Modeling and Simulations of TCP MANET Worms

Mohamed Abdelhafez[1], *George Riley*[1], *Robert G. Cole*[2] *and Nam Phamdo*[2]

[1]Department of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332-0250
{mohamed.hafez,riley}@ece.gatech.edu

[2]Johns Hopkins University
Applied Physics Laboratory
Laurel, Maryland 20723-6099
{robert.cole,nam.phamdo}@jhuapl.edu

Abstract

Mobile Ad-hoc Networks (MANETs) are used for emergency situations like disaster–relief, military applications, and emergency medical situations. These applications make MANETs attractive targets for cyber–attacks and make the development of counter–measures paramount.

The study of worm behavior is critical to the design of effective counter measures in MANET environments. This paper studies the behavior of TCP based worms in MANETs. We develop analytical models for the spread of TCP worms in the MANET environment that account for payload–size, bandwidth–sharing, radio range, nodal density, packet discards and several other parameters specific to MANETs. We present numerical solutions for the models and verify the results using high fidelity packet–level simulations.

The results show that the analytical model developed here matches the results of the packet–level simulation in all cases except when topologies result in a high probability of disconnected clusters. Our simulation studies show that under many cases, due to the resource constrained nature of the MANET and its underlying wireless layers, the TCP-based worms rapidly become self-throttling. This may benefit the design of effective mitigation technologies in these critical networking environments.

1 Introduction

Internet worms are programs that can replicate and propagate on the Internet by exploiting security flaws in some services. Once resident on a host computer, the worm implements a search strategy for the selection of future host targets. This involves an algorithm for choosing a host IP address from the total IP address range. Various target host selection algorithms have been discussed, analyzed and found within Internet worms. Once a target host is selected, the worm attempts to transfer its payload to the target. If successful, these newly infected hosts continue the infection process. This results in the well known exponential growth of the number of infected hosts as reflected in the Standard Epidemic Model [1].

Worms have demonstrated that they can cause serious damage to the economy. In 2001 the Code Red worm infected 360,000 hosts in 14 hours [10]. The direct costs of recovering from this epidemic (including subsequent strains of Code Red) have been estimated to be in excess of $2.6 billion [11]. In 2002 the Slammer worm infected 90% of its vulnerable hosts (75,000) in less than 10 minutes [9], the estimated loss was about $1 billion [18]. In 2003 the Blaster worm was estimated to have infected more than 500,000 systems worldwide and the cost to North American companies was $1.3 billion [18]. However, a more recent report showed that the number of infections was actually between 8 million and 16 million systems [8]. In 2004 the Witty worm had a malicious payload that targeted firewalls. Not only did it spread to additional hosts, but it also formatted a portion of the hard drive of the infected host [15].

According to [17] the severity of the worm threat has grown recently with (i) the increasing degree to which the Internet has become part of a nation's critical infrastructure , and (ii) the recent, widely publicized introduction of very large, very rapidly spreading Internet worms, such that this technique is likely to be particularly current in the minds of attackers.

The effect of worms on a Mobile Ad-hoc Network (MANET) topology is much more serious, due to the resource constrained nature of such a network. According to the recent DARPA BAA Defense Against Cyber Attacks on MANETS [6], "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."

A MANET is a self-configuring network of mobile nodes that act as routers and hosts, and are connected by wireless links. The topology of MANETs is arbitrary and dynamic. MANETs can operate in a standalone

fashion, or may be connected to the Internet. Because of the fact that MANETs require minimal configuration and are quickly and easily deployed, they are suitable for emergency situations like disaster–relief, military applications, and emergency medical situations. These applications make MANETs attractive targets for cyber–attacks and make the development of counter–measures paramount. As such, we have embarked on a program to investigate worm propagation and mitigation in MANETs [3] [4].

Here we extend our prior analysis to the investigation of TCP-based worms; our previous work focused on UDP-based worms. Our investigations involve extensive, high fidelity simulations of TCP-based worms using the *Georgia Tech Network Simulator* (GTNetS) [14]. Further, we develop and investigate a model of the TCP worm propagation in MANETs. The model results are compared against the simulation experiments. The model is an extension to the Standard Epidemic Model, which is

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

where $i(t)$ is the probability of nodal infection at time t, and β is the rate at which a given infected node is successful in infecting other susceptible nodes.

For a simple, UDP-based flash worm, β is generally set to the product of: i) the inverse of the UDP packet transmission time onto the communication interface of the infected host, times ii) the probability that the packet is addressed to a susceptible host, times iii) the probability that the UDP packet is not lost in transit due to network congestion. The first term is simply proportional to the communications line speed divided by the size of the single UDP packet. The second term is usually taken as the ratio of the susceptible host population divided by the entire address space, assuming a worm which implements a random address search strategy. Zou et. al. [2], have suggested that the last term be approximated by $[1 - i(t)]^{\eta}$ where η is a fitting parameter. This term estimates the probability of packet receipt success at the susceptible host under conditions of buffer overflows within the network.

For a TCP-based worm, β must assume a somewhat different form for two reasons: i) the rate at which an infected node can transmit the worm to other nodes is related to the number of simultaneous TCP connections divided by the mean time for a TCP connection to transmit the worm payload, and ii) network congestion does not decrease the probability of receipt of the payload at the susceptible host, but instead congestion slows the time to transmit the payload due to bandwidth competition. Bandwidth competition can slow the TCP transmit times due to increased bandwidth sharing and increased packet losses. Therefore, we investigate a TCP model which accounts for bandwidth sharing and includes mechanisms within the underlying 802.11 Link and Physical layers which cause packet discards at moderate to high loads.

2 Related Work

Several studies were carried out to analyze and model the propagation of computer worms in digital communication networks. In [19] the authors present the different kinds of worms depending on their scanning strategies, worm carrier mechanism, possible payload and plausible attackers who would employ such a worm. In [17] the authors provide an extensive investigation into the mechanisms of worm propagation and their performance. They also provide some improvements for the worms and the effort needed to mitigate worm propagation throughout the Internet.

Zou et. al. [2], studied the Code Red worm outbreak and provided an analysis of its propagation by accounting for two factors: i) the dynamic countermeasures taken by ISPs and users, and ii) the slowed infection rate due to the rampant propagation of the worm causing congestion and troubles to some routers. They derived a general Internet worm model called the *two-factor worm model*.

The most relevant work to this paper is [3] and [4]. In [3] the authors investigated the impact of communications and mobility effects on worm propagation mechanisms in MANETs, where they found that network delays and channel congestion had a large impact on the UDP-based worm propagation behavior. They also provided a set of relatively simple analytical models that reproduced these communications. In [4] the authors discussed the effect of mitigation techniques on the UDP-based worm spread in MANETs and provided analytical models and simulation experiments to validate their findings. The authors represented the mitigation technologies as having a constant detection time represented by a lifetime parameter of the worm, after which the worm dies and stops infection of other hosts. These studies were limited to UDP worms. In this paper we extend their simulation models to be used in GTNetS and to include TCP style worms in MANETs as well.

3 The TCP Worm Propagation Model

We first investigate the performance of TCP worm propagation through analytic models. Our analytic modeling describes the 802.11 wireless MANET as residing in one of two states: a low load state where the number of TCP flows in the network is relatively small and a higher load state where the number of TCP flows is moderate to high. In the state with a small number of flows we develop a bandwidth-sharing expression for β which accounts for a slowing of the worm propagation as a result of competition for the radio channel bandwidth,

without however causing significant packet losses. In the state with a moderate number of TCP flows we develop a model that accounts for high probabilities of packet discards as a result of collisions and 802.11 retry limits, but not resulting from buffer overflows. This follows the work of Fu et al. [5], who found that 802.11 networks settle into a state where the nodal probability of packet losses becomes flat as more and more transmitters (or flows) are added to the network.

3.1 Low Number of Flows

This model applies to small values for the probability of nodal infections.
Define:

$i(t)$	=	probability of infection
b	=	bandwidth of the radio channel (Bps)
d	=	nodal density (nodes/sq.meter)
r	=	radio range of the channel (meters)
c	=	radio interference range factor
$n(t)$	=	mean number of infected neighbors
α	=	(zero load) TCP throughput in proportion to the channel bandwidth

Assuming perfect sharing of channel bandwidth during the transmission of a TCP worm payload, the channel bandwidth is partitioned equally to each of the neighboring TCP transmissions. Thus, the portion of the channel bandwidth available to each TCP transmission is

$$\bar{b} = \frac{b}{(n(t)+1)} \tag{2}$$

Assuming uniform placement of nodes in the MANET, we write

$$\bar{b} = \frac{b}{[\pi d(r(1+c))^2 i(t)+1]} \tag{3}$$

So, we consider each infected node seeing a time-varying available bandwidth because of an increasing probability of infection over time. The Standard Epidemic Model becomes

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

where β is now time dependent.

For a single threaded TCP operation, as modeled in our simulation studies discussed below, let τ_{tcp} be the average TCP throughput for the transmission of the worm payload. Then, the time to transmit the TCP worm payload is

$$t_{tcp} = \frac{P_w}{\tau_{tcp}} \tag{5}$$

where P_w is the payload size of the worm. From the above, modified Standard Epidemic Model, $\beta(t)$ is

$$\beta(t) = \frac{1}{t_{tcp}(t)} = \frac{\tau_{tcp}(t)}{P_w} \tag{6}$$

and

$$\tau_{tcp}(t) = \alpha \bar{b}(t) \tag{7}$$

where α is the proportion of the available channel bandwidth that a TCP connection is able to obtain under zero load situations, see for example, [7] [12] and [13]. Hence, α is a function of the mean number of hops across the MANET, the packet size, etc. We assume that α is a constant with respect to time. Inserting these expressions into the above Epidemic Model yields

$$\frac{di(t)}{dt} = \left[\frac{\alpha b}{P_w(1+\pi d(r(1+c))^2 i(t))}\right] i(t)[1-i(t)] \tag{8}$$

This expression is comparable to the expression for the UDP-based Flash worm proposed by Zou et. al., [2]

$$\frac{di(t)}{dt} = \beta[1-i(t)]^{\eta} i(t)[1-i(t)] \tag{9}$$

These equations are different because they consider the different effects of network congestion. Our TCP worm model is predicting a diminishing TCP throughput due to channel sharing at higher infection probabilities. While Zou et al.'s model is predicting a decreasing probability of end-to-end packet delivery success due to buffer overflow under increased network competition at higher infection probabilities.

3.1.1 Analytic Results

In this section we investigate the analytic solution to our TCP worm model given in Eq.(8). Following the method of factoring used to solve the Standard Epidemic Model of Eq.(1), we rewrite Eq.(8) as

$$\frac{di(t)}{dt} = \gamma_{low} i(t) \left[\frac{1-i(t)}{1+\theta i(t)}\right] \tag{10}$$

where $\gamma_{low} = \alpha b / P_w$ and $\theta = \pi d(r(1+c))^2$. We factor this expression into

$$(1+\theta i(t)) \left[\frac{1}{i(t)} + \frac{1}{1-i(t)}\right] di(t) = \gamma_{low} dt \tag{11}$$

Integrating both sides of this equation and rearranging terms yields

$$\frac{i(t)}{i(o)} \left[\frac{1-i(o)}{1-i(t)}\right]^{1+\theta} = e^{\gamma_{low} t} \tag{12}$$

or

$$\frac{i(t)}{[1-i(t)]^{1+\theta}} = g(i_0) e^{\gamma_{low} t} \tag{13}$$

where

$$g(i_0) = \frac{i_0}{[1-i_0]^{1+\theta}} \tag{14}$$

Here $i_0 = i(t=0)$. This is as far as we can get in writing the explicit solution to our TCP model. For general values of θ, we cannot solve this expression for $i(t)$.

However, when $\theta = 1,\ 2\ or\ 3$ this expression represents a quadratic, cubic or quartic expression in $i(t)$, respectively. For other values of θ, i.e., θ real or $\theta > 3$, no known explicit solutions exist.

We can determine the general asymptotic behavior of $i(t)$ as $t \rightarrow \infty$ from Eq.(13). The right hand side of Eq.(13) clearly approaches infinity as $t \rightarrow \infty$. This implies that the left hand side of Eq.(13) also approaches infinity, which can only happen if $i(t \rightarrow \infty) = 1$. Also, by writing $i(t) \approx 1 - \epsilon$ where for large t, $\epsilon << 1$, we can perform an expansion of Eq.(13) in terms of ϵ. This yields the follow expression for $i(t \rightarrow \infty)$,

$$\lim_{t\rightarrow\infty} i(t) \approx 1 - g^{-1/(1+\theta)} e^{-\gamma_{low} t/(1+\theta)} + ... \quad (15)$$

Clearly, the larger θ is, the slower is the convergence of $i(t)$ toward unity, reflecting that fact that greater bandwidth competition is slowing the propagation of the TCP-based worm.

While it is interesting that results for the asymptotic behavior is available, we will find that in 802.11 wireless networks with TCP worms, the results of this low load model will apply only for very small probabilities of infection, i.e., $i(t) < 0.2$. We now turn our attention to the derivation of a TCP worm propagation model for moderate to high numbers of TCP flows.

3.2 Moderate to High Number of Flows

We rely on the fact, shown in [5], that the network saturates as the number of TCP flows increases. In this saturated state, many of the network performance characteristics become independent of further increases in the number of TCP flows. This allows us to derive a simple relationship between the TCP throughput versus the number of TCP flows in the network.

In this saturated state, the per node packet loss rate becomes a fixed constant independent of further increases in the number of TCP flows. Further, the packet loss rate is a result of collisions due to hidden terminal issues and not buffer overflow. In fact, they show that the mean buffer occupancy in this saturated state is extremely low and they find that little, if any, packets are lost through buffer overflow as verified through simulation studies. In 802.11 networks, nodes will discard a data packet in the event that the node has attempted to send an RTS seven times without success. Here seven is a default parameter of the Medium Access Control (MAC) protocol. Hence, packets handled by the nodes are either transmitted to the next hop or are discarded due to a failure of the node to gain access to the channel after seven attempts. The explanation for the network saturation is that as the number of flows increases, the number of "backlogged nodes", i.e., those nodes with packets to transmit, quickly approaches N, the total number of nodes in the network. Once in this state, the network performance saturates in terms of the packet loss rate and the overall network throughput. This behavior does not change as further increases in the number of TCP flows occur.

Define:

p = the nodal packet loss probability
u = the nodal packet processing rate
m = the number of "backlogged" nodes
f = the number of flows in the MANET
l = the mean number of hops per path

The TCP flows are generated by our TCP worm, and hence we have that $f = N \times i(t)$. To estimate the dependence of m on f let us assume the following model. At a minimum, $m \geq f$, because by definition each flow has a different source node in our worm model. Further, because each flow on average makes l hops through the network, we know that m is greater than f. In fact, we can estimate the probability that a node is not backlogged given f as follows. As previously stated, at least f nodes are backlogged, one for each flow. Of the remaining $N - f$ nodes, imagine that each flow randomly travels over l nodes. Hence,

$$Pr\{node\ not\ backlogged | f\ flows\} = \left(\frac{N-f-l}{N-f}\right)^f \quad (16)$$

Given that f nodes are backlogged as sources of the f flows and the remaining nodes are backlogged according to one minus the probability in the above equation, we have that

$$m = f + (N-f)\left\{1 - \left(\frac{N-f-l}{N-f}\right)^f\right\} \quad (17)$$

This functional relationship between m and the f shows that the network soon becomes saturated as the number of flows is randomly increased within the network. In fact, our simulation studies, indicate that this occurs when $i(t)$ is much less than 0.2.

We now analyze the relationship of the per flow throughput across the saturated network versus increased number of flows in terms of a simple flow model. In the saturated state, the network is characterized by p, the per node packet loss rate, which is independent of f in the saturated state. Further, we define u as the per node packet processing rate, where packet processing includes both the time to successfully transmit a packet to the next node as well as the time to fail to transmit a data packet because of a failure to gain access to the channel and hence ending up discarding the packet. In the saturated network state, u is also independent of the number of active flows in the network. Finally, because network routing is independent of network load, we know that the mean path length, l, is also independent of the number of flows. So the quantities

p, u, and l, characterizing aspects of the network performance, are independent of the number of flows when the network reaches the saturated state.

Let $f_{r,in}$ be the average flow rate into the network for a single flow, and let $f_{r,out}$ be the average flow rate out of the network for a single flow. Given that each flow traverses (on average) l hops in the network and that each node has an average packet loss rate of p which is independent of the number of flow, we have that

$$f_{r,out} = f_{r,in}(1-p)^l \tag{18}$$

Therefore, the per flow loss rate is

$$p_{flow} = f_{r,in} - f_{r,out} = f_{r,out}\left(\frac{1}{(1-p)^l} - 1\right) \tag{19}$$

Equating the total network packet loss rate for N nodes and for f flows we get

$$N \times u \times p = f \times p_{flow} \tag{20}$$

or

$$f_{r,out} = \frac{up(1-p)^l}{i(t)(1-(1-p)^l)} \tag{21}$$

where we have used the fact that $f = N \times i(t)$.

3.2.1 Analytic Results

When the 802.11 network is in the saturated state we have derived an expression for the flow rate per TCP flow in the network, Eq.(25) above. Assuming this is roughly equal to the TCP throughput, we get the following result for $\beta(t)$,

$$\beta(t) = \frac{\tau_{tcp}}{P_w} = \frac{up(1-p)^l}{P_w i(t)(1-(1-p)^l)} = \frac{\gamma_{sat}}{i(t)} \tag{22}$$

and the corresponding SEM becomes

$$\frac{di(t)}{dt} = \gamma_{sat}[1 - i(t)] \tag{23}$$

This expression has a simple solution, given by

$$i_s(t) = 1 - (1 - i^*)e^{-\gamma_{sat}t} \tag{24}$$

where we have defined (or labeled) $i_s(t)$ as the evolution of the probability of worm infection when the network is in the saturated state, and we have indicated the solution's initial condition as i^*, which we also define as the transition point between the low load network behavior and the network moderate load behavior.

3.3 Combined Results

We now combine our results for the low load and the moderate to high load regimes. Equation(10) for the low load regime was

$$\frac{di(t)}{dt} = \gamma_{low} i(t)\left[\frac{1-i(t)}{1+\theta i(t)}\right] \qquad for\ i < i^* \tag{25}$$

Parameter Description	*Range*	*Base Case*
Number of hosts	50-150	50
Initial population size	1-20	1
Transport layer protocol	TCP	TCP
Simultaneous connections	1	1
Range of vulnerable Addresses	50 - 500	50
Transmission Rate (Mbps)	0.1 - 2.0	2.0
Time delay(μ seconds)	2	2
Transmission range (m)	100 - 500	250
Area of topology (m^2)	1000	1000
Payload size (KBytes)	0.4 - 4000	4
Simulation time (seconds)	200	200

Table 1. Parameter definition for simulation experiments.

Equation(27) for the moderate to high load regime was

$$\frac{di(t)}{dt} = \gamma_{sat}[1 - i(t)] \qquad for\ i > i^* \tag{26}$$

Let us define i^* as the value of the infection probability where the transition from low load behavior to saturated network behavior occurs. We can pick the transition point, i.e., i^*, as a fitting parameter which is chosen to best fit the simulation data.

Note that our combined TCP model makes the following assumptions:

- A single threaded TCP operation.
- A throughput model for the time to transmit the TCP worm payload, which assumes a large payload in relation to the TCP segment size in the network.
- Sufficient nodal density and radio transmission range to maintain connectivity across the MANET cluster.
- No background traffic.

It is relatively straightforward to incorporate the effects of multi-threaded TCP operation. Work to relax the assumption of large payloads may not be extremely useful because we would expect that most TCP worms have relatively large payloads. It may be possible to incorporate topological effects into our models to account for probabilities of island formation at low densities or small radio ranges, although we have not investigated this to date. We plan to investigate improvements to our model relaxing these assumptions in future studies.

4 Simulation

In this section, we present the simulation experiments conducted using *Georgia Tech Network Simulator* (*GTNetS*).

GTNetS has an application that models the spread of a computer worm. The worm is designed as an application

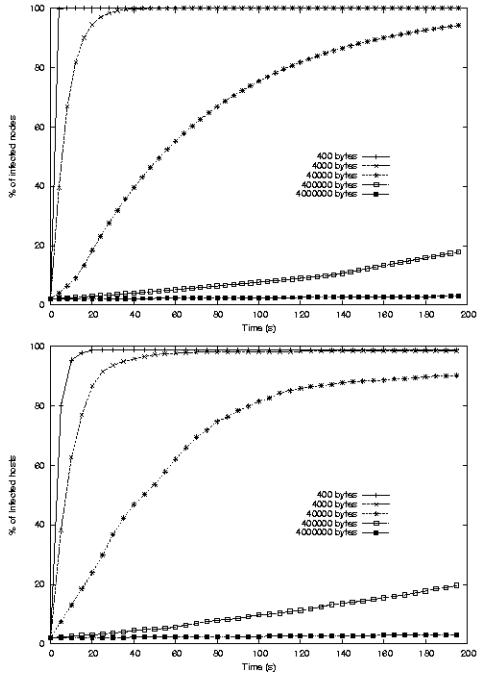

Figure 1. The TCP Model results (top) for various worm payload sizes compared with simulation results (bottom).

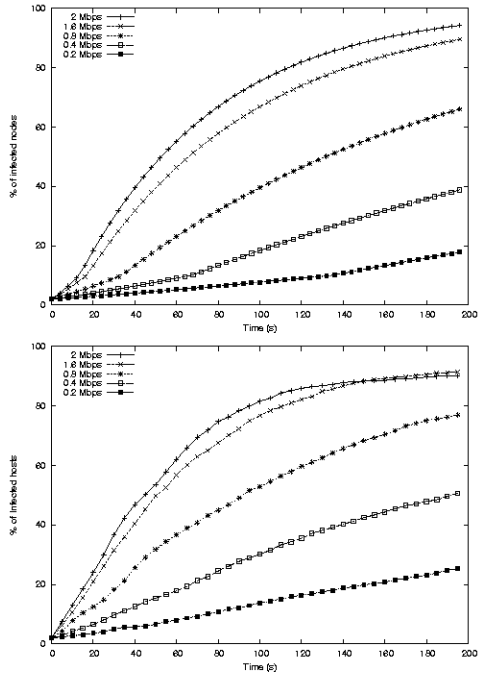

Figure 2. The TCP Model results (top) for various transmission rates with simulation results (bottom).

that exists on all susceptible nodes, which is listening on a specific port for incoming packets. When the worm application receives the infectious packet it is activated and starts choosing targets to send infectious packets to them.

There are different models for worms as discussed in [16]. The models include a number of parameters that specify the behavior of the worm

The MANET nodes are initially arranged in a rectangular grid, where they are uniformly placed across the grid. For our mobility studies, the Random Waypoint model was used to describe the motion of the nodes during the propagation of the TCP-based worm through the MANET.

Table 1 define our baseline MANET TCP worm simulation model parameters.

4.1 Results

In our experiments we create the MANET topology and set the simulation parameters according to Table 1 baseline case. We then start the worm infection in the initial population and measure its spread against time for varying one parameter at a time and compare the average of the results of 30 runs with the output of the TCP worm model described in Section 3.

Figure 1 shows the results of varying the TCP payload size. Here it is clear that for payload sizes in excess of 4 KBytes, the worm propagation soon congests the capacity of the radio links and the rate of spread decreases dramatically. Also apparent is the fact that for small payloads, the time for the worm to overrun the entire network is extremely short. This is one of the reasons the DARPA program in [6] was so concerned about worm attacks against tactical MANETs. As mentioned before, the analytic modeling compares well with the simulation results shown in Figure 1.

Figure 2 shows the results of the TCP worm model and simulations after varying the transmission rate of the wireless channel, ranging from 0.1 Mbps to 2.0 Mbps. It is clear from the figures that as the transmission rate decreases the worm spread flattens due to saturation of the network and the infection growth tends to become linear. The model does a very good job in qualitatively representing the simulation results.

Figure 3 shows the results of the TCP worm model and simulations after varying the initial infected population size, ranging from 1 to 20 nodes. The model does a good job in qualitatively representing the simulation results. The results show as expected that with increasing the initial population, the worm spread rate is increased. The increase is not as significant as might be expected because this is a low scanning worm (only one simultaneous connection).

Figure 4 shows the results of the TCP worm model and simulations after varying the radio range of the nodes, ranging from 100 meters to 500 meters. It is clear

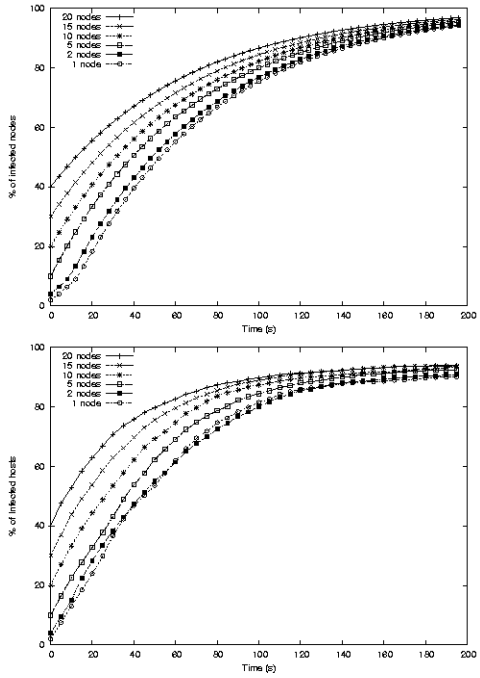

Figure 3. The TCP Model results (top) for various initial population size with simulation results (bottom).

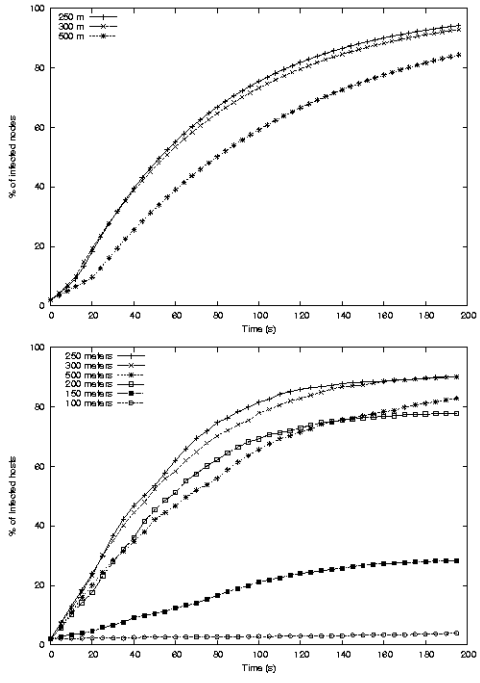

Figure 4. The TCP Model results (top) for various radio ranges with simulation results (bottom).

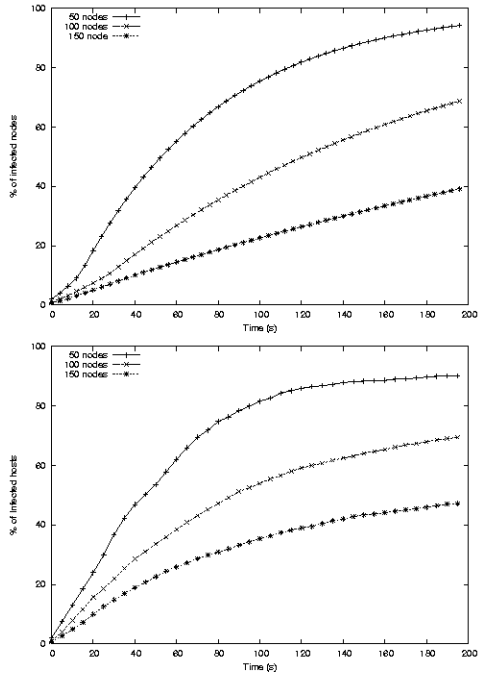

Figure 5. The TCP Model results (top) for various number of nodes with simulation results (bottom).

from the simulation results that for low radio ranges some of the nodes can not communicate with each other and therefore the final infection probability is very low. As the radio range increases to 250 meters the final infection probability improves, afterwords the increase in radio range has a negative effect on the worm spread due to more bandwidth competition between nodes. The TCP worm model captures the effect of bandwidth competition and packet discards for topologies where the network remains connected with a high probability. But the model breaks down at low radio ranges where connectivity begins to break down.

Figure 5 shows the results of the TCP worm model and simulations after varying the number of nodes (nodal density). The simulation results show the effect of increased contention with increasing nodal density, which results in an increase in the packet drop rate.

5 Conclusion

We have presented a study of TCP worm propagation in MANETs. We investigated the impact of payload size, channel bandwidth, initial infection probabilities, packet discards due to collisions in the wireless channel, radio range and routing protocols on the effectiveness of the worm propagation. Previous studies have proposed analytic models of UDP-based worm propagation in MANETs. Here, we develop an analytic model of

TCP-based worm propagation in MANETs. The model compares well to our simulation results. The model captures the effects of variable payload sizes (for large payloads), channel bandwidths, initial conditions, and radio range. The model does not include topological considerations and hence does not predict situations where the MANET becomes disconnected due to either low nodal densities or short radio ranges. This effect will be the topic of future investigations. The model relies on the fact that the wireless network exists in one of two states; a low load state where packet discards are rare and the TCP flows share channel bandwidth and a moderate to high load state where the nodal packet discard probability is flat with respect to increases in the number of flows. This effect was discovered by Fu, et al., [5], and is confirmed by our simulation results.

We believe that our studies will aid in the design of efficient counter measures for worm attacks in MANETs. All these factors need to be addressed when designing an efficient mitigation technique. Further studies of worm propagation and mitigation in the challenging networking environment afforded by MANETs is required. In future studies we hope to further quantify the behavior of TCP-based worms and to investigate the efficiency of specific worm mitigation technologies.

Acknowledgments

We would like to thank Z. Fu for his help in explaining the results in [5] and for other clarifying discussions.

References

[1] N. Bailey. *The Mathematical Theory of Infectious Diseases and it's Applications*. Hafner Press, New York, 1975.

[2] C.C.Zou, W.Gong, and D. Towsley. Code red worm propagation modeling and analysis. In *In Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 138–147, November 2002.

[3] R. G. Cole. Initial studies of worm propagation in manets. In *Army Science Conference (ASC)*, Orlando, FL, USA, 2004.

[4] R. G. Cole, N. Phamdo, M. A. Rajab, and A. Terzis. Requirements on worm mitigation technologies in manets. In *PADS '05: Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation*, pages 207–214, Washington, DC, USA, 2005. IEEE Computer Society.

[5] Z. Fu, P. Zerfos, H. Luo, S. Lu, L. Zhang, and M. Gerla. The impact of multihop wireless channel on tcp throughput and loss. In *IEEE Infocomm 2003*, August 2003.

[6] T. P. Ghosh, A.K. Defense against cyber attacks on mobile, ad hoc network systems (manets). In *BAA04-18 Proposer Information Pamphlet (PIP)*, Defense Advanced Research Projects Agency (DARPA) Advanced Technology Office (ATO), April 2004.

[7] G. Holland and N. Vaidya. Analysis of tcp performance over mobile ad hoc networks. In *Mobicom*, 1999.

[8] R. Lemos. Msblast epidemic far larger than believed. *CNET News.com*, April 2004.

[9] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver. Inside the slammer worm. *IEEE Magazine of Security and privacy*, 1(4):33–39, July/August 2003.

[10] D. Moore, C. Shannon, and J. Brown. Code-red: a case study on the spread and victims of an internet worm. In *Proceedings Internet Measurement Workshop (IMW)*, Marseille, France, November 2002.

[11] D. Moore, C. Shannon, G. M. Voelker, and S. Savage. Internet quarantine: Requirements for containing self-propagating code. In *Proceedings IEEE INFOCOM*, San Francisco, CA, USA, March 2003.

[12] S. Papanastasiou, M. Ould-Khaoua, and L. Mackenzie. On the evaluation of tcp in manets. In *Proceedings of the International Workshop on Wireless Ad Hoc Networks*, May 2005.

[13] D. D. perkins and H. D. Hughes. Tcp performance in mobile ad hoc networks. In *Proceedings of the Intl. Symp. on Perf. Eval. of Computer and telecommunications Systems*, July 2001.

[14] G. F. Riley. The Georgia Tech Network Simulator. In *Proceedings of the ACM SIGCOMM workshop on Models, methods and tools for reproducible network research*, pages 5–12. ACM Press, 2003.

[15] C. Shannon and D. Moore. The spread of the witty worm. Technical report, CAIDA, April 2004.

[16] M. I. Sharif, G. Riley, and W. Lee. Simulating internet worms. In *Proceedings of the Twelvth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'04)*, 2004.

[17] V. P. Stuart Staniford and N. Weaver. How to 0wn the internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, San Francisco, CA, USA, August 2002.

[18] J. Swartz. Cops take a bite, or maybe a nibble, out of cybercrime. *USA TODAY*, September 2003.

[19] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham. A taxonomy of computer worms. In *Proceedings of the 2003 ACM CCS workshop on Rapid Malcode (WORM'03)*, pages 11–18, Washington, DC, USA, 2003.