Encounter-based Worms: Analysis and Defense

Sapon Tanachaiwiwat and Ahmed Helmy
University of Southern California
Department of Electrical Engineering
Los Angeles, CA
{tanachai, helmy}@usc.edu

I. INTRODUCTION

Most work on worm propagation have focused on modeling single worm type in well connected wired network [3]. However, many worms are shifting their territory to the wireless mobile phone. The characteristics of worms in mobile networks are different from random-scan network worms. Worms in mobile networks depend on user encounter pattern. Many of those worms rely on Bluetooth to broadcast their replications to vulnerable phones, e.g. Cabir and ComWar.M [6]. Since Bluetooth radios have very short range e.g. 10-100 meters, hence, the worms need neighbors in close proximity to spread out their replications. This spreading pattern is very similar to spread of packet replications in encounter-based networks [2, 4] i.e. flooding the copies of messages to all close neighbors. An earlier study in encounter-based networks actually used the term "*epidemic routing*" [7] to describe the similarity of this routing protocol to disease spreading.

Using traditional approaches such as gateways or firewalls for worm propagation in encounter-based networks is inefficient. 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 [1]. This approach uses an automatic generated beneficial worm to terminate malicious worms and patch the vulnerable hosts to prevent reinfection from malicious worms. We define this type of worm interaction as *aggressive one-sided interaction* [5]. Before we can use this approach at full potential, we need to understand the worm interaction in this environment. To achieve this goal, we choose to model such worm behavior mathematically.
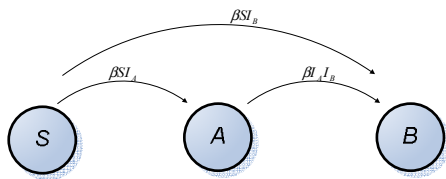

Figure 1 Aggressive one-sided interaction

We propose a mathematical model that has predator worm (B) terminating prey worm (A). Assume that each user encounters another random user with constant rate of β . Let S be the number of vulnerable hosts that are not yet infected by any worm, i.e. susceptible. Let I_A and I_B be the number of infected hosts by prey and predator accordingly. Hence from the state transition diagram in fig.1, the susceptible rate and infection rates of prey and predator are

$$\frac{dS}{dt} = -\beta SI_A - \beta SI_B$$

$$\frac{dI_A}{dt} = \beta SI_A - \beta I_A I_B$$

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

We call this set of equations "*aggressive one-sided interaction model*".

II. MODEL ACCURACY

We start by investigating accuracy of our aggressive one-sided interaction model when compared with encounter-level worm simulation (1000 nodes with uniform encounter pattern, 100 runs). Our simulation assumes the uniform encounter pattern that is independent of location and history of previous encounters. As seen in fig. 2, we find that our aggressive one-sided interaction model is very close (off by 3.8%) to our worm simulation results (for instantaneous infected hosts of prey and predators).
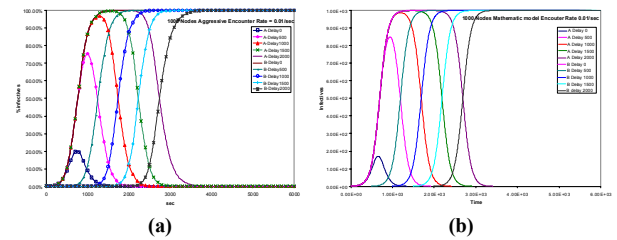

Figure 2 Comparison of (a) simulation results and (b) aggressive one-sided interaction model

II. INHERITED IMMUNIZATION

We further investigate the effect of inherited immunization against the prey in encounter-based networks. We gauge the effectiveness of termination by using the total infectives, i.e. the number of vulnerable hosts that have been infected at least once by prey. We show the distribution of 100-run simulation results in fig. 3. We see that even very low immune host percentage such as 1%; when compared with no immunization, can reduce the infection by 16.5% of vulnerable hosts, 26% of vulnerable hosts with 10% immune, and 37.2% of vulnerable hosts with 20% immune hosts. We can enhance the effect of

immunization by coupling with aggressive one-sided interaction. Now, with only 1% immune, it can reduce the total infectives to as low as 29% (or 79% improvement over immunization only).
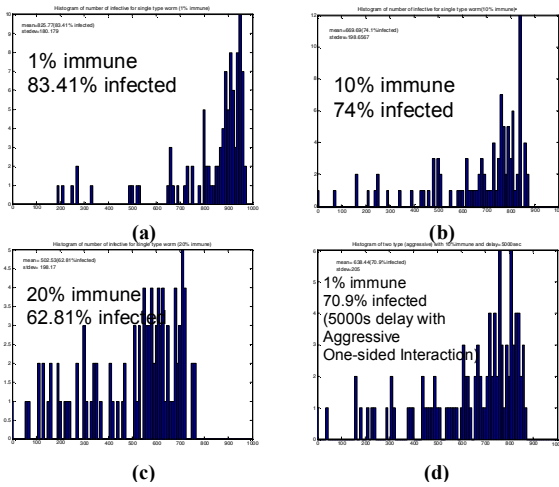

(a)

(b)

(c)

(d)

Figure 3 Effects of immunization effect on prey infectives

III. TWO-GROUP ENCOUNTERS

Because real users have heterogeneous encounter behavior, we want to incorporate these behaviors in our aggressive one-sided interaction model. We start by modeling simple two group encounter behaviors. For two-group modeling, we need 3 different encounter rates: two intra-encounter rates for encounters within each group, and one inter-encounter rate for encounters between groups.

For two-group with aggressive one-sided interaction and the unchanged group assumption, we can extend the above model by introducing the inter encounter rate (within the same group) and intra encounter rate (with different group) of prey and predator whose groups are classified by the inter encounter rate and intra encounter rate.
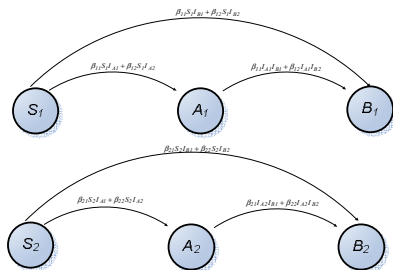

Figure 4 Two-group, one-sided Interaction

Assume that each user from group 1 encounters each other with constant rate of β_{11} and with group 2 members with constant rate of β_{12}. Let S_1 be the number of vulnerable hosts in group 1 that have not yet infected by any worm, i.e. susceptible. Let I_{A1} and I_{B1} be the number of infected hosts in group 1 by prey and predator accordingly. Hence from the state transition in fig. 4, the infection rates of prey and predator are in group 1 are

$$\frac{dI_{A1}}{dt} = \beta_{11}S_1I_{A1} + \beta_{12}S_1I_{A2} - \beta_{11}I_{A1}I_{B1} - \beta_{12}I_{A1}I_{B2}$$

$$\frac{dI_{B1}}{dt} = \beta_{11}S_1I_{B1} + \beta_{12}S_1I_{B2} + \beta_{11}I_{A1}I_{B1} + \beta_{12}I_{A1}I_{B2}$$

Similarly, with the same notation patterns for group 1, the infection rates of prey and predator for group 2 can be derived as follows.

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

$$\frac{dI_{B2}}{dt} = \beta_{21}S_2I_{B1} + \beta_{22}S_2I_{B2} + \beta_{21}I_{A2}I_{B1} + \beta_{22}I_{A2}I_{B2}$$

As shown in fig. 5 (a) and 5 (c), our simulation results show that fast predator (encounter rate = 0.1/sec) can reduce fast and slow prey (encounter rate = 0.01/sec) most effectively. Prey infectives are contained to the maximum less than 10% of total population in the first and 1% in the latter. However, slow predator can only contain fast prey infectives to the maximum at 50% in fig. 5 (b) and contain slow prey infectives at 20% in fig. 5 (d).
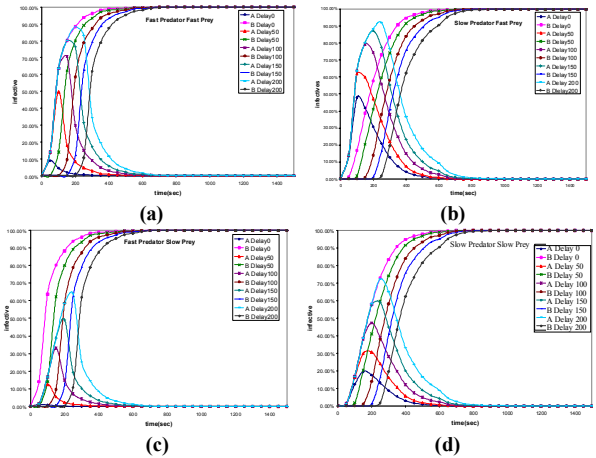

(a)

(b)

(c)

(d)

Figure 5 Two groups of population: slow (encounter rate=0.01/sec) and fast encountered groups (encounter rate= 0.1/sec and encounter between group =0.001/sec) (a) prey and predator in fast group (b) prey in fast group and predator in slow group (c) prey in slow group and predator in fast group (d) prey and predator in fast group (Delay is the reaction time in sec of predator after launch of first prey)

Earlier we assume that each node does not change group memberships during its active encounter duration. Now we relax that assumption showing the state diagram for two-group, one-sided interaction with group transition. Let the transition rate from group 1 susceptible hosts to group 2 susceptible hosts be λ_1 (λ_2 for group 2 to 1). Let the transition rate from group 1 prey infected hosts to group 2 prey infected hosts be μ_1 (μ_2 for group 2 to 1). Finally, let the transition rate from group 1 predator infected hosts to group 2 predator infected hosts be ω_1 (ω_2 for group 2 to 1). Due to limited space in this paper, we only show the transition diagram of this interaction below in fig. 6 below.
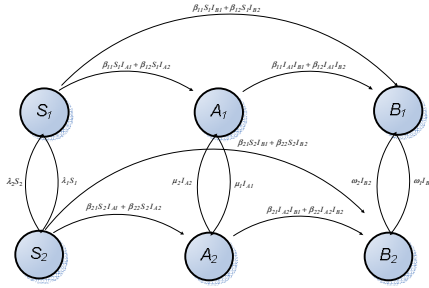
Figure 6 Two-group, one-sided interaction with group transitions

## IV. ATTENUATED VACCINATION AND TERMINATION

Variances of individual node's encounter pattern may cause some predator infectives issuing much more worm replications more than others. Hence more communication overhead is generated by those nodes. We try to reduce the overhead of excessive communication for individual predator by using counter-based termination. With the counter-based approach, predator infective increases the counter every time it terminates prey or patches the new nodes; once the counter reaches the limit, the predator will terminate itself. As shown in fig. 7, we experiment by varying those counter values in the simulation to see the effects of such strategy. The simulation shows that communication overhead is reduced significantly (40%) especially with counter limit=1. However, when we add the limit that the predator can issue at most one worm replication (either to terminate prey or vaccinate the susceptible hosts) to other vulnerable hosts, then prey's total infectives and individual life span are doubled (109% increase for total infectives and 76% for individual life span) when compared with regular aggressive one-sided interaction approach without counter limit.

V. SUMMARY AND FUTURE WORK

We develop the aggressive one-sided interaction worm model for understanding the distributed security response mechanism using beneficial worm in encounter-based network. In addition, we propose the two-group concept on worm propagation in encounter-based networks. We simulate such worm interaction and find that the inter-encounter rate plays an important role in determining total infectives. We attenuate the vaccination and termination rate to reduce unnecessary communication overhead of individual predator infective, finding that the counter limit that controls the attenuation must be carefully assigned to have equivalent performance as the approach without counter limit does. Further study is needed on modeling encounter patterns of real users. We plan to extract such users' behavior from wireless LAN trace of major universities, e.g. University of Southern California, and Dartmouth College.
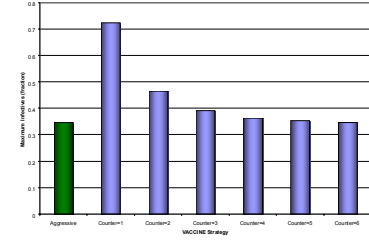
(a)
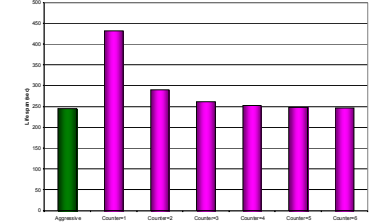
(b)
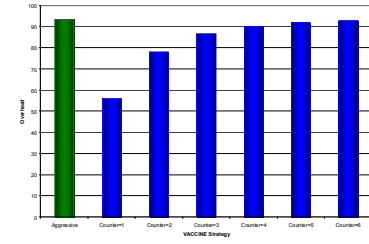
(c)

Figure 7 Effects of counter limit on (a) total infectives (b) individual life span (c) overhead.

References

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

[2] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass and J. Scott, "Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms" IEEE INFOCOM, April 2006

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

[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] S. Tanachaiwiwat, A. Helmy, "VACCINE: War of the Worms in Wired and Wireless Networks", IEEE INFOCOM 2006, Barcelona, Spain Poster and Demo Session

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

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