5 Spreading Dynamics

5.1 Introduction

In a retrospect of the human history, one can easily realize that the human civilization has always been accompanied with epidemics, such as malaria, orthopoxvirus variola, measles, pestis, typhoid fever, AIDS, SARS, avian flu, etc. The networking of human society greatly improves the public healthcare system, thereby reducing the treat of various diseases, and yet ironically it also enhances the wide spread of epidemics due to frequent individual contacts through the human relationship network.

Compared to the biological epidemics, computer viruses are much easier to spread over the huge Internet worldwide, and have much longer lifetimes [1]. Major computer viruses may be roughly classified into (i) boot-sector viruses which infect the boot sectors of floppies and hardware devices, (ii) file viruses which infect application programs, and (iii) macro viruses which infect data files directly, as well as (iv) some hybrid types of viruses in a certain combination of these basic ones. The first serious virus capable of infecting PCs was perhaps the Brain virus developed in Pakistan in 1986. Many viruses were born since then, and just in year 2000 alone it was estimated that there were more than 48,000 identified viruses on the Internet [2]. Statistics show that more than 80% computers were contaminated by viruses in China in 2004, and in that year the infamous “Worm Sasser” attacked several hundred thousands of computers over the world within just a couple of weeks. Digital viruses seem quite capable of reaching their long-lasting and almost endemic steady states, regardless of the virus strains, in a fast and easy manner. Experts warned that, if not extremely carefully protected, the whole Internet could totally collapse in seconds! Countless incidents of these kinds have already provoked some very serious rethinking: given the seemingly effective and advanced medical and electronic prevention and management systems today, how could biological diseases and computer viruses spread so fast and so wide? It turns out that the complex networks theory may provide some sensible analysis on, or even a meaningful solution to this commonly concerned question.

A biological system (species, population, or cell) or a computer unit (AS, router, or PC) can be defined as a node in a network, connected together by certain edges (contact or connection), in a particular topology. A conventional theory believes that only if the spreading speed is increasing to pass a relatively large positive threshold can virus outbreak become possible. However, the recent study of Pastor-Satorras and Vespignani [2,3] reveals that a scale-free network can well model such virus spread and, on the contrary, that as the network size increases the threshold tends to zero, which means that a small source of virus is sufficient to cause a wide prevalence over the entire huge network. On the other hand, human societies have prominent small-world features which normally make diseases quite easy to propagate.

In this chapter, the network-based *epidemic threshold theory* for epidemics, as well as its immunization strategies and spread dynamics, are studied using computer virus propagation as typical examples.

5.2 Epidemic Threshold Theory

The study of epidemics has a fairly long history, with several successful mathematical models available in the literature [4-6].

In a typical epidemic propagation model, the states of all individuals in a population are classified into:

- S (Susceptible) – healthy state (can be infected by others)
- I (Infected) – infected state (can infect others)
- R (Recovered) – recovered state (can be infected or cannot be infected again)

Different combinations of these two states lead to different models, such as SIS and SIR models.

Recently, the classical theories of epidemic spread and threshold have been revisited for various community structures such as random-graph, small-world and scale-free network frameworks. In a network, if two nodes are connected then they are considered to have "contact". Thus, if one node is "infected" by a virus and the other is "susceptible," then with a certain probability the latter may become infected as time goes on. Throughout a virus spreading process, if an infected node is cured at some time, then it may become susceptive again or may have immunity forever. In the latter case, this node may be considered being removed from the network in the consequent discussion of further virus spreading over the network.

5.2.1 Epidemic Models

Consider a population of N connected individuals, described by a network of N nodes. Let the number of healthy nodes be $S(t)$, infected nodes be $I(t)$, and recovered nodes be $R(t)$ at time $t \geq 0$, initially $S(0) = S_0$, $I(0) = I_0$, and $R(0) = R_0 = 0$. For convenience in computation, one may normalize the three variables by dividing them by N, and in doing so they also have the meaning of "density" (percentage), with $S(t) + I(t) + R(t) = 1$ for all $t \geq 0$.

Assume that the lifetime of a virus or disease is much shorter than the lifetime of the

nodes in the population; therefore, birth and death of nodes are not taken into consideration in the following study.

Suppose that the probability of a node becoming "infected" from "susceptible" is v, and the probability of a node being cured and becomes "susceptible" again is δ. Then, define the virus *effective spreading rate* as

$$\lambda = \frac{v}{\delta} \tag{5-1}$$

One extreme case is that all cured nodes immediately become susceptible again, which corresponds to $\delta = 1$, thus $\lambda = v =$ probability of a node becomes infected.

SI Epidemic Model

Suppose $R(t) = 0$ for all $t \geq 0$. Consider the rate of increase in the density of infected nodes, from time t to time $t + \Delta t$, which is given by

$$\frac{I(t+\Delta t) - I(t)}{\Delta t} \approx [\lambda S(t)] I(t)$$

In the limit $\Delta t \to 0$, one has $\frac{dI(t)}{dt} = \lambda S(t) I(t)$. Since $S(t) = 1 - I(t)$, this becomes the so-called Logistic model:

$$\frac{dI(t)}{dt} = \lambda [1 - I(t)] I(t), \qquad I(0) = I_0 \tag{5-2}$$

This equation has a solution

$$I(t) = \frac{1}{1 + \left(I_0^{-1} - 1\right) e^{-\lambda t}} \tag{5-3}$$

Clearly, $I(t) \to 1$ as $t \to \infty$, meaning that all nodes are infected eventually. This is true if no infected nodes are cured and then recovered in the process.

SIS Model

Again, consider the case of $R(t) = 0$. But, now, suppose that the rate of recovery from "infected" back to "susceptive" is δ, namely, $S(t) = \delta I(t)$. It then follows from (5-2) that

$$\frac{dI(t)}{dt} = \lambda [1 - I(t)] I(t) - \delta I(t), \qquad I(0) = I_0 \tag{5-4}$$

This equation has a solution

$$I(t) = \begin{cases} \left\{ \dfrac{1}{1 - \dfrac{\delta}{\lambda}} + \left(I_0 - \dfrac{1}{1 - \dfrac{\delta}{\lambda}} \right) e^{-\left(1 - \frac{\delta}{\lambda}\right)\lambda t} \right\}^{-1}, & \delta \neq \lambda \\ \dfrac{1}{\lambda t + I_0^{-1}}, & \delta = \lambda \end{cases} \tag{5-5}$$

There are three cases:

(i) $\delta > \lambda$: This means that recovering is faster than infecting. It follows from (5-5) that $I(t) \to 0$ as $t \to \infty$, implying that the virus will die out eventually.

(ii) $\delta < \lambda$: This means that recovering is slower than infecting. It follows from (5-5) that $I(t) \to \left(1 - \frac{\delta}{\lambda}\right)$ as $t \to \infty$, implying that a certain fraction of nodes will remain being infected. In particular, if $\delta << \lambda$ then $I(t) \sim 1$ as $t \to \infty$, implying that almost all nodes will be infected eventually.

(iii) $\delta = \lambda$: This is a threshold, determining whether or not the virus will spread.

SIR Model

Now, suppose $R(t) > 0$, namely, some nodes will be cured therefore recovered and become susceptive again. In this case, one can similarly establish the following model:

$$\begin{cases} \dfrac{dI(t)}{dt} = \lambda S(t) I(t) - \delta I(t) \\ \dfrac{dS(t)}{dt} = -\lambda S(t) I(t) \\ \dfrac{dR(t)}{dt} = \delta I(t) \\ I(0) = I_0, \quad S(0) = S_0, \quad R(0) = 0 \end{cases} \tag{5-6}$$

By qualitative analysis or numerical solutions, one can find the following:

(i) $S_0 > \frac{\delta}{\lambda}$: Virus will spread out for some time, but eventually die out.

(ii) $S_0 \le \frac{\delta}{\lambda}$: Virus will die our quickly.

5.2.2 Epidemic Thresholds on Homogenous Networks

Furthermore, consider the situation where the network topology is homogeneous (such as a random-graph network or a small-world network), where the node-degree distribution has a peak at its average value $\langle k \rangle$, and then decays exponentially fast for small $k << \langle k \rangle$ and large $k >> \langle k \rangle$. For simplicity, based on the homogeneity, assume that each node has degree $k_i \approx \langle k \rangle$, $i = 1,2,...,N$. For simplicity, moreover, assume that all cured nodes immediately become susceptible again, which corresponds to $\delta = 1$ in (5-1).

If the node-degree correlations are neglected, the infected node density function $I(t)$ satisfies (5-4), namely

$$\frac{dI(t)}{dt} = \lambda\langle k\rangle\,[1-I(t)]I(t) - I(t), \qquad I(0) = I_0 \tag{5-7}$$

where the second term indicates that the infected node is recovered at a rate of unity, namely, always recovered immediately; the first term represents the average fraction of nodes being infected by an infected node, which depends on the effective spreading rate λ, node degree $\langle k\rangle$, and the number of nodes connecting to the healthy nodes, $1-I(t)$. Since only the situation with $I(t)<<1$ is concerned, all possible higher-order terms in $I(t)$, due to the use of the approximation $\langle k\rangle$, are neglected on the right-hand side of this equation.

By letting the right-hand side of (5-7) be equal to zero, one obtains the steady density of infected nodes, as

$$I(\infty) = \begin{cases} 0, & \lambda < \lambda_c \\ 1-\dfrac{\lambda_c}{\lambda}, & \lambda \geq \lambda_c \end{cases} \tag{5-8}$$

where the *epidemic threshold* is

$$\lambda_c = \frac{1}{\langle k\rangle} \tag{5-9}$$

This implies that there is a finite epidemic threshold $\lambda_c > 0$: over this threshold, the infected node can propagate the disease to the whole network, eventually leading to a certain equilibrium state, and in this situation the network is said to be in the active phase; under this threshold, the number of infected nodes decays exponentially, therefore disease will not be able to spread out, and in this situation the network is said to be in the absorbing phase, as illustrated by Fig. 5-1 [7].

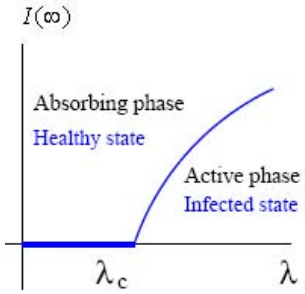


Fig. 5-1 Phase transition of the SIS model on a homogeneous network [7]

5.2.3 Statistical Data Analysis

Some real data on computer networks, however, show quite different behaviors.

Define the *virus prevalence* to be the ratio of the average number of computers infected by virus versus the total number of all computers in a network of concern, and define the *virus surviving probability* $P_s(t)$ to be the percentage of nodes that are alive since birth till the current time t. Figure 5-2 shows the computer virus prevalence in the 50 months from February 1996 to March 2000, on the boot-sector,

file, and macro viruses [3]. It can be seen that after a sharp initial drop, there is an exponential decay with an associate characteristic time τ (months), which depends on the given strain of computer virus.

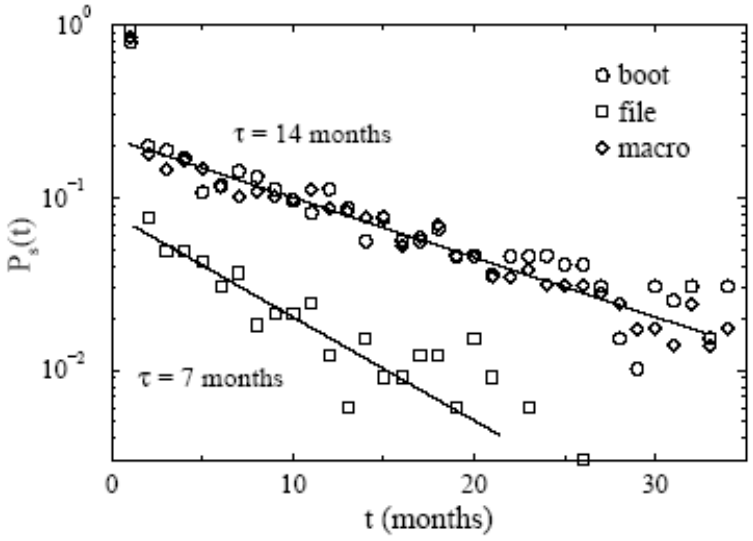


Fig. 5-2 Virus surviving probabilities for three main strains of computer viruses [3]

The above statistical data show that the computer virus on the real Internet actually did not propagate as fast and wide as one may imagine. If these strains of viruses were propagating over a homogeneous network then the virus prevalence has to be lower than the epidemic threshold since the surviving probabilities are so low (see Fig. 5-2), and yet the virus effective spreading rate must be higher than this epidemic threshold since the lifetimes of these viruses are so long (see Fig. 5-1). These contradictory phenomena imply that the computer network must be inhomogeneous.

5.2.4 Epidemic Thresholds on Scale-Free Networks

Now, consider the epidemic thresholds of some heterogeneous networks, typically scale-free networks.

Denote the relative density of infected degree-k nodes in a population by $\rho_k(t)$. Its mean-field equation is [8]

$$\frac{\partial \rho_k(t)}{\partial t} = -\rho_k(t) + \lambda k[1-\rho_k(t)]\Theta(\rho_k(t)) \tag{5-10}$$

Here, $\Theta(\rho_k(t))$ is the probability of an edge connecting to an infected degree-k node, λ is the effective spreading rate, and higher-order terms are also neglected assuming that $\rho_k(t) << 1$.

Let $\rho_k(t) \to \rho_k$ as $t \to \infty$. Then, by setting the right-hand side of (5-10) be zero, one obtains

$$\rho_k = \frac{k\lambda\Theta(\lambda)}{1+k\lambda\Theta(\lambda)} \tag{5-11}$$

This implies that higher-degree nodes have higher probabilities to be infected.

It should be noted that Θ depends on the heterogeneity of the network. For uncorrelated scale-free networks, namely, there is no correlation between any pair of nodes with different degrees, since the probability of an edge connecting to a node with degree s is given by $sP(s)/\langle k\rangle$, one has

$$\Theta(\lambda)=\frac{1}{\langle k\rangle}\sum_k kP(k)\rho_k \tag{5-12}$$

Thus, solving equations (5-11) and (5-12) for ρ_k and $\Theta(\lambda)$ yields

$$\Theta=\frac{1}{\langle k\rangle}\sum_k kP(k)\frac{\lambda k\Theta}{1+\lambda k\Theta} \tag{5-13}$$

which has a trivial solution $\Theta=0$. The epidemic threshold λ_c should be determined such that when $\lambda>\lambda_c$ the probability Θ has a nonzero solution. In so doing, the following condition must be satisfied:

$$\frac{d}{d\Theta}\left(\frac{1}{\langle k\rangle}\sum_k kP(k)\frac{\lambda k\Theta}{1+\lambda k\Theta}\right)\Bigg|_{\Theta=0}\geq 1$$

namely,

$$\sum_k \frac{kP(k)\lambda k}{\langle k\rangle}=\frac{\langle k^2\rangle}{\langle k\rangle}\lambda\geq 1$$

which yields

$$\lambda_c=\frac{\langle k\rangle}{\langle k^2\rangle} \tag{5-14}$$

For scale-free networks with $2<\gamma\leq 3$ in the power laws, as $N\to\infty$, one has $\langle k^2\rangle\to\infty$, therefore $\lambda_c\to 0$. This means that diseases can easily break out because the epidemic thresholds are so small in such networks.

5.2.5 Epidemic Thresholds on BA Scale-Free Networks

As a typical scale-free network example, consider the BA network. Since its average degree and degree distribution are (Theorem 3-10, Chapter 3)

$$\langle k\rangle=\int_m^\infty kP(k)dk=2m,\quad P(k)=2m^2k^{-3}$$

it follows from (5-12) that

$$\Theta(\lambda)=m\lambda\Theta(\lambda)\int_m^\infty\frac{1}{k}\frac{dk}{1+k\lambda\Theta(\lambda)}=m\lambda\Theta(\lambda)\log\left(1+\frac{1}{m\lambda\Theta(\lambda)}\right)$$

so that

$$\Theta(\lambda)=\frac{e^{-1/m\lambda}}{\lambda m}\left(1-e^{-1/m\lambda}\right)^{-1} \tag{5-15}$$

Next, calculate ρ as follows:

$$\begin{aligned}\rho &= \sum_k P(k)\rho_k \\ &= 2m^2\lambda\Theta(\lambda)\int_m^\infty \frac{1}{k^2}\frac{dk}{1+k\Theta(\lambda)} \\ &= 2m^2\lambda\Theta(\lambda)\left[\frac{1}{m}+\lambda\Theta(\lambda)\log\left(1+\frac{1}{m\lambda\Theta(\lambda)}\right)\right]\end{aligned} \tag{5-16}$$

Then, substituting (5-15) into (5-16) gives [8]

$$\rho \sim 2e^{-1/(m\lambda)} \tag{5-17}$$

The right-hand side of the above is nonnegative, and it becomes zero if and only if $\lambda = 0$, implying that the epidemic threshold of the BA scale-free networks is $\lambda_c = 0$.

Figure 5-3 shows a comparison of the relationships between ρ and λ in the SIS model on a WS small-world network and a BA scale-free network, respectively [7]. It shows that the effective spreading rate λ on the BA network tends to zero continuously and smoothly, implying that it virtually has no positive threshold λ_c, so for any $\lambda > 0$ virus can easily propagate throughout the network and finally reach a steady state. This demonstrates the fragility of scale-free networks against virus spreading.

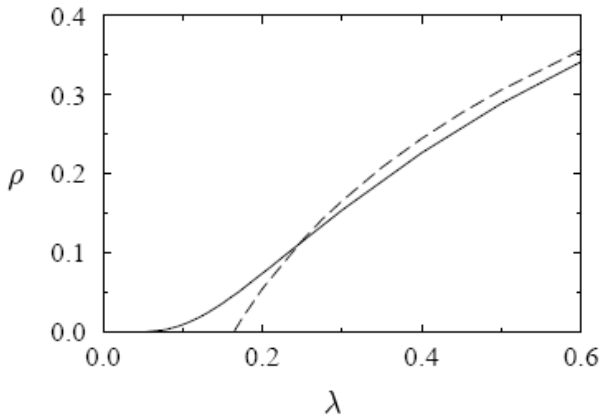


Fig. 5-3 Relations between ρ and λ in an SIS model:
WS network (dash curve) and BA network (solid curve) [7]

In the last chapter, it was shown that the Internet is rapidly growing following a scale-free manner with the degree distribution in a power-law form. Therefore, it is not surprising to see that computer viruses can spread all over the Internet easily and quickly. Yet, fortunately, on the real Internet, it is also found that the λ value is very small ($\lambda << 1$), leading to a low propagation speed. This is also consistent with the observation that the epidemic threshold of a scale-free network vanishes fairly slowly, as the size of the network expands even quickly towards infinity.

Figure 5-4 shows a semi-logarithmic plot of the relation between the density of infected nodes ρ and the effective spreading rate λ in a BA scale-free network

model with different sizes, where "+" corresponds to $N = 10^5$, small squares to $N = 5\times10^5$, "×" to $N = 10^6$, and small circles to $N = 5\times10^6$. It implies that $\rho(\lambda) \sim e^{-c/\lambda}$ for a constant $c > 0$, independent of the size of the network.

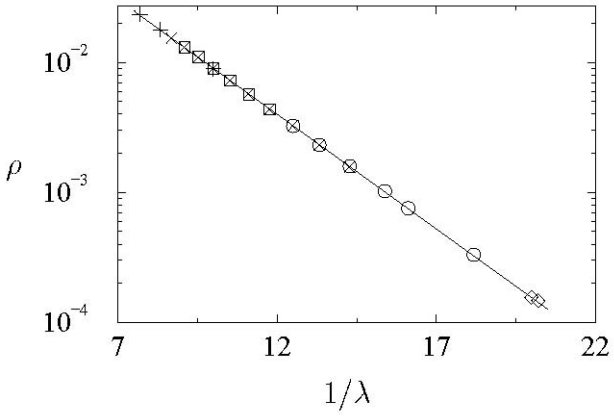


Fig. 5-4 Relation between ρ and λ in BA networks [7]

Figure 5-5 shows the virus surviving probability $P_s(t)$ versus time t for the same four networks discussed above in Fig. 5-4, from small to large (top down) in sizes. It indicates that on any finite-sized scale-free network, epidemic will eventually die out. This is reasonable because there is a finite probability of all nodes being cured from the infection at the same time as epidemic propagates on the network. Moreover, the bigger the network is, the slower the disease dies out. Theoretically, the lifetime is infinite only in the limiting case of $N \to \infty$, a well-known feature of the virus surviving probability in finite-sized absorbing-state networks poised about a critical point [7].

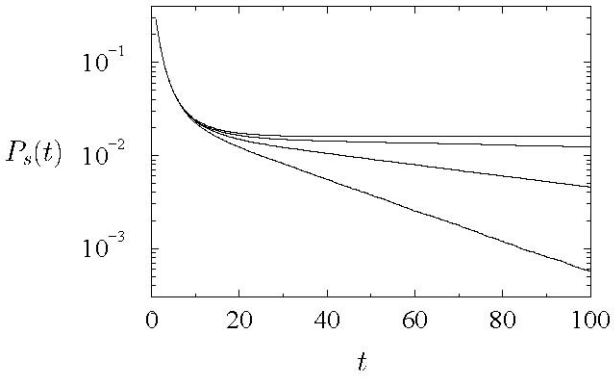


Fig. 5-5 Relation between $P_s(t)$ and t in BA networks [7]

5.2.6 Epidemic Thresholds on Finite-Sized Scale-Free Networks

For a finite-sized scale-free network, introduce a maximum connectivity k_c, which depends on the size N of the network. An SIS model, established on a scale-free network with node-degree distribution $P(k) \sim k^{-\gamma}\exp(-k/k_c)$, has a nonzero epidemic threshold [9]:

$$\lambda_c(k_c) \sim \left(\frac{k_c}{m}\right)^{\gamma-3} \tag{5-18}$$

where m is the minimum nonzero number of edges being added to the network (i.e., the new edges brought in by the new nodes) during the formation of the scale-free network. The limit $\gamma \to 3$ corresponds to a logarithmic divergence, which is described by

$$\lambda_c(k_c) \sim \frac{1}{m \ln(k_c m)} \qquad (\text{for } \gamma \to 3) \tag{5-19}$$

Figure 5-6 shows a comparison, λ_c versus λ_c^H, of the epidemic threshold values on a finite-sized scale-free network and on a homogeneous network of the same size [7]. It can be seen that in the scale-free network with $\gamma = 2.5$, even for relatively small k_c, its threshold is only about 1/10 of the homogeneous network. It can also be seen that as k_c increases or $N \to \infty$, the threshold of the scale-free network can still tend to zero, implying the fragility of a finite-sized scale-free network against virus spreading.

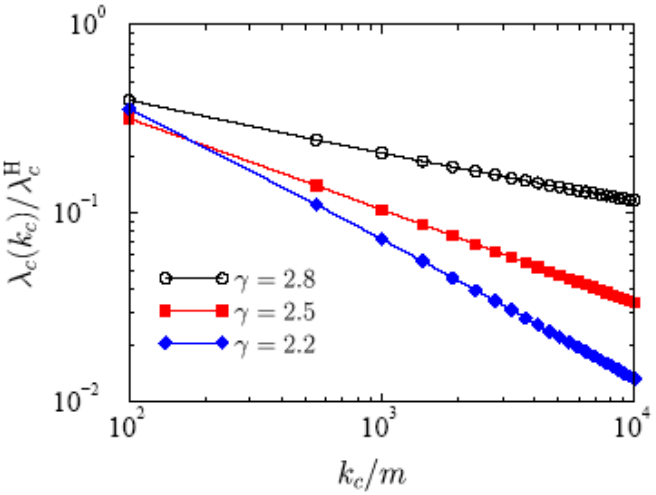


Fig. 5-6 Comparison of epidemic threshold values on two types of networks [7]

It is interesting to point out that the above conclusions about the SIS model hold also for the SIR model in general, namely, the epidemic spreading threshold properties are not affected by the differences of the two epidemic models. The SIR model will be briefly introduced below in Section 5.2.9.

5.2.7 Epidemic Thresholds on Correlated Networks

The above discussions were mainly restricted on uncorrelated scale-free networks, namely, there is no connectivity correlation between any pair of nodes with different degrees in the network. Many networks, scale-free or not, such as the Internet actually are correlated networks, and on a correlated network the epidemic threshold turns out to be quite different [10].

In a correlated network, let $P(k'|k)$ be the conditional probability of a degree-k' node connecting to a given degree-k node. If this probability is independent of k,

then the situation reduces to the uncorrelated case discussed above. Suppose that the degree distribution $P(k)$ and this $P(k'|k)$ satisfy the following normalized balance conditions:

$$\sum_k P(k) = \sum_{k'} P(k'|k) = 1$$
$$kP(k'|k)P(k) = k'P(k|k')P(k') \equiv \langle k \rangle P(k,k')$$

where the symmetric function $(2-\delta_{kk'})P(k,k')$ describes the joint probability of the connectivity of degree-k and degree-k' nodes, in which $\delta_{kk'}=1$ if $k=k'$ or $=0$ otherwise. Further, define a connectivity matrix $C_{kk'}=\left[kP(k'|k)\right]$. Then, it can be verified [10] that

$$\lambda_c = \lambda_{\max}^{-1} \tag{5-20}$$

where $\lambda_{\max}$ is the maximum eigenvalue of matrix $C_{kk'}$. For uncorrelated networks, $\lambda_{\max} = \left\langle k^2 \right\rangle \Big/ \left\langle k \right\rangle$, leading to the same conclusion drawn for uncorrelated networks above. Therefore, the epidemic threshold on a network, correlated or not, is essentially determined by the maximum eigenvalue of the connectivity matrix $C_{kk'}$.

It was shown, however, that in an SIS model, the epidemic incidence on a correlated network is smaller than that on an uncorrelated network with the same node-degree distribution [11]. Although the basic properties of the epidemic threshold do not vary according to the node-degree correlations, the spreading lifetime on a corrected network is generally longer than that on an uncorrelated network. Therefore, on a finite-sized correlated network, the epidemic threshold usually is larger than that on an uncorrelated network, indicating that correlated networks are more robust than uncorrelated networks in resisting virus propagation.

5.2.8 Epidemic Thresholds on Some Generalized Scale-Free Networks

Consider a class of generalized scale-free networks with power-law node-degree distribution [8]

$$P(k) = (1+\mu)m^{1+\mu}k^{-2-\mu} = (\gamma-1)m^{\gamma-1}k^{-\gamma} \tag{5-21}$$

where m is the smallest nonzero degree of network nodes, typically $m=1$, and the epidemic threshold $\lambda = 2+\mu$: when $0<\mu<1$ (i.e., $2<\gamma<3$), $\lambda_c = 0$; when $\mu>1$ (i.e., $\gamma>3$), $\lambda_c = \dfrac{\mu-1}{m\mu}$. In particular, it was observed [12-14] that when $\mu>2$ (i.e., $\gamma>4$), the epidemic threshold of a scale-free network is almost the same as that of a homogeneous (e.g., random-graph, small-world) network.

From a biological systems point of view, when $\gamma>1$, one should have $\lambda_c=0$. Moreover, based on different optimal selection criteria, for different scale-free networks (even with the same power-law exponent γ), there is no common effective immunization strategy [15].

Noticing that many real networks have a node-degree distribution not completely

power-law nor completely exponential, but rather, their combination. Thus, one may define a preferential attached probability

$$\Pi_i \sim (1-p)k_i + p$$

When $0 \le p \le 1$, this gives a hybrid homogeneous and heterogeneous model of scale-free and random-graph networks. It was shown that in this model, no matter how large the effective spreading rate λ is, there is always a fraction of node not being infected [16]. This also explains the existence of nonzero epidemic threshold λ_c in such hybrid type of networks.

In a scale-free network with a household structure, such as a typical social network, if the infection status is distinctive for inside and outside families, and if each member of a family has a recovery rate faster than the infection rate in the same family, then eventually every family will be immunized as a group, although a disease could still propagate on the scale-free network in the sense that scattered individuals in some families can still be infected and disease can still spread over the whole network [17].

5.2.9 SIR Model of Epidemic Spread

So far the discussions have been restricted to the SIS model. In this subsection, the SIR model will be introduced.

Consider a population (network) of N individuals (nodes), each is either in the Susceptible (S), or Infected (I), or Recovered (R) state. Let $\rho_{S,k}(t)$, $\rho_{I,k}(t)$ and $\rho_{R,k}(t)$ be the densities of the S, I and R states of nodes of degree k at time t, respectively. Then, these densities are related by means of the normalization condition

$$\rho_{S,k}(t) + \rho_{I,k}(t) + \rho_{R,k}(t) = 1, \text{ for all } t \ge 0$$

Define the total number of recovered nodes at time t by

$$R(t) = \sum_k P(k)\rho_{R,k}(t)$$

where $P(k)$ is the node-degree distribution of the network. Denote its prevalence (in steady state) by

$$R_\infty = \lim_{t\to\infty} R(t)$$

At the mean-field level, for undirected random-graph type of uncorrelated sparse networks, the above densities satisfy the following system of differential equations:

$$\frac{d\rho_{I,k}(t)}{dt} = -\rho_{I,k}(t) + \lambda k \rho_{S,k}(t)\Theta(t)$$

$$\frac{d\rho_{S,k}(t)}{dt} = -\lambda k \rho_{S,k}(t)\Theta(t) \qquad (5\text{-}22)$$

$$\frac{d\rho_{R,k}(t)}{dt} = \rho_{I,k}(t)$$

where λ is the effective spreading rate and $\Theta(t)$ represents the average density of infected nodes pointed at by a given edge. In general, the probability that an edge points to an infected node with degree k is proportional to $kP(k)\rho_{I,k}(t)$. Notice that the infected node pointed by the edge has previously received virus through an edge that cannot be used for virus transmission anymore, since its originating node had been recovered therefore it is immune to the virus. Hence, the above probability should be modified to be $(k-1)P(k)\rho_{I,k}(t)$, so that

$$\Theta(t) = \frac{1}{\langle k \rangle}\sum_k (k-1)P(k)\rho_{I,k}(t) \qquad (5\text{-}23)$$

A combination of system (5-22) and equation (5-23), along with the natural initial conditions

$$\rho_{R,k}(0) = 0\,, \quad \rho_{I,k}(0) = \rho_k^0 \quad \text{and} \quad \rho_{S,k}(0) = 1 - \rho_k^0$$

completely defines the SIR model of virus spreading on a random-graph type of uncorrected network with node-degree distribution $P(k)$.

Assume that initially infected nodes are uniformly distributed, namely, $\rho_k^0 = \rho^0$ for all k at time $t = 0$. In this case, in the limit $\rho^0 \to 0$, namely, starting from free infected nodes, one has $\rho_{I,k}^0(0) \approx 0$ and $\rho_{S,k}(0) \approx 1$. Under these assumptions, the second and third equations in system (5-22) can be directly integrated, yielding

$$\rho_{S,k}(t) = e^{-\lambda k \phi(t)} \quad \text{and} \quad \rho_{R,k}(t) = \int_0^t \rho_{I,k}(\tau)d\tau \qquad (5\text{-}24)$$

where

$$\phi(t) = \int_0^t \Theta(\tau)d\tau = \frac{1}{\langle k \rangle}\sum_k (k-1)P(k)\rho_{R,k}(t)$$

which, based on (5-24), gives

$$\frac{d\phi(t)}{dt} = \frac{1}{\langle k \rangle}\sum_k (k-1)P(k)\rho_{I,k}(t)$$

$$= \frac{1}{\langle k \rangle}\sum_k (k-1)P(k)[1 - \rho_{R,k}(t) - \rho_{S,k}(t)]$$

$$= 1 - \frac{1}{\langle k \rangle} - \phi(t) - \frac{1}{\langle k \rangle} \sum_k (k-1) P(k) e^{-\lambda k \phi(t)} \qquad (5\text{-}25)$$

If equation (5-25) can be solved, then one can obtain the total epidemic prevalence (in steady state) $\rho_{S,k}(\infty)$ as a function of $\phi_\infty = \lim_{t\to\infty} \phi(t)$. Notice that in the steady state, $\rho_{I,k}(\infty) = 0$, since nodes are either all infected or all recovered, so the infection density will not change any more. Thus, using $\rho_{R,k}(\infty) = 1 - \rho_{S,k}(\infty)$, one obtains

$$R_\infty = \sum_k P(k) \left[1 - e^{-\lambda k \phi_\infty} \right]$$

However, for a general node-degree distribution $P(k)$, equation (5-25) cannot be solved. Nevertheless, one can still obtain some useful information about the asymptotic behavior of the virus spreading. Indeed, since $\rho_{I,k}(\infty) = 0$ and consequently $\lim_{t\to\infty} d\phi(t)/dt = 0$, from equation (5-25) one obtains the following steady-state equation:

$$\phi_\infty = 1 - \frac{1}{\langle k \rangle} - \frac{1}{\langle k \rangle} \sum_k (k-1) P(k) e^{-\lambda k \phi_\infty}$$

This equation has a fixed-point solution $\phi_\infty = 0$. In order to have a nonzero solution for ϕ_∞, which would mean a prevalence $R_\infty > 0$, it is necessary that

$$\frac{d}{d\phi_\infty} \left[1 - \frac{1}{\langle k \rangle} - \frac{1}{\langle k \rangle} \sum_k (k-1) P(k) e^{-\lambda k \phi_\infty} \right] \Bigg|_{\phi_\infty = 0} \geq 1$$

This condition implies that

$$\frac{\lambda}{\langle k \rangle} \sum_k k(k-1) P(k) \geq 1$$

yielding the epidemic threshold

$$\lambda_c = \frac{\langle k \rangle}{\langle k^2 \rangle - \langle k \rangle} \qquad (5\text{-}26)$$

below which $R_\infty = 0$ and above which $R_\infty > 0$.

5.3 Immunization on Complex Networks

Since scale-free networks are fragile to virus attacks, which cause serious and wide outbreaks, immunization (vaccination) becomes especially important for this type of

networks. This section introduces three typical effective immunization strategies, namely, Random Immunization (or, Uniform Immunization), Targeted Immunization (or, Selected Immunization), and Acquaintance Immunization.

5.3.1 Random Immunization

Random immunization means to randomly select a fraction of nodes from the network to immune. In so doing, although large nodes have higher risk to be infected and small nodes are relatively safe, each of them has an equal chance to be chosen for immunization.

Let the immunity, namely the density of immunized nodes, be denoted by g. Then, the threshold of the corresponding random immunization strategy is given by [3]

$$g_c = 1 - \frac{\lambda_c}{\lambda} \tag{5-27}$$

and the steady density of infected nodes is

$$\begin{cases} \rho_g = 0 & g > g_c \\ \rho_g = \left(\dfrac{g_c - g}{1 - g} \right) & g \le g_c \end{cases} \tag{5-28}$$

Substituting the epidemic threshold formula (5-14) into (5-27) gives

$$g_c = 1 - \frac{1}{\lambda} \frac{\langle k \rangle}{\langle k^2 \rangle} \tag{5-29}$$

Clearly, as the size of the network grows, one has $\langle k^2 \rangle \to \infty$ so that the immune threshold of the scale-free network $g_c \to 1$ and consequently $\lambda_c \to 0$. This means that if a scale-free network is randomly immunized then almost every node in the network has to be immunized, implying that random immunization for a scale-free network is quite inefficient and expensive.

5.3.2 Targeted Immunization

As discussed above, scale-free networks seem to rule out the efficiency of the simple-minded uniform immunization strategy. Instead, by taking advantage of the heterogeneity of the scale-free networks, one may adopt a targeted immunization strategy, in which one progressively immunes the most highly connected nodes that are likely received the diseases from, and also spreading the diseases to, many other nodes. Once these big nodes are immunized, conceptually their edges are removed, loosing connections with the other nodes thereby reducing or even completely blocking the way of virus spreading over the network.

For BA scale-free networks, the immunization threshold is [18]

$$g_c \sim e^{-\frac{2}{m\lambda}} \tag{5-30}$$

which shows that a very small immunization threshold can be obtained for a very large range of effective spreading rate λ. In other words, on scale-free networks, targeted immunization has a much smaller immunization threshold than random immunization therefore is much more efficient.

Figure 5-7 shows a comparison between the two, targeted versus random, immunization strategies on a BA scale-free network model, where g is the immunity (namely, the density of immunized nodes), ρ_0 is the steady infection density before immunization, ρ_g is the steady infection density after immunization, and the ratio of ρ_g / ρ_0 indicates the effect of the immunization. It can be seen that the two immunization strategies have different efficiencies: for random immunization, the ratio decreases slowly and becomes zero only when $g \to 1$, and yet for the targeted immunization this is achieved for $g_c \approx 0.16$, which is very small as compared to 1. It implies that much less nodes are needed to be immunized by the targeted strategy than the random strategy to achieve a perfect immunization of the entire network.

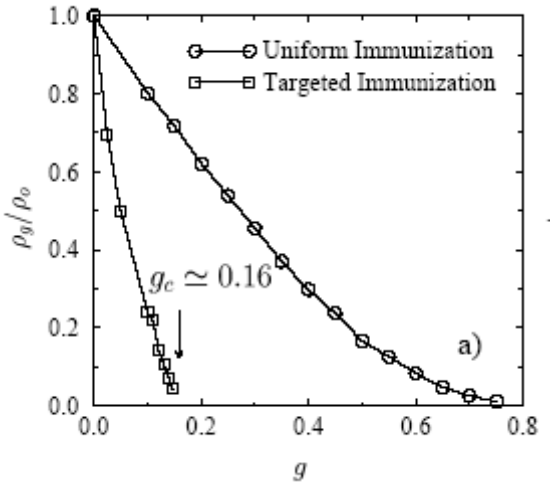


Fig. 5-7 Comparison of two immunization strategies on a BA network [7]

Applying the targeted immunization strategy to an SIS model of the Internet at the AS level, similar results can be obtained as shown in Fig. 5-8 [1]. The figure clearly demonstrates that random immunization does not give a rapid decrease of the prevalence of the ratio ρ_g / ρ_0, but the targeted immunization with a small effort (only 2% of total population is immunized) can lead to a drastic reduction of the ratio.

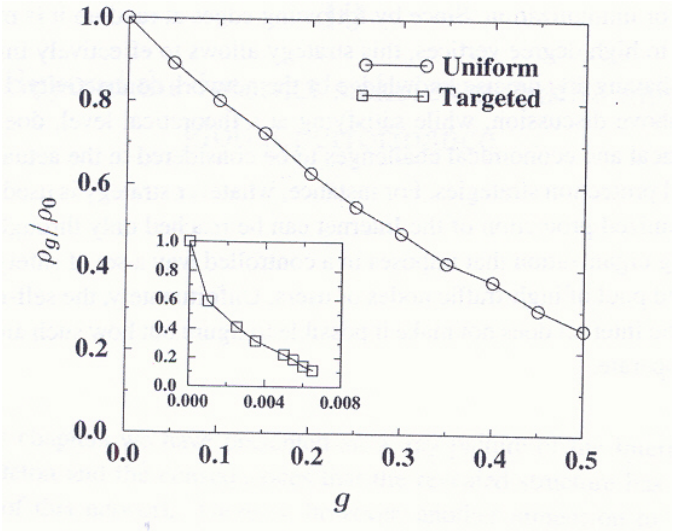


Fig. 5-8 Comparison of two immunization strategies on the AS-level Internet [1]

It should be remarked that while the targeted immunization strategy is very effective on scale-free networks, it requires precise knowledge of the network structure in order to identify and immunize the big nodes with large numbers of connections. This is obviously not practical, at least not desirable, in applications. Some remedies were therefore proposed, to use only local information available on the networks [19,20]. In the case of the Internet, users frequently install and upgrade their anti-virus software, so that their PCs can immune to the new computer viruses, which by nature is a localized immunization strategy. From a global point of view, however, due to the scale-free characteristic of the Internet, even when a large number of small nodes (PCs) have been immunized by their local anti-virus software, computer viruses spreading over the whole network still cannot be completely terminated in general.

5.3.3 Acquaintance Immunization

Acquaintance immunization is a localized strategy. The basic idea of acquaintance immunization is to randomly select a fraction f of nodes from the population of N nodes and then randomly select one of its neighbors for immunization [20]. This scheme only requires information about the randomly selected node and its neighbors, but not the global network. In a scale-free network, it is more likely a small node would be first selected at random, but then since most small nodes are connected to big nodes it is relatively easier to find a big node from among its neighbors to immunize. As a result, the immunization is much more efficient.

Figure 5-9 shows a comparison of the immunization threshold f_c in terms of the fraction f of nodes versus λ, for random, targeted and acquaintance immunization schemes on a scale-free network model [21], where the network size is $N = 10^6$. In the figure, empty circles correspond to random immunization; empty triangles, acquaintance immunization; empty diamonds, two-acquaintance (randomly select two neighbors) immunization; empty squares, targeted immunization. It can be seen that targeted immunization is better than acquaintance immunization, while they both are better than the random scheme. In the figure, solid circles and solid triangles represent the corresponding assortative networks, which show some but insignificant effects on the immunization strategies over the corresponding networks (marked by empty circles and empty triangles).

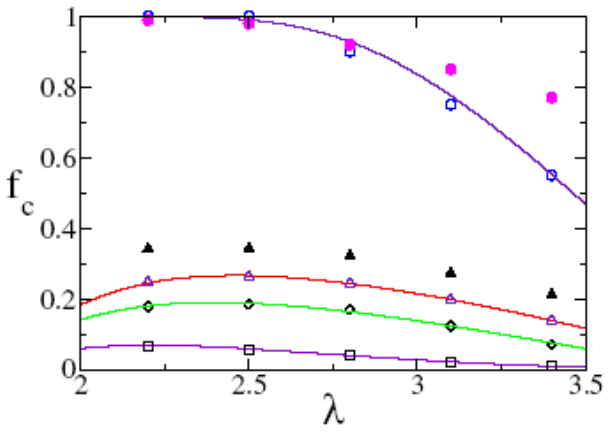


Fig. 5-9 Comparison of immunizations: threshold f_c versus λ [21]

5.4 Computer Virus Spreading over the Internet

Computer viruses are usually referred to as some small computer programs that can reproduce themselves by infecting other programs and computers, which continuously grow and spread out thereby messing up or even completely destroying the regular functioning of the computers and their programs. When a virus is active inside a computer, it is able to copy itself in many different ways into the codes of some programs of the computer. When the infected computer program is run into another computer, typically the code of the virus is executed first thus continues to infect other programs in the new computer. This process repeats endlessly, leading to the collapse of a local or even global network of computers eventually, causing tremendous technological and economical disasters.

Major computer viruses may be roughly classified into (i) boot-sector viruses, which infect the boot sectors of floppies and hardware devices, (ii) file viruses, which infect application programs, iii) macro viruses, which infect data files directly, as well as (iv) some hybrid types of viruses in a certain combination of these basic ones, for instance those aiming at some special technologies or applications such as Java, ActiveX, and HTML and so on. The first virus capable of infecting PCs was perhaps the Brain virus developed in Pakistan in 1986. Many viruses were born since then, and in year 2000 it was estimated that there were more than 48,000 identified viruses on the Internet [2].

Computer worms, on the other hand, are most aggressive cyber-organisms (larger and more sophisticated programs) with much more powerful abilities to attack computers. The first worm of this kind was found in 1999, named Melissa, which shut down the Internet e-mail systems that got clogged with infected e-mails propagating from the worm. In general, a worm is capable of sending itself to all e-mail addresses in the e-mail address book of the computer which received an infected e-mail. The worm will then be sent out by this computer in every e-mail. This makes worms very effective in spreading. One of the infamous worms was the I-Love-You bug, first discovered in Hong Kong, which infected more than 78 million computers worldwide in just four days in year 2000. Another extremely virulent worm is the Nimda worm found in 2001, which used multiple methods of infection to spread among both Windows server and user machines, including file infections, massive e-mails of infected attachments, web-server attacks, and even LAN propagation via shares. In about the same time, many more worms appeared, such as the well-known Lover Letter in 2000 and Sircam in 2001, which are among the most damaging ones. Today, many computer worms can quickly spread over different networks and make use of different protocols. The active worms, for example, do not rely on any user intervention to progagate, but can “guess” IP address to attack.

Therefore, understanding how computer viruses and worms are propagating over networks is extremely important for their prevention and control.

5.4.1 Random Constant Spread Model of the Code-Red Worm

The so-called random constant spread (RCS) model [22] is used to mimic the outbreak of the code-red worm, found in 2001, which attacked computers running Microsoft's IIS web servers.

The RCS model assumes that the worm had a good random number of generator which is properly seeded; the network size is fixed — ignoring both patching of systems during the worm spread and normal deploying and removing of systems or turning on-off of systems at nights, and ignoring any spread of the worm behind firewalls on provate Intranets.

Let K be the initial infection rate per hour, namely, the number of susceptible hosts which an infected host can find and attack at the start of the process when few other hosts were infected. It is assumed that this K is a constant, independent of the processor speed, bandwidth, network topology, and the locations of the infected nodes in the network, etc. Moreover, it is assumed that an infected node randomly picks another node to attack and that any node, once has been infected, will stay as is but cannot be infected again (at least, will not affect the rate of spreading).

Now, let N be the number of susceptible nodes, which is assumed to be constant, in the network and $a = a(t)$ be the proportion of infected nodes at time t. Then, since the rate of infection is K, an infected node will find and then infect a total of $K(1-a)$ nodes each time. Also, since the total number of infected nodes is Na, the rate of all nodes to be infected in the next short time duration dt will be $(Na)K(1-a)$, where N is a constant by assumption. Consequently, one has

$$\frac{d(Na)}{dt} = (Na)K(1-a)$$

or

$$\frac{da}{dt} = Ka(1-a) \tag{5-31}$$

which is the logistic equation, with solution

$$a = \frac{e^{K(t-t_0)}}{1+e^{K(t-t_0)}} \tag{5-32}$$

where t_0 is the initial time of the incident. It is clear from (5-32) that the infection rate $a \to 1$ as $t \to \infty$, implying that all nodes will eventually be infected.

Figure 5-10 [22] shows the hourly probe rate data for the inbound port 80 at the Chemical Abstracts Service in the USA, during the reemergence of the Code-Red-I on

August 1, 2002. It is clear that the above model can well predict the real situation.

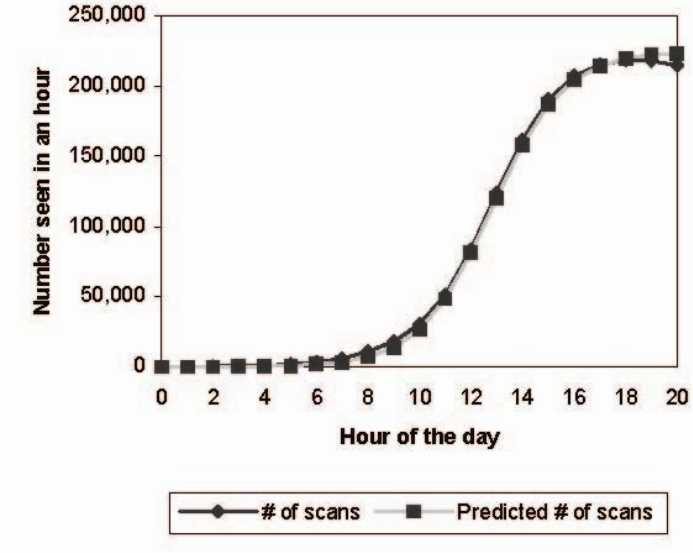


Fig. 5-10 Hourly probe rate data during the reemergence of Code-Red-I [22]

5.4.2 A Compartment-Based Model of Computer Worms

Many new types of worms propagate extremely fast on the Internet, such as those named “Flash”, “Warhol” and the “Slammer” found in 2003 which, within the first 10 minute, already attacked 90% of vulnerable hosts running Microsoft’s SQL servers or MSDE (MS Desktop Edition) 2000 that had buffer overflow vulnerability. In comparison, Code Red would need about 37 minutes to damage the same number (about 75,000) of hosts.

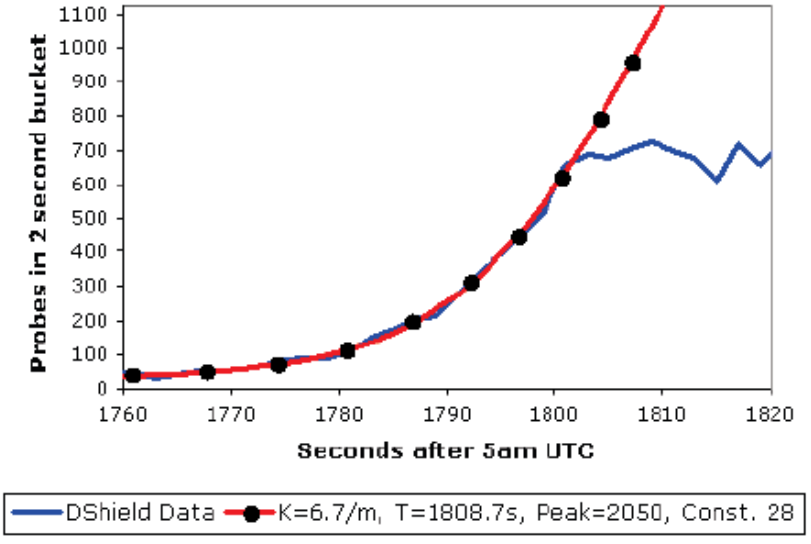


Fig. 5-11 Slammer worm growth: real data versus model prediction [23]

Since the spread of the Slammer worm is based on random scanning, in theory the RCS model discussed in the previous subsection should be appropriate for its description. However, as can be seen from Fig. 5-11 [23], real data on 19 July 2001 show that the model is good only in the beginning stage of the process but then

significantly differs from the data after some time because the data are saturated. More precisely, Fig. 5-11 shows the total number of times that Slammer scanned the network. In about three minutes, the worm reached its maximum scanning speed but then suddenly slowed down. One explanation is that the majority of computers on the real network do not have enough bandwidths for the worm to continue to propagate exponentially, therefore sooner or later it will become saturated.

Notice that the Slammer distinguishes itself from the Code Red in the transmission mechanism: the exploit used by Slammer was based on the UDP (User Datagram Protocol) while Code Red is based on the TCP (Transition Control Protocol). The former offers a limited amount of services when messages are exchanged between computers (network limited); while the latter is a connection-oriented which creates and maintains connections until the time at which the messages to be exchanged by the application programs at each end have been exchanged (latency limited).

In order to better describe the spreading pattern of worms like Slammer, a model that can reflects the bandwidth limitation on the real Internet is desirable. This consideration led to a new model called *compartment-based mode*, used to describe the spreading over the AS-level Internet [23].

Suppose that inside a single AS (or a densely connected region of an AS) on the Internet a worm propagates unhindered, for which the RCS model discussed in the previous subsection could be used. Let N_i be the number of susceptible hosts in the i th AS, denoted as AS_i, and a_i be the proportion of the infected hosts among them. Let also K be the average rate of spreading spread, which is assumed a constant in each AS_i, and let $P_{IN,i}$ be the probability of a host infects another host inside the same AS_i and $P_{OUT,i}$ be the probability of a host in AS_i infects a host in another AS. The following equation describes the internal and external worm infection on AS_1 in a simple system with only two AS:

$$N_1 da_1 = \left[\underbrace{N_1 a_1 K P_{IN,1} dt}_{Internal} + \underbrace{N_2 a_2 K P_{OUT,2} dt}_{External} \right] (1 - a_1)$$

The equation about AS_2 is similar. Thus, the system describing both of the two AS can be established by combining them together, as

$$da_1 / dt = \left[a_1 K P_{IN,1} + \frac{N_2}{N_1} a_2 K P_{OUT,2} \right] (1 - a_1)$$

$$da_2 / dt = \left[a_2 K P_{IN,2} + \frac{N_1}{N_2} a_1 K P_{OUT,1} \right] (1 - a_2)$$

Assuming that the worm randomly generate or select an IP address from the network, one has $P_{IN,i} = N_i / N$ and $P_{OUT,i} = 1 - P_{IN,i} = N_j / N$, $j \neq i$, yielding

$$da_i / dt = \left[a_i K \frac{N_i}{N} + \sum_{\substack{j=1 \\ j \neq i}} \frac{N_j}{N_i} a_j K \frac{N_i}{N} \right] (1 - a_i), \quad i = 1, ..., N$$

namely,

$$da_i / dt = \left[a_i K \frac{N_i}{N} + \sum_{\substack{j=1 \\ j \neq i}} \frac{N_j}{N} a_j K \right] (1 - a_i), \quad i = 1, ..., N \tag{5-33}$$

This system of nonlinear ordinary differential equations shows that in AS_i, the worm spreads inside the AS following the RCS model for a certain period of time, until it reaches out to infect another AS. This system can be solved numerically and, under some further realistic assumptions and approximations, a simulated solution curve is shown in Fig. 5-12 [23]. From the figure, one can see the sudden stop and gradual decay of the attack rate (worm growth rate), matching the real data curve shown in Fig. 5-11 quite well at least in shape.

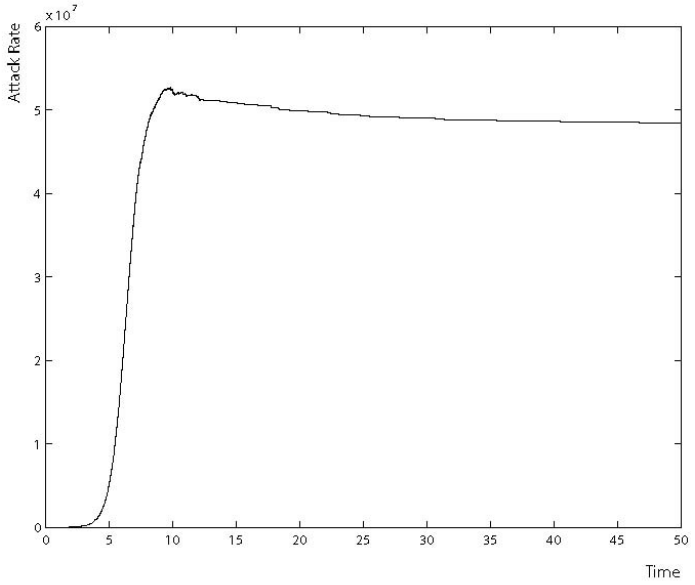


Fig. 5-12 Simulated worm attack rate [23]

5.4.3 Spreading Models of Email Viruses

Email is the most common service and application of the Internet. In fact, most Internet hosts run email services that manage the addresses in their respective domains, therefore any email service can use the domain name system of the Internet to retrieve the IP address of any other email server, connects to that server, and then transfer emails to the intended receivers in that domain via some standard communication protocols.

The wide connection of the Internet and convenience of email communications, on the other hand, enable viruses to spread out extremely easily by attaching themselves to emails. Since emails are private matters and email users usually trust their partners therefore keep and forward most, if not all, emails that they had received to other partners, email viruses were out-breaking frequently and severely in the past. Typical examples include the Milessa (1999), I-Love-You (2000), Nimda (2001), Win32/Sircam (2001), the Chinese versions of Worm.Klez.cn.b (2002) as well as Worm.SoBig.c and Worm.Mimail.C (2003), and SCO bomb (2004), etc.

To understand the topological characteristics of the email networks, a report on the

investigation of the email service in the Kiel University, Germany in 2002 shows that this campus email network with $N = 59{,}812$ nodes (including 5165 student accounts) has an average degree $\langle k \rangle = 2.88$, one giant cluster with 56,969 nodes and several small clusters with 150 nodes or less, following a power-law degree distribution $k^{-\gamma}$ with exponent $\gamma = 1.81$, as shown in Fig. 5-13 [24].

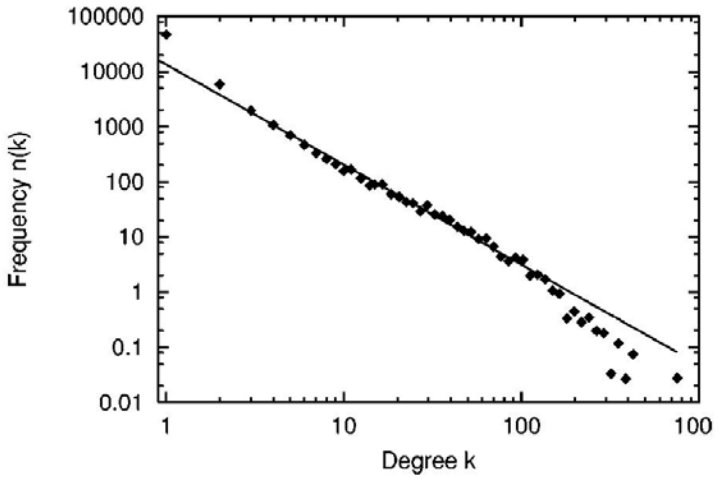


Fig. 5-13 Node-degree distribution of email network in Kiel University in 2002 [24]

In another study [25], in order to model a local email network, consider it as a undirected graph with two major factors of viruses on email usage: Let T_i be the email checking time of user i, $i = 1,2,..., |V|$, which itself is a random variable denoted by T; let P_i be the probability of opening the incoming email attachment, $i = 1,2,..., |V|$, which itself is a random variable denoted by P, where $|V|$ is the total number (volume) of emails, which is a very large integer in general.

Assume that all users behave independently, for example, they are checking their emails independently; each checking time T_i of user i is exponentially distributed with a mean $E[T_i]$; and T and P are independent Gaussian random variables with $T \sim N(\mu_T, \sigma_T^2)$ and $P \sim N(\mu_P, \sigma_P^2)$.

An email is said to be infected once the user opens a virus-infected email attachment. Let N_0 be the number of initially infected users who send out virus-contaminated emails to their neighbors. Let N_t be the number of infected users at time t during the virus propagation process, thus $N_0 \le N_t \le |V|$ for $t \ge 0$. Assume that the email transmission time is neglected.

In simulations, consider the above email network model with $N = 100{,}000$ and $\langle k \rangle = 8$. Following a set of real data on 800,000 Yahoo emails, which as a local network has a power-law node-degree distribution with exponent $\gamma = 1.7$, using the above model with $T \sim N(40,400)$, $P \sim N(0.5,0.09)$, $N_0 = 2$ to perform some simulations. The simulations are concerned with the average number of infected users, $E[N_t]$, for the measures of reinfection, initially infected nodes, network topology and

email checking time, etc., where each $E[N_t]$ is obtained by averaging 100 repeated simulations.

Reinfection versus Non-Reinfection

Reinfection means that a user will send out virus-contaminated emails whenever he/she opens a virus-contaminated email attachment. Thus, a receiver may repeatedly receive virus-contaminated emails from the same infected user. The W32/Sircam is one example of this reinfection mechanism. Non-reinfection, on the other hand, means that each infected user sends out virus-contaminated emails once only, after which he/she will not send out any virus-contaminated emails if he/she opens a virus-contaminated email attachment again. Melissa and Love Letter are two examples of this non-reinfection mechanism.

Figure 5-14 shows that in the case of reinfection, more users are being infected since the users receive more virus-contaminated emails [25].

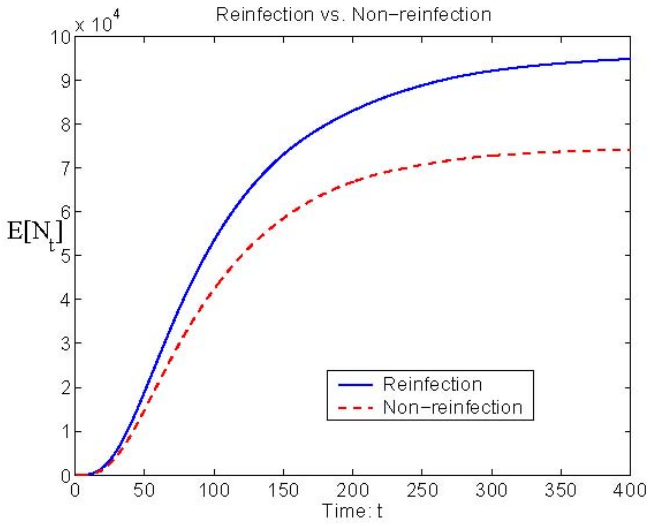
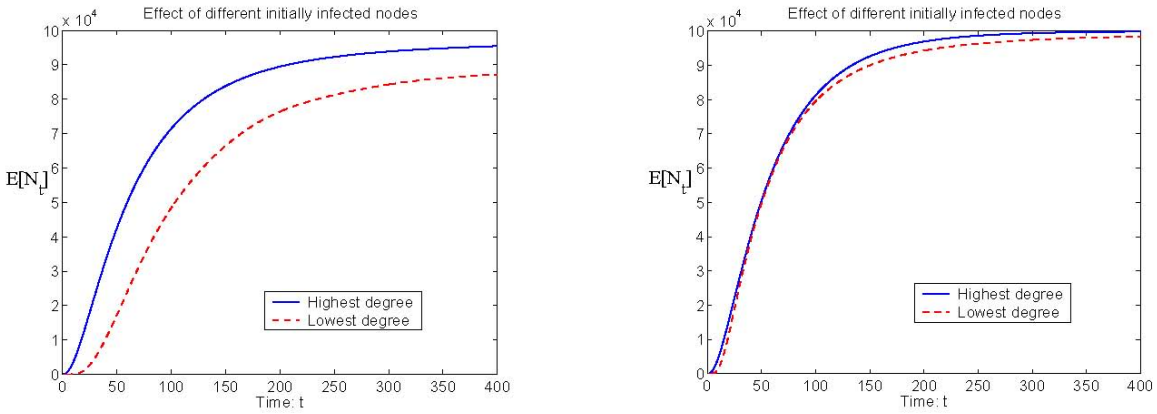


Fig. 5-14 Comparison of $E[N_t]$ between reinfection and non-reinfection [25]

Initially Infected Users with Large and Small Node Degrees

Figure 5-15 [25] compares the average numbers of infected users, $E[N_t]$, for two networks with $\langle k \rangle = 8$ and $\langle k \rangle = 20$, respectively. It shows that the initially infected nodes are more important in a sparsely connected network (with $\langle k \rangle = 8$) than a densely connected network (with $\langle k \rangle = 20$) of the same size and the same type.



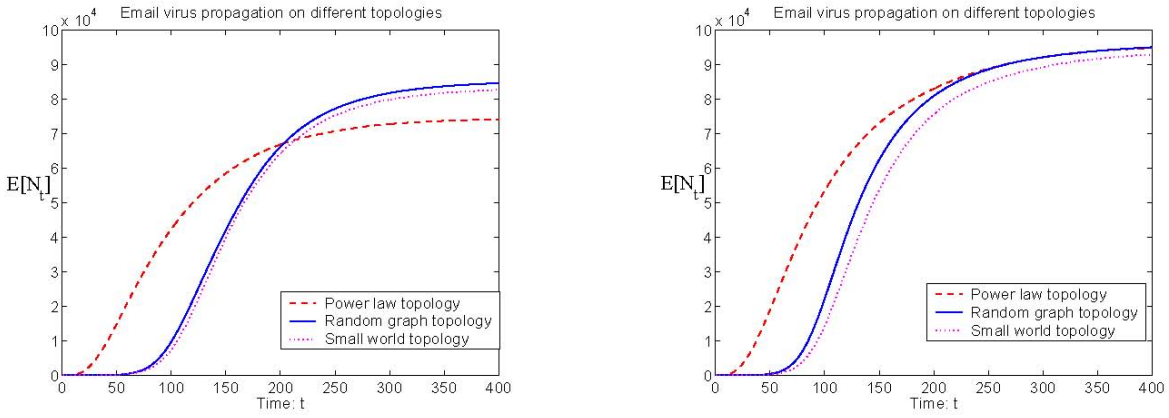
a. Network with average degree 8

b. Network with average degree 20

Fig. 5-15 Comparison of $E[N_t]$ between different initial conditions [25]

Topological Effects: Random-Graph, Small-World and Scale-Free Networks

Figure 5-16 [25] compares the behaviors of email virus propagation over networks with different topologies: random-graph, small-world and scale-free networks, all on networks of 100,000 nodes with the same average degree $\langle k \rangle = 8$. In this study, the power-law network has the highest degree 1833 and lowest degree 3, with exponent $\gamma = 1.7$. Figure 5-16 shows that email virus propagation patterns over random-graph and small-world networks are similar, implying that the main factor on the propagation is the short average path-length characteristic but not the clustering coefficient of the network. On the other hand, email virus seems to propagate much faster in scale-free networks than the other two, because an infected large node will send out more virus-contaminated emails. Since in the scale-free network, most nodes have degree lower than the average value, they are not easy to be infected, therefore eventually the scale-free network has less nodes being infected as compared to the other two models.



a. Non-reinfection case

b. Reinfection case

Fig. 5-16 Comparison of $E[N_t]$ between networks in different topologies [25]

Effect of the Power-Law Exponent

For scale-free networks with different power-law exponents, the average numbers of infected nodes, $E[N_t]$, have different behaviors, as shown in Fig. 5-17. Since the network with a smaller exponent has more big nodes, the speed of being infected is faster. The two curves show that big nodes are like "virus amplifiers" in email virus propagation at the beginning. However, after most big nodes have been infected, the virus spreading process quickly enters a second phase of propagation to infect small nodes, where the network with a smaller exponent has more small nodes therefore the speed of being infected becomes lower.

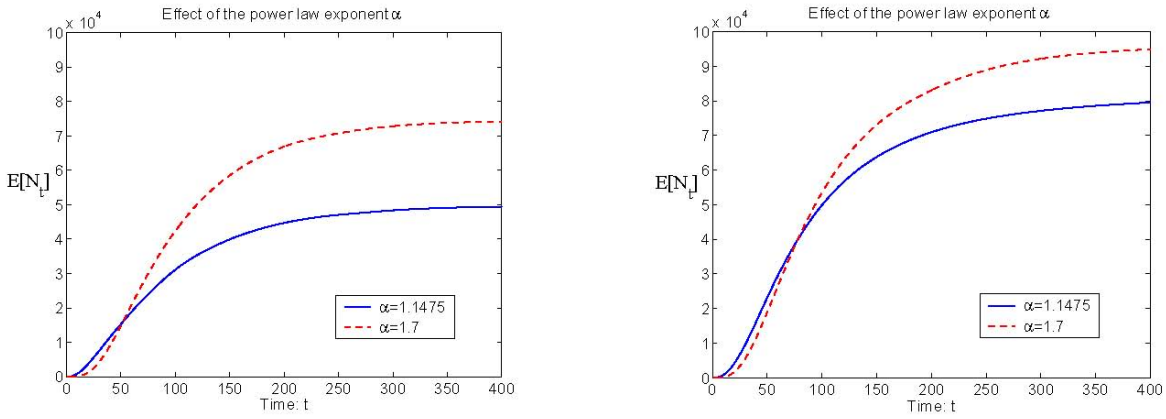


Fig. 5-17 Effect of exponent γ $(=\alpha)$ on $E[N_t]$ [25]

Effects of the Email Checking Time

By changing the distribution of the email checking times, different effects on the average number of infected nodes may vary. Figure 5-18 shows a comparison of the effects on $E[N_t]$ by different distributions of the checking times: exponential, Erlang, and constant (uniform) [25]. It is clear that the more variable the distribution, the faster the virus propagation.

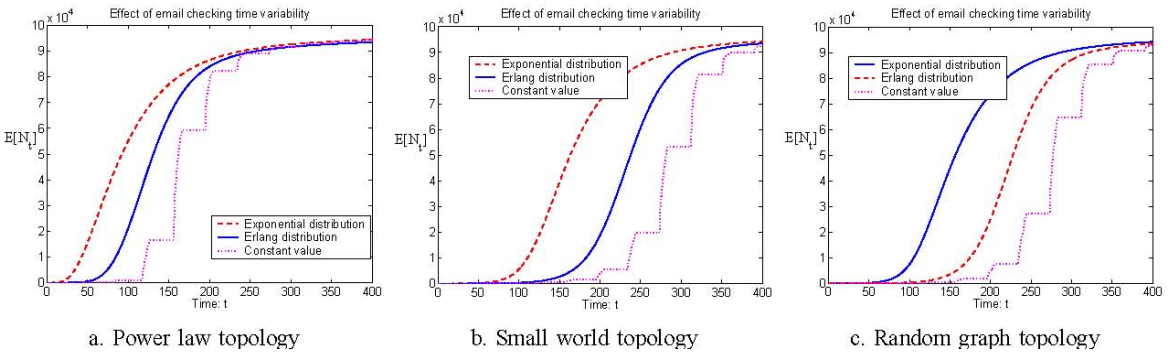


Fig. 5-18 Effects of different checking-time distributions on $E[N_t]$ [25]

It should be noted that the above model of email virus propagation is not entirely realistic. For instance, it assumes that the probability P_i of opening an email attachment by user i is constant. Actually, many knowledgeable and experienced users can identify virus-contaminated email attachments and delete them right away. Although non-experienced users would always open the attachments with probability 1, most of them can learn and gradually become experienced. This means that the probability should not be a constant in reality.

Finally in this subsection, the random SHIR model for email virus spreading is briefly introduced, where emails are processed through four states: Susceptible (S), Hidden (H), Infectious (I), and Recovered (R) [26]. Figure 5-19 compares the email virus propagation of the SHIR model on a scale-free network, where the horizontal axis is the time (unit: day) and the vertical axis is the number of infected nodes. Here, the comparison is given to both closed and open systems, where the closed system restricts emails to travel only inside a community of users while the open system allows emails to be sent to users in other communities. It can be seen that in the closed system, the numbers of nodes in hidden and infected states increase quickly at the beginning but then decay and die out also rapidly. In the open system, however, these numbers are fluctuating and oscillating, showing no sign of convergence.

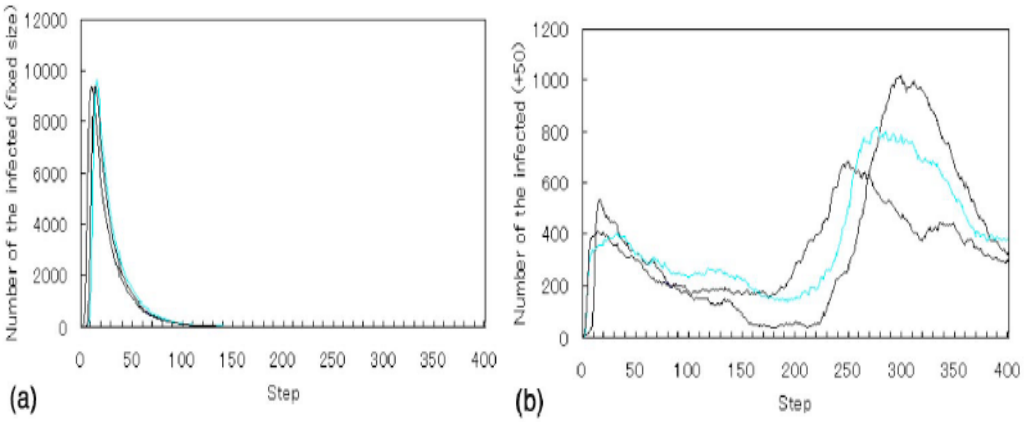


Fig. 5-19 Email virus propagation in the SHIR model [26]
(a) closed system (b) open system

5.4.4 Effects of Computer Virus on Network Topologies

It has been seen that network topologies significantly affect the virus spreading patterns over the networks. On the contrary, when a computer virus propagates over a network, it traverses part of the network therefore could affect the topology of this part of the network as the medium of virus spreading [27]. Of course, another part of the network over which the virus never travels will be left unchanged. In most cases, the topology of the virus-traveling network is determined by the spread and replication of virus. Most viruses and worms spread through different formats at different rates to different extents, which often change the spreading-path topologies on the underlying networks quite significantly.

For a more precise discussion, consider the following four types of technological

networks, all vulnerable to attacks:

A. a network of computers connected via Internet Protocol (IP);

B. a network of shared administrator accounts for desktop computers;

C. a network of email address books;

D. a network of email messages mutually sending among different users.

Network A is the IP network, where each computer has a 32-bit IP address and there is a routing infrastructure that supports communications between any two addresses. Consider IP addresses as nodes on the network. It is known that many computer worms such as Nimda and Slammer can spread over this IP network.

Network B is a product of the common operating-system feature that allows computer system administrators to read and write data on the disks of networked machines. Some worms like Nimda and Bugbear can spread by self-copying from disk to disk over this network.

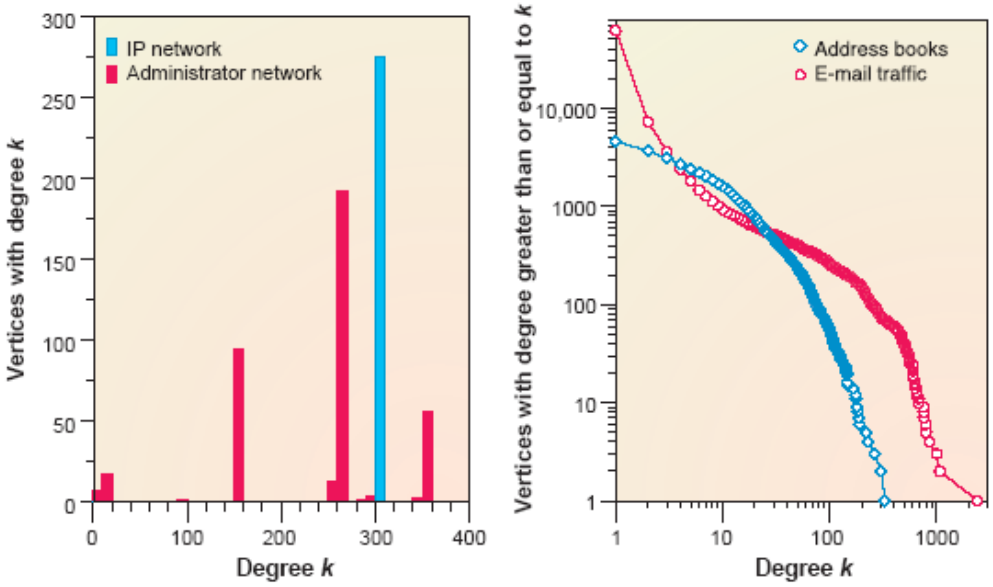
Network C is a directed graph with nodes representing users and a connection between two users exists if one user's email address appears in another's address book. Many email viruses such as I-Love-You use address books to spread, so can spread over this network.

Network D is an undirected version of network C, in which nodes represent computer users and two users are connected if they have exchanged emails recently. Some viruses like Klez can spread over this network.

Figure 5-20 (a) shows the node-degree distributions of networks A and B on a system with 518 users and 382 machines, while (b) shows the cumulative degree distributions of networks C and D, with data collected from a large university and plotted in log-log scale. In network A, all nodes have the same degree, so its distribution is a discrete delta (the highest histogram), while in network B the distribution consists of several discrete peaks corresponding to different classes of computers, administrators, or administrative strategies (the short histograms). It can be seen that networks C and D do not follow power-laws but instead have long tails showing the heterogeneity of their topologies. This implies that targeted immunization may be effective for these two types of email networks. In fact, calculation shows that the epidemic threshold of targeted immunization is 0.1 on network C and 0.8 on network D.

In the above four types of networks, different virus replication and spreading patterns may lead to their different traveling-path topologies on the underlying networks. Therefore, it is desirable to have a control strategy that is immune to the change in network topology and thus does not require any knowledge of infections before an outbreak. Such a control strategy has to be highly effective against malicious infections but harmless to normal activities. The so-called throttling scheme is one of such control strategies [28], which limits the number of new connections a computer can make to other computers in a given period of time, thereby limiting the spreading rates of the viruses if they appear. Although this scheme does not completely

eliminate infections, it works quite well to render a virus harmless or make it be easily controlled by other means.



(a) node-degree distributions of A, B; **(b)** cumulative degree distributions of C, D

Fig. 5-20 Four types of networks [27]

5.5 Other Spreading Phenomena on Complex Networks

There are many natural and social phenomena that behave like computer virus spreading on complex networks. Rumors spreading, social opinions formation, languages evolution, human and animal epidemics, man-made systems (such as power grids) cascading failures, and so on, are just some of the most familiar ones. In this section, a couple of representative such examples are briefly discussed.

5.5.1 Rumors Spreading over Social Networks

Rumors spread over human communities in a way very similar to computer viruses propagation, which can also be described by an SIR epidemic propagation model.

A human communication network is more likely a small-work network. Let n_S, n_I and n_R be the numbers of susceptible (never heard the rumor), infected (heard the rumor) and recovered (no longer believe the rumor) individuals in a community of N individuals. Assume, for simplicity, that any susceptible individual will be infected if he/she has contact with an infected individual, and that any infected individual will become recovered if he/she has contact with a recovered individual. Thus, a mean-field SIP model can be derived, as described by [29]

$$\begin{cases} \dot{n}_S = -n_S \dfrac{n_I}{N} \\ \dot{n}_I = n_S \dfrac{n_I}{N} - n_I \dfrac{n_I + n_R}{N} \\ \dot{n}_R = n_I \dfrac{n_I + n_R}{N} \end{cases} \tag{5-34}$$

As the rumor spreads out, the community will be divided into two groups: individuals who heard the rumor but then became recovered, n_R; individuals who never heard the rumor, n_S. Thus, as $N \to \infty$, the ratio $r = \dfrac{n_R}{N} \to r^* \approx 20\%$ in a simulation, which implies that in a large community, only about $\dfrac{1}{5}$ people would hear a rumor but the rumor will die out eventually.

Computer simulation on a NW small-world network model, starting from a K-neighboring ring (Section 4.3.2, Chapter 3), shows that when the rewiring probability is below a threshold probability, $p < p_c$, the ratio $r = \dfrac{n_R}{N}$ will decay to zero; while if $p > p_c$, one has $r \sim |p - p_c|^{\beta}$, where p_c decreases as K increases but $\beta \approx 2.2$ is constant.

Studies [29] seem to indicate that when n_R is small, the correlation of n_R and n_I, as well as the correlation of n_R and the extinction time T, have a power-law form; yet when n_R is very large, if p increases and T decreases, then both n_I and n_R increase, implying that rumor spreads out very effectively.

Another model divides a human community into Ignorants (never heard the rumor, similar to Susceptible), Spreaders and Stiflers (heard the rumor but did not believe it), in different proportions represented by $i(t)$, $s(t)$ and $r(t)$, respectively. The model employs the following mean-field equation [30]:

$$\begin{cases} \dfrac{di(t)}{dt} = -\lambda \langle k \rangle i(t) s(t) \\ \dfrac{ds(t)}{dt} = \lambda \langle k \rangle i(t) s(t) - \alpha \langle k \rangle s(t) \left[s(t) + r(t) \right] \\ \dfrac{dr(t)}{dt} = \alpha \langle k \rangle s(t) \left[s(t) + r(t) \right] \end{cases} \tag{5-35}$$

where $\lambda \langle k \rangle$ is the probability of an Ignorant being infected when he/she meets a Spreader, and $\alpha \langle k \rangle$ is the probability of a Spreader becomes a Stifler when he/she meets a Stifler (or a Spreader). In this model, however, there is no nonzero threshold of rumor propagation rate.

Further extending the above rumor-spreading dynamical system to a heterogeneous network yields the following mean-field equations [30]:

$$\begin{cases} \dfrac{di_k(t)}{dt} = -\lambda k i_k(t) \displaystyle\sum_{k'} \frac{k'P(k')s_{k'}(t)}{\langle k \rangle} \\ \dfrac{ds_k(t)}{dt} = \lambda k i_k(t) \displaystyle\sum_{k'} \frac{k'P(k')s_{k'}(t)}{\langle k \rangle} - \alpha k s_k(t) \sum_{k'} \frac{k'P(k')\left[s_{k'}(t)+r_{k'}(t)\right]}{\langle k \rangle} \\ \dfrac{dr_k(t)}{dt} = \alpha k s_k(t) \displaystyle\sum_{k'} \frac{k'P(k')\left[s_{k'}(t)+r_{k'}(t)\right]}{\langle k \rangle} \end{cases} \quad (5\text{-}36)$$

where $i_k\langle t\rangle, s_k\langle t\rangle, r_k\langle t\rangle$ are the proportions of Ignorants, Spreaders and Stiflers in a group of degree-k individuals, respectively. This system leads to a conclusion that the stead-state value of $r(t)$ depends on the infection rate $\alpha\langle k\rangle$ and is independent of the node-degree of the rumor source node. This, however, is very different from virus-spreading SIR models where the number of eventually recovered individuals is correlated with the degree of the virus source node.

5.5.2 Some Generalized Models of Spreading Dynamics

Biological, social and technological data-spreading models might be categorized into two classes: Poisson model and Threshold model, where in the former the spreading via continuous contact is independent of the contact probability, while in the latter there is a threshold over which the infection rate will explode. The classical SIR models belong to the former, and all models discussed in Section 5.2 above belong to the latter. Noticing that these two types of models both ignore the exposure of infected individuals to the others, a generalized model was proposed as follows [31].

Consider a population of N individuals (nodes), where each node is in the S, I or R state. At each time t, node i randomly connects to node j via contact. If node i is in S state and j in I state, then with probability p node i will receive an amount of infection, $d_i(t) > 0$, where all $\{d_i(t)\}$ have a distribution $f(d)$. Every node retains the total amount of infection received in the past time duration T, which equals

$$D_i(t) = \sum_{t'=t-T+1}^{t} d_i(t') \quad (5\text{-}37)$$

When $D_i(t) > d_i^*$, a threshold, node i will be infected. During the time period of T, the probability of S-state nodes being infected through contact with K ($K \le T$) I-state nodes is

$$P_{\inf}(K) = \sum_{k=1}^{K} \binom{K}{k} p^k (1-p)^{K-k} P_k \quad (5\text{-}38)$$

During this time period of T, the average number of nodes who received k times of infections is

$$P_k = \int_0^\infty g(d^*) P\left(\sum_{i=1}^{k} d_i \ge d_i^* \right) dd^* \quad (5\text{-}39)$$

where $g(d^*)$ is the distribution function of the amount threshold d_i^*, and $P\left(\sum_{i=1}^{k} d_i \geq d_i^*\right)$ is the probability of the sum of k amounts being larger than the corresponding threshold.

When $d_i = d_i^* = \bar{d}$ and $p < 1$, equation (5-38) reduces to that of the classical SIR model, as shown in Fig. 5-21 (a), where when $p = 1$ and $d^* > \bar{d}$, the change of $d_i(t)$ determines whether equation (5-38) is stochastic (Fig. 5-21 (b)) or deterministic (Fig. 5-21 (c)). Clearly, by choosing appropriate functions $f(d)$ and $g(d^*)$, equation (5-38) covers even more models for virus spreading.

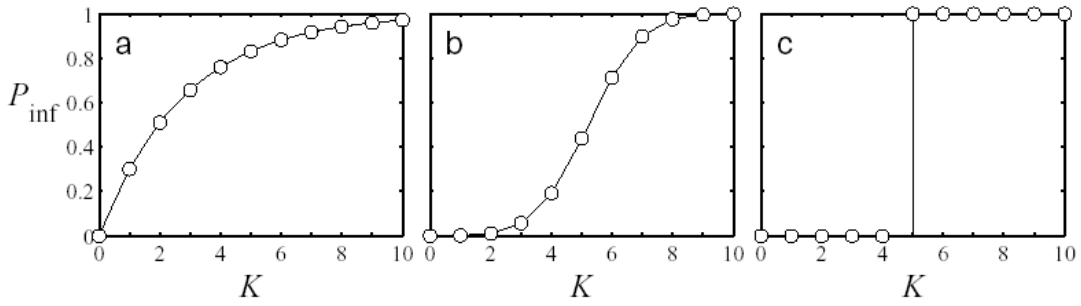


Fig. 5-21 Three cases of the generalized spreading model [31]

When $D_i(t) < d^*$, the infected nodes will "recover" with probability r, but the recovered nodes can still be infected again, with probability ρ. This means that the ISI mode is a special case of the above generalized virus spreading model with $r = 1$ and $\rho = 1$. Therefore, the equilibrium value (fixed point) ϕ^* of the infected nodes in the population satisfies the following equation:

$$\phi^* = \sum_{k=1}^{T} \binom{T}{k} \left(p\phi^*\right)^k \left(1 - p\phi^*\right)^{T-k} P_k \tag{5-40}$$

Let P_1 and P_2 be the probability that a node will be infected as the result of one exposure and that of two exposures, respectively. Simulations show that when $P_1 \geq P_2/2$, the generalized model has a stability change (i.e., bifurcation) at the (bifurcation) point $p_c = (1/TP_1) < 1$: for $p \leq p_c$, the fixed point ϕ^* is stable, while for $p > p_c$, it is unstable in the sense that $\phi^* > 0$, implying the epidemic is spreading out. The existence of p_c means that the generalized model is equivalent to an SIR model, called the Epidemic Threshold Model, whose fixed point curve is shown in Fig. 5-22 (a). Similarly, when $P_2/2 > P_1 \geq 1/T$ and $1/T > P_1$, the generalized model is referred to as the Vanishing Critical Model or Pure Critical Mass Model, whose fixed point curves are shown in Figs. 5-22 (b) and (c), respectively.

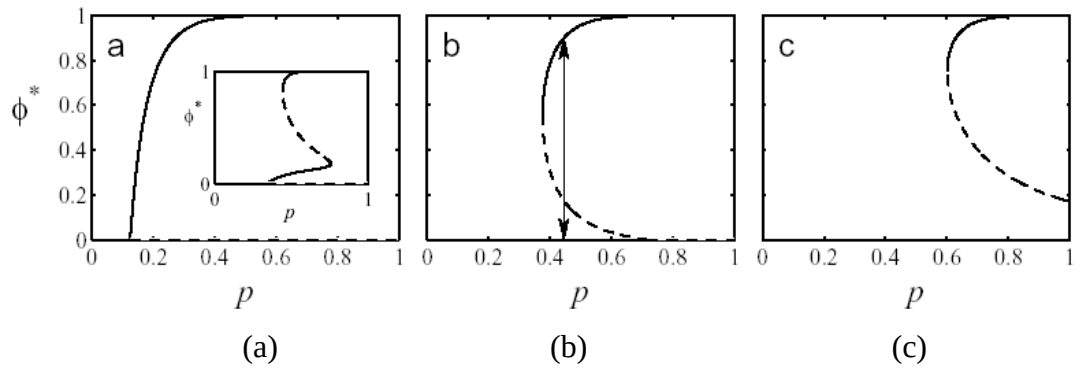


Fig. 5-22 Fixed point curves for three contagion models [31]

Analysis shows that the individuals in the group corresponding to P_1 are much easier to be infected as compared to other individuals in the population, and they are responsible for the virus spreading over the whole population [31].

5.6 Spreading Dynamics on Complex Networks

The spreading threshold theory only considers the steady state, namely the asymptotic behaviors, of the spreading process, leaving alone the complex dynamics existing in the process such as oscillations, bifurcations and even chaos. These complex dynamics and their regulation and control are oftentimes very important in understanding and prevention of virus spreading over complex networks, therefore have been extensively studied in the literature [32-39]. A brief overview of these topics can be found in, e.g., [40], and some recent progress can be found in, e.g., [41].

References

[1] http://www.avira.com/en/threats/section/wildlist_intro/index.html

[2] Pastor-Satorras R, Vespignani A. Evolution and Structure of the Internet. Cambridge: Cambridge University Press, 2004.

[3] Pastor-Satorras R, Vespingnani A. Epidemic spreading in scale-free networks. *Phys. Rev. Lett.*, 2001, 86(4): 3200-3203

[4] Bailey N T J. The Mathematical Theory of Infectious Diseases and Its Applications. New York: Hafner Press, 1975

[5] Anderson R M, May R M. Infectious Diseases in Humans. Oxford: Oxford University Press, 1992

[6] Diekmann O, Heesterbeek J A P. Mathematical Epidemiology of Infectious Disease: Model Building, Analysis and Interpretation. John Wiley & Son publisher, 2000

[7] Pastor-Satorras R, Vespignani A. Epidemics and immunization in scale-free networks. In *Handbook of Graphs and Networks*, Bornholdt S., Schuster H. G. (eds.), WILE-YVCH publisher, 2003

[8] Pastor-Satorras R, Vespignani A. Epidemic dynamics and endemic states in complex networks. *Phys. Rev. E,* 2001, 63: 066117

[9] Pastor-Satorras R, Vespignani A. Epidemic dynamics in finite size scale-free networks. *Phys. Rev. E*, 2002, 65: 035108

[10] Boguñá M, Pastor-Satorras R. Epidemic spreading in correlated complex networks. *Phys. Rev. E*, 2002, 66: 047104

[11] Moreno Y, Gómez J B, Pacheco A F. Epidemic incidence in correlated complex networks. *Phys. Rev. E*, 2003, 68: 035103

[12] Moreno Y, Pasto-Satorres, Vespignani A. Epidemic outbreaks in complex heterogeneous networks. *Eur. Phys. J. B*, 2002, 26: 521-529

[13] May R M, Llod A L. Infection dynamics on scale-free networks. *Phys. Rev. E*, 2001, 64: 066112

[14] Neuman M E J. Spread of epidemic diseases on networks. *Phys. Rev. E,* 2002, 64: 016128

[15] Volchenkov D, Volchenkova L, Blanchard Ph. Epidemic spreading in a variety of scale free networks. *Phys. Rev. E,* 2002, 66: 046137

[16] Liu Z H, Lai Y C, Ye N. Propagation and immunization of infection on general networks with both homogeneous and heterogeneous components. *Phys. Rev. E*, 2003, 67: 031911

[17] Liu J Z, Wu J S, Yang Z R. The spread of infectious disease on complex networks with household-structure. *Physica A*, 2004, 341: 273-280

[18] Pastor-Satorras R, Vespignani A. Immunization of complex networks. *Phys. Rev. E*, 2001, 65: 036134

[19] Dezsö Z, Barabási A L. Halting viruses in scale-free networks. *Phys. Rev. E*, 2002, 65: 055103

[20] Cohen R, Havlin S, Ben-Avraham D. Efficient immunization strategies for computer networks and populations. *Phys. Rev. Lett*., 2003, 91: 247901

[21] Madar N, Kalisky T, Cohen R, *et al*. Immunization and epidemics dynamics in complex networks. *Eur. Phys. J. B*, 2004, 38: 269-276

[22] Staniford S, Paxson V, Weaver N. How to own the Internet in your spare time. *Proceedings of the 11th USENIX Security Symposium*, August 2002, 149-167

[23] Serazzi G, Zanero S. Computer virus propagation models. *Performance Tools and Applications to Networked Systems, Lecture Notes in Computer Science*, Vol.

2964, 2004, 26-50.
[24] Ebel H, Mielsch L-I, Bornholdt S. Scale-free topology of e-mail networks. *Phys. Rev. E*, 2002, 66: 035103
[25] Zou C C, Towsley D, Gong W B. Email virus propagation modeling and analysis. Technical Report TR-CSE-03-04, University of Massachusetts, Amherst 2003
[26] Hayashi Y, Minoura M, Matsukubo J. Oscillatory epidemic prevalence in growing scale-free networks. *Phys. Rev. E*, 2004, 69: 016112
[27] Balthrop J, Forrest S, Newman M E J, Williamson M M. Technological networks and the spread of computer viruses. *Science*, 2004, 304: 527-529
[28] Williamson M M. Resilient infrastructure for network security. *Complexity*, 2004, 9: 34-40
[29] Zanette D H. Dynamics of rumor propagation on small-world networks. *Phys. Rev. E*, 2002, 65: 041908
[30] Moreno Y, Nekovee M, Pacheco A F. Dynamics of rumor spreading in complex networks. *Phys. Rev. E*, 2004, 69: 066130
[31] Dodds P S, Watts D J. Universal behavior in a generalized model of contagion. *Phys. Rev. Lett.*, 2004, 92: 218701
[32] Barthelemy M, Barrat A, Pastor-Satorras R, *et al*. Velocity and hierarchical spread of epidemic outbreaks in complex networks. *Phys. Rev. Lett.*, 2004, 92: 178701
[33] Newman M E J, Watts D J. Scaling and percolation in the small-world network model. *Phys. Rev. E*, 1999, 60: 7332-7342
[34] Moukarzel C F. Spreading and shortest paths in systems with sparse long-range connections. *Phys. Rev. E*, 1999, 60(6): R6263
[35] Yang X S. Chaos in small-world networks. *Phys. Rev. E*, 2001, 63: 046206
[36] Yang X S. Fractals in small-world networks with time-delay. *Chaos, Solitons & Fractals*, 2002, 13: 215-219
[37] Li C G, Chen G. Local stability and Hopf bifurcation in small-world delayed networks. *Chaos, Solitons & Fractals*, 2004, 20: 353-361
[38] Li X, Chen G, Li C G. Stability and bifurcation of disease spreading in complex networks. *International Journal of Systems Science*, 2004, 35: 527-536
[39] Ramani A, Carstea A S, Willox R, Grammaticos R, Affiliation, B. Oscillating epidemics: a discrete-time model. *Physica A*, 2004, 333: 278-292
[40] Li X, Chen G. Models, dynamics, and control of spreading in complex networks: A survey. *Dynamics of Continuous, Discrete and Impulsive Systems, Series B*, 2006, 13: 109-116
[41] Schwarz I B, Shaw L B. Rewiring for adaptation. *Physics*, 2010, 3: 17

