Correlation Model of Worm Propagation on Scale-Free Networks

Zoran Nikoloski[1], Narsingh Deo[2], Ludek Kucera[1]

October 1, 2005

[1] *Department of Applied Mathematics, Faculty of Physics and Mathematics, Charles University, Malostranske Nam. 25, 118 00 Praha 1, Czech Republic, e-mail: nikoloski@kam.mff.cuni.cz*

[2] *School of Computer Science, University of Central Florida, Orlando Fl, 32816, USA*

Abstract

The problem of network worms is worsening despite increasing efforts and expenditure on cyber security. Worm propagation is a random process that creates a complex system of interacting agents (worm copies) over the propagation medium—a scale-free graph, representing real-world networks. Understanding the propagation of network worms on scale-free graphs is the first step towards devising effective techniques for worm quarantining. After presenting the drawbacks of existing mean-field models, we develop a pair-approximation (correlation) model of worm propagation that employs the salient network characteristics—order, size, degree distribution, and *transitivity*. Inclusion of the transitivity shows significant improvement over existing pair-approximation models. The validity of the model is confirmed by comparing the numeric solution of the model to results from our individual-based simulation. Our model demonstrates that the network structure has considerable impact on the propagation dynamics when the worm uses local propagation strategies.

Keywords: propagation, network worm, scale-free graph, correlation model

1 Introduction

Network worms represent a serious threat to confidentiality, integrity, and availability of computer resources on the Internet. The existing automated network-security solutions (*e.g.*, anti-virus software, firewalls, and intrusion detection systems) and human-dependent counter measures (e.g., software patching, traffic blocking) have been deemed inadequate for timely detection and control of worm propagation [10, 42, 43]. Since the problem of network worms is worsening every year despite increasing efforts and expenditure on cyber-security [10],

devising techniques for controlling their propagation is of great practical importance [29]. An important first step in developing control strategies is (1) to understand the dynamics of worm propagation and (2) how worm propagation is affected by the network structure.

Cyber attacks employ *malicious mobile-code* (*MMC*)—a program designed to perform a malicious action by propagate copies of itself to computers, having a known vulnerability, on a network. MMCs can be classified into three broad categories based on the extent of human intervention required for their propagation [24], namely: autonomous, human-dependent, and hybrid. Furthermore, based on their actions, MMCs may be grouped into three classes: Trojan horses, computer viruses, and network worms. A *Trojan horse* is a program that is given (fraudulently) the same name as a legitimate piece of software, but, when executed, it performs a malicious act. A *computer virus* is an MMC that modifies resident programs to perform malicious actions on a single computer. Like Trojan horses, computer viruses require human intervention to propagate on a network.

A *network worm* is a stand-alone program that propagates autonomously by sending copies of itself to other computers on the network. A computer is considered *compromised* if it hosts a replica of the worm. A worm *propagates* by sending a copy of *autonomous MMC* (*AMMC*) to a host, having the exploited vulnerability detected through *scanning* and *probing*. Therefore, the worm propagation is a random process that generates a complex system of interacting agents (AMMCs) over the propagation medium—a scale-free network. A recent study [47] has shown that: (1) probing attempts are in the range from one to three millions per day, (2) sources and destinations of intrusion are uniformly distributed among *Autonomous Systems*, (3) scanning of ports other than 80 (HTTP), characteristic for Code Red and Nimda, constitute 40% to 80% of all intrusion attempts, and (4) while vertical and, in particular, horizontal scans are prevalent [37], other methods such as coordinated and stealthy scans are widely used.

The size of an AMMC is relatively small (less than a hundred KB), and the scan and probe pieces are negligibly small (a kilobyte and a dozen bytes, respectively) [35, 36, 41]. The code of Sapphire Worm, for example, consisted of only 376 bytes [25]. Thus, the only immediately observable effect of an attack on a network is an increase in the routing-related requests [11, 22], as the worm keeps probing different hosts. Due to the short time required for their propagation, worms can inflict considerable damage to the networks. For instance, CodeRed Worm [9] infected 150,000 computer systems in 14 hours. The damage inflicted by Nimda [8] to 86,000 computer systems, has been estimated to $13 billion [10]. On January 24, 2003, the Sapphire Worm, taking advantage of a known vulnerability in Microsoft's SQL Server 2000, spread across different networks, including Bank of America's network of 13,000 ATMs [25]. Since a malicious worm has the capacity for global impact on today's network-dependent society, developing models of propagation and control is a first step towards a comprehensive network-security solution.

An important question in modeling worm propagation on a scale-free net-

work is whether the population of computers (whose communication is captured by the network) is to be represented in groups based on average degree and risk of transmission or whether the computers and their communication are to be explicitly simulated. The latter level of detail provides a powerful tool as it allows the structure of the network to be included in the control techniques. Between the extremes of networks whose represented by a complete graph (see Section 3) and individual-based simulation on scale-free networks, it is possible to divide the population of computers into groups with similar characteristics—*e.g.*, degree (number of contacts)—and derive a set of equations describing the propagation dynamics. Thus, the contact structure can be captured by *stratifying* the modeled population.

Our contribution here is a mathematical model of worm propagation that makes use of information about network structure—order, size, degree distribution, and clustering coefficient (transitivity). We compare the results of the model with an individual-based simulation of worm propagation on scale-free graphs that model the Internet (obtained from the Oregon Route View project). We point out that, although the introduction of the Internet has arguably made the assumption of sparseness no longer valid, the idea of *locality* (especially in the case of analytical modeling of local propagation strategies) is still applicable, and, therefore, used in our model.

The paper is organized as follows: In Section 2, we discuss adequate models for the propagation medium—the Internet, and define two abstractions of the Internet topology: the Microscopic Internet graph and the Macroscopic Internet graph. In Section 3, we present a comprehensive survey of the existing models for worm propagation and control by (1) categorizing the models into seven classes and (2) identifying their advantages and disadvantages. Derivation of a pair-approximation SIS and SIR model for worm propagation on scale-free graphs is presented in Section 4. Finally, to test the accuracy of our approach, in Section 5 we present a comparative empirical study of our pair-approximation model, the mean-field model, and the model of propagation on Erdös-Renyi graphs versus the results of the individual-based simulation.

2 Adequate Model for the Propagation Medium

Due to the diversity of exploited vulnerabilities, network worms can propagate on various types of networks. A (physical) *network* is a collection of interconnected computers, each with its distinct IP address. Such a network can be represented by a connected, undirected graph $G = (V, E)$, with the nodes as computers and the edges as the (physical) communication links (*e.g.*, wire, optical cable). Since G is connected, communication between any arbitrary pair of nodes u and v, takes place through a u, v-path in G. Although graph G, just defined, represents a physical network, it may also represent a logical (or virtual) network. For example, in an *e-mail graph*, a node v would represent a user and the (directed) edges emanating from v would go to all the individuals in the e-mail *address book* of v. Likewise, in a *webgraph* each node u would rep-

resent a web page and each (directed) edge emanating from $u$would represent a hyperlink coming out of web page u.

Despite the differences in what they model, these graphs have the following similar characteristics: (1) degree distribution, (2) clustering coefficient, and (3) average distance. We note that a scale-free random graph model cannot be accepted as a valid representation of a real-world network if it satisfies only these three characteristics. To clarify these characteristics, we give the following definitions:

Definition 1: *The degree distribution gives the probability that a node, chosen uniformly at random, is of degree d.*

Empirical studies of real-world networks have demonstrated that the degree distribution falls in the class of so-called scale-free (power-law) probability distributions, such that $P(d(v) = d) = d^{-f}$ ($f$is the exponent of the power-law degree distribution).

Definition 2: *Given a graph $G = (V, E)$ and a node $v \in V$ of degree $d(v)$, the clustering coefficient C_v of node v is defined as the ratio between the total number of edges incident on all pairs of neighbors of v and the number of edges in a clique formed by the neighbors of v.*

The *clustering coefficient* of G is the average of clustering coefficients over all nodes. The clustering coefficient of G has values in the range $0 \leq C \leq 1$. There is yet another measure of clustering in graphs, called *transitivity* [28].

Definition 3: *Transitivity is the ratio between the number of triangles and the total number of paths of length three.*

Definition 4: *Average distance of G is the mean over all shortest distances between any connected nodes.*

The Internet can be modeled on two levels: microscopic and macroscopic. In the *Microscopic Internet graph*, nodes stand for routers and hosts, while edges represent communication links. The *Macroscopic Internet graph* can be thought of as a contraction of the Microscopic Internet graph: here, each node represents an Autonomous System (which incorporates a number of routers). To simplify the analysis, parallel edges and loops (having negligible influence in modeling propagation) will be deleted from the *Macroscopic Internet graph.* Two nodes in the *Macroscopic Internet graph* are adjacent if there is at least one pair of routers (belonging to different Autonomous Systems) that can communicate. Note that both, the Microscopic and the Macroscopic Internet graphs are undirected. Faloutsos *et al.* [14] studied both graphs, and concluded that the degree distribution follows a power-law. In the Microscopic Internet graph, the exponent of the power-law f had a value of 2.48, while in the Macroscopic Internet graph, the exponent ranged between $f = 2.15$ and $f = 2.2$ (studies were

performed between 1997 and the end of 1998). Govindan and Tangmunarunkit [15] mapped the connectivity of nearly 150,000 router interfaces, confirming the power-law exponent of $f = 2.3$. The studies of Yook *et al.* [48] conducted between 1997 and 1999 showed that the Macroscopic Internet graph has a clustering coefficient in the range from 0.18 to 0.3 and an average distance between 3.70 and 3.77.

3 Existing Models of Worm Propagation

Due to the strong analogy between network worms and infectious diseases, epidemiological models have been widely used in modeling worm's propagation. Since a worm propagates along the edges of a network, we will use graph-theoretic terms to describe the existing epidemiological models of propagation. Epidemiological models are based on two simplifications [16]: (1) At any given time t, each node can be in one of a finite number of states, *e.g.* susceptible, quarantined-susceptible, removed-susceptible, infectious, quarantined-infectious, removed-infectious, and detected. The choice of which states to include in a model depends on the characteristics of the particular worm being analyzed and the purpose of the model; and (2) Translation of the worm transmission mechanism into a probability that a node will infect another node. In a similar way, transitions between other states of the model are described by simple probabilities. Epidemiological models can be analyzed analytically or by means of simulation.

The propagation takes place on a graph G with n nodes and m edges. Let $S(t)$ denote the number of susceptible nodes at time t, $Q_s(t)$ be the number of quarantined-susceptible nodes, $R_s(t)$ be the number of removed-susceptible nodes, $I(t)$ be the number of infectious nodes, $Q(t)$ be the number of quarantined-infectious, and $R(t)$ denote the number of removed nodes. The fraction of nodes in a particular state is represented by the lower case letter. Let β denote the rate at which susceptible nodes are infected. Most models of propagation assume β is constant, averaging out the differences in processor speed, network bandwidth, and location of the infectious node. The existing models also assume that a node cannot be infected multiple times.

Susceptible-Infectious (SI) model: In this class of models, once a susceptible node becomes infectious, it does not change its state. These models can be used in the study of the *worst-case propagation*, when automated and human counter-measures are not available. Let the average degree of an infectious node be $\overline{d}$, and the fraction of infectious nodes at time t be $i(t)$. The expected number of susceptible neighbors that can be infected by a given infectious node is $\overline{d}(1 - i(t))$. Since there are $I(t)$ infectious nodes, the total rate of newly-infected nodes is $\beta\overline{d}(1 - i(t))\, i(t)$. The general SI model is described by the differential equation (1):

$$\frac{di(t)}{dt} = \beta\overline{d}(1 - i(t))\, i(t), \tag{1}$$

with boundary conditions: $i(0) = \dfrac{I(0)}{n} > 0$ and for all $t \geq 0$, $i(t) + s(t) = 1$. The solution of equation (1) for the fraction of infectious nodes is the *logistic curve*: $i(t) = \dfrac{i(0)\ e^{\beta' t}}{1 - i(0) + i(0)\ e^{\beta' t}}$, where $\beta' = \beta \overline{d}$. The *S-shaped curve* describing the fraction of infectious nodes has three regions: (1) *slow start*, when only few nodes are infected at every time step, (2) *exponential growth*, when the number of newly-infected nodes grows exponentially, and (3) *equilibrium state*, when the number of infectious nodes assumes some value around which it fluctuates steadily.

If the worm propagates on the complete graph on n nodes, K_n, where $\overline{d} = (n-1)$, the model (1) can asymptotically be written as:

$$\frac{di(t)}{dt} = \beta (1 - i(t)) I(t), \tag{2}$$

with boundary conditions: $i(0) = \dfrac{I(0)}{n} > 0$ and for all $t \geq 0$, $i(t) + s(t) = 1$. One then has that $i(t) = \dfrac{i(0)\ e^{\beta (n-1) t}}{1 - i(0) + i(0)\ e^{\beta (n-1) t}}$. Staniford *et al.* [35] applied model (2) to fit the data collected by the Chemical Abstracts Services from the propagation of CodeRed I Worm, and estimated the product $\beta (n-1)$ for Code Red I to be 1.8. However, they used the number of scanned nodes, which is much larger than the number of infectious nodes, thus, leading to erroneous conclusions. Weaver [41] and Wagner *et al.* [38] used this model to study four local propagation strategies: hit-list, topological, permutation, and local-subnet, although we must note that the complete graph as underlying topology is inappropriate for studying such local strategies.

Zou *et al.* [50] used a modification of model (2) to analyze a *trend-detection* mechanism based on the traffic-anomaly created by worms. The detection system is composed of distributed ingress and egress sensors for worm activity. When the monitoring system receives a surge of illegitimate scans, a Kalman filter is activated to estimate the parameter β. Since in the early stage the propagation exhibits exponential growth with constant, positive rate, the model can be described as $I(t) = (1 + \beta n\, dt)\ I(t-1)$. The authors derived a bias-correction formula for estimation of the number of infectious nodes at time t, $I(t)$, from the number of observed infectious nodes $Z(t)$: Let σ be the average number of scans sent by an infectious node. After time interval dt, the expected number of scans observed by u monitors is $\beta u I(t) \sigma dt / 2^{32}$ (assuming the Internet is a complete graph), while the probability that any of the $I(t) - Z(t-1)$ infectious nodes are observed is $1 - \left(1 - u/2^{32}\right)^{\sigma dt}$. When the estimate of β starts oscillating around a positive constant value, the worm has been detected. Yet, it is not evident how the topology might affect Zou *et al.*'s detection mechanism.

In Erdös-Renyi random graphs with edge-density p, the expected degree of

a node is $p\,(n-1)$. The propagation on these graphs can be described as:

$$\frac{di\,(t)}{dt} = \beta p\,(n-1)\,(1-i\,(t))\,i\,(t)\,, \tag{3}$$

with solution: $i\,(t) = \dfrac{i\,(0)\ e^{\beta\,p(n-1)t}}{1-i\,(0)+i\,(0)\ e^{\beta p\,(n-1)t}}$.

Susceptible-Infectious-Susceptible (SIS) model: In this class of models, an infectious node recovers at some rate, and thus it becomes susceptible again. These models can be used in the study of worm's propagation when some computers are temporarily turned off but are not patched (*e.g.*, the case of Code Red I worm). Let the average degree of an infected node be $\overline{d}$, and the rate at which an infectious node recovers be γ. The rate of newly-infected nodes is proportional to the expected fraction of susceptible neighbors, the number of infected nodes, and the probability β. The rate at which infectious nodes recover is proportional to the number of infectious nodes and rate γ. The system of differential equations (4) describes the general SIS model:

$$\frac{di\,(t)}{dt} = \beta\overline{d}\,(1-i\,(t))\,i\,(t) - \gamma i\,(t) \tag{4}$$

with boundary conditions $i\,(0) = \dfrac{I\,(0)}{n}$, and for all $t \geq 0$, $i\,(t) + s\,(t) = 1$. From equation (4), $\dfrac{di\,(t)}{dt} < 0$ if and only if $s\,(t) < \dfrac{\gamma}{\beta\overline{d}} = \delta$. Thus, the worm "dies out" if the initial fraction of susceptible nodes is below the *epidemic threshold* $\dfrac{\gamma}{\beta\,\overline{d}}$. The solution of (4) gives a functional form for the fraction of infectious nodes: $i\,(t) = \dfrac{(1-\delta)\,i\,(0)}{i\,(0)+(1-\delta-i\,(0))\ e^{-\,(\beta'-\gamma)t}}$, where $\beta' = \beta\overline{d}$. If the worm propagates on the complete graph on n nodes, K_n, where $\overline{d} = (n-1)$, the model (4) can asymptotically be written as [34]:

$$\frac{di\,(t)}{dt} = \beta\,(1-i\,(t))\,I\,(t) - \gamma i\,(t)\,, \tag{5}$$

with solution $i\,(t) = \dfrac{(1-\delta)\,i\,(0)}{i\,(0)+(1-\delta-i\,(0))\ e^{-\,(\beta(n-1)-\gamma)t}}$.

Solomon [34] studied a modification of model (5) where the rate γ is a weighted average of the rate γ_1 (for computers not running anti-virus software), applicable to the fraction of infectious nodes, and the rate γ_2 (for computers running the most recent version of anti-virus software), applicable to the fraction of susceptible nodes, *i.e.*, $\gamma = \gamma_1 i\,(t) + \gamma_2\,(1-i\,(t))$. With this modification Solomon found that the necessary effectiveness of the anti-virus software (described by the rate γ) should be 0.5 in order to stop the propagation before it achieves exponential growth.

Kephart *et al.* [18, 19] employed model (4) to study the effects of three topologies on the propagation of *viruses*: Erdös-Renyi random graphs, regular

lattices of degree eight, and hierarchical random graphs. For the Erdös-Renyi random graphs with $\overline{d} \geq 5$, simulation results coincide with the predictions of the model. The simulation study of propagation on 100-by-100 lattice demonstrates quadratic growth, in contrast with the exponential growth characteristics for the complete graph and Erdös-Renyi graphs. The hierarchically-clustered random graphs in this study are generated as follows: given a rooted tree of height h, in which every node has a degree $(d+1)$ (*i.e.*, it has d successors), the nodes of the graph are the leaves of the tree. Two nodes, u and v, are made adjacent with probability $P(h(w))$ proportional to the height of node w—the first common ancestor of nodes u and v. In his simulation, Kephart used $P(h(w)) = \alpha p^{h(w)}$, where parameter p is used to control the degree of localization (when p tends to 0, the graph is composed of isolated nodes, while when p approaches 1, the topology of the hierarchically-clustered random graph is asymptotically that of the Erdös-Renyi random graphs). Here, the propagation shows sub-exponential growth. Further simulation studies conducted by Kephart [19] shows that sparsely-connected (random) graphs inhibit the propagation.

Previous models are limited in their accuracy due to their simplistic treatment of timing factors, such as *infection delay*—the length of time between the instant of worm's arrival at a node and the instant when this node becomes infectious to its neighbors. Model (4) could be altered to incorporate the infectious delay, as follows [40]:

$$\frac{di(t)}{dt} = \beta \overline{d} e^{-\gamma \varepsilon} (1 - i(t)) i(t - \varepsilon) - \gamma i(t), \tag{6}$$

where $i(t-\varepsilon) = 0$ for $t < \varepsilon$. At time $t \geq \varepsilon$, the fraction of infectious nodes is the same as the fraction of infectious nodes at time $(t-\varepsilon)$, since all nodes infected between $(t-\varepsilon)$ and t are delayed. The term $e^{-\gamma\varepsilon}$ accounts for the transfer of a node from infectious to susceptible state during the delay period. Equation (6) belongs to the class of non-linear delayed differential equations, which can be solved under the assumption $i(t-\varepsilon) = i(t)$. Wang *et al.* [40] support their analytical solution with simulation similar to that of *Kephart et al.* [18], and show that the epidemic threshold depends not only on the average degree, but also on the infection delay. In addition, Kim *et al.* [20] performed a simulation study of the propagation on a subgraph of the Internet, using a constant delay equal to the average round-trip time obtained from real-life traffic.

Pastor-Satorras *et al.* [30] modified model (4) to study the effects of the scale-free Barabasi-Albert topology on the propagation with rate of recovery $\gamma = 1$. Since a scale-free degree distribution is not concentrated around its mean value, the model must include differential equation for every group of nodes of degree k:

$$\frac{di_k(t)}{dt} = \beta k (1 - i_k(t)) \Theta\left(\{i_k(t)\}_{d_{\min}}^{d_{\max}}\right) - i_k(t), \tag{7}$$

where $\Theta\left(\{i_k(t)\}_{k=d_{\min}}^{d_{\max}}\right)$ describes the probability that a susceptible node of

degree k is adjacent to an infectious node. For a scale-free network, the probability that an edge is incident on a node of degree k is $kP(k)/\overline{d}$. The average probability that an edge is incident on an infectious node is then $\Theta(t) = \frac{1}{\overline{d}} \sum_{k=d_{\min}}^{d_{\max}} kP(k)\, i_k(t)$. The conclusion of this model is that scale-free topologies do not have epidemic-threshold. The authors also argued that the cut-off in the scale-free distribution forces a non-zero epidemic threshold. We point out that the result of this study is limited to scale-free topologies without degree-correlations. Contrary to this result, the simulation study of Eguiluz *et al.* [13] demonstrates that in the so-called *structured scale-free networks*, where adjacent nodes share large number of common neighbors, there exists a non-zero threshold even in the limit of large n.

While the results of the presented studies are valuable, a model, where nodes that have recovered and are no longer susceptible, could better approximate the realistic propagation of a worm when human counter-measures are in place.

Susceptible-Infectious-Removed (SIR) model and its variations: In this class of models, an infectious node can be removed (*i.e.*, it can no longer spread the worm). This model can be used to study the effects of software patching and traffic blocking. At any time t, a node can be susceptible, infectious, or removed. Let γ be the rate at which infectious nodes are removed. Using analogous arguments as in the previous section, the general SIR model can be written as:

$$\begin{aligned} \frac{di(t)}{dt} &= \beta\overline{d}\,(1 - i(t))\, i(t) - \gamma i(t), \\ \frac{dr(t)}{dt} &= \gamma i(t), \end{aligned} \tag{8}$$

with boundary conditions: $i(0) = \frac{I(0)}{n} \geq 0$, $r(0) = \frac{R(0)}{n} \geq 0$, and for all $t \geq 0$, $i(t) + s(t) + r(t) = 1$. The epidemic threshold for SIR models is analogous to the one in SIS models. Zou *et al.* [49] used a modification of the system (8) to determine the effect of human counter-measures (on removing both susceptible and infectious nodes) and the decreasing rate $\beta(t)$. This so-called *two-factor* model assumes complete graph as underlying topology, and a constant fraction of the removed-infectious nodes at any time t:

$$\begin{aligned} \frac{di(t)}{dt} &= \beta(t)\,(1 - r(t) - r_s(t) - i(t))\, i(t) - \frac{dr(t)}{dt}, \\ \frac{dr(t)}{dt} &= \gamma i(t), \\ \frac{dr_s(t)}{dt} &= \mu\,(1 - r(t) - r_s(t) - i(t))\,(r(t) + i(t)), \\ \beta(t) &= \beta(0)\,(1 - i(t))^{\eta}. \end{aligned} \tag{9}$$

It is unclear, however, how the parameters have been chosen in order to fit the data from the Code Red I worm propagation.

Boguna *et al.* [5] studied the SIR model, with the probability $\gamma = 1$, on scale-free topologies. Using the notation introduced in previous sub-section, the

model can be formulated as follows:

$$\begin{aligned} \frac{di_k(t)}{dt} &= \beta k\left(1-i_k(t)\right)\Theta\left(\left\{i_k(t)\right\}_{d_{\min}}^{d_{\max}}\right)-i_k(t), \\ \frac{dr_k(t)}{dt} &= \gamma i_k(t), \end{aligned} \tag{10}$$

which can be solved if one assumes that $i(0)$ is very small in the beginning of the propagation. Pastor-Satorras *et al.* [30] conducted a simulation study to investigate the effects of node-immunization (*i.e.* node-removal) on the propagation, before the worm is introduced in the network. They demonstrated that random immunization is inefficient in slowing down the propagation; however, immunization targeted at nodes of highest degrees can significantly inhibit the growth of propagation. While the latter result seems interesting, the authors argue that detecting nodes of high degrees in scale-free networks is a difficult problem.

Similarly, the simulation study of Wang *et al.* [39] examines the effects of immunization of nodes on the propagation on two topologies: rooted trees and clustered networks (composed of cliques inter-connected with small number of edges). The simulation's parameter is the *propagation fan out*—number of nodes to which the worm can send replicas at each time step. The time needed for the worm to propagate from one node to another is assumed to be one time tick. The first set of simulation is conducted on networks where no immunized nodes exist to determine the number of times a node is re-infected (called *re-infection count*). Two types of immunization are simulated—random and selective. Random immunization performs better on rooted trees as there is only one path between any two nodes; thus, it is possible to cut off an entire sub-tree of the network, which is not the case with the clustered network. For the case selective immunization in rooted trees, nodes with highest re-infection counts were chosen (note, these nodes coincide with nodes with largest degrees). In the case of clustered networks, two strategies are used: first based on the re-infection count, and second on the weighted sum of the inter-cluster and inner-cluster degrees for every node. The first strategy was able to contain the propagation, but results in a higher propagation rate. The second could slow down the propagation rate, but was unable to contain the propagation.

The principal disadvantage of the studies in [39] and [30] is that immunization is static, *i.e.*, a fraction of nodes is immunized before the worm starts propagating. In reality, the counter-measures should be dynamic in nature to play important role in slowing down the propagation of the worm.

Susceptible-Infectious-Detected-Removed (SIDR) model: This model was analyzed by Williamson *et al.* [45] in order to determine the effectiveness of the behavior-blocking approach called virus throttling [44]. Virus-throttling is an automatic mechanism for slowing a worm's propagation. Here, a node can be in one of the four states: susceptible, infectious, detected (in which the virus has been detected and cannot actively spread further), and removed. The model assumes complete graph as underlying topology. The model involves two stages: in the first stage, prior to the release of the virus signature, nodes progress from

susceptible to infectious state at some rate β. In the second stage, after some time from the start of the propagation, the virus is detected at some rate γ. Two quantities are studied: the number of infectious nodes and the duration of propagation. The model incorporates virus throttling by dividing the nodes into two groups—throttled and un-throttled. If a throttled node is infected, it does not spread the virus, and immediately enters the detected state. The result of this study show that when more than half of the nodes have throttles, even a late signature will result in a small outbreak.

Susceptible-Infectious-Removed-Susceptible (SIRS) model: Wang *et al.* [40] used a modification of SIS model (4) to study the node's vigilance against infection: Once an infectious node is removed, it remains in this state for a length of time ν, called *vigilance period*, after which the removed node becomes susceptible again. Here, the susceptibility of a node is modeled via a parameter ϕ that takes values between 0 (indicating complete susceptibility) and 1 (indicating immunity). The model is described by the non-linear delay differential equation (11):

$$\frac{di\left(t\right)}{dt}=\beta\overline{d}\left(1-i\left(t\right)-\int_{t-\nu}^{t}i\left(t\right)\right)i\left(t\right)-\gamma i\left(t\right) \tag{11}$$

whose solution shows that the number of infectious nodes decreases as the vigilance period increases. It is worth noting the node's vigilance has no impact on the epidemic threshold.

Compartmental epidemiological models: Compartmental epidemiological models are used with stratified population. The topology in this models is the Macroscopic Internet graph, where every node represents a dense region—Autonomous System (AS). These models can be used to study intra-AS propagation, with the assumption that within an AS (with n_j nodes) the worm propagates as on a complete graph K_{n_j}. The infectious attempts can then be modeled as being external or internal to an AS. If the macroscopic Internet graph has k nodes, the SI compartmental model can be written as:

$$\frac{di_j\left(t\right)}{dt}=\left[\sum_{l=1}^{k}\beta\,\frac{n_l}{N}i_l\left(t\right)\right]\left(1-i_j\left(t\right)\right), \tag{12}$$

where $1\leq j\leq k$. Here, the parameter N denotes the total number of IP addresses. Serazzi *et al.* [33] used model (12) to derive equations for the bandwidth consumption at each node. For the SIR compartmental model, Liljenstam *et al.* [23] obtained:

$$\begin{aligned}\frac{di_j\left(t\right)}{dt}&=\left[\sum_{l=1}^{k}\beta\,\frac{n_l}{N}i_l\left(t\right)\right]\left(1-i_j\left(t\right)\right)-\gamma i_j,\\ \frac{dr_j\left(t\right)}{dt}&=\gamma i_j\left(t\right),\end{aligned} \tag{13}$$

where, again, $1\leq j\leq k$. Liljenstam *et al.* [23] used model (13) to study the destabilizing effects of worm propagation on the network infrastructure,

since the compartmental approach allows for inclusion of limited details about communication protocols. In this simulation study, the scan traffic is modeled by using a combination of the average scan rate, individual infection rates, and size of address space for each AS.

Discrete-time approximation models: Chen *et al.* [6] developed a deterministic approximation model of propagation on a complete graph K_n. If σ is the average scanning rate, with the assumption that the total number of nodes is 2^{32}, the average number of newly-infected nodes at step $(t+1)$ is $(S(t) - I(t)) \left[1 - \left(1 - 1/2^{32}\right)^{\sigma I(t)}\right]$. If the probability of removal is γ, in the next time step $\gamma I(t)$ nodes will become susceptible. Thus, the propagation can be described by a system of recurrences for the number of infectious and susceptible nodes.

4 Pair-approximation model on Scale-Free Networks

The existing epidemiological models on scale-free graphs [30, 49] do not explicitly give the system of differential equations for the propagation dynamics. The comparative studies include either simulation of worm's propagation on a macroscopic level or a system of differential equation for propagation on Erdös-Renyi and regular graphs. Thus, in all models described in Section 3, it is not evident how a realistic, scale-free network structure might affect the worm propagation.

Worm propagation is a random process that takes place on networks, such as: the Internet, World Wide Web, e-mail network, modeled as large scale-free random graphs. Using the salient features of the underlying scale-free graphs, here, we develop a realistic model of worm's propagation and techniques for dynamic quarantining. Cast in the SI framework, our model can be used to study the worst-case propagation and determine the optimal time for undertaking preventive action. On the other hand, cast in the SIR framework, this model can be used in the study of quarantining techniques against network worms.

Our model of worm's propagation belongs to the class of *pair-approximation network models*. The benefit of this class of models is that it can incorporate the spatial structure that the existing epidemiological models of propagation ignore. A survey of pair-approximation models is given by Rand [32]. In the pair-approximation model, the variables are the fractions of pairs of nodes in certain states. Usually, these equations contain higher-order correlations (*e.g.*, triples of nodes in certain states) which are approximated by the lower-order correlations. For the most part, previous work on pair-approximation models describes processes on regular-lattices. Our model extends the work by Earnes and Keeling [12] (for triangle-free networks) and Bauch [2] (for dynamic partnerships), and makes pair-approximation applicable to various scale-free topologies.

Next, we present the derivation of the system of differential equations describing the propagation in the SIS framework. Let $N(u)$ be the neighborhood of a node u, $p_t(i_u)$ the probability that, at time t, node u is infectious, and let

$p_t(s_u, i_v)$ be the joint probability that two adjacent nodes u and v are susceptible and infectious, respectively. The time evolution of the state of a single node in the SIS epidemic process can be written in the following form:

$$\begin{aligned} &\frac{dp_t(i_u)}{dt} = \beta \sum_{v \in N(u)} p_t(s_u, i_v) - \gamma p_t(i_u), \\ &p_t(s_u) + p_t(i_u) = 1. \end{aligned} \tag{14}$$

One can also develop an equation for the time evolution of $p_t(s_u, i_v)$ which in turn involves higher-order correlations. To solve this problem, we resort to some approximation scheme: For instance, the SIS epidemiological model assumes that $p_t(s_u, i_v) = p_t(s_u)\, p_t(i_v)$, and thus neglects correlation between states of nodes. In our approach, $p_t(i_u)$ and $p_t(s_u, i_v)$ are kept as variables of interests while the higher-order correlations are expressed, via some appropriate approximation, in terms of these quantities. The time evolution of $p_t(s_u, i_v)$ can be derived by using the Kolmogorov forward equation:

$$\begin{aligned} \frac{dp_t(s_u, i_v)}{dt} = &-(\beta + \gamma)\, p_t(s_u, i_v) - \beta \sum_{w \in N(u) - v} p_t(i_w, s_u, i_v) \\ &+\beta \sum_{w \in N(v) - u} p_t(s_u, s_v, i_w) + \gamma p_t(i_u, i_v). \end{aligned} \tag{15}$$

Let Λ_a be the set of integers, representing the degrees of the neighbors for all nodes of degree a, and $[ab]$ be the number of edges incident on nodes of degrees a and b. Furthermore, let X, Y, and Z represent a state of a node (*e.g.*, susceptible and infectious).

Given a node u of degree a and a node v of degree b, define

$P_t(X_a, Y) = \frac{1}{a} \sum_{d(u)=a, d(v) \in \Lambda_a} P_t(x_u, y_v)$, and

$P_t(X_a, Y_b, Z) = \frac{1}{[ab]} \sum_{d(u)=a, d(v)=b, d(w) \in \Lambda_b} P_t(x_u, y_v, z_w)$.

Remark:

$P_t(X_a, Y) = \sum_{k \in \Lambda_a} P_t(X_a, Y_k)$ and $P_t(X_a, Y_b, Z) = \sum_{k \in \Lambda_b} P_t(X_a, Y_b, Z_k)$.

Let $E[X_a]$ denote the number of nodes of degree a in state X, $E[X_a Y_b]$ the number of pairs of nodes of degree a, in state X, adjacent to nodes of degree b, in state Y, and $E[X_a Y_b Z_c]$ denote the number of triples where a node of degree b, in state Y, is adjacent to a node of degree a and a node of degree c, in state X and Z, respectively. By multiplying equation (14) by n_a, the number of nodes of degree a in the graph G, one can obtain the following equation:

$$\frac{dE[I_a]}{dt} = \beta \sum_{k \in \Lambda_a} E[S_a I_k] - \gamma E[I_a], \tag{16}$$

where $E[S_a] + E[S_b] = n_a$. Similarly, one can transform equation (15) to obtain:

$$\frac{dE[S_a I_b]}{dt} = -(\beta + \gamma)\, E[S_a I_b] - \beta \sum_{k \in \Lambda_a} E[I_k S_a I_b] + \beta \sum_{k \in \Lambda_b} E[S_a S_b I_k] + \gamma E[I_a I_b]. \tag{17}$$

Let φ_{abc} denote the transitivity among nodes of degree a, b, and c, *i.e.*, the ratio of the number of 3-cycles to the number of connected triples whose nodes are of degree a, b, and c. To approximate the third moment $E[X_aY_bZ_c]$, one can use the definition of multiplicative moments of two variables [17, 32] and the transitivity φ_{abc}, to find:

$$E[X_aY_bZ_c] = \frac{b-1}{b}\frac{E[X_aY_b]\,E[Y_bZ_c]}{E[Y_b]}\left((1-\varphi_{abc}) + \varphi_{abc}\frac{n^2}{2m}\frac{E[X_aZ_c]}{E[X_a]\,E[Z_c]}\right). \tag{18}$$

Similarly, one can derive formulae for the other second moments and appropriate approximation of the third moments to obtain the following pair-approximation for the SIS framework:

$$\begin{aligned}
&\frac{dE[I_a]}{dt} = \beta \sum_{k\in\Lambda_a} E[S_aI_k] - \gamma E[I_a],\\
&\frac{dE[S_a]}{dt} = \gamma E[I_a] - \beta \sum_{k\in\Lambda_a} E[S_aI_k],\\
&\frac{dE[S_aS_b]}{dt} = -\beta\left(\sum_{k\in\Lambda_a} E[I_kS_aS_b] + \sum_{k\in\Lambda_b} E[S_aS_bI_k]\right) + \gamma\left(E[S_aI_b] + E[I_aS_b]\right)\\
&\frac{dE[S_aI_b]}{dt} = -(\beta+\gamma)E[S_aI_b] - \beta\left(\sum_{k\in\Lambda_a} E[I_kS_aI_b] - \sum_{k\in\Lambda_b} E[S_aS_bI_k]\right)\\
&+\gamma E[I_aI_b],\\
&\frac{dE[I_aI_b]}{dt} = \beta\left(E[S_aI_b] + E[I_aS_b] + \sum_{k\in\Lambda_a} E[I_kS_aI_b] + \sum_{k\in\Lambda_b} E[I_aS_bI_k]\right)\\
&-2\gamma E[I_aI_b].
\end{aligned} \tag{19}$$

Now, the system of differential equations (19) can be numerically solved by using the approximation given in equation (18). Note that our model differs from the one presented in [2] and [12] since we take into consideration the transitivity φ_{abc}, which turns out to have a significant effect on the outcome of the model (see Section 5).

Model (19) can be altered to obtain the system of differential equations (20),

describing the dynamics of propagation in the SIR framework:

$$
\begin{aligned}
&\frac{dE\left[I_a\right]}{dt} = \beta \sum_{k\in\Lambda_a} E\left[S_a I_k\right] - \gamma E\left[I_a\right], \\
&\frac{dE\left[S_a\right]}{dt} = -\beta \sum_{k\,\in\,\Lambda_a} E\left[S_a I_k\right], \\
&\frac{dE\left[R_a\right]}{dt} = \gamma E\left[I_a\right], \\
&\frac{dE\left[S_a S_b\right]}{dt} = -\beta \left(\sum_{k\in\Lambda_a} E\left[I_k S_a S_b\right] + \sum_{k\,\in\,\Lambda_b} E\left[S_a S_b I_k\right] \right), \\
&\frac{dE\left[S_a I_b\right]}{dt} = -\left(\beta+\gamma\right) E\left[S_a I_b\right] - \beta \left(\sum_{k\in\Lambda_a} E\left[I_k S_a I_b\right] - \sum_{k\,\in\,\Lambda_b} E\left[S_a S_b I_k\right] \right), \\
&\frac{dE\left[S_a R_b\right]}{dt} = -\beta \sum_{k\in\Lambda_a} E\left[I_k S_a R_b\right] + \gamma E\left[S_a I_b\right], \\
&\frac{dE\left[I_a I_b\right]}{dt} = \beta \left(E\left[S_a I_b\right] + E\left[I_a S_b\right] + \sum_{k\in\Lambda_a} E\left[I_k S_a I_b\right] + \sum_{k\in\Lambda_b} E\left[I_a S_b I_k\right] \right) \\
&-2\gamma E\left[I_a I_b\right], \\
&\frac{dE\left[I_a R_b\right]}{dt} = \beta \sum_{k\in\Lambda_a} E\left[I_k S_a R_b\right] + \gamma \left(E\left[I_a I_b\right] - E\left[I_a R_b\right] \right).
\end{aligned}
\tag{20}
$$

5 Pair-approximation Model vs. Individual-based Simulation

Our goal is to test the accuracy of the pair-approximation model (19) in comparison to: (1) the individual-based simulation of the worm propagation on a Macroscopic Internet graph (on n nodes and average degree $\overline{d}$), and (2) the standard SIS model (which ignores correlation) on two topologies: the complete graph on n nodes (model (5)) and the Erdös-Renyi graph on n nodes with average degree $\overline{d}$ (model (4)).

The empirical study is conducted on Macroscopic Internet graphs. To obtain the Macroscopic Internet graphs, we used the data for inter-connectedness of the Internet on the Autonomous System level collected by the University of Oregon Route View Project and made available by NLANR (National Laboratory of Applied Network Research). We considered snapshots of the Internet of various order and size, shown in Figure 1. The pre-processing step consists of determining parameters for model (19): for given degrees a, b, and c, the number of adjacent nodes of degree a and b, the set Λ_a, and the transitivity φ_{abc} are determined.

Next, we developed an individual-based simulation of the stochastic propagation process on a Macroscopic Internet graph. The individual-based simulation has two advantages: First, the propagation process and the underlying topology can be controlled to simulate different scenarios. Second, this simulation

Date	Order	Size
08.11.1997	3015	5156
02.04.1998	3522	6324
03.07.1998	3797	6936
02.10.1998	4180	7768
14.01.1999	4517	8376
02.04.1999	4885	9276
02.07.1999	5357	10328
02.10.1999	5861	11313
02.01.2000	6474	12572
03.04.2000	7246	14629
02.07.2000	7956	15943
02.10.2000	8836	17823
02.01.2001	9048	18172
16.03.2001	10515	21455

Figure 1: Macroscopic Internet graphs used in simulations

provides very precise and detailed information about the propagation dynamics without any biases which might be present in real data. The individual-based simulation combines Monte Carlo simulation of events, taking place at given rates, with an event-scheduler that determines the order in which events happen in the system. The scheduler is implemented as a priority queue. The system is composed of nodes that can be either susceptible or infectious. There are two types of events that can take place: infection and curing. If a node u is infectious, it attempts infection of each of its neighbors at rate β. Node u might be cured, and, thus, become susceptible, at rate γ. Let as assume that u has been cured at time t, and has been re-infected at time $t + dt$. Any infection generated by the node u in the time interval $[t, t + dt)$ can be discarded by the scheduler. The event of u attempting infection of an already infectious neighbor v at time t is also discarded by the scheduler.

We simulated worm propagation in the Susceptible-Infectious framework in order to determine the time the worm takes to infect all nodes of a given graph G. Simulations were performed on ten Macroscopic Internet graphs (the results for four graphs, identified by the top entry in the left-most column appear in Figure 2). To determine how choice of the initial node influences the propagation, we first determined the labels of three nodes with smallest degrees and three nodes with highest degree, shown in the first and second column of each table in Figure 2. The rest of the entries show the average time over 100 simulations for the worm to propagate on all nodes by starting from a pre-specified initial node and spreading with infectious rate β. The general results of the experiments can be summarized as follows:

1. *The time to propagate to all nodes decreases with the increase of the degree of the initial node.*
   As an infectious node of higher degree has bigger pool of susceptible nodes, it gives the worm the possibility to establish a considerable fraction of infectious nodes in the early stages of the propagation. On average, the

propagation to all nodes of G initiated from a node of maximum degree takes time by 5% shorter compared to the propagation that starts from a node of minimum degree.

2. *The time to propagate to all nodes increases with the increase of the order of the graph.*
   Given two graphs G_1 and G_2, $|V(G_1)| < |V(G_2)|$, whose degree distributions follow the same scale-free distribution, have diameters $D(G_1)$ and $D(G_2)$, respectively, such that $D(G_1) < D(G_2)$. Therefore, on a graph with greater diameter the worm takes longer time to infect all nodes.

3. *The time to propagate to all nodes does not strictly decreases with the increase of the infectious rate β.*
   In other words, there is a value of the infectious rate β at which the function $t(\beta)$ has a local minimum, as shown in Figure 3. According to the simulation results shown in Figure 2, the value of $\beta = 1.5$ seems to be invariant and depends only on the exponent of the scale-free degree distribution of the graph G. The reason for such behavior is that, at the local minimum, rapidly-building correlations between the states of adjacent nodes hinder the propagation by lowering the number of available susceptible nodes. This observation is of *particular interest* as it provide the means to "control" the propagation of a fast-spreading worm by reducing its rate to the threshold value.

Figures 4 and 5 below, show the number of infectious nodes as a function of time, comparing the three deterministic models with two results of the stochastic individual-based simulation. Neither the mean-field model nor the Erdös-Renyi (or a $\overline{d}$-regular graph on n nodes) satisfactorily predicts the level of propagation (*i.e.*, the number of infectious nodes at a given time). The second-order Runge-Kutta numerical solution of the proposed pair-approximation model (18), (19) with results of the second pre-processing task as input, performs matches the results of the individual based simulation.

The model on $\overline{d}$-regular graphs underestimates the equilibrium level because it does not include the nodes of high degrees (*i.e.*, the *core* of the scale-free graph). The mean-field model consistently over-estimates the number of infectious nodes because the correlations and graph structure, that may inhibit propagation, are ignored. In contrast, our pair-approximation model includes both nodes of various degrees and correlations between states of nodes, and gives an accurate representation of the stochastic propagation process.

Remark: Two numerical algorithms for solving the system of differential equations—Euler's method and Runge-Kutta method—were compared. For small values of dt, such as 0.001 used in the simulation, even the Euler's method produces good results.

6 Conclusion

Developing an accurate model for the worm propagation is of critical importance not only for understanding better the worm's behavior but also for devising techniques to contain such cyber attacks. The existing studies include either simulation of worm propagation on a macroscopic level or a system of differential equation for propagation on Erdös-Renyi and regular graphs. Moreover, in all existing models of worm propagation, it is not evident how the network structure might affect the dynamics of the stochastic propagation process. Our contribution here is twofold: (1) a model of propagation on a scale-free graph G which takes as input: the number of nodes, number of edges, number of edges incident on nodes of certain degrees, and transitivity of the graph, and (2) implementation of an individual-based simulation for worm propagation that can be cast in different epidemiological frameworks. The accuracy of the model is tested by comparing the numerical solution (by second-order Runge-Kutta method) of the pair-approximation model to the results from the individual-based simulation on scale-free Macroscopic Internet graphs. Our model has the potential to be used in developing realistic techniques for propagation control—topic of an ongoing research.

References

[1] Albert R, Jeong H, Barabasi AL: Diameter of the World Wide Web. Nature 1999; 401: 130 - 131.

[2] Bauch CT: A Versatile ODE Approximation to a Network Model for the Spread of Sexually Transmitted Diseases. Journal of Mathematical Biology 2002; 45: 375 - 395.

[3] Berk VH, Gray RS, Bakos G: Using Sensor Networks and Data Fusion for Early Detection of Active Worms, in: Proc. of SPIE conference on Sensors, and Command, Control, Communications and Intelligence, 2002.

[4] Berk VH, Bakos G: Designing a framework for Active Worm Detection on Global Networks, in Proc. of IEEE International Workshop on Information Assurance, 2003.

[5] Boguna M, Pastor-Satorras R, Vespignani A, Epidemic Spreading in Complex Networks with Degree Correlations, in: Pastor-Satorras R(ed): Lecture Notes in Physics, 2003; 625: 127 - 147.

[6] Chen Z, Gao L, Kwiat K: Modeling the Spread of Active Worms, in: Proc. of IEE INFOCOM, 2003.

[7] Chen LC, Carley KM: The Impact of Network Topology on the Spread of Anti-Virus Countermeasures, CASOS Working paper, available at: http://www.casos.ece.cmu.edu, 2003.

[8] CERT Coordination Center, Advisory CA-2001-26, available at: http://www.cert.org/advisories/CA-2001-26.html 2001.

[9] CERT Coordination Center, Advisory CA-2001-19, available at: http://www.cert.org/advisories/CA-2001-19.html 2002.

[10] Computer Security Institute, Ninth Annual Computer Crime and Security Survey, available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf 2004.

[11] Cowie J, Ogielski AT, Premore BJ, Yuan Y: Global Routing Instabilities Triggered by Code Red II and Nimda, available at: http://www.renesys.com/projects/bgp_instability 2001.

[12] Earnes KTD, Keeling MJ: Modeling Dynamic and Network Heterogeneities in the Spread of Sexually Transmitted Diseases, in: Proc. of National Academy of Sciences, 2002; 99: 13330 - 13335.

[13] Eguiluz VM, Klemm K: Epidemic Threshold in Structured Scale-free Networks. Physics Review Letters, 2002; 89: 108701.

[14] Faloutsos M, Faloutsos P, Faloutsos C: On Power-Law Relationships of the Internet Topology, in: Proc. of SIGCOMM, 1999.

[15] Govindan R, Tangmunarunkit H: Heuristics for Internet Map Discovery, in: Proc. of the IEEE INFOCOM, 2000.

[16] Hethcote HW: Mathematics of Infectious Diseases. SIAM Review, 2000; 42: 599 - 653.

[17] Keeling MJ: The Effects of Local Spatial Structure on Epidemiological Invasions, in: Proc. of the Royal Society of London B, 1999; 266: 859 - 867.

[18] Kephart JO, White SR: Directed-Graph Epidemiological Models of Computer Viruses, in: Proc. of IEEE Symposium on Security and Privacy, 1991; 343.

[19] Kephart JO: How Topology Affects Population Dynamics, in: Langton CG (ed), Artificial Life III, Addison-Wesley, 1994.

[20] Kim K, Radhakrishnan S, Dhall SK: Measurement and Analysis of Worm Propagation on Internet Network Topology, in: Proc. of IEEE Conference on Computer Communications and Networks, 2004.

[21] Kumar R, Raghavan P, Rajagopalan S, Tomkins A, Upfal E: Random Graph Models for the Web Graph, in: Proceedings of FOCS, 2000; 57 - 65.

[22] Lan K, Hussain A, Dutta D: Effects of Malicious Traffic on the Network, in: Proc. of PAM, 2003.

[23] Liljenstam MN, Berk, VH, Gray RS: Simulating Realistic Network Worm Traffc for Worm Warning System Design and Testing, in: Proc. of ACM Workshop on Rapid Malcode, 2003.

[24] Mirkovic J, Martin J, Reiher P: A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, 2004; 34: 39 - 53.

[25] Moore D, Paxson V, Savage S, Shannon C, Staniford S, Weaver N: Inside the Slammer Worm, available at: http://www.computer.org/security/v1n4/j4wea.htm 2003.

[26] Moore D, Shannon C, Voelker GM, Savage S: Internet Quarantine: Requirements for Containing Self-Propagating Code, in: Proc. of IEEE INFOCOM 2003.

[27] Moore D, Network Telescopes, Presentation at DIMACS Large-scale Internet Attacks Workshop, available at: http:// www.caida.org 2003.

[28] Newman MEJ, Strogatz SH, Watts DJ: Random Graph Models of Social Networks, in: Proc. of National Academy of Science of the USA, 2002; 99: 2566 - 2572.

[29] Nikoloski Z, Deo N: The Game of Cops and Robbers on Graphs: A Model for Quarantining Cyber Attacks. Congressus Numerantium, 2003; 162: 193 - 215.

[30] Pastor-Satorras R, Vespignani A: Epidemics and immunization in scale-free networks, in: Bornholdt S, Schuster HG (ed): Handbook of Graphs and Networks: From the Genome to the Internet, Wiley-VCH, 2002; 113 - 132.

[31] Pennock DM, Flake GW, Lawrence S, Glover EJ, Giles CL: Winners don't Take All: Characterizing the Competition for Links on the Web, in: Proc. of National Academy of Sciences of the USA, 2002; 99: 5207 - 5211.

[32] Rand DA: Correlation Equations and Pair Approximation for Spatial Ecologies, in: McGlade J (ed): Advanced Ecological Theory, Principles and Applications, Blackwell Science, 1999; 100 - 142.

[33] Serazzi G, Zanero S: Computer Virus Propagation Models, in: Calzarossa MC, Gelenbe E (ed): Lectures Notes in Computer Science, 2004; 2965: 26 - 50.

[34] Solomon A: Epidemiology and Computer Viruses, available at: http://vx.netlux.org/lib/static/vdat/epepidem.htm 1990.

[35] Staniford, S, Paxson V, Weaver N: How to Own the Internet in Your Spare Time, in: Proc. of the USENIX Security Symposium, 2002; 149 - 167.

[36] Vivo M, Vivo G, Koeneke R, Isern G: Internet Vulnerabilities Related to TCP/IP and T/TCP, Internet Security Attacks at the Basic Level. Operating Systems Review, 1998; 32: 4 - 15.

[37] Vivo M, Carrasco E, Isern G, Vivo G: A Review of Port Scanning Techniques. ACM SIGCOMM Computer Communication Review, 1999; 29 41 - 48 .

[38] Wagner A, Dubendorfer T, Plattner B, Hiestand R: Experiences with Worm Propagation Simulations, in: Proc. of ACM workshop on Rapid Malcode, 2003; 34 - 41.

[39] Wang C, Knight JC, Elder MC: On Computer Viral Infection and the Effect of Immunization, in: Proc. of the Annual Computer Security Applications Conference, 2000.

[40] Wang Y, Wang C: Modeling the Effects of Timing Parameters on Virus Propagation, in: Proc. of ACM Workshop on Rapid Malcode, 2003; 61 - 66.

[41] Weaver N: Potential Strategies for High-speed Active Worms: A Worst Case Analysis, available at: http://www.cs.berkeley.edu/∼nweaver/worms.pdf (2002).

[42] Weaver N, Paxson V, Staniford S, Cunningham R: A Taxonomy of Computer Worms, in: Proc. of ACM Workshop on Rapid Malcode, 2003.

[43] Weaver N, Paxson V, Staniford S, Cunningham R: Large Scale Malicious Code: A Research Agenda, available at: http://www.cs.berkeley.edu/∼nweaver/large_scale_malicious_code.pdf 2003.

[44] Williamson MM: Throttling Viruses: Restricting Propagation to defeat Malicious Mobile Code, in: Proc. of Annual Computer Security Applications Conference, 2002; 61.

[45] Williamson MM, Leveille J: An Epidemiological Model of Virus Spreading and Cleanup, in: Proc. of Virus Bulletin Conference, 2003.

[46] Wu J, Vangala S, Gao L, Kwiat K: An Effective Architecture and Algorithm for Detecting Worms with Various Scan Techniques, in: Proc. of the Network and Distributed System Security Symposium, 2004.

[47] Yegneswaran V, Barford P, Ullrich J: Internet Intrusions: Global Characteristics and Prevalence, in: Proc. of ACM SIGMETRICS International Conference on Measurement and Modeling of computer systems, 2003;, 138 - 147.

[48] Yook S-H, Jeong H, Barabasi AL: Modeling the Internet's Large-scale Topology, in: Proc. of National Academy of Sciences of the USA, 2002; 99: 13382 - 13386.

[49] Zou CC, Gong W, Towsley D: Code Red Worm Propagation Modeling and Analysis, in: Proceedings of ACM conference on Computer and Communications Security, Washington, 2002; 138 - 147.

[50] Zou CC, Gong W, Towsley D, Gao L: Monitoring and Early Detection for Internet Worms, in: Proc. of ACM Conference on Computer and Communication Security, 2003.

[51] Zou CC, Gong W, Towsley D: Worm Propagation Modeling and Analysis under Dynamic Quarantine Defenses, in: Proc. of ACM Workshop on Rapid Malcode, 2003.

AS graph 02.10.1998		beta				
		0.2	0.5	0.9	1.5	1.8
min degree	node					
1	47	18.3675	7.89627	4.74167	3.20504	3.55996
2	17	18.0627	7.91097	4.6643	3.19542	3.46717
3	22	18.4302	7.76855	4.69197	3.14913	3.33457
max degree	node					
590	5	17.158	7.73703	4.45511	3.01981	3.34582
524	12	16.9676	7.37089	4.50048	2.96612	3.39495
355	10	17.2982	7.48106	4.5871	3.10994	3.2987

1pt

AS graph 02.07.1999		beta				
		0.2	0.5	0.9	1.5	1.8
min degree	node					
1	63	18.3734	7.98559	4.81368	3.24062	3.42445
2	19	18.5593	8.17793	4.70665	3.19895	3.48956
3	15	18.5207	7.93869	4.74685	3.18794	3.343
max degree	node					
1193	2	17.4871	7.43152	4.44526	2.98155	3.39874
674	10	17.6827	7.58919	4.57659	3.11	3.41901
588	7	17.5386	7.70924	4.63347	3.10909	3.38447

1pt

AS graph 02.07.2000		beta				
min degree	node	0.2	0.5	0.9	1.5	1.8
1	15	19.8676	8.42701	5.11502	3.42114	3.71483
2	18	20.1391	8.62913	5.15767	3.41545	3.56204
3	23	19.4788	8.44671	5.05909	3.3409	3.5603
max degree	node					
1772	2	18.9615	8.0676	4.97258	3.29313	3.48871
961	9	19.2357	8.28964	4.90184	3.33247	3.49154
802	7	18.9133	8.24647	4.96538	3.34996	3.47815

1pt

AS graph 16.03.2001		beta				
min degree	node	0.2	0.5	0.9	1.5	1.8
1	44	21.0673	8.91663	5.35035	3.57629	3.76316
2	37	21.385	8.90863	5.35318	3.47916	3.74718
3	34	20.6299	8.93965	5.33861	3.54236	3.64725
max degree	node					
2277	2	20.1728	8.44475	4.98278	3.37857	3.58247
1231	13	20.3132	8.67817	5.248	3.46303	3.62322
899	15	20.4644	8.87768	5.2025	3.42517	3.69419

Figure 2: Time to propagate to all nodes of a Macroscopic Internet graph for five different values of the parameter β.

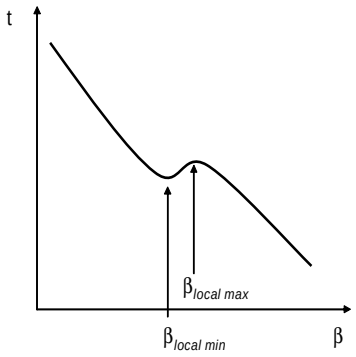

Figure 3: Time to infect all nodes as a function of the rate β is not a strictly decreasing function

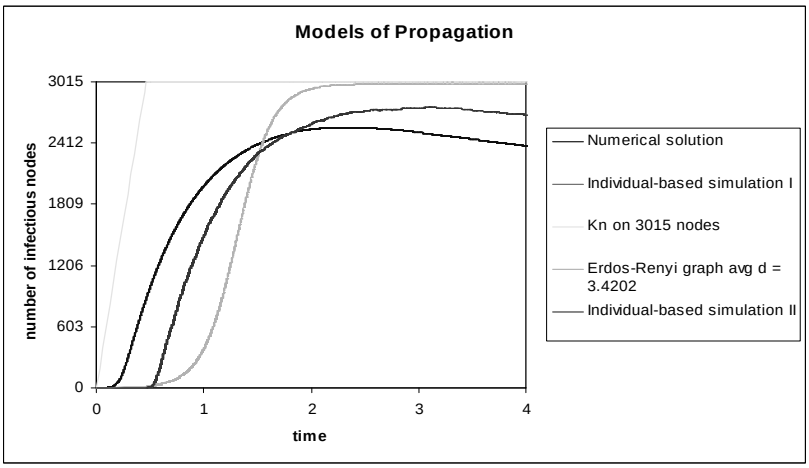

Figure 4: Susceptible-Infectious-Susceptible models of propagation—numerical solution of pair-approximation model, individual-based simulation of propagation on an Internet graph $n = 3015$ and $m = 5156$, propagation on complete graph $n = 3015$, propagation on Erdos-Renyi random graphs with $\overline{d} = 3.4202$; parameters of propagation $\beta = 1.8, \gamma = 0.05$

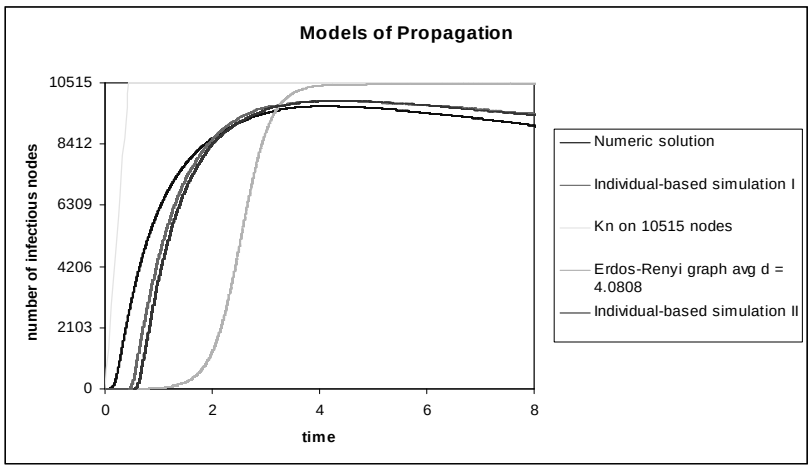

Figure 5: Susceptible-Infectious-Susceptible models of propagation—numerical solution of pair-approximation model, individual-based simulation of propagation on an Internet graph $n = 10515$ and $m = 21455$, propagation on complete graph $n = 10515$, propagation on Erdos-Renyi random graphs with $\overline{d} = 4.0808$; parameters of propagation $\beta = 0.9, \gamma = 0.02$