Computer Worm Ecology in Encounter-based Networks (Invited Paper)

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

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

***Abstract*— 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 for deterring worm propagation in encounter-based networks is inappropriate. Because this type of network is highly dynamic and has no specific boundary, we need a fully distributed security response mechanism. We propose the worm interaction approach that relies upon automated beneficial worm generation aiming to alleviate problems of worm propagations in such networks. This work is motivated by the 'War of the Worms' of the Internet worms between competing worms such as NetSky, Bagle and MyDoom. To understand the dynamic of worm interactions and its performance, we mathematically model several classes of worms and interactions using ordinary differential equations and analyze their behaviors.**

I. INTRODUCTION

An encounter-based network is a frequently-disconnected wireless ad-hoc networks 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 single worm type in well-connected wired network. However, many new worms are targeting wireless mobile phones. The characteristics of worms in mobile networks are different from random-scan network worms. 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 [14]. Since Bluetooth radios have very short range around 10-100 meters, the worms need neighbors in close proximity to spread out their replications. Hence, we call this "encounter-based worms". This worm spreading pattern is very similar to spread of packet replications in delay tolerant networks [16, 20], i.e., flooding the copies of messages to all close neighbors. An earlier study in encounter-based networks actually used the term "*epidemic routing*" [16] to describe the similarity of this routing protocol to disease spreading.

Using traditional approaches such as gateways or firewalls for deterring 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 the worm interaction approach that relies upon automated beneficial worm generation [1]. This approach uses an automatic generated beneficial worm to terminate malicious worms and patch vulnerable hosts.

Our work is motivated by competitions of these Internet worms. In 2004, majority of worm outbreaks are caused by the "War of the Worms" between NetSky, Bagle and MyDoom. In this paper, we try to answer following questions: How is the war of the worms affects the worm propagation in encounter-based networks? What are the possible variants of wars of the worms? and how can we incorporate the encounter characteristics to the worm propagations.

This scenario is described as "worm interactions" in which one or multiple types of worm terminate or patch other types of worms. In this paper, we show that the interaction causes significant change in the traditional one-type propagation pattern. Furthermore different types of interactions show entirely different patterns. Originally propagation patterns of worms follow variants of phase transition patterns. Hence, we develop a comprehensive novel worm ecology model extending the epidemic model [7] for several classes of worm interactions based on their behaviors, capabilities and strategies. Our worm ecology model consists of aggressive one-sided, conservative one-sided, aggressive two-sided and, two-group aggressive one-sided worm interactions. Our worm interaction models focus on worm behaviors and group behavior in encounter-based networks

Our main contribution in this paper is our proposed new comprehensive *Worm Interaction Model* categorizing worm interactions by worm types, sidedness, aggressiveness, and group. This worm interaction model can be extended to support more complicated current and future worm interactions in encounter-based networks.

Next we discuss related work in Section II. Then, in Section III, we explain worms' behaviors in our model and their parameters in details. We discuss multi-group aggressive one-sided interaction in Section IV. In Section IV, we conclude our work and discuss the future work.

Much of this work was performed at the University of Southern California with support from NSF awards: CAREER 0134650, ACQUIRE 0435505 and Intel.

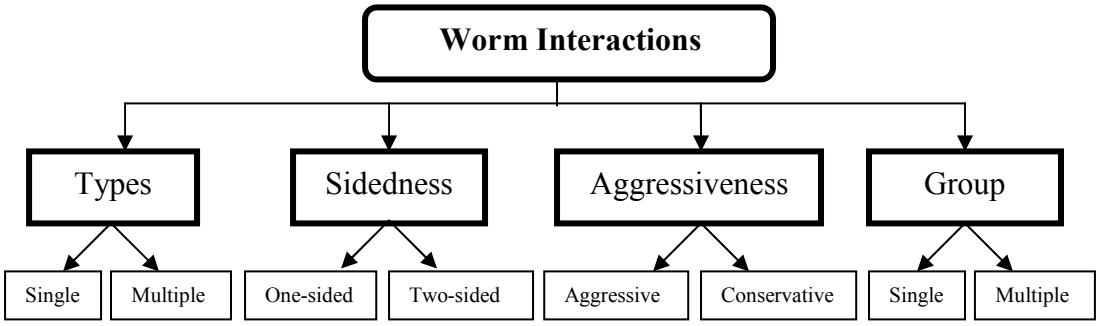


Fig.1. Worm Interaction Classification

II Related Work

Worm-like message propagation or epidemic routing has been studied for delay tolerant network applications [16, 20]. 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, similarly to generic flooding but without producing redundant messages. Performance modeling for epidemic routing in delay tolerant networks [20] based on ODE is proposed to evaluate the delivery delay, loss probability and power consumption. They also propose the concept of anti-packet to stop unnecessary overhead from forwarding extra packets copies after the destination has received the packets. This can be considered as a special case of non-zero delay of aggressive one-sided interaction which consider in our model.

Epidemic model and its variance, a set of ordinary differential equations, were earlier used to describe the contagious disease spread including *SI, SIS, SIR SIRS, SEIR* and *SEIRS* models [3, 7, 15] in which *S, I, E, R* stand for Susceptible, Infected, Exposed and Recovered state respectively. We can see the pattern similarity of computer worm infection and the disease spread in which both of them depending on node's status, i.e., vulnerable, infected or recovered) and encounter pattern. For the Internet worms, numerous worm propagation models have been investigated in earlier work [5, 6, 8, 21]. However, only few works [1, 10, 12, 13] consider worm interaction among different worm types. Our work is focusing more on understanding of how we can systemically categorize and model worm propagation and interaction among each other 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. The modified code will retain portion of attacking method so it would choose and attack the same set of susceptible hosts. In this paper, we model this as aggressive one-sided worm interaction. Other active defense such as automatic patching was also investigated in [17]. Their work assumes a patch server and overlay network architecture. We provide the mathematical model that can explain the behavior of automatic-generated beneficial worm and automatic patch distribution using one-sided worm interaction. In [17] authors assume patch blocking by worms after infection, and hence this scenario yields aggressive two-sided worm interaction which we model in this paper. Our work aims to understand and evaluate automated worm (with patch) generation but we do not address details of vulnerabilities nor related software engineering techniques to generate patches or worms. Active defense using beneficial worms is also mathematically modeled in [10]; however, the work focuses only on one-sided worm interaction for delay-limited worms. Our work in [13] focuses more on aggressive one-sided worm interaction and impact on networks infrastructure while this work concentrates on worm behaviors resulting from comprehensive worm interactions in encounter-based networks.

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 dynamics of susceptible and infected hosts over the course of time.

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

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 hosts in the least amount of time, and if possible, undetected by antivirus or intrusion detection systems. Our beneficial worm, on the other hand, aims to eliminate opposing worms or limit the scope of opposing worms' infection. We want to investigate the worm propagation caused by various types of interactions.

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. 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 prey from infected nodes by 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. Initial-infected-host ratio: the ratio of infected hosts of one worm type to another worm type at their initial release time of both worms. Let Y be an initial-infected-host ratio of predator to prey,

$$Y \equiv \frac{I_{B(0)}}{I_{A(0)}} \qquad (1)$$

where $I_A(0)$ and $I_B(0)$ = number of initial infected hosts of prey and predator respectively at their released times.

To estimate how much *relative* characteristics of predator and prey impact on their propagations, we develop the concept of *similarity* and *difference* to gain insight into initial-infected-host ratio.

Let Y_i and Y_j be the initial-infected-host ratio for network i and network j, respectively. Let $I_{B(0)_i}$ and $I_{B(0)_j}$ be the initial predator infected host for network i and network j, respectively. Let $I_{A(0)_i}$ and $I_{A(0)_j}$ be the initial prey infected host for network i and network j, respectively. Let $S_{(0)_i}$ and $S_{(0)_j}$ be the initial susceptible host for network i and network j, respectively. Let N_i and N_j be the total vulnerable hosts for network i and network j, respectively where $N_i = S_{(0)_i} + I_{A(0)_i} + I_{B(0)_i}$ and $N_j = S_{(0)_j} + I_{A(0)_j} + I_{B(0)_j}$.

Table I.
PAREMETERS AND DEFINITIONS

Parameter	Definition
S	Susceptible hosts: hosts that can be infected by either prey or predator
I_A, I_B	Prey infected hosts: hosts infected by prey, Predator infected hosts: hosts infected by predator
N	Total number of vulnerable hosts in the networks: it is the sum of number of susceptible hosts, prey infected hosts and predator infected hosts
β	Pair-wise contact rate: frequency of a pair of nodes make a contact with each other
Y	Initial-infected-hosts ratio: ratio between predator infected hosts and prey infected hosts at t = 0.
l	Initial-infected host-ratio multiplicative factor: the number to identify each initial-infected-host ratio.
E_A	Epidemiological threshold: number indicating the possibility of prey outbreak

Y_i is *similar* to Y_j only when $\frac{I_{B(0)_i}}{I_{A(0)_i}} = \frac{I_{B(0)_j}}{I_{A(0)_j}}$ where $N_i = kN_j$ and $k = 1,2,3,\ldots$, otherwise it is said to be *different*.

For example Y_1= 1:1 is similar to Y_2= 2:2 but the first ratio has $I_{A(0)} = I_{B(0)} = 1$ and the latter has $I_{A(0)} = I_{B(0)} = 2$. To differentiate between Y_1 and Y_2, we use *initial-infected-host-ratio multiplicative factor* l_i which l_1=1.0 for Y_1 and l_2=2.0 for Y_2 where we use Y=1:1 as the absolute reference.

c. Epidemiological threshold: the number to determine whether prey outbreak occurs. It is the ratio of prey increase rate to prey decrease rate where prey infection rate is $\frac{dI_A}{dt}$.

Let E_A be epidemiological threshold. To stop the prey outbreak (i.e., prey initial infection), we need $E_A \le 1.0$ which derived from $\frac{dI_A}{dt} \le 0.0$ at t=0. We can systemically derive *minimum* initial-infected-host ratio based on *epidemiological threshold* for each type of worm interactions.

The contact rate is the frequency of encounter for pairs of nodes, where an encounter occurs when the 2 nodes are within radio range. Let β be a contact rate of a prey infected host and of a predator infected host.

We assume uniform contact rate for all pairs of nodes and their encounter behavior does not directly impact each other and both predator and prey starts encounter other hosts at the same time on same set of susceptible hosts. For the later assumption, this is only true that if both predator and prey enter the network simultaneously and the signatures of both worms are known before they interact with each other or signature can be promptly generated as soon as prey arrives. However, non-zero delay worm interaction can also be derived from our model. We assume that in one encounter, worm is successfully transferred from one host to another.

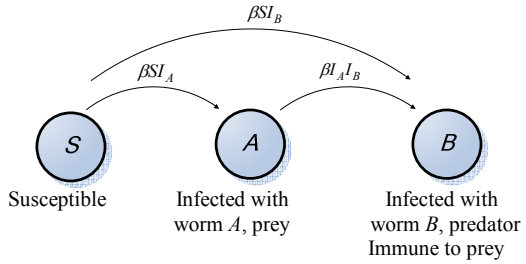


Fig. 2. Aggressive one-sided interactions

B. *One-sided interaction (Prey/Predator Model)*

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

There are two types of interactions considered in the one-sided interaction: aggressive, and conservative. The aggressive predator terminates its prey and vaccinates susceptible hosts while the *conservative* predator only terminates its preys but will *not* vaccinate susceptible hosts.

a. Aggressive one-sided interaction

In this model, a beneficial worm, predator has the capability to terminate and patch a malicious worm, prey as well as vaccinate susceptible hosts. Simplified interaction between Welchia and Blaster and between Code Green and Code Red can be represented by this model. As shown in fig.2, susceptible hosts' decrease rate is determined by manual vaccination and the contact of susceptible hosts with the prey infected hosts causing the prey infection or with the predator infected hosts causing the vaccination. Hence, the susceptible rate is

$$\frac{dS}{dt} = -\beta S(I_A + I_B)\,. \tag{2}$$

Since the prey relies on susceptible hosts to expand its population, the increase of prey infection rate is determined by the contacts of susceptible hosts and prey infected hosts. The decrease of prey infection rate is determined by prey termination caused by the contacts of prey infected hosts and predator infected hosts. Hence the prey infection rate is

$$\frac{dI_A}{dt} = \beta I_A(S - I_B)\,. \tag{3}$$

Because the predator can terminate its prey as well as vaccinate susceptible hosts, the increase of predator infection rate is determined by the contacts of predator with either the susceptible hosts or prey infected hosts.

$$\frac{dI_B}{dt} = \beta I_B(S + I_A)\,. \tag{4}$$

From (3), the epidemiological threshold for prey is

$$E_A = \frac{\text{prey increase rate}}{\text{prey decrease rate}} = \frac{\beta S I_A}{\beta I_A I_B} = \frac{S}{I_B}\,. \tag{5}$$

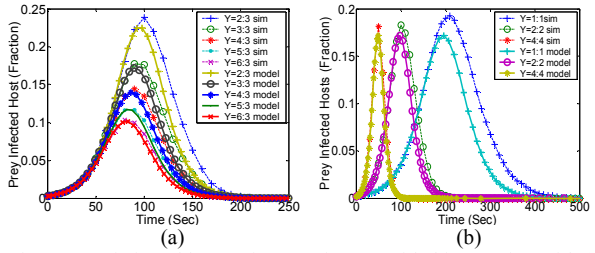


Fig. 3. Prey infected hosts of aggressive one-sided interaction with (a) different initial-infected-host ratio (b) similar initial host ratio

If we want the prey to be contained by its predator, i.e., $E_A < 1$ at t=0, we assume $I_A(0)$ and $I_B(0) > 0$, we requires that the minimum infected host ratio to be

$$Y \geq \frac{S(0)}{I_A(0)}\,. \tag{6}$$

To see the importance of initial host ratio, we plot numerical solutions from our aggressive one-sided interaction model using four sets of variables in this model: *similar* initial host ratios with and *different* initial host ratios of 1000 uniform-encounter nodes in fig. 3(a) and 500, 1000, and 2000 uniform-encounter nodes in fig.3 (b).

We validate our models through the encounter-level simulations. We simulate 1,000 mobile nodes for *similar* initial host ratios and 500, 1000 and 2000 nodes for *different* initial host ratios with β = 6x10^{-5} sec^{-1}. Each simulation runs 1,000 rounds and we plot mean values for each time instance.

We can observe that the increase of initial infected host reduce the maximum of prey infected hosts from 25% to 10% of total population as shown in fig.3 (a). In fig.3 (b), we keep the ratio of susceptible hosts to initial predator infected hosts to initial prey infected hosts similar, e.g., Y_1=1:1 with S_1=498, Y_2=2:2 with S_2=996 and Y_3=4:4 with S_3=1992. We can observe that all maximum infected host fractions of prey for different I_i are the same. This means that the number of total vulnerable hosts (N) does not affect the relative fraction of infections

($I_A(\max)/N$) as long as $S:I_B:I_A$ are similar and β are the same.

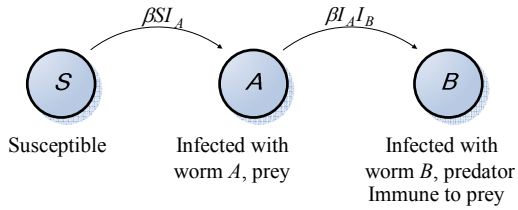


Fig.4. Conservative one-sided interactions

b. Conservative one-sided interaction

In a conservative interaction, a predator has the capability to terminate a prey but does not vaccinate susceptible hosts. Hence the predator infected hosts change depends solely on population of the prey infected hosts.

We show the state transition of conservative one-sided interactions in fig.4. The susceptible hosts are now only converted to prey infected hosts but not to predator infected hosts (i.e., $\beta SI_B = 0$) . Hence, the decrease of susceptible hosts in this model is determined by the prey infection caused by the contact between susceptible hosts and the prey infected hosts. Hence

$$\frac{dS}{dt} = -\beta SI_A . \tag{7}$$

Since the prey behavior is the same as of aggressive one-sided interaction, the prey infection rate can be derived similarly.

$$\frac{dI_A}{dt} = \beta I_A(S - I_B) . \tag{8}$$

As mentioned earlier, predator infected hosts growth rate depends only on prey termination. Thus, predator infection rate is

$$\frac{dI_B}{dt} = \beta I_A I_B . \tag{9}$$

From (4) and (9), we can see that the increase of predator infected hosts in this model is much slower than that of aggressive one-sided interaction because $\beta I_A I_B < \beta(S + I_A)I_B$.

From (8), the epidemiological threshold for prey is

$$E_A = \frac{\beta SI_A}{\beta I_A I_B} = \frac{S}{I_B} . \tag{10}$$

Similarly to aggressive one-sided interaction, we requires that minimum initial-infected-host ratio to be

$$Y > \frac{S(0)}{I_A(0)} \tag{11}$$

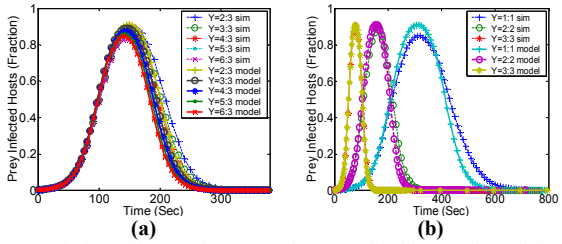


Fig. 5. Prey infected hosts of conservative one-sided interaction with (a) with different initial-infected-host ratios (b) similar initial host ratios

Again, we validate our models through the encounter-level simulations. We simulate and model 1,000 mobile nodes for *similar* initial host ratios and 500, 1000 and 2000 nodes for *different* initial host ratios with $\beta = 6\text{x}10^{-5}$ sec^{-1}. Each simulation runs 1,000 rounds and we plot mean values for each time instance.

As shown in fig. 5 (a) and (b), because of slower predator infection rate, the prey infected hosts are required more time to be completely terminated causing much higher maximum prey infected host than that of the aggressive one-sided interaction.

The effects of increase of initial-infected-host ratios on the conservative one-sided interaction are much weaker than that of the aggressive one-sided interaction. In this model, if automated worm generation produces the same worm characteristics with *Y*=1:1, it would optimally limit the prey maximum infected hosts to 95% of population which is much worse than that of aggressive one-sided interaction which 17% of population.

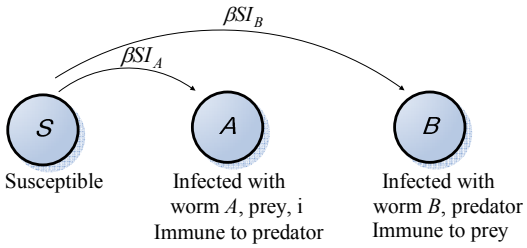


Fig. 6. Aggressive Two-sided Interaction

C. Two-sided interaction (Predator/Predator Model)

a. Aggressive two-sided interaction

In this model, 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 hosts but unable to remove a predator *A* from predator *A*'s infected hosts because it is blocked by predator *A*. Both predator A and B blocks each other (i.e., $\beta I_A I_B = 0$).

This aggressive two-sided interaction model is extended from the aggressive one-sided interaction model explained in the earlier section. In automated patching systems [19], their worm-like patch distribution falls into this category. The automated patching assumes that each worm patches its own host to prevent infection from other worm is closely related to this model.

We show the state transition of this model in fig.6. Similar to that of the aggressive one-sided interaction, the change of susceptible hosts is caused by the prey infection and the predator infection. Hence the susceptible rate for this model is

$$\frac{dS}{dt} = -\beta S(I_A + I_B)\,. \qquad (12)$$

Because the predator A cannot terminate the predator B and vice versa, the predator A infection rate is only determined by the predator A infection caused by the contacts between the susceptible hosts and the predator A infected hosts. Since this is the two-sided interaction, the predator B infection rate can be derived similarly to infection rate of predator A.

$$\frac{dI_A}{dt} = \beta S I_A \qquad (13)$$

$$\frac{dI_B}{dt} = \beta S I_B\,. \qquad (14)$$

From (13), the epidemiological thresholds for the predator A are

$$E_A = \frac{\beta S I_A}{0} = \infty \qquad (15)$$

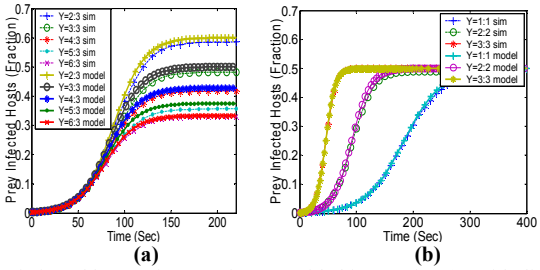
Hence we know that E_A will be always greater than 0 at t=0.

Similarly to aggressive and conservative one-sided worm interaction, we validate our models through the encounter-level simulations. We simulate and model 1,000 mobile nodes for *similar* initial host ratios and 500, 1000 and 2000 nodes for *different* initial host ratios with β = 6x10^{-5} sec^{-1}. Each simulation runs 1,000 rounds and we plot mean values for each time instance.

Unlike the aggressive and conservative one-sided interaction, we can observe that the predator A will not be completely terminated but only to be contained (i.e., prey cannot infect susceptible hosts more than certain fraction of total vulnerable hosts). To be more specific, from fig.7 (a) that if we want to contain predator A to be lower than 40% then we need initial-infected-host ratio at least *similar* to Y=5:3.

The relationships of similar initial-infected-host ratios with varied l_i are still the same as those of the aggressive and conservative one-sided interaction.

We can further observe with initial-infected-host ratios, based on prey maximum infected hosts (lowest to highest), we can rank aggressive one-sided interaction first, aggressive two-sided interaction second and conservative one-sided interaction last.



(a) **(b)**

Fig. 7. Prey infected hosts of aggressive two-sided interaction (a) with different initial-infected-host ratios (b) similar initial host ratios

Note that we do not model conservative two-sided worm interaction because both predator A and predator B infection rate are simply 0.0 and hence, no possibility of outbreak for predator A.

IV. MULTI-GROUP ENCOUNTERS

In addition to number of types, sidedness, aggressiveness, we are also interested in modeling multi-group encounters where each group is classified by their contact rate. For two-group modeling, we need 3 different contact rates: two intra-contact rates for encounters within each group, and one inter-contact rate for encounters between groups. We can simply call the higher inter-contact rate as the fast group, and the other, the slow group. For n groups, we need n intra-contact rates and $\binom{n}{2}$ inter-contact rates.

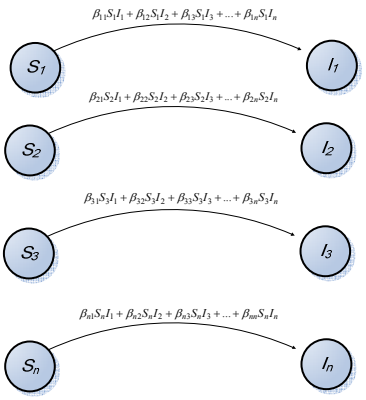


Fig. 8. One-worm-type Multi-group Propagation

The state diagram of one-worm-type multi-group worm propagation without interaction is shown below in fig. 8. As we can see here, we assume that each group has specific size of nodes whose contact rates are not changed during their encounter period. Each node of each group can encounter any member of any group.

Hence, once it transits to infected host state, its original contact rate that associates with the group is unchanged. We show the one-type worm propagation in n-group encounter in fig 8 above.

Since there is no interaction with only one type of worm, as well as unchanged contact rate, given n groups in the networks, the susceptible rates for group n is

$$\frac{dS_n}{dt} = -\beta_{n1}S_nI_1 - \beta_{n2}S_nI_2 - \beta_{n3}S_nI_3 - \ldots - \beta_{nn}S_nI_n \quad (16)$$

where β_{nm} is the contact rate between member of group n and group m (β_{nn} is the contact rate within group n), S_n is the number of susceptible hosts of group n and I_m is the number of infected hosts in group m ($1 \le m \le n$).

The infection rates for group n are derived as the negative of susceptible rates for group n above. Hence, the infection rate is

$$\frac{dI_n}{dt} = -\frac{dS_n}{dt} \quad (17)$$

For two-group with one-sided interaction and the unchanged group assumption, we can extend the above model by extending from one type to two types of worms and adding transitions from susceptible to both prey and predator. The susceptible rates, prey and predator infection rates for both groups are

$$\frac{dS_1}{dt} = -\beta_{11}S_1(I_{A1} + I_{B1}) - \beta_{12}S_1(I_{A2} + I_{B2}) \quad (18)$$

$$\frac{dS_2}{dt} = -\beta_{21}S_2(I_{A1} + I_{B1}) - \beta_{22}S_2(I_{A2} + I_{B2}) \quad (19)$$

$$\frac{dI_{A1}}{dt} = \beta_{11}I_{A1}(S_1 - I_{B1}) + \beta_{12}(S_1I_{A2} - I_{A1}I_{B2}) \quad (20)$$

$$\frac{dI_{A2}}{dt} = \beta_{21}(S_2I_{A1} - I_{A2}I_{B1}) + \beta_{22}I_{A2}(S_2 - I_{B2}) \quad (21)$$

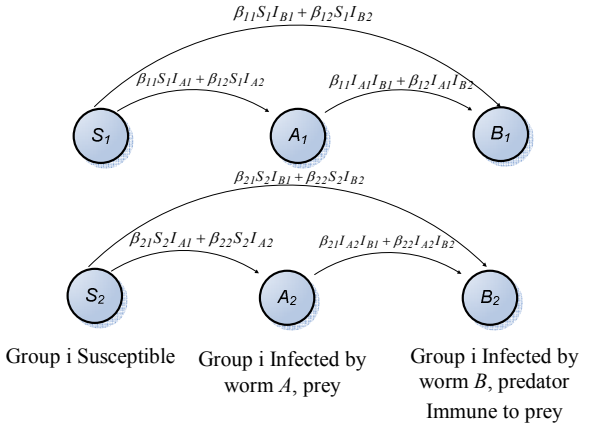


Fig. 9 Two-group, aggressive one-sided Interaction

$$\frac{dI_{B1}}{dt} = (S_1 + I_{A1})(\beta_{11}I_{B1} + \beta_{12}I_{B2}) \quad (22)$$

$$\frac{dI_{B2}}{dt} = (S_2 + I_{A2})(\beta_{21}I_{B1} + \beta_{22}I_{B2}) \quad (23)$$

where β_{11} and β_{22} are the intra-contact rates of group 1 and group 2, respectively. β_{12} and β_{21} are inter-contact rate between group 1 and 2 and inter-contact rate between group 2 and group 1, respectively, I_{A1} and I_{A2} are the number of prey infected hosts in group 1 and group 2, respectively, I_{B1} and I_{B2} are the number of predator infected hosts in group 1 and group 2, respectively.

Hence, epidemiological threshold for group 1, which is the ratio of prey increase rate in group1 and prey decrease rate in group 1, and epidemiological threshold for group 2, which is the ratio of prey increase rate in group 2 and prey decrease rate in group 2, are:

$$E_{A1} = \frac{S_1(\beta_{11}I_{A1} + \beta_{12}I_{A2})}{I_{A1}(\beta_{11}I_{B1} + \beta_{12}I_{B2})} \quad (24)$$

$$E_{A2} = \frac{S_2(\beta_{21}I_{A1} + \beta_{22}I_{A2})}{I_{A2}(\beta_{21}I_{B1} + \beta_{22}I_{B2})} \quad (25)$$

If $\beta_{11} > \beta_{22}$ and $\beta_{12} = \beta_{21}$, we call β_{11} (contact rate of group 1) "fast contact rate" and β_{22} (contact rate of group 2) "slow contact rate". If initial predator infected host is in group 1, then we call this scenario fast predator, otherwise, we call it slow predator. If initial prey infected host is in group 1, we call this scenario fast prey, otherwise, we call it slow prey.

As shown in fig. 10, we show four different cases: "slow prey, slow predator", "slow prey, fast predator", "fast prey, slow predator" and "fast prey, fast predator". The initial prey infected host and initial predator infected host are both 1. We validate our models through the encounter-level simulations. We simulate and model 1,000 mobile nodes (500 nodes in group 1 and 500 nodes in group 2) with $\beta_{11} = 3\text{x}10^{-5}$ sec^{-1} for group 1, $\beta_{22} = 6\text{x}10^{-5}$ sec^{-1} for group 2 and $\beta_{12} = \beta_{21} = 1\text{x}10^{-5}$ sec^{-1}. Each simulation runs 1,000 rounds and we plot mean values for each time instance.

With the same contact rate set, i.e., fast contact rate, slow contact rate and inter-contact rate, prey maximum infected hosts are different for different cases in the same network. As expected, in "slow prey, fast predator" case, the maximum of prey infected hosts are the lowest among other case. On the other hand, in "fast prey, slow predator" case, the maximum of prey infected hosts are the highest among other case. The differences of the highest and the lowest of the maximum of prey infected hosts can be as high as 5 times. As an initial prey infected host is in group 2 (fast predator), this infected host infects more susceptible hosts in group 2 because of its faster contact rate. Hence, it causes other nodes in the same group to be prey infected host in much faster rate and more difficult to be entirely removed. The opposite characteristics of prey infected hosts are expected if an initial infected host is in group 1.

To understand and be able to better predict worm behavior in multi-group worm interaction, additional concepts on *similarity* and *difference* for groups are required.

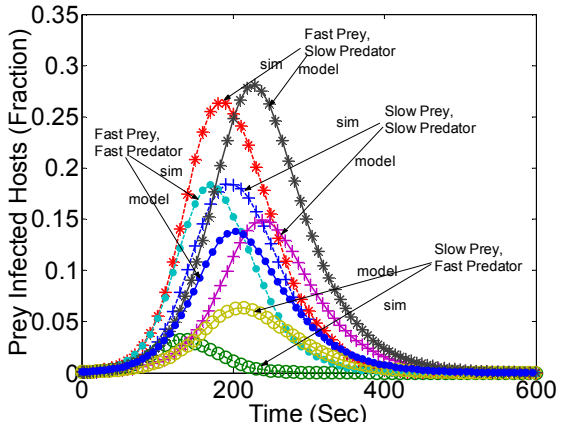


Figure 10 Two groups of population: slow (contact rate=$3x10^{-5}$) and fast encountered groups (contact rate= $6x10^{-5}$/sec and contact rate between group =$1x10^{-5}$/sec)

Earlier we assume that each node does not change group memberships. Now we relax the assumption and we show the state diagram for two-group, aggressive one-sided interaction with group transition below in fig. 11 where λ_{12} and λ_{21} represents transition rates from S_1 to S_2, and from S_2 to S_1, respectively, μ_{12} and μ_{21}, represents transition rates from A_1 to A_2 and from A_2 to A_1, respectively, ω_{12} and ω_{21} represents transition rates from B_1 to B_2 and from B_2 to B_1, respectively.

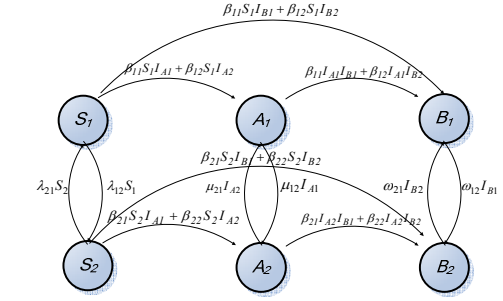


Figure 11 Two-group, one-sided Interaction with group transition

This group transition can be easily integrated to the earlier two-group aggressive one-sided interaction as following:

$$\frac{dS_1}{dt} = -\beta_{11}S_1(I_{A1}+I_{B1}) - \beta_{12}S_1(I_{A2}+I_{B2}) + (\lambda_{21}S_2 - \lambda_{12}S_1) \quad (26)$$

$$\frac{dS_2}{dt} = -\beta_{21}S_1(I_{A1}+I_{B1}) - \beta_{22}S_1(I_{A2}+I_{B2}) - (\lambda_{21}S_2 - \lambda_{12}S_1) \quad (27)$$

$$\frac{dI_{A1}}{dt} = \beta_{11}I_{A1}(S_1 - I_{B1}) + \beta_{12}(S_1I_{A2} - I_{A1}I_{B2}) + (\mu_{21}I_{A2} - \mu_{12}I_{A1}) \quad (28)$$

$$\frac{dI_{A2}}{dt} = \beta_{21}(S_2I_{A1} - I_{A2}I_{B1}) + \beta_{22}I_{A2}(S_2 - I_{B2}) - (\mu_{21}I_{A2} - \mu_{12}I_{A1}) \quad (29)$$

$$\frac{dI_{B1}}{dt} = (S_1 + I_{A1})(\beta_{11}I_{B1} + \beta_{12}I_{B2}) + (\omega_{21}I_{B2} - \omega_{12}I_{B1}) \quad (30)$$

$$\frac{dI_{B2}}{dt} = (S_2 + I_{A2})(\beta_{21}I_{B1} + \beta_{22}I_{B2}) - (\omega_{21}I_{B2} - \omega_{12}I_{B1}) \quad (31)$$

Similar to (24) and (25), epidemiological threshold for group 1 and 2 are:

$$E_{A1} = \frac{S_1(\beta_{11}I_{A1} + \beta_{12}I_{A2}) + \mu_{21}I_{A2}}{I_{A1}(\beta_{11}I_{B1} + \beta_{12}I_{B2}) + \mu_{12}I_{A1}} \quad (32)$$

$$E_{A2} = \frac{S_2(\beta_{21}I_{A1} + \beta_{22}I_{A2}) + \mu_{12}I_{A1}}{I_{A2}(\beta_{21}I_{B1} + \beta_{22}I_{B2}) + \mu_{21}I_{A2}} \quad (33)$$

V. Summary and Future Work

In this paper, we propose a novel and comprehensive worm interaction models for the encounter-based networks. Worm interactions can be categorized by number of types, sidedness, aggressiveness, and group. We show that worm propagations are significantly influenced by worm interactions and different worm interactions yield entirely different worm propagation patterns. For example, the maximum prey infected hosts in aggressive one-sided interaction is only 20% of maximum prey infected hosts in conservative one-sided interaction. Worm interaction models represented here are motivated by the real Internet worm interactions and automated worm response.

In multi-group encounter-based networks, the initial prey infected host affects the overall infection level significantly. The effect of different contact rates and the size of each group (according to its scan rate) are subject to further investigation. Our future work focuses more on simulation results based on wireless trace analysis and test bed for worm propagations and interactions in real encounter-based networks. The insight developed in an analysis will be used to provide guidelines for security of worm counter-measures in future mobile networks.

References

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

[2] R. Dantu, J. Cangussu, and A. Yelimeli, "Dynamic Control of Worm Propagation," *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)* Volume 2 - Volume 2 2004

[3] J. C. Frauenthal. *Mathematical Modeling in Epidemiology*. Springer-Verlag, New York,1988

[4] Analysis of the Sapphire Worm - A joint effort of CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE (http://www.caida.org/analysis/

security/sapphire)
[5] A. Ganesh, L. Massoulie and D. Towsley, “The Effect of Network Topology on the Spread of Epidemics,” in *IEEE INFOCOM* 2005.
[6] Z. Chen, L. Gao, and K. Kwiat, “Modeling the Spread of Active Worms*”, IEEE INFOCOM* 2003
[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," *IEEE INFOCOM* 2003.
[9] D. M. Nicol, M Lijenstam, and J. Liu, “Multiscale Modeling and Simulation of Worm Effects on the Internet Routing Infrastructure,” *Proceedings of the Performance Tools* 2003 Conference Urbana, IL, September 2003
[10] D. M. Nicol, “Models and Analysis of Active Worm Defense”, *Proceeding of Mathematical Methods, Models and Architecture for Computer Networks Security Workshop* 2005.
[11] P. Szor, *The Art of Computer Virus Research and Defense* (Symantec Press) 2005
[12] S. Tanachaiwiwat, A. Helmy, "VACCINE: War of the Worms in Wired and Wireless Networks," Technical Report CS 05-859, Computer Science Department, USC
[13] S. Tanachaiwiwat, A. Helmy, "Analyzing the Interactions of Self-Propagating Codes in Multi-hop Networks," *Eighth International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS*) accepted as Brief Announcement, November 2006, Dallas, Texas
[14] Trend Micro Annual Virus Report 2004 http://www.trendmicro.com
[15] H. Trottier and P. Phillippe, "Deterministic Modeling Of Infectious Diseases: Theory And Methods," The Internet Journal of Infectious Diseases ISSN: 1528-8366
[16] A.Vahdat and D. Becker. *Epidemic routing for partially connected ad hoc networks*. Technical Report CS-2000.
[17] 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.
[18] N. Weaver, S. Staniford, V. Paxson, “Very Fast Containment of Scanning Worms,” 13th *USENIX Security Symposium*, Aug 2004
[19] N. Weaver, I. Hamadeh, G. Kesidis, and V. Paxson. “Preliminary Results Using Scale-Down to Explore Worm Dynamics,*” Proceedings of the ACM WORM 2004 Workshop on Rapid Malcode*, Fairfax, VA, Oct. 2004
[20] X. Zhang, G. Neglia, J. Kurose, and D. Towsley. “Performance Modeling of Epidemic Routing,” to appear Elsevier Computer Networks journal, 2007
[21] C. C. Zou, W. Gong and D. Towsley, “Code red worm propagation modeling and analysis," Proceedings of the 9th *ACM CCS* 2002