our proposed metrics, especially *TL*, *AL*, *TA*, and *TR* (*TA* is subject to the time of the last-node arrival). In addition, we find that immunization (*i*) is still a very important factor to reduce relative *TI*, relative *MI*, *TL*, and *TR,* in the *"Slow predator"* case, but it does not have much impact in the "*Fast predator*" case, since there is not much room for improvement (except *TL*). However, unlike uniform-encounter worm interaction, we find that *cooperation only helps reduce relative TI, relative MI, TL, AL, and TR in the "Fast predator" case*.

In Fig. 10d-f, relative *TI,* relative *MI, and TL* with "*Slow predator*" almost linearly decrease to zero with an increase of *i*. Hence*, large immunization can offset large delay*. Surprisingly, as shown in Fig. 10g and m, *AL* with "*Fast predator*" did not show significant improvement over *AL* with "*Slow predator*".

Our model seems to more accurately predict the metrics in the "*Slow predator*" case, in which the delay and batch arrival patterns are the major factors. On the other hand, for the "*Fast predator", TI* and *MI* (Fig.10j-k) are more sensitive to fine-grained non-uniform encounter patterns in which we simplify them to only two-group encounters. With the number of groups precisely estimated, the accuracy of the metrics estimations can be drastically improved.

V. SUMMARY AND FUTURE WORK

In this paper, we propose a general worm interaction model addressing worm interaction types, network characteristics, and node characteristics for encounter-based networks. In addition, new metrics as a performance evaluation framework for worm interactions are proposed. We find that a predator is most effective in aggressive one-sided worm interaction. In addition, we find that in uniform and realistic encounter-based networks, immunization and delay are the most influential node characteristics for total prey-infected nodes, maximum prey-infected nodes, and total prey lifespan. Cooperation and *on-off* behaviors greatly affect average individual prey lifespan, time to secure all nodes, and time to remove all preys in uniform encounter-based networks. Furthermore, for multi-group uniform-encounter-based networks, large group size with fast contact rate helps limit total prey-infected nodes and maximum prey-infected nodes. Fast contact rates between groups reduce average individual prey lifespan, time to secure all nodes, and time to remove all preys. Our model shows very good agreement with uniform-encounter simulation results.

Based on realistic mobile networks measurements, we find that batch arrivals are common in the trace and are likely to take place in any encounter-based networks. In addition, we also find that the contact rate

and the number of unique encounters of users are highly skewed. This network characteristic causes worm infection behavior to deviate from our predictions, even though the general trends remain similar to the model. We believe that our general worm interaction model can be extended to incorporate fine-grained and dynamic user groups to enhance the accuracy of prediction.

In such networks, immunization and timely predator deployment seem to be more important factors than cooperation. Hence, enforcing early immunization and having a mechanism to identify a high-contact-rate group to deploy an initial predator-infected node is critical to containing worm propagation in encounter-based networks. These findings provide insight that we hope will aid in the development of counter-worm protocols in future encounter-based networks.

References

[1] F. Castaneda, E.C. Sezer, J. Xu, *"WORM vs. WORM: preliminary study of an active counter-attack mechanism"*, ACM workshop on Rapid malcode, 2004

[2] Z. Chen, L. Gao, and K. Kwiat, "*Modeling the Spread of Active Worms*", IEEE INFOCOM 2003

[3] D.E. Cooper, P. Ezhilchelvan, and I. Mitrani, *A Family of Encounter-Based Broadcast Protocols for Mobile Ad-hoc Networks*, In Proceedings of the Wireless Systems and Mobility in Next Generation Internet. 1st International Workshop of the EURO-NGI Network of Excellence, Dagstuhl Castle, Germany, June 7-9 2004

[4] W. Hsu, A. Helmy, "*On Nodal Encounter Patterns in Wireless LAN Traces*", The 2nd IEEE Int.l Workshop on Wireless Network Measurement (WiNMee), April 2006.

[5] W. Hsu, A. Helmy, "*On Modeling User Associations in Wireless LAN Traces on University Campuses*", The 2nd IEEE Int.l Workshop on Wireless Network Measurement (WiNMee), April 2006.

[6] A. Ganesh, L. Massoulie and D. Towsley, *The Effect of Network Topology on the Spread of Epidemics*, in IEEE INFOCOM 2005.

[7] W. O. Kermack and A. G. McKendrick: "*A Contribution to the Mathematical Theory of Epidemics"*. Proceedings of the Royal Society 1997; A115: 700-721.

[8] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "*Internet Quarantine: Requirements for Containing Self Propagating Code*", in IEEE INFOCOM 2003.

[9] D. M. Nicol, "*Models and Analysis of Active Worm Defense*", Proceeding of Mathematical Methods, Models and Architecture for Computer Networks Security Workshop 2005.

[10] P. Szor, "*The Art of Computer Virus Research and Defense*" (Symantec Press) 2005

[11] S. Tanachaiwiwat, A. Helmy, "*Worm Ecology in Encounter-based Networks (Invited Paper)*" *IEEE Broadnets* 2007

[12] S.Tanachaiwiwat, A. Helmy, "*On the Performance Evaluation of Encounter-based Worm Interactions Based on Node Characteristics*" ACM CHANTS 2007, Mobicom Workshop.

[13] Trend Micro Annual Virus Report 2004 http://www.trendmicro.com

[14] H. Trottier and P. Phillippe, "*Deterministic Modeling Of Infectious Diseases: Theory And Methods*" The Internet Journal of Infectious Diseases ISSN: 1528-8366

[15] A.Vahdat and D. Becker. *Epidemic routing for partially connected ad hoc networks*. Technical Report CS-2000.

[16] M. Vojnovic and A. J. Ganesh, *"On the Effectiveness of Automatic Patching"* , ACM WORM 2005, The 3rd Workshop on Rapid Malcode, George Mason University, Fairfax, VA, USA, Nov 11, 2005.

[17] X. Zhang, G. Neglia, J. Kurose, and D. Towsley. "*Performance Modeling of Epidemic Routing*", to appear Elsevier Computer Networks journal, 2007

[18] C. C. Zou, W. Gong and D. Towsley, "*Code red worm propagation modeling and analysis*" Proceedings of the 9th ACM CCS 2002

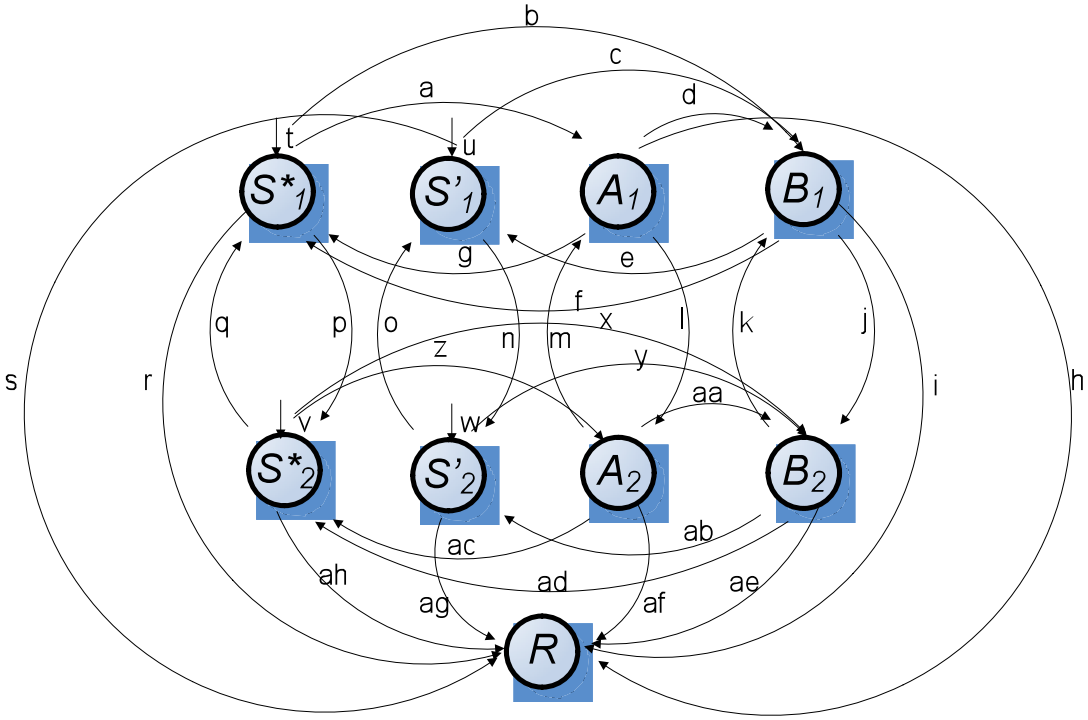
Sapon Tanachaiwiwat holds a B.S. in Electrical Engineering from the Mahidol University, Bangkok; a M.S. in Electrical Engineering, and a Ph.D. in Computer Engineering, both from the University of Southern California. His doctoral dissertation focuses on the analysis of worm propagations and interactions in wired and wireless computer networks. He has participated in the ACQUIRE project (Active Query in Wireless Sensor Networks) funded by the National Science Foundation.
His main research interests are in modeling, designing and implementing algorithms and protocols for large-scaled simulation and real-time systems. He is a project manager at the Innovative Scheduling, Inc. He is currently involved in building a decision support system for routing of locomotives to shops for quarterly maintenances. This project involves developing and implementing algorithms for real-time routing of locomotives to shops such that locomotives reach shops just-in-time and consistent with the shop capacities.

Ahmed Helmy received the BS degree in electronics and communications engineering with highest honors and the MS Eng. Math. degree from Cairo University, Egypt, in 1992 and 1994, respectively, and the MS degree in electrical engineering and the PhD degree in computer science from the University of Southern California (USC) in 1995 and 1999, respectively. He is an associate professor and the founder and director of the wireless networking laboratory in the Computer and Information Science and Engineering (CISE) Department, University of Florida, Gainesville. From 1999 to 2006, he was an assistant professor of electrical engineering (EE) at the University of Southern California. He was also the founder and director of the wireless networking laboratory at USC. He was a key researcher in the network simulator (NS-2) and the protocol independent multicast (PIM-SM) projects in the Information Sciences Institute (ISI), USC. His research interests lie in the areas of network protocol design and analysis for mobile ad hoc and sensor networks, mobility modeling, design and

testing of multicast protocols, IP micromobility, and network simulation. In 2002, he received the US National Science Foundation (NSF) CAREER Award. In 2000, he received the USC Zumberge Research Award, and in 2002, he received the best paper award from the IEEE/IFIP International Conference on Management of Multimedia and Mobile Networks and Services (MMNS). In 2003, he was the EE nominee for the USC Engineering Jr. Faculty Research Award and a nominee for the Sloan Fellowship. In 2004 and 2005, he got the best merit ranking in the EE-USC faculty. In 2007, he was a winner in the ACM MobiCom SRC research competition. He has been an area editor of the Adhoc Networks Journal, published by Elsevier, since 2007 (editor since 2004). He is the co-chair for the IFIP/IEEE MMNS 2006 and IEEE INFOCOM Global Internet Workshop 2008 and the vice chair for IEEE ICPADS 2006 and HiPC 2007. He has been the ACM SIGMOBILE workshop coordination chair (for ACM MobiCom, MobiHoc, MobiSys, and SenSys) since 2006. He served on the program committees for numerous IEEE and ACM conferences in the areas of computer and wireless networks.

Table I. Parameters and definitions

Parameter	Definition
S, S_n	Susceptible nodes: the number of nodes in the whole population that can be infected by either prey or predator, the number of susceptible nodes of group *n*
S^*_n, S'_n	Number of susceptible nodes of group *n* that can be infected by either prey or predator, the number of susceptible nodes of group *n* that can be infected by predator only
I_A , I_B	Prey-infected nodes: the number of nodes infected by prey in a whole population, Predator-infected nodes: the number of nodes infected by predator in a whole population
I_{An} , I_{Bn}	Prey-infected nodes: the number of nodes infected by prey in group *n*, Predator-infected nodes: the number of nodes infected by predator in group *n*
N, N^*, N_n	Total number of vulnerable nodes in the networks: it is the sum of the number of susceptible nodes, prey-infected nodes, and predator-infected nodes, total number of cooperative-susceptible nodes in a whole population, total number of vulnerable nodes of group *n*
β , β_{nm}	Pair-wise contact rate: a frequency that a pair of nodes makes contact with each other in a whole population, a contact rate between a member in group *n* and a member in group *m*.
δ	Encounter rate: the frequency that a node encounters any other node in the same network
Y	Initial-infected-nodes ratio: the ratio between predator-infected nodes and prey-infected nodes in the whole population at $t = 0$.
c	Cooperation: a node's willingness to forward messages for others in the population (fraction)
i	Immunization: immune nodes (fraction) of the whole population that will not be infected by prey
p	On-off behavior: "*on*" nodes can participate in forwarding packets, while "*off*" nodes cannot (probability)
d	Delay: the time differences between initial prey-infected nodes and initial predator-infected nodes
a	Re-susceptible: infected nodes can become susceptible again
$K_{S^*_1 I_{A1} I_{A2}}$, $K_{S^*_2 I_{A1} I_{A2}}$, $K_{S^*_1 I_{B1} I_{B2}}$, $K_{S^*_2 I_{B1} I_{B2}}$, $K_{S'_1 I_{B1} I_{B2}}$, $K_{S'_2 I_{B1} I_{B2}}$, $K_{I_{A1} I_{B1} I_{B2}}$, $K_{I_{A2} I_{B1} I_{B2}}$	State transition indicators: the numbers (0 or 1) used to identify the types of worm interaction types
$\Delta_{S^*_1}$, $\Delta_{S^*_2}$, $\Delta_{S'_1}$, $\Delta_{S'2}$	Batch arrival (and departure) rate: the rate that new vulnerable nodes join (or leave) into the networks
$\lambda_{S^*_n S^*_m}, \lambda_{S'_n S'_m}, \lambda_{I_{An} I_{Am}}, \lambda_{I_{Bn} I_{Bm}}$	Group transition rate: rates of susceptible nodes, susceptible nodes which are immune to prey, prey-infected nodes, predator-infected nodes in group *n* become susceptible nodes, susceptible nodes which are immune to prey, prey-infected nodes, predator-infected nodes in group *m*, respectively



$a : pK_{S^*_1 I_{A1} I_{A2}} S^*_1 (\beta_{11} I_{A1} + \beta_{12} I_{A2})$

$b : pK_{S^*_1 I_{B1} I_{B2}} S^*_1 (\beta_{11} I_{B1} + \beta_{12} I_{B2})$

$c : pK_{S'_1 I_{B1} I_{B2}} S'_1 (\beta_{11} I_{B1} + \beta_{12} I_{B2})$

$d : pK_{I_{A1} I_{B1} I_{B2}} I_{A1} (\beta_{11} I_{B1} + \beta_{12} I_{B2})$

$e : \alpha i I_{B1}$

$f : \alpha (1-i) I_{B1}$

$g : \alpha I_{A1}$

$h : \gamma I_{A1}$

$i : \gamma I_{B1}$

$j : (\lambda_{I_{B1} I_{B2}} - \lambda_{I_{B2} I_{B1}}) I_{B1}$

$k : (\lambda_{I_{B2} I_{B1}} - \lambda_{I_{B1} I_{B2}}) I_{B2}$

$l : (\lambda_{I_{A1} I_{A2}} - \lambda_{I_{A2} I_{A1}}) I_{A1}$

$m : (\lambda_{I_{A2} I_{A1}} - \lambda_{I_{A1} I_{A2}}) I_{A2}$

$n : (\lambda_{S'_1 S'_2} - \lambda_{S'_2 S'_1}) S'_1$

$o : (\lambda_{S'_2 S'_1} - \lambda_{S'_1 S'_2}) S'_2$

$p : (\lambda_{S^*_1 S^*_2} - \lambda_{S^*_2 S^*_1}) S^*_1$

$q : (\lambda_{S^*_2 S^*_1} - \lambda_{S^*_1 S^*_2}) S^*_2$

$r : \gamma_S S^*_1$

$s : \gamma_S S'_1$

$t : \Delta_{S^*_1}$

$u : \Delta_{S'_1}$

$v : \Delta_{S^*_2}$

$w : \Delta_{S'_2}$

$x : pK_{S^*_2 I_{B1} I_{B2}} S^*_2 (\beta_{22} I_{B2} + \beta_{12} I_{B2})$

$y : pK_{S'_2 I_{B1} I_{B2}} S'_2 (\beta_{22} I_{B2} + \beta_{12} I_{B1})$

$z : pK_{S^*_2 I_{A1} I_{A2}} S^*_2 (\beta_{22} I_{A2} + \beta_{12} I_{A1})$

$aa : pK_{I_{A2} I_{B1} I_{B2}} I_{A2} (\beta_{22} I_{B2} + \beta_{12} I_{B1})$

$ab : \alpha i I_{B2}$

$ac : \alpha I_{A2}$

$ad : \alpha (1-i) I_{B2}$

$ae : \gamma I_{B2}$

$af : \gamma I_{A2}$

$ag : \gamma_S S'_2$

$ah : \gamma_S S^*_2$

Figure 1(a): General worm interaction model state diagram

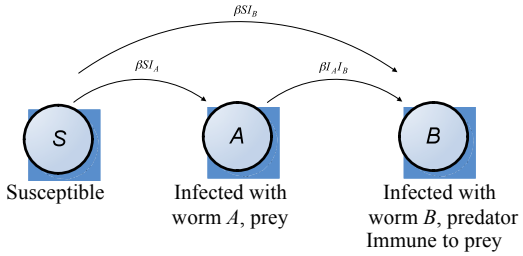


Figure 1(b): Aggressive one-sided interactions

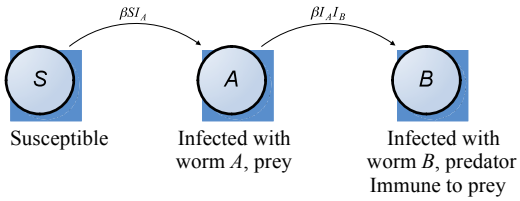


Figure 1(c): Conservative one-sided interactions

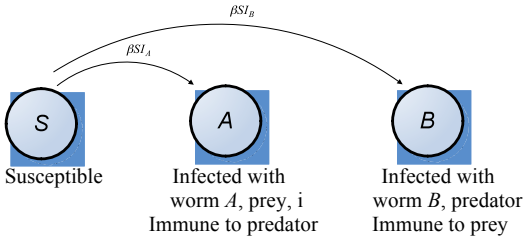


Figure 1(d): Aggressive Two-sided Interaction

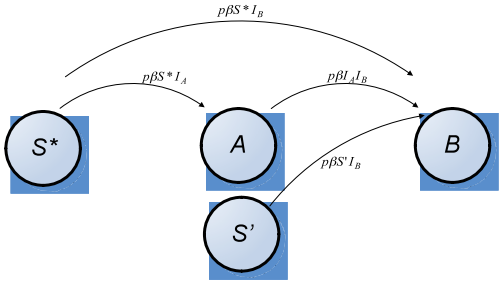
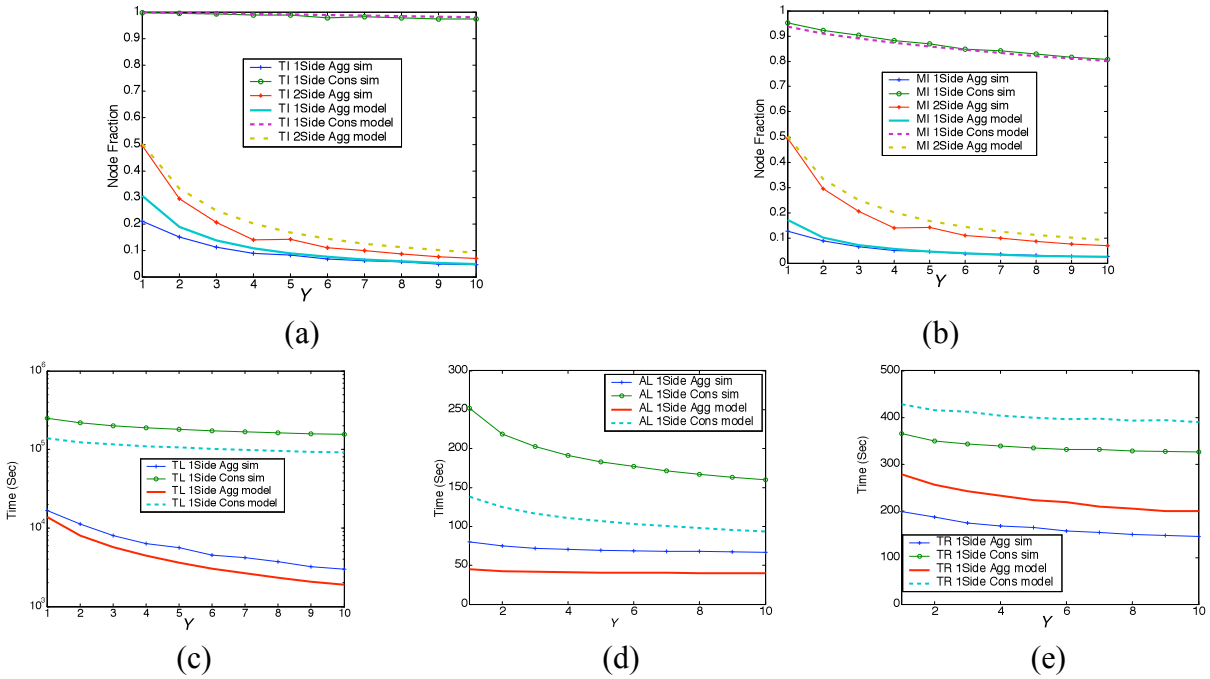


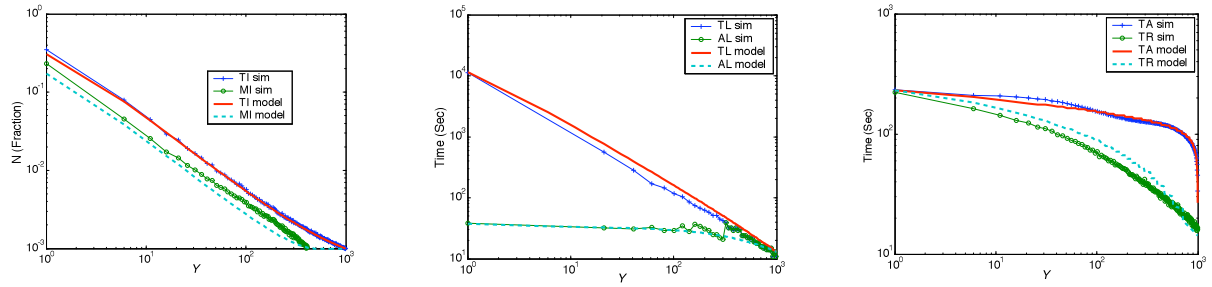
Figure 1(e): Aggressive one-sided interaction with node characteristics



(a) (b)

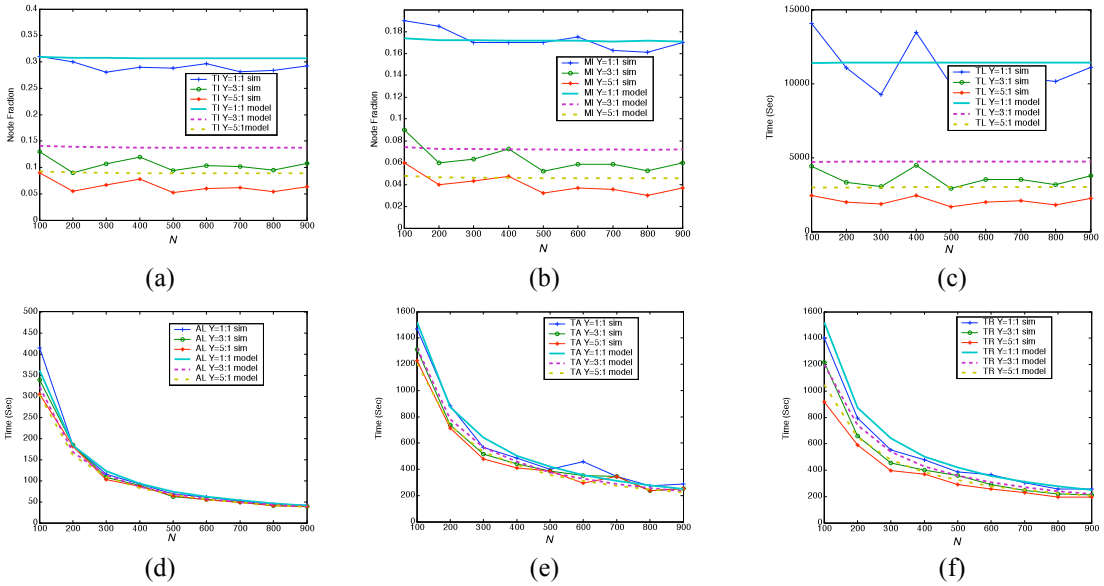
(c) (d) (e)

Figure 2: Relationships of worm characteristics with *Y*



(a) (b) (c)

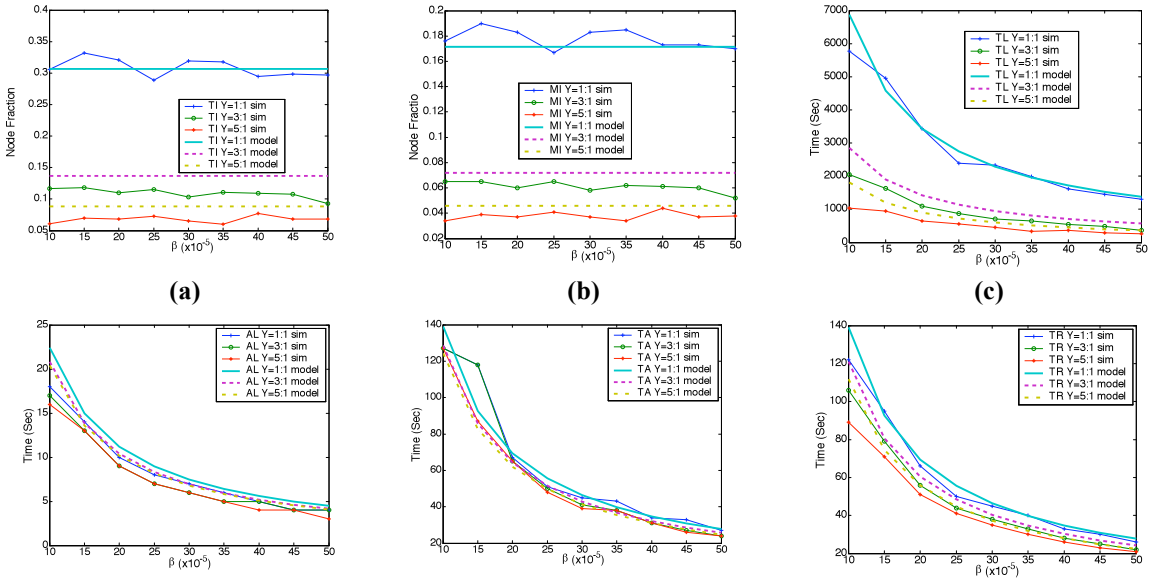
Figure 3: Relationships of aggressive one-side interaction with *Y*



(a) (b) (c)

(d) (e) (f)

Fig. 4 Relationships of *N* with metrics



(a) (b) (c)

(d) (e) (f)

Fig. 5 Relationships of *β* with metrics

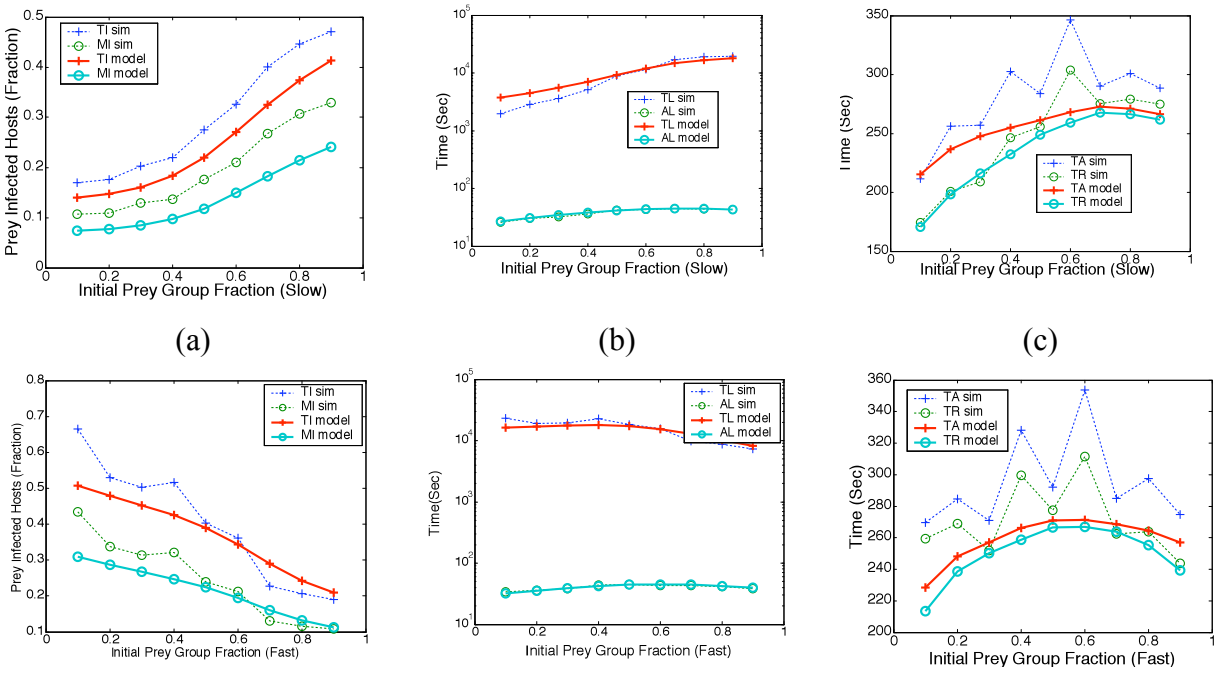


Figure 6: Effects of group size in two-group population: slow group (contact rate=6x10^{-5} sec^{-1}) and fast groups (contact rate= 9x10^{-5} sec^{-1} and contact rate between group =3x10^{-5} sec^{-1}) for Slow prey Fast predator (a, c and e) and Fast prey Slow predator (b, d and f) models

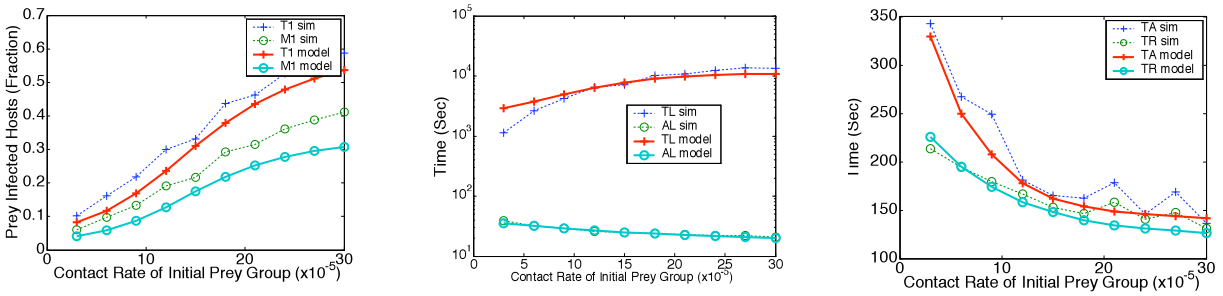


Figure 7: Effects of initial-prey-infected-node group's contact rate in a two group population: varied-contact-rate of initial-prey-infected-node group (contact rate=3 to 30x10^{-5} sec^{-1}) and fixed-contact-rate of initial predator group (contact rate= 15x10^{-5} sec^{-1} and contact rate between group =3x10^{-5} sec^{-1})

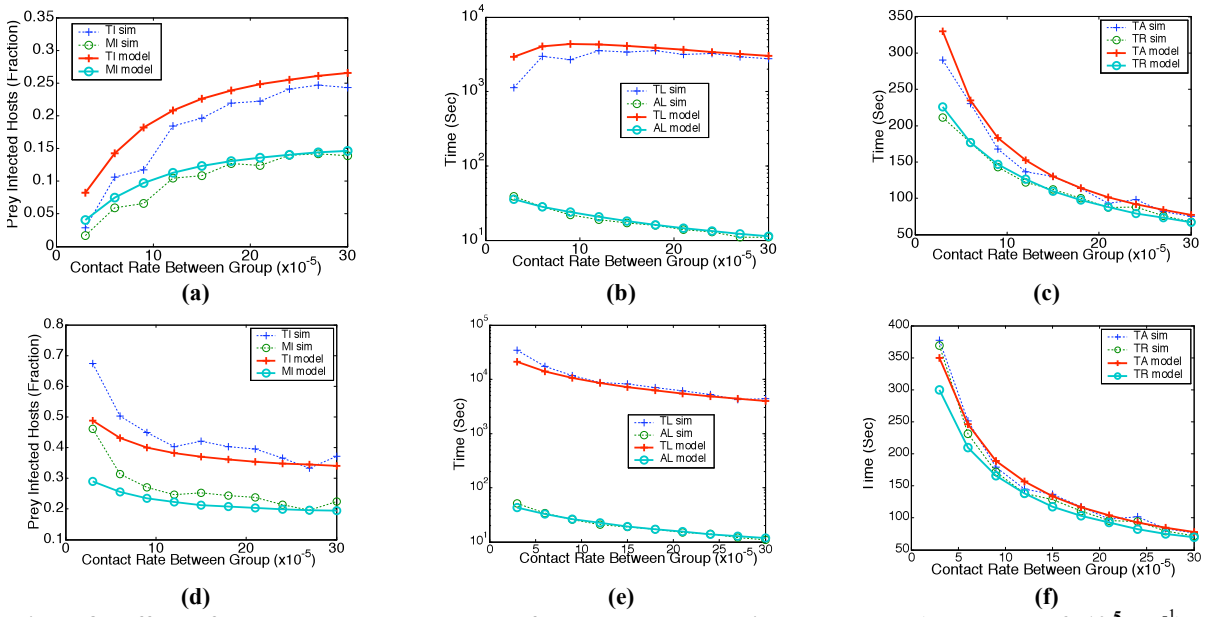
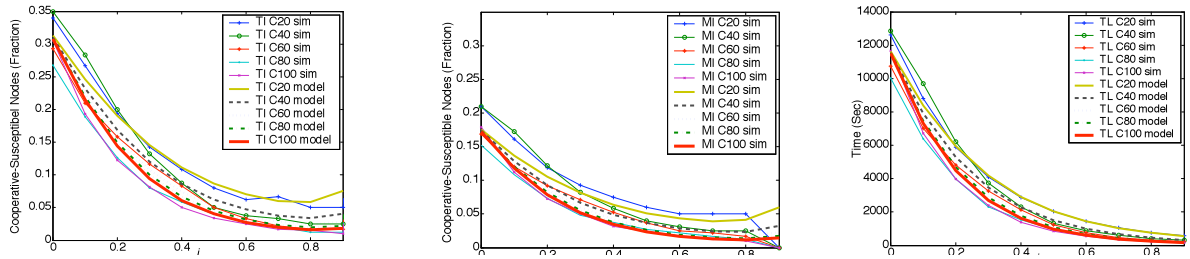


Figure 8: Effects of contact rate between groups of a two-group population: slow group (contact rate=$3x10^{-5}$ sec^{-1}) and fast encountered groups (contact rate= $15x10^{-5}$ $sec^{-1}$and contact rate between group =3 to $30x10^{-5}$ sec^{-1}) for Slow prey Fast predator (a, c and e) and Fast prey Slow predator (b, d and f)



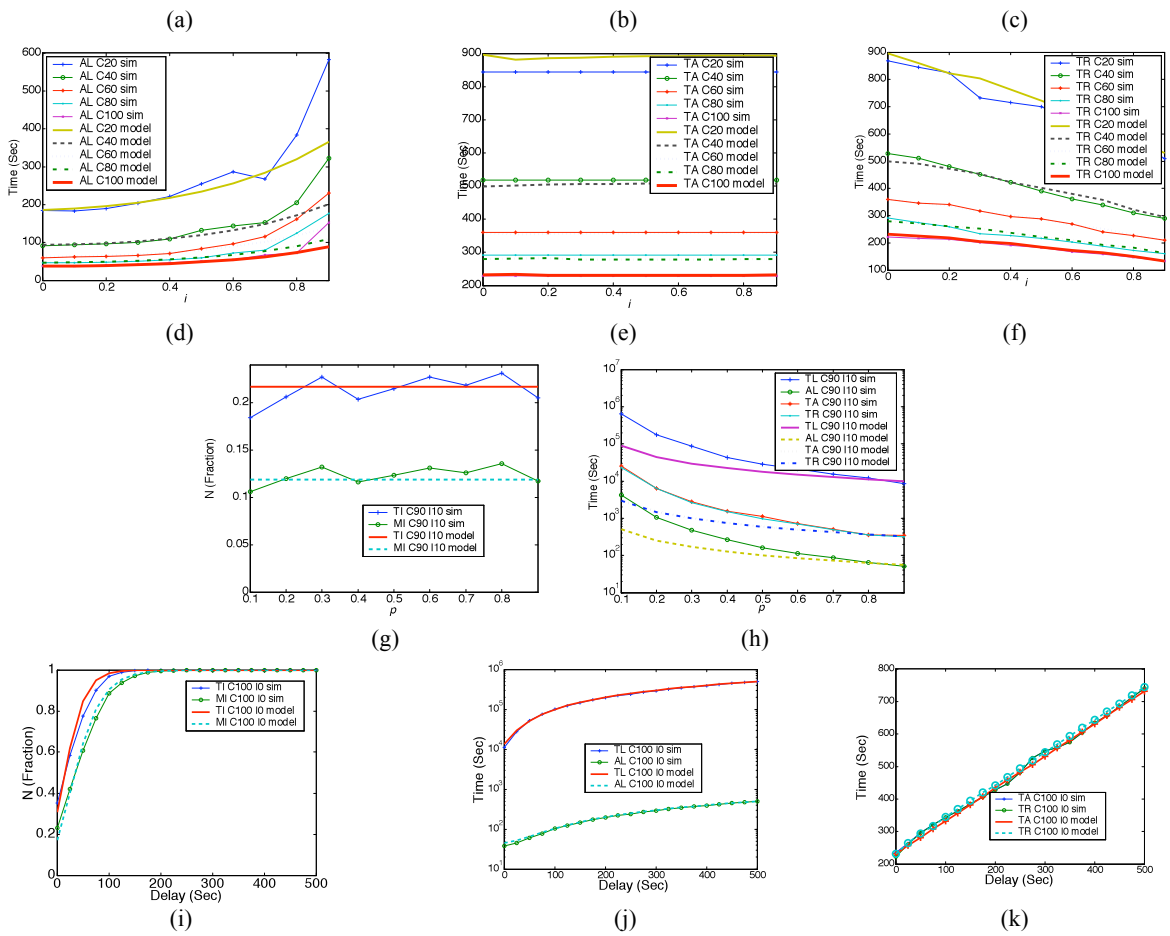
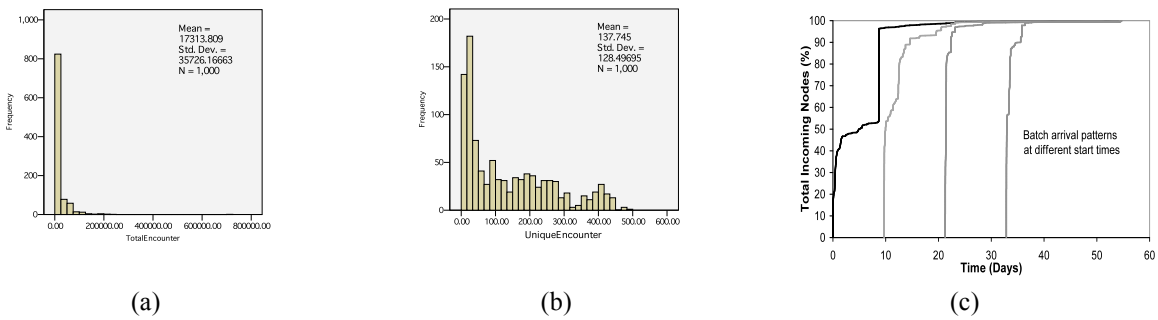


Figure 9: Effects of cooperation (*c*), immunization (*i*), *on-off* behavior (*p*), and delay (*d*) on uniform-encounter worm interactions



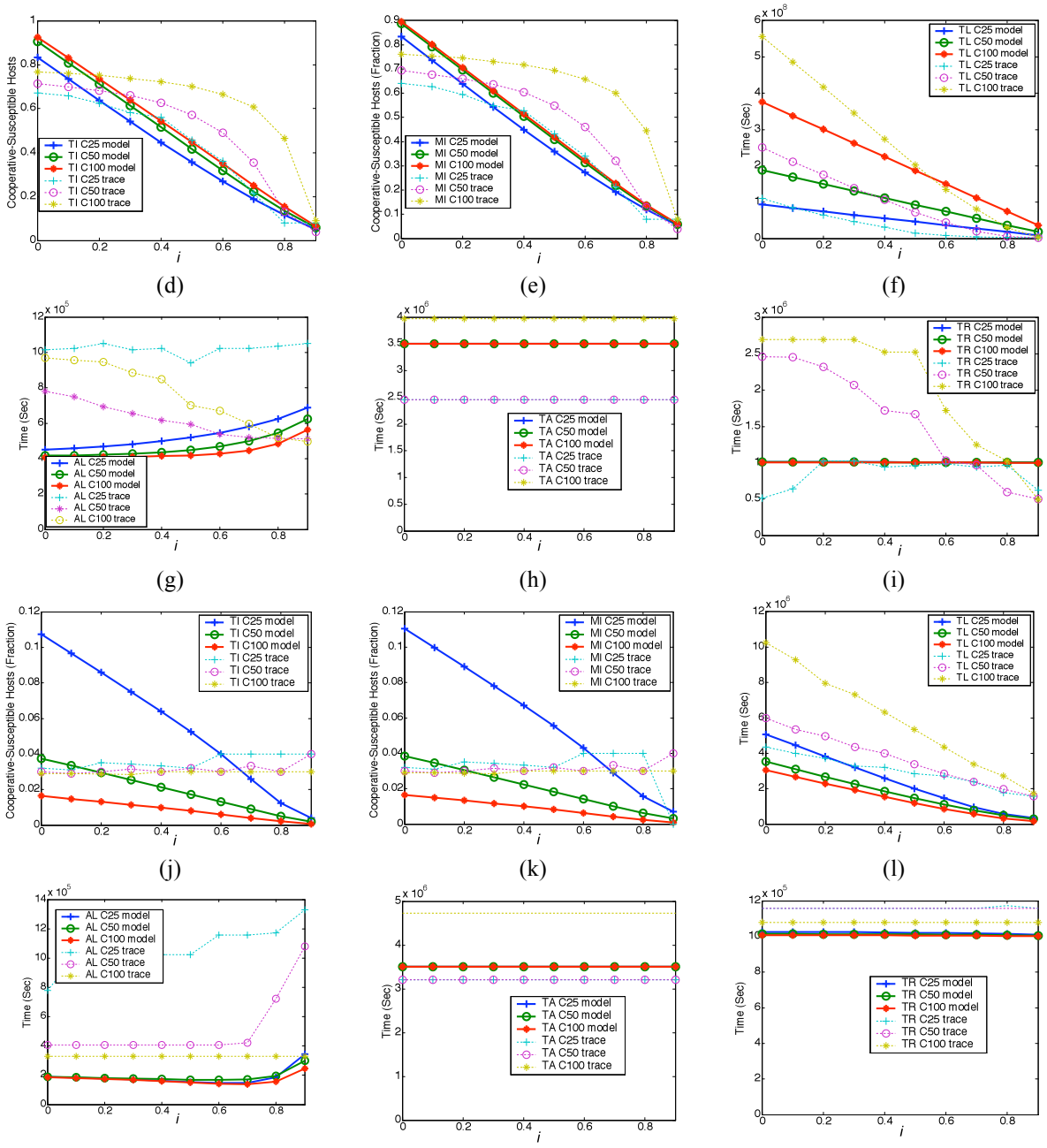


Figure 10: Trace-based statistics and simulation results: histograms of (a) total encounter/node, (b) unique encounter/node and (c) batch arrival pattern, and effects on cooperation (*c*) and immunization (*i*) on *TI* , *MI* ,*TL*, *AL* , *TA*, and *TR* in non-uniform-encounter worm interaction, in (d)-(i) initial predator-infected hosts in slow contact-rate and late group, (j)-(o) initial predator-infected hosts in fast contact-rate and early group