REQUIREMENTS ON WORM MITIGATION TECHNOLOGIES IN MANETS

Robert G. Cole and Nam Phamdo*
JHU Applied Physics Laboratory
{robert.cole,nam.phamdo}@jhuapl.edu

Moheeb A. Rajab and Andreas Terzis†
Johns Hopkins University
{moheeb,terzis}@cs.jhu.edu

Abstract

This study presents an analysis of the impact of mitigation on computer worm propagation in Mobile Ad-hoc Networks (MANETS). According to the recent DARPA BAA - Defense Against Cyber Attacks on MANETS *[4], "One of the most severe cyber threats is expected to be worms with arbitrary payload that can infect and saturate MANET-based networks on the order of seconds". Critical to the design of effective worm counter measures in MANET environments is an understanding of the propagation mechanisms and the performance of the mitigation technologies. This work aims to advance the security of these critical systems through increased knowledge of propagation mechanisms, performance and the effect of mitigation technologies. We present both analytic and simulation analysis of mitigation effectiveness. The ultimate goal of these studies is to develop an accurate set of performance requirements on mitigation techniques to minimize worm propagation in tactical, battlefield MANETS.*

1. Introduction

The Defense Advanced Research Program Agency (DARPA) believes that computer worms present a severe security threat against tactical, battlefield Mobile Ad Hoc Networks (MANETS). There is much emphasis within the recently released DARPA Broad Agency Announcement on Digital Cyber-Attacks in MANETS [4] on computer worm propagation, mitigation and isolation. For this reason we have initiated a program to study computer worm propagation and mitigation in tactical, battlefield MANETS. In this paper, we extend previous work [3] by investigating the effectiveness of mitigation technologies in military MANETs. The primary goal of this research effort is the generation of a set of performance requirements on mitigation technologies in order to ensure their success in tactical, battlefield MANETS. This objective drives some of the modeling parameters we choose to investigate in this study. We present both analytic and computer simulation studies of mitigation effectiveness in minimizing the spread of the computer worm under a variety of conditions. We study the effects of mitigation response time, nodal mobility and channel congestion on the final state of the worm propagation.

Our initial studies in [3] investigated the impact of communications and mobility effects on worm propagation mechanisms in MANETS. There we found that network delays and channel congestions had a large impact on the worm propagation effects. We also found that a set of relatively simple analytic models reproduced these communications effects quite well. In this paper, we extend our previous work by focusing on the impact of mitigation on worm propagation in MANETS under various network conditions. We also present a simple analytic model of mitigation, discuss its predictions and compare these to simulation results. Our main results in this paper are:

- There are network conditions, i.e., channel congestion, under which mitigation technologies can actually promote the spread of infection by reducing competition between probes on common communications channels.
- Our simple analytic model of mitigation does a reasonable job of estimating the steady state infection probability when compared to our simulation results and may eventually be useful in developing engineering tools for the design of mitigation techniques.
- The analytic model of mitigation has some rather interesting properties: a) it has multiple stationary state solutions, one $c(\infty) = 1$ and $c(\infty) < 1$ where $c(t)$ is the probability of infection by time t, b) a critical $c(0)$ exists, $c_c(0)$, for which $c(0) < c_c(0)$ implies that $c(\infty) = c_c(\infty) < 1$ independent of $c(0)$, while $c(0) > c_c(0)$ implies that $c(\infty) > c_c(\infty) < 1$ which monotonically increases as $c(0)$ increases.

* Power Projection Systems Department, 11000 Johns Hopkins Road., Laurel, Maryland 20723.
† Computer Science Department, 3400 N. Charles Street, Baltimore, Maryland 21218.

The rest of this paper is organized as follows. Section 2 provides a brief overview of previous work related to our studies within this paper. Section 3 provides an analysis of the Standard Epidemic Model, discusses its assumptions and relationship to worm propagation in communications networks. This section also analyzes our simple analytic model of mitigation. Simulation studies are then presented in Section 4, followed by a brief discussion on mitigation in Section 5. We end the paper with conclusions.

2. Previous Studies

Previous studies have analyzed and modeled the propagation of computer worms in digital communications networks. [13] provides an extensive investigation into the mechanisms of worm propagation and their performance, addressing specifically the Code Red I and II worms as well as the Nimda worm. They also provide an interesting discussion on potential strategies to build better worms and efforts necessary to mitigate worm propagation throughout the Internet. [6] and [7] provide an investigation of the Code Red worms propagating through the Internet. Relevant to our work, they provide an interesting discussion and analysis of performance requirements on several mitigation technologies through simulation studies of Internet-like networks.

[16] provides an excellent analysis of mathematical models of worm propagation through the Internet. Notably, they discuss the Kermack-Mckendrick model for the removal of infected nodes from the system. They also propose a heuristic expression for inter-worm competition for Internet bandwidth and develop a "Two Factor Worm Model" for their studies.

[14] addresses the issues of finite propagation times and infected node removal (or death) on propagation rates. They provide both analytic models and simulation results of these effects for Internet-like environments. [12] provides a thorough literature review of worm propagation models and studies. Interestingly, they also review various models of mitigation techniques of computer worm propagation.

[10] presents an analysis and simulation study of the performance of a novel, distributed mitigation technology referred to as *Network Telescopes*. This study demonstrates the value of this distributed and collaborative technique for rapid identification of worm infection and its role in mitigation. [11] investigates, through analysis and simulation, the impact of the non-uniform distribution of nodes within the Internet.

3. Analytic Models

In this section we discuss a relatively simple analytical model of worm propagation and mitigation in computer networks. We draw upon previous models, but derive simplified forms while maintaining their critical aspects. Our hope being to encourage the development of explicit solutions useful to engineers in future studies.

The standard analytic model used in the literature to analyze worm propagation in computer networks is the Standard Epidemic Model, see, e.g., [1]),

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)]/N \tag{1}$$

where N is the total size of the susceptible population, $I(t)$ is the number of infected nodes at time t, and β is the rate at which a given infected node probes the total, susceptible population of nodes.

Key assumptions in the derivation of the Standard Epidemic Model applied to worm propagation in computer networks are:

- *Uniform Medium* - all nodes, their nature and distribution, are assumed equivalent. In the MANET environments we focus on here, this is true. However, details of the nodal distribution and non-uniformity can have a large impact on the nature of the worm propagation and counter measures to prevent its spread, see, e.g., [11].
- *Action at a Distance* - as soon as an infected probe is queued for transmission to another host, it is immediately received by that host. This implies that all hosts always have routes established to all other hosts and hence there exists no time required for the route discovery process. It also implies that there exists no queuing, transmission or propagation delays within typical, bandwidth constrained, tactical, battlefield MANETS. This effect can be significant in MANETS.
- *Independent Infection Agents* - there exists no interaction between the infection probes propagating through the infection media, i.e., the communication network. In networks, and prominently in MANETS, this ignores two effects, a) sharing access to a common radio channel and b) probe losses due to overloading the limited bandwidth and finite sized communication buffers. These effects can be quite large in MANETS.
- *Zero Death Rate* - once a node is infected it never dies or gets cured. Instead, it is forever infected and generating infection probe packets. This assumption is related to the modeling of mitigation mechanisms within the MANETS and to the determination of their effectiveness in protecting the network nodes.
- *No Incubation Period* - as soon as the infection probe packet reaches the susceptible computer hosts, it can immediately begin transmitting infection probes to the

other hosts. This may be significant in modeling stealth worms.

The Standard Epidemic Model is derived from the following difference equation,

$$I(t+\Delta t) \approx I(t) + \beta I(t)\Delta t[N - I(t)]/N + O((\Delta t)^2) \quad (2)$$

where $O((\Delta t)^2)$ represents terms of order $(\Delta t)^2$. Here, $\beta I(t)\Delta t$ is the effective number of probes which are sent into the target network and $[N - I(t)]/N$ represents the probability that a probe encounters a susceptible, non-infected node. In the limit that $\Delta t \to 0$, dividing through by Δt, we get

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)]/N \quad (3)$$

Defining the probability of infection as $i(t) = I(t)/N$, we rewrite the equation as

$$\frac{di(t)}{dt} = \beta i(t)[1 - i(t)] \quad (4)$$

An explicit solution to the Epidemic Model, obtained by factoring and integration, is given by

$$i(t) = \frac{e^{\beta(t-T)}}{1 + e^{\beta(t-T)}} \quad (5)$$

where T is determined by the initial condition $i(t = 0)$.

Typically, β is written as

$$\beta = \beta_0(\frac{N}{2^{32}}) \quad (6)$$

where β_0 represents the rate at which an individual, infected node probes for other nodes and $N/2^{32}$ represents the likelihood that a randomly chosen 32-bit IPv4 address is a susceptible node. Other strategies are employed and modeled accordingly through appropriate definitions of β. In order to concentrate on those aspects unique to MANET networks, we assume that the infected worms only generate probes to nodes within the MANET. In this case, β will be set to the rate at which an individual infected node generates and transmits probes. This represents a worse case strategy from the perspective of generating performance requirements on mitigation techniques and assumes that the worms will have access to a table of nodes comprising the MANET. However, it is somewhat artificial in the sense that the infected nodes choose from the table of nodes randomly. Clearly, additional node selection strategies should be the subject of future investigations.

The Kermack-Mckendrick model [5] addresses the issue of the removal process of infected nodes. In the context of computer worm propagation, [16] applied the Kermack-Mckendrick model in their study of the Code Red worm. This extension to the Standard Epidemic Model addresses

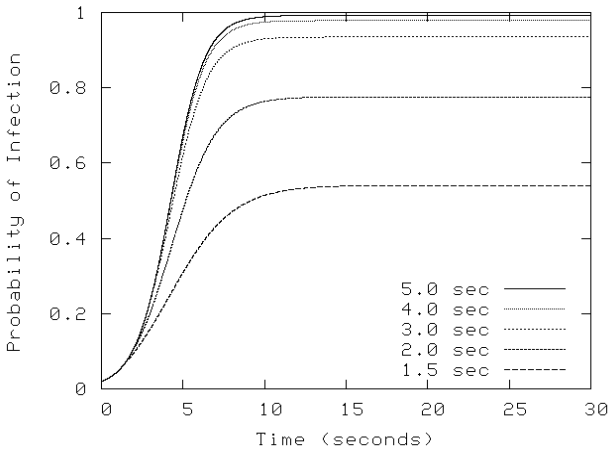

Figure 1. The baseline MANET worm propagation results in the presence of a mitigation technology.

the *Infinite Lifetime* assumption discussed above and is important in the context of our mitigation technology discussion below. We can derive a relatively simple analytic model of the performance of mitigation technologies as follows. Let $c(t)$ be the probability that a host has been infected by the worm by time t. This represents both the probability of hosts currently infected, $i(t)$, and the probability of hosts either quarantined or rehabilitated (and no longer susceptible to further infection), $r(t)$. Let us assume a simple model of the mitigation technology, i.e., that it takes a fixed amount of time, δ, for the mitigation response to act on the infected hosts. Then, following the same argument to derive the Standard Epidemic model above, we get

$$(t < \delta) \quad \frac{dc(t)}{dt} = \beta c(t)[1 - c(t)] \quad (7)$$

$$(t > \delta) \quad \frac{dc(t)}{dt} = \beta(c(t) - c(t - \delta))[1 - c(t)] \quad (8)$$

Note, this equation can also be derived from the more complex "Two Factor Worm Model" found in [16], by substituting $c(t) = i(t) + r(t)$. Further, given that infected nodes older than δ seconds are rehabilitated, then $r(t) = c(t - \delta)$. Finally, we implicitly assume that $c(0)$ consists of newly infected nodes, i.e., $c(0) = i(0)$. The expression in Eq.(8) modifies the Standard Epidemic model above by arguing that the total probe rate within the network is modified by the removal of the nodes which had been infected prior to $t - \delta$ seconds ago.

This equation is written for two separate time regimes due to the discontinuity in the slope of $c(t)$ at $t = \delta$,

$$\lim_{\varepsilon \to 0} \frac{dc(\delta + \varepsilon)}{dt} - \frac{dc(\delta - \varepsilon)}{dt} = -\beta c(0)[1 - c(\delta)] \quad (9)$$

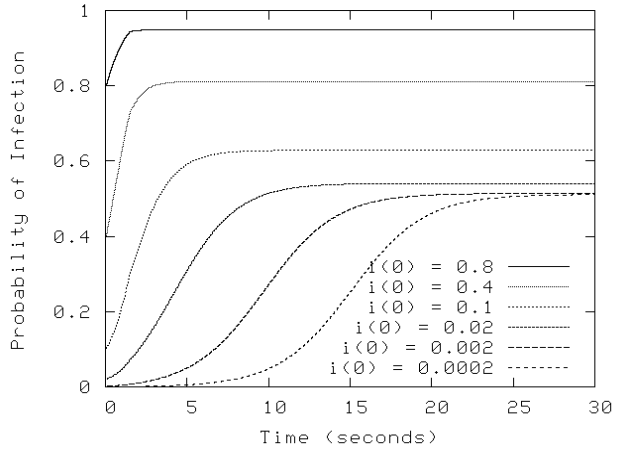

Figure 2. The effects of initial conditions on the final system state - 1.5 second mitigation response time.

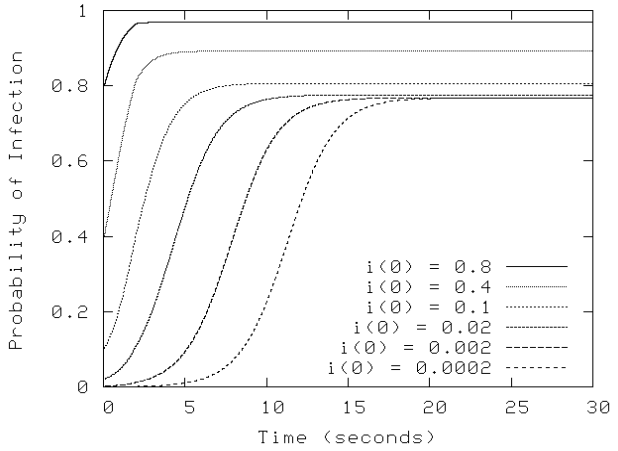

Figure 3. The effects of initial conditions on the final system state - 2.0 second mitigation response time.

The value of analytic models of relative simplicity is the explanation of the system dynamics which they afford. The steady state ($t \rightarrow \infty$) solution to the Standard Epidemic Model is $i(\infty) = 1$, which is apparent from Eq.(1) by setting the RHS of the equation to 0 yielding $1 - i(\infty) = 0$. The mitigation equation above affords the same solution for $c(\infty)$. The interesting question is whether the mitigation equation affords other steady state solutions as well. If we perform a Taylor Series expansion of $c(t-\delta)$ in Eq.(7) in terms of $c(t)$, we get

$$\frac{dc(t)}{dt} = \beta(\delta\frac{dc(t)}{dt})[1-c(t)] \tag{10}$$

Canceling the derivatives on both side of this expression yields

$$c(\infty) = 1 - (\beta\delta)^{-1} \tag{11}$$

Therefore, we suspect that there exist steady state solutions to Eq.(7) where $c(\infty)$ is less than unity, implying that the mitigation technology was effective in stopping the spread of the infection before the entire population was affected. Further, the faster the mitigation technology in detecting a infected node, the more effective the technology in limiting the final infection probability.

In Figure 3 we show the results of a numerical integration of Eq.(7). Here, we set $c(0) = 0.01$ and use 10,000 integration points over the range of the plot. We see that indeed there are steady state solutions where $c(\infty) < 1$ and that the final value of $c(\infty)$ decreases as the value of δ decreases.

In Figures 2 and 3 we show the results of varying the initial conditions on the final steady state solution. These

Table 1. Numerical tests for $c_c(\infty)$.

δ	No. Int. Pts.	$c(0)$	$c_c(\infty)$
1.5	$2x10^5$	$2x10^{-12}$	0.51
2.0	$2x10^5$	$2x10^{-12}$	0.77
3.0	$2x10^5$	$2x10^{-12}$	0.93
4.0	$2x10^5$	$2x10^{-12}$	0.98
5.0	$2x10^5$	$2x10^{-12}$	0.99

plots exhibit some interesting behavior. For small values of $c(0)$, i.e., $c(0) < c_c(0)$, the steady state solution is independent of the initial condition. However, for larger initial conditions, i.e., $c(0) > c_c(0)$, the steady state solution uniformly increases with larger initial conditions until finally the steady state solution of $c(\infty) = 1$ is approached. Based upon this behavior, we know that our simple expression in Eq.(11) is wrong, as it is independent upon initial conditions. We know this not to be the case from these figures. Further, if we try to interpret Eq.(11) as $c_c(\infty)$, we see from Table 1, that it does not well represent this value either. In Table 2, we investigate the impact of integration step sizes in determining $c_c(\infty)$. From these results, we are confident that the numerical integration results are correct. It remains an open area of investigation as to why the Taylor Series expansion of $c(t)$ fails to find the correct steady state.

Table 2. Numerical tests in search of $c_c(\infty)$.

δ	No. Int. Pts.	$c(0)$	$c_c(\infty)$
1.5	$2x10^5$	0.04	0.57
1.5	$2x10^5$	0.02	0.54
1.5	$2x10^5$	0.002	0.51
1.5	$2x10^5$	$2x10^{-4}$	0.51
1.5	$2x10^5$	$2x10^{-8}$	0.51
1.5	$2x10^5$	$2x10^{-12}$	0.51
1.5	$2x10^7$	$2x10^{-12}$	0.51

4. Simulation Studies

We present a comparison of the above model to a set of mitigation simulation studies. The NS2 simulation tool [8] was used to simulate the spread of the worm infection throughout a MANET. The version 2.27 of NS2 already contained an application which simulated the spread of a computer worm. We modified the NS2 application in order to a) simulate an isolated MANET, b) allow us to plant the initial infection seed at random in the MANET at time zero and c) allow us to define a fixed, finite lifetime to an infected node (which dies at a lifetime of δ).

Because the dynamics specific to a MANET are of interest, we simplified the simulation and analysis in the following ways:

- Simple Worm Model - we assume the worm propagates through the transmission of a single UDP packet of size *P*. We simulate the effects of bandwidth competition by varying the channel bandwidth while holding the size of the infection data constant.
- MANET Aware Model - the worm chooses nodes at random to infect, but only targets nodes within the MANET. We wanted to focus this study on MANET specific issues, without the added complexity of modeling and simulating on-MANET versus off-MANET probe traffic.
- Modified Random WayPoint Mobility Model - we assume that the nodes move independent of one another according to the Random WayPoint model, modified in order to address the concerns raised in [15]. Other, more realistic, mobility models will be studied in the future, see, e.g. [2].
- AODV Routing Protocol - the NS2 simulation tool supports a number of MANET routing protocols. For our initial studies we choose the AODV routing protocol [9]. Future studies will include other routing protocols.

Table 3. Baseline case parameter definitions.

Parameter Description	Range	Base Case
Number of Hosts	50	50
Address Block Search	50	50
Transmission Rate (Mbps)	0.1 - 2.0	2.0
Transmission Range (m)	250	250
Topographic Range (m^2)	1000^2	1000^2
Nodal Mobility (mps)	1 - 10	1
Routing Protocol	AODV	AODV
Probe Size (bytes)	400	400
Probe Rate (probes/sec)	1	1

- 802.11 MAC and Physical Layer - The NS2 simulation tool provides models of the 802.11 MAC and Physical layer protocols. Further, we utilized the NS2 Two Ray radio propagation model with an effective transmission range of 250 meters.

The parameters in Table 3 define our Baseline MANET simulation model.

Several simulations of the Baseline Case were conducted for δ values of 1.5, 2.0, 3.0, 4.0 and 5.0 seconds. For each set of conditions, we ran thirty independent simulation runs and averaged their results. These averaged results are presented in Figure 4. These simulation results show the same qualitative behavior as shown in the numerical results of Figure 3. We see that the impact of a mitigation technology applied to this environment is negligible for response times, i.e., δ's, larger than 3 seconds. Remember that we have assumed a focused search strategy for our infection agents and that the probe rate per infected node, i.e., β, is unity. In Figure 5 we overlay the model predictions from Figure 3 onto the simulation results from Figure 4. The model seems to do a reasonable job in predicting the steady state value for the infection probability for values of δ equal to 2 seconds and higher. However, for the case of $\delta = 1.5$ seconds, the model over estimates the steady state value of the infection probability.

We know from our discussion of the Standard Epidemic Model in the Section 3, that Eq.(7) is an extremely simplified model within the context of its application to MANET environments. In [3] we explicitly discussed the impact of the various assumptions inherent to the Standard Epidemic Model and analyzed the effectiveness on enhanced models incorporating the effects of network delays and bandwidth competition on worm propagation. As an example, in Figure 6 we modeled the impact finite network delays using Eq.(6) from [3]. Here we set $\delta = 2$ seconds and varied the network delays, ranging from 0 seconds (implicitly assumed previously in this paper) to 0.5 seconds. We see that

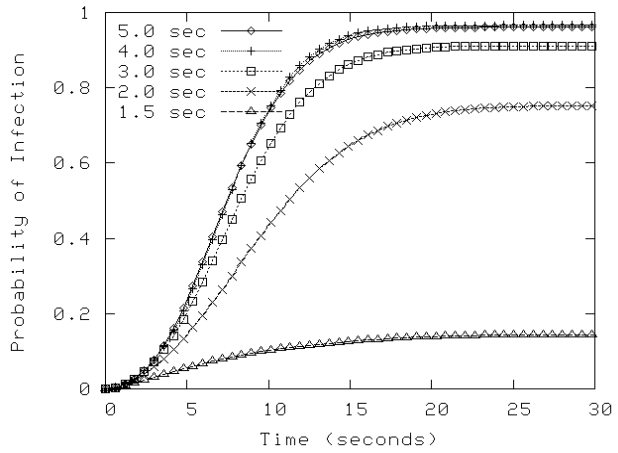

Figure 4. The results from the simulation studies of the MANET.

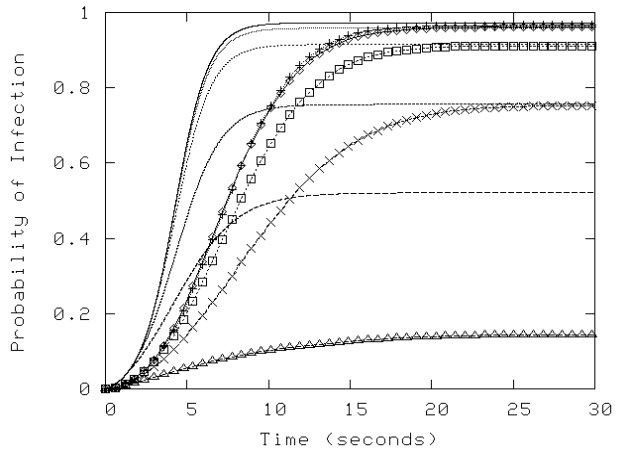

Figure 5. Overlay of the analytic model results on the simulation results.

the finite network delay slows the initial spread of the worm due to the finite delays in time between an infected node sending out an infection probe and an infected node receiving the probe. This propagation delay reduces the resultant overall infection probability. Other effects impact the longer term behavior of the worm propagation, e.g., mobility and bandwidth competition.

In Figure 7 we investigate the impact of nodal mobility. Our baseline case set the nodal mobility to 1.0 meters per second (mps). The mobility model used is the Random Way Point model modified according to the discussion found in

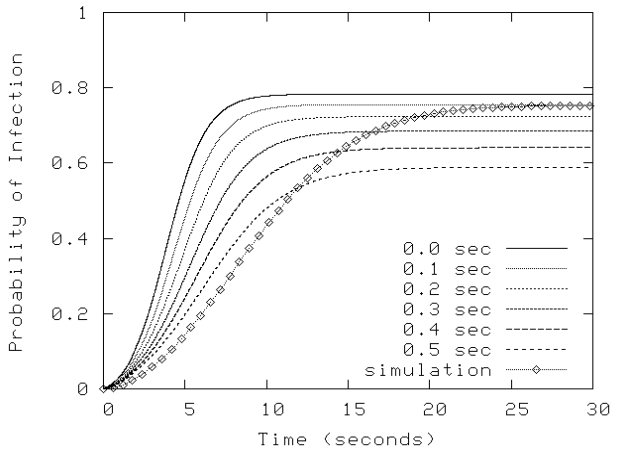

Figure 6. Effects of network delay on worm infection results.

[15]. We present simulation results for mobilities ranging from a low of 1.0 mps to a high of 10.0 mps. Here we set the mitigation response time to 2.0 seconds, which seems to be within the range of interesting effects for the baseline parameter set. The impact of mobility within the range investigated, seems to have little impact of the nature of the worm propagation. For low probabilities of infection, the curves are essentially indistinguishable. At high probabilities of infection, there may be some slight differences in $c(\infty)$ between the various mobilities, but not enough to see any clear relationship.

In Figure 8 we present results for channel bandwidth of 200 Kbps. We discussed the effects of competition between worm probes under conditions of limited bandwidth in the MANET in [3]. In this study, we choose to reduce the channel bandwidth 10 fold, from our baseline of 2.0 Mbps down to 200 Kbps. Our previous investigations showed this bandwidth to result in severe channel congestion due to the relatively high number of infection probes being injected into the network as the probability of infection grows. All other parameters are set to their baseline parameter set values. In this figure we vary the mitigation response time from a high of $\delta = 20$ seconds to a low of $\delta = 1.5$ seconds. From above, we expect that a mitigation response time greater than 5.0 seconds will have little impact on the final infection probability. From the figure we see little difference between the $\delta = 20.0$ and the $\delta = 5.0$ seconds behavior; perhaps the $\delta = 5.0$ seconds showing a slightly higher final infection probability as compared to the $\delta = 20.0$ seconds results. This trend continues as we reduce the mitigation response time down to a $\delta = 2.0$ seconds. Finally, when $\delta = 1.5$ seconds, the final probability of infection drops way down as

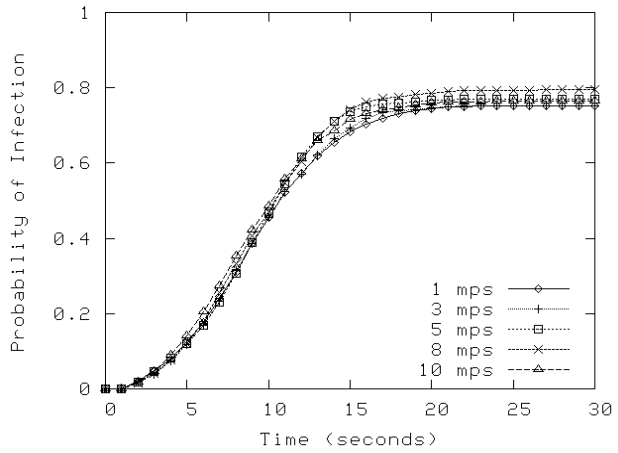

Figure 7. Effects of mobility on the performance of the mitigation technology.

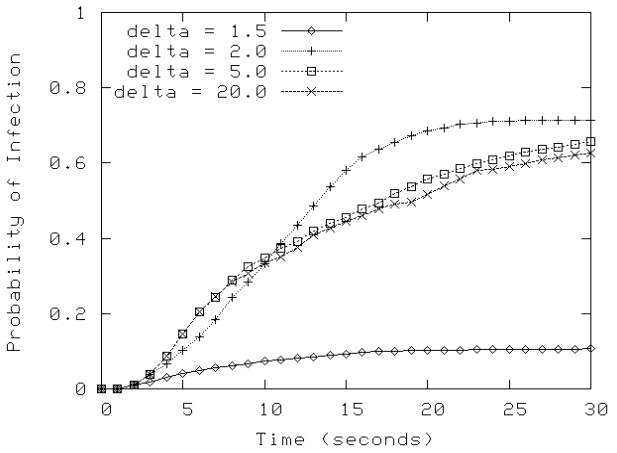

Figure 8. Effects of congestion on the performance of the mitigation technology.

we initially would expect. Therefore it seems that there is a range of δ's for which a mitigation technology may actually increase the performance of the worm propagation under conditions of channel congestion. This effect is similar to the situation in population dynamics where the presence of predation actual improves the health of the population. In our study, the predation is the mitigation technology and the population is the infected nodes. Future studies are necessary to a) better analyze the conditions under which this behavior occurs and b) develop analytic models for the prediction of this behavior.

5. Discussion of Mitigation Technologies in MANETS

Modeling investigations presented thus far have focused on greedy worm propagation mechanisms whereby the worms propagate at a high rate, eventually stressing the underlying communication infrastructure. In these situations, it is reasonable to expect that intrusion detection monitoring systems would detect the worm propagation traffic patterns and could be used to initiate some form of response, e.g., nodal quarantines, nodal patches, etc. However, as our discussion of impact of congestion on worm propagation rates above suggests, there may be conditions where the presence of a mitigation technology actually encourages the propagation of the worms by reducing channel congestion. More work is necessary to better understand this effect.

The above numerical model addresses only the mean behavior of the propagation. In order to derive meaningful requirements for mitigation technologies, we need to investigate the effectiveness of the mitigation technologies in keeping the worm infection probability below some value, say, 95 percent of the time. [7] studied this question in the context of the larger, wired Internet. They examined, through simulation of several potential mitigation technologies such as *Address Blacklisting* and *Content Filtering*, the spread of a computer virus through a large scale network. The focus of [7] was on the effectiveness of these mitigation technologies in reducing the worm infection versus the probing rate of the worm. They evaluated the effectiveness of these technologies in terms of various confidence levels.

Clearly this is the direction we need to take our studies in order to generate performance requirements on potential mitigation technologies. Figure 9 gives us an idea of the variability in the worm propagation in our baseline MANET by plotting out the individual histories from a set of 30 simulation runs. The parameters used for this set of runs were the *Baseline Case* with the $\delta = 4$ seconds. The mean value numerical models may not satisfy our needs to generate useful requirements on mitigation technologies. Our future investigations will require further simulation studies and perhaps the development of meaningful stochastic differential equations for worm propagation in computer networks.

6. Conclusions

We have presented a brief study of mitigation of computer worm propagation in MANETS. We investigate the validity of a simple mitigation model through simulation studies. Our simple model, however, is shown to have rather interesting behavior. We suspect that models of this type will be useful in developing engineering rules for design

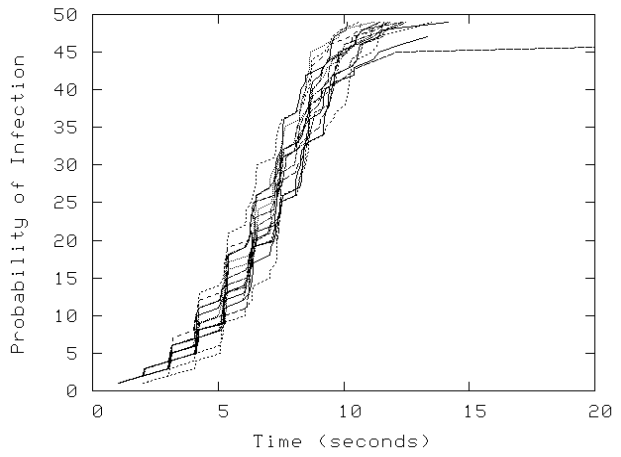

Figure 9. The individual state traces from the simulation study of the MANET with a mitigation response of 4 seconds.

and deployment of mitigation technologies. We discussed efforts to extract steady state solutions from this model. Clearly further work in this area is warranted. We compared the model predictions with simulations of an idealized mitigation technology in a MANET environment. The simplified analytical model of these environments predicted reasonably well the long term effectiveness of the mitigation technologies. Or simulation studies showed conditions under which the presence of mitigation actually aided the overall spread of the worm.

Our ultimate goal is to generate performance requirements on potential mitigation technologies in these MANET environments. We concluded this report with a brief discussion of the effectiveness of mitigation technologies and future investigations. Clearly, there is a subtle interplay between the worm agent, the mitigation technology and the communications infrastructure. More work is necessary to better understand these subtleties.

Acknowledgements

We would like to acknowledge Sue Lee of JHU/APL for suggesting this investigation and for her initial encouragement, beneficial discussions and a host of references on the topic. We also wish to acknowledge the support and encouragement of Don Duncan at JHU/APL.

References

[1] Bailey, N.T., *The Mathematical Theory of Infectious Diseases and it's Applications*, Hafner Press, New York, 1975.

[2] Camp, T., Boleng, J. and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research", *Wireless Communication and Mobile Computing (WCMC)*, vol. 2, no. 5, 2002.

[3] Cole, R.G., "Initial Studies of Worm Propagation in MANETs for Future Combat Systems", *The Army Science Conference 2004 (ASC2004), Orlando, FL, November 2004.*

[4] Ghosh, A.K., Technical POC, *Defense against Cyber Attacks on Mobile, Ad Hoc Network Systems (MANETS)*, BAA04-18 Proposer Information Pamphlet (PIP), Defense Advanced Research Projects Agency (DARPA) Advanced Technology Office (ATO), 16 April 2004.

[5] Frauenthal, J.C., *Mathematical Modeling in Epidemiology*, Springer-Verlag, New York, 1980.

[6] Moore, D. and C. Shannon, "Code-Red: a Case Study on the Spread and Victims of an Internet Worm", in *Proceedings of the 2002 SIGCOMM Internet Measurement Workshop*, Marseille, France, pp. 273-284, November 2003.

[7] Moore, D., et al., "Internet Quarantine: Requirements for Containing Self-Propagating Code", in *Proceedings of the 2003 SIGCOMM Internet Measurement Workshop*, Marseille, France, pp. 273-284, November 2003.

[8] The Network Simulator - 2, *http://www.isi.edu/nsnam/ns/*, 2004.

[9] Perkins, C.E. and E.M. Royer, "The Ad Hoc On-Demand Distance-Vector Protocol", in *Ad Hoc Networking*, C.E. Perkins (ed.), Addison-Wesley, 2001.

[10] Rajab, M.A., Monrose, F. and A. Terzis, "An Evaluation of Collaborative Monitoring for Worm Defense", *HiNRG Technical Report 2004-03*, 2004.

[11] Rajab, M.A., Monrose, F. and A. Terzis, "On the Effectiveness of Distributed Worm Monitoring", *HiNRG Technical Report 2005-01*, 2005.

[12] Serazzi, G. and S. Zanero, "Computer Virus Propagation Models", *preprint*, 2001.

[13] Staniford, S., Paxson, V. and N. Weaver, "How to Own the Internet in Your Spare Time", in *Proceedings of the 11th USENIX Security Symposium*, 2002.

[14] Wang, Y. and C. Wang, "Modeling the Effects of Timing Parameters on Virus Propagation", in *WORM'03*, Washington D.C., October 2003.

[15] Yoon, J., Liu, M. and B.D. Noble, "Random Way Point Considered Harmful", in *INFOCOM '03*, San Francisco, April 2003.

[16] Zou, C.C., Gong, W. and D. Towsley, "Code Red Worm Propagation Modeling and Analysis", in *CCS'02*, Washington, D.C., November 2002.