Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 462747, 13 pages
doi:10.1155/2012/462747

*Research Article*

# Toward a Practical Technique to Halt Multiple Virus Outbreaks on Computer Networks

**Kjell Jørgen Hole**

*Department of Informatics, University of Bergen, PB 7803, 5020 Bergen, Norway*

Correspondence should be addressed to Kjell Jørgen Hole, kjell.hole@ii.uib.no

Received 30 March 2012; Accepted 23 October 2012

Academic Editor: Khoa Le

The author analyzes a technique to prevent multiple simultaneous virus epidemics on any vulnerable computer network with inhomogeneous topology. The technique immunizes a small fraction of the computers and utilizes diverse software platforms to halt the virus outbreaks. The halting technique is of practical interest since a network's detailed topology need not be known.

## 1. Introduction

Malicious software, or malware, on the Internet can cause serious problems, not only for services like email and the web, but for electricity, transport, finance, and healthcare services due to their increasing Internet dependence. Infectious malware like viruses and worms are especially troublesome as they often spread too fast for human-assisted detection and early removal. Because classical signature-based approaches to malware defense do not provide adequate protection [1], there is currently a need for alternative defensive approaches.

While authors [2–8] have long debated the benefits of using added software diversity to halt malware, few results [9] actually show when diversity increases a network's robustness to malware epidemics. We demonstrate that reasonable software diversity prevents malware from controlling much of the information on a network but only when the network's topology is homogeneous. If a diverse network is inhomogeneous, then malware on the hubs, that is, the nodes with the most connections, can still control much of the information. We show how node immunization and software diversity together can halt infectious malware on inhomogeneous networks.

In this paper, the term "virus" denotes any form of infectious malware, and we consider the Internet as a collection of networks infected by many different viruses [10]. The viruses are allowed to reinfect machines because it is important to halt viruses that adapt over time. In the future, adaptive viruses could, with help from their creators, exploit new vulnerabilities and thus reinfect machines even after software patches have been installed.

Viruses spread by exploiting vulnerabilities in the operating system and application layers of a network. We build a model simulating multiple simultaneous outbreaks on a single layer. The network of attacked machines is modeled by a graph with different node types representing the software diversity. Since the spreading patterns of viruses vary with the considered layer and the exploited vulnerabilities [11], we model different network topologies to show that the proposed technique can halt viruses with different inhomogeneous spreading patterns.

Using the framework of network science [12], other authors have studied how to halt viruses on network monocultures with a single-software platform [13–18]. We first analyze a technique to halt multiple simultaneous virus outbreaks on inhomogeneous networks with diverse software platforms and known hubs. The halting technique is then extended to diverse inhomogeneous networks with unknown hubs [15]. The technique immunizes a small percentage of all nodes and introduces a reasonable amount of platform diversity [19, 20] to prevent the viruses from spreading. When the halting technique is applied to inhomogeneous networks, later virus outbreaks are quickly eliminated.

## 2. Characterizing Diversity

Two computing platforms on a network are distinct when they have no exploitable vulnerability in common.

A collection of platforms can be divided into classes of mutually distinct platforms, that is, no two platforms from different classes have a common vulnerability. Here, we only consider the platforms' OSes and web browsers. The OSes and browsers are assumed downloaded from application stores utilizing compilers with "diversity engines" to generate different binary images [19]. Assuming that the compilers generate roughly equally large classes of distinct downloadable images, the number of classes is a measure of the platforms' software diversity.

To understand why we concentrate on the diversity of OSes and web browsers, consider the computing platforms at the hardware, network, OS, and application levels. Let the hardware diversity be the number of microprocessors with different instruction set architectures. The small number of unique microprocessors limits the hardware diversity in current and forceable systems. Further, hardware diversity is "nullified" by byte code interpreters or instruction set emulators at the OS level.

The network level's ability to prevent virus spreading is also limited because all realizations of a communication protocol must have the same functionality. Since different OSes have similar but not equal functionalities, there is a greater potential for creating diversity at the OS level. At the application level, the diversity of web browsers is important since regular users utilize browsers most of the time. Current realizations of multibrowser technologies like Java Virtual Machines, Adobe Flash player, and JavaScript are problematic because they simplify virus attacks across different platforms.

Today, limited diversity is obtained by deploying different OSes like Windows and Mac OS X and different web browsers like Internet Explorer and Safari. Much larger diversity is possible if future application stores utilize compiler-generated diversity to make many distinct downloadable software images [19].

In the following section, we establish an epidemiological model with adjustable diversity. Since virus writes control the spreading mechanisms of viruses, we are likely to see widely different and surprising spreading patterns in the future. Thus, we do not attempt to model the details of how viruses spread. Instead the epidemiological model can incorporate any homogeneous or inhomogeneous network of vulnerable machines. In this paper, we extend well-established network models from Network Science [12] that are known to model different topological aspects of the Internet. The epidemiological model is also created to facilitate mathematical analyses.

## 3. Epidemiological Model

Let a computer network be infected by different viruses. The network is modeled as an undirected graph with $M$ edges and $N$ nodes of different types. The node types represent machines with distinct software on the OS or application layer and the edges represent virtual communication lines. There is at most one edge between two nodes and no edge connects nodes to themselves. If there is an edge between two nodes, then these nodes are *neighbors*. The *degree* of a node is the number of neighbors. The nodes' average degree is $\langle k \rangle = (2M)/N$.

The topology of the network depends on the considered software layer, and the vulnerabilities exploited to spread the viruses. Email viruses and viruses on the web travel over *inhomogeneous* networks on which a few nodes, the *hubs*, have very large degrees $k \gg \langle k \rangle$ [11]. An inhomogeneous scale-free network is a graph whose degree distribution follows a power law, that is, the probability of a node having $k$ neighbors is proportional to $k^{-\gamma}$. The well-established Barabási and Albert (BA) model [21] grows a scale-free network with exponent $\gamma = 3$ modeling the web. The hubs are encoded by the power law's tail. Figure 1(a) depicts a BA network with $N = 40$ nodes and average degree $\langle k \rangle = 2$.

The Watts-Strogatz (WS) model [22] generates a *homogeneous* network with node degrees $k \approx \langle k \rangle$ capturing the "small world" property of the Internet [12]. All nodes are placed on a circle. Initially, each node has $K$ neighbors in the clockwise direction and $K$ neighbors in the counterclockwise direction. With probability $r$, $0 \leq r \leq 1$, each of the $K$ clockwise edges is reconnected to a node chosen uniformly at random over the entire ring (with duplicate edges and self-loops forbidden). The WS network with $N = 10$ and $K = 2$ in Figure 1(b) has $\langle k \rangle = 4$ and no hubs.

All BA and WS networks, as well as other networks introduced later, have $L$ different node types $l = 1, 2, \ldots, L$ for $1 \leq L \ll N$. Each node type occurs $N_l$ times. A node chosen uniformly at random is of type $l$ with probability $N_l/N$ for $N = \sum_l N_l$. One of the generalized entropy functions measures the *diversity* of a network [23]. Because we will assume that $N_l = N/L$, the diversity is equal to the number of node types $L$ with the convention that a network with only a single type, called a *monoculture*, has no diversity. The networks in Figure 1 have diversity $L = 3$.

Multiple simultaneous virus epidemics are modeled by $L$ susceptible-infected-susceptible (SIS) models [13, 24] operating on the same network topology but affecting $L$ disjoint subsets of nodes with different types. There are $L$ types of viruses. Each type of virus infects a particular software platform, that is, node type. Initially, all nodes are susceptible. At time step $t = 0$, the generic model selects uniformly at random $S$ ($\geq 1$) nodes of each type $l$ and infects the nodes. These $L \cdot S$ initially infected nodes are called *seeds*. The stars in Figure 1 represent the seeds. For each time step $t = 1, 2, 3, \ldots$, any infected node of type $l$ infects any susceptible neighbor of type $l$ with *infection probability* $p_l$, $0 < p_l \leq 1$. At the same time, any infected node of type $l$ recovers with *recovery probability* $q_l$, $0 \leq q_l \leq 1$.

When $q_l > 0$ for some $l$, a node can repeat the SIS life cycle many times. The result is a *stochastic* model with long-term dynamics, where it is assumed that the infections and recoveries are updated in a random asynchronous order. When $p_l = 1$ and $q_l = 0$ for all $l$, the $L$ SIS models become $L$ susceptible-infected models. The generic model is *deterministic* in this case since a virus infects all reachable nodes with 100% probability. Consequently, the spreading process is completely determined by the network's topology and configuration of node types. Because no node recovers from an infection, there are no long-term dynamics. The spreading simply stops when all reachable nodes are infected.

## 4. Impact of Virus Outbreaks

To measure the impact of viruses on a network, one possibility is to count the infected machines. Another possibility is to consider the *availability* of the information on all virtual communication lines. While an infected machine should continue to operate nearly as normal to forestall virus detection, a virus can still stop selected information on the machine's communication lines. A node in the generic model whose adjacent edges are all controlled by viruses is said to be *isolated* because the availability of any incoming and outgoing information cannot be guaranteed. The seven nodes with only red edges in Figure 1(a) are isolated. Note that *a node is isolated when it is infected or when all its neighbors are infected*.

A susceptible node always becomes isolated when it is infected since the virus on the node itself controls all adjacent edges. When an infected node recovers because the virus is removed, only the adjacent edges connecting to infected neighbors remain under control of viruses. Hence, a susceptible (i.e., not infected) node can only be isolated if all its neighbors are infected. It can be argued that we should also count a healthy node when a few but not all of its neighbors are infected. The author has ignored these partially isolated nodes to simplify the mathematical analysis in Appendix A.

Consider the deterministic model with $p_l = 1$ and $q_l = 0$ for all $l$. If the network is a monoculture with $L = 1$ node type, then a susceptible node with an infected neighbor will also become infected. Hence, the number of isolated nodes equals the number of infected nodes. When an inhomogeneous network has $L > 1$ node types, the number of isolated nodes is in general larger than the number of infected nodes. Consider a node of type $l$ with a few neighbors of types $l' \neq l$. Even if the node itself is not infected, it is easily isolated by viruses on the few neighbors. These viruses control all edges connecting to the susceptible node. (Only 3 of the 7 isolated nodes in Figure 1(a) are infected.) Since the number of infected nodes can seriously underrepresent the ability of multiple virus outbreaks to control the availability of information on a diverse inhomogeneous network, we count the number of isolated nodes. Gorman et al. [10] were possibly the first to use this measurement.

*4.1. Average Node Isolation.* The generic model was implemented in NetLogo [25]. Initially, we utilize the *deterministic* model to compare the average fractions of isolated nodes on inhomogeneous networks with hubs and homogeneous networks without hubs. It is reasonable to set the recovery probabilities to $q_l = 0$ because many viruses, especially self-propagating worms, spread too fast for human-assisted detection and early removal. The infection probabilities are set to $p_l = 1$ to quickly determine the maximum possible number of isolated nodes. To explore the full effect of varying the diversity $L$, we assume (nearly) equally many nodes per type.

First, we evaluate inhomogeneous BA networks with $10^4$ nodes and average degree $\langle k \rangle = 2$. Figure 2(a) plots the average fraction of isolated nodes for an increasing number of node types $L = 2, 3, \ldots, 7$ and an increasing number of seeds $S = 1$, 3, 5, and 10 per node type. Every discrete data point is averaged over hundred random configurations of node types and seeds for each of hundred random BA networks. BA monocultures with $L = 1$ have an average fraction of isolated nodes equal to one (not shown in Figure 2(a)) because they are connected graphs. Going to $L = 2$, the average fraction of isolated nodes decreases with roughly 85% or more depending on the number of seeds $S$ per node type. For $L = 7$, the average fraction reduces to no more than 3% for $S \leq 10$.

Second, we consider homogeneous WS networks with $10^4$ nodes, average degree $\langle k \rangle = 6$, and rewiring probability $r = 4\%$. Figure 2(b) shows the average fraction of isolated nodes for an increasing number of node types $L$ and an increasing number of seeds $S$ per node type. Each data point is generated as before. For $L \geq 3$ and $S \leq 10$, the average fraction of isolated nodes is less than 3%. While the WS networks have a larger average degree than the BA networks, the BA networks still need larger diversity $L$ to reduce the average fraction of isolated nodes to 3%.

Finally, we consider an inhomogeneous network with more dominant hubs than the considered BA networks. The dominant hub (DH) network represents a possible inhomogeneous spreading pattern for an outbreak of multiple viruses. The DH network has 10670 nodes and 22002 edges. The largest hub has degree 2312, which is nearly 11% of the total number of edges. Figure 2(c) depicts the average fraction of isolated nodes in the DH network for $L = 4, 8, \ldots, 40$. Each data point is averaged over $10^3$ random configurations. The fraction of isolated nodes reduces much more slowly and levels off at a higher value than for the other networks. For $L = 40$, the average fraction is about 23% for $S = 10$ and 3% for $S = 1$.

Inspections reveal that the big hubs in the DH network isolate a large number of low-degree nodes, many of which are not infected. Figure 2(d) plots the DH network's differences between the average fraction of isolated nodes and the average fraction of infected nodes for $S = 10$. The DH network has a large difference for all $L = 1, 2, \ldots, 7$, roughly 40% for $L = 4$. The simulation results in Figure 2 and the analysis in Appendix A show that the difference for random BA networks is much smaller, and the difference for random WS networks is essentially zero because they have no hubs.

According to the plots in Figure 2, the average fraction of isolated nodes in both homogeneous and inhomogeneous networks drops when the diversity $L$ increases. However, a significant fraction remains even for large $L$ when a network contains big hubs. Further, the remaining fraction of isolated nodes grows with increasing number of seeds $S$ per node type (see Figure 2(c)). These observations were confirmed by simulations based on eight more DH networks and many additional BA and WS networks.

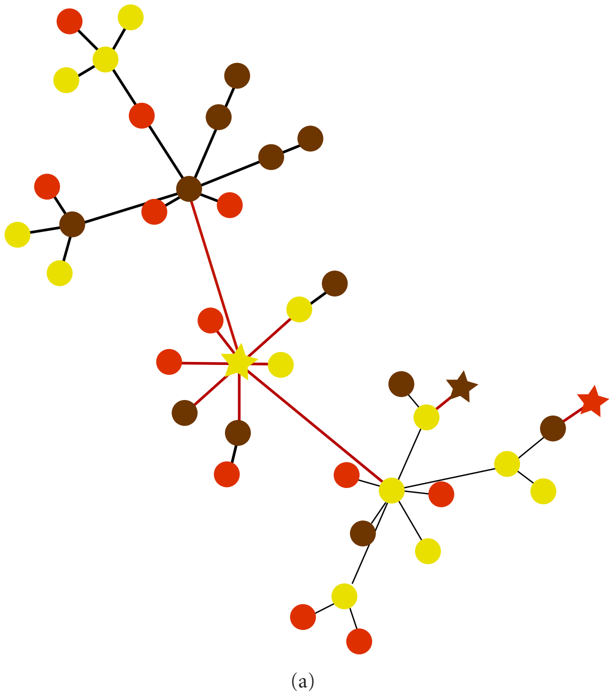


Figure 1: Diverse (a) BA network and (b) WS network seeded with viruses at time step $t = 0$. Both networks have $L = 3$ different colored node types. Circular nodes are susceptible and star-shaped nodes are infected. There is $S = 1$ seed for each node type. Only the $L \cdot S = 3$ seeds are infected since the viruses have not started to spread. The viruses infecting the seeds control all adjacent edges (shown in red). The BA network has four isolated nodes in addition to the three infected seeds. Only the seeds are isolated in the WS network.

*4.2. Influence of Reinfected Hubs.* We now study the *stochastic* model to determine the hubs' influence on the fraction of isolated nodes in diverse inhomogeneous networks with reinfections of nodes.

When there are $N_l = N/L$ nodes per type, an arbitrary node is a seed with probability $S/N_l = (SL)/N$, where $S$ is the number of seeds per node type. Since a node of degree $D$ has roughly $D \cdot N_l/N = D/L$ neighbors of the same type, a node's number of neighboring seeds of the same type is estimated by

$$\frac{(SL)}{N} \cdot \frac{D}{L} = \frac{(SD)}{N}. \qquad (1)$$

The right-hand side of (1) is independent of the number of node types $L$. The number of seeds $S$ per node type can be large in practice because botnets are used to seed viruses. Hence, a hub with very large degree $D$ is likely to be infected by a seed during the first time steps of a model run, even if the diversity $L$ is large.

A hub of type $l$ is infected with probability $p_l \cdot (SD)/N$ during the model's first-time step. Infection will almost surely occur when $p_l \cdot (SD)/N \approx 1$. During the following time steps, the hub will infect many of its $D/L$ neighbors with the same type, where $L \ll D$ for current networks. Even more neighbors will be isolated. In particular, all degree-one neighbors of any type $l' \neq l$ will be isolated but not infected. When the hub recovers with probability $q_l$ during a time step, it will be quickly reinfected by one of the $D/L$ neighbors. Since the neighbors ensure that the hub is infected nearly all the time, a nonzero fraction of isolated nodes is maintained over time even when $L$ is large.

Many simulations using the stochastic model confirm the hubs' important role in making the fraction of isolated nodes much larger than the fraction of infected nodes. As seen from Figure 3, if the largest hub on a DH or BA network is immunized, that is, made permanently resistant to virus attacks, then the instantaneous fraction of isolated nodes drops significantly. There is no easily detectable reduction in the instantaneous fraction of infected nodes, confirming that the largest hub isolates many susceptible (i.e., not infected) nodes. The large fluctuations in the instantaneous fraction of isolated nodes in Figure 3(a) is due to temporary recovery of hubs.

The instantaneous fraction of isolated nodes will eventually go to zero because there is a non-zero probability that all nodes become susceptible in any finite-size network. However, the nonzero averaged fraction of isolated nodes was stable for very many time steps during the simulations. Hence, when hubs are reinfected, multiple virus outbreaks cause substantial long-term node isolation even for high node diversity $L$.

## 5. Halting Technique

Our goal is to halt multiple simultaneous virus outbreaks on any inhomogeneous network without changing its topology. The halting technique should drive the fraction of isolated nodes to zero in the stochastic model. For the deterministic

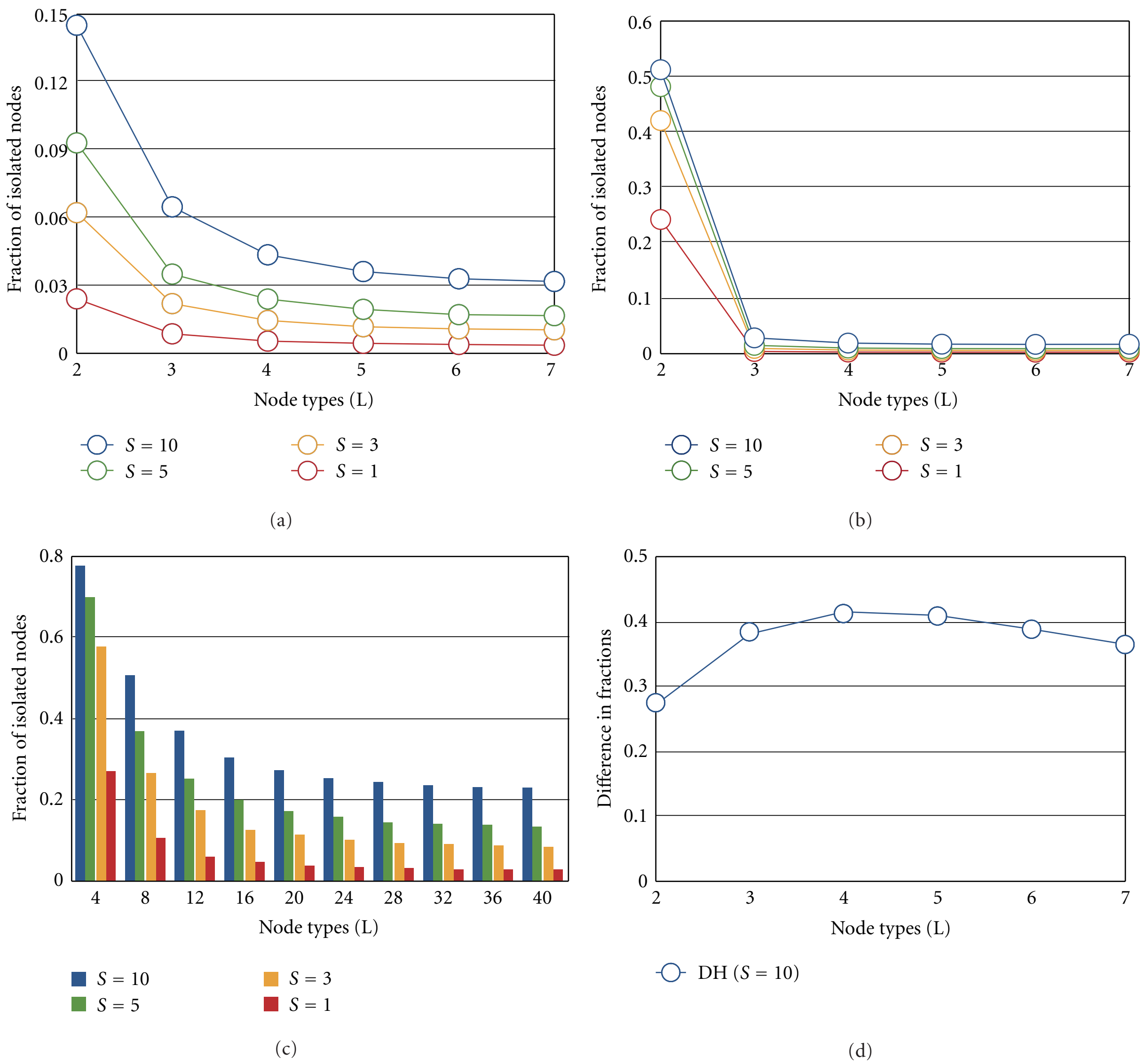


Figure 2: Average fraction of isolated nodes in (a) random BA networks with $\langle k \rangle = 2$; (b) random WS networks with $\langle k \rangle = 6$ and rewiring probability $r = 4\%$; (c) single DH network with $\langle k \rangle = 4.12$. (d) Difference between average fractions of isolated and infected nodes for $S = 10$ in the DH network.

model with a total of $L \cdot S$ seeds, the fraction of isolated nodes should not be much larger than $(LS)/N$ after the viruses have spread. Since node diversity alone only eradicates viruses on homogeneous networks, we suggest the following two-step technique.

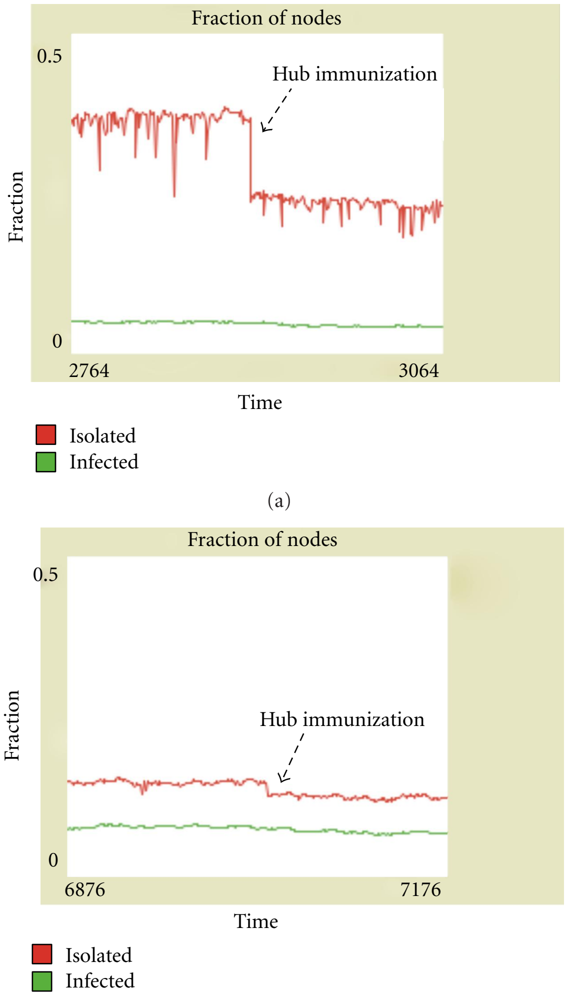
(1) Immunize enough large-degree nodes in a network to create a homogeneous subnet when the immunized nodes and their adjacent edges are removed.

(2) Ensure that the node diversity of the homogeneous subnet is large enough to halt (and possibly remove) multiple simultaneous virus outbreaks.

*5.1. Deterministic Example.* To illustrate the technique, we consider a second inhomogeneous DH network with 22963 nodes, maximum degree 2390, and average degree 4.22. Deterministic spreading of all infections is obtained by setting the infection probability $p_l = 1$ and recovery probability $q_l = 0$ for all $l$. The model first runs without applying the halting technique.

Figure 4(a) depicts the DH network without edges before the viruses start to spread. The four node types have different colors. The 164 largest hubs have bigger size and are placed on top of the other nodes. Twenty seeds of each type are colored red to signify infections (only a few are visible).

The seeds infect the hubs during the first few time steps of the model run. The hubs again isolate very many low-degree nodes. When the run terminates, as shown in Figure 4(b), all infected nodes are colored red, and all susceptible nodes with only infected neighbors are colored white. The red and white nodes together constitute 18314 isolated nodes, that is, no less than 80% of all nodes.



(a)

(b)

Figure 3: Instantaneous fractions of isolated nodes (red line) and infected nodes (green line) in diverse (a) DH network and (b) random BA network. The vertical drop in each instantaneous fraction of isolated nodes is due to immunization of the largest hub only.

Figure 4(c) shows the same DH network, but now with immunized, dark-pink-colored hubs. Further, the number of node types is increased from four to six. Figure 4(d) highlights the isolated nodes after the viruses have spread. The $6 \cdot 20 = 120$ seeds only generated 283 isolated nodes or 1% of all nodes.

*5.2. Stochastic Model Analysis.* While our goal is to prevent future virus epidemics, we continue to study the case where $L$ simultaneous virus outbreaks have already spread over the stochastic model. The halting technique's first objective is then to immunize enough of the largest-degree nodes to obtain a homogeneous subnet of susceptible and infected nodes. To determine how many of the nodes to immunize, consider the two statements $\mathcal{A}$: "network is homogeneous" and $\mathcal{B}$: "fractions of isolated and infected nodes are equal." We argue that $\mathcal{A}$ and $\mathcal{B}$ are equivalent statements.

Let $p_l = p > 0$ and $q_l = q > 0$ for all $l$. Appendix A shows that when a homogeneous network is modeled as a random Erdös and Rényi graph [12], the fractions of isolated and infected nodes are essentially equal, that is, $\mathcal{A}$ implies $\mathcal{B}$ in this case. The same implication holds for generalized random networks with arbitrary "thin-tail" degree distribution. More generally, let $h$ denote the fraction of infected nodes. The likelihood that an arbitrary node is isolated but not infected on a homogeneous network is approximated by $(1-h)h^{\langle k \rangle}$, which goes to zero as the average degree $\langle k \rangle$ increases.

To show that $\mathcal{B}$ implies $\mathcal{A}$, is equivalent to show $\neg\mathcal{A}$ implies $\neg\mathcal{B}$ where $\neg$ denotes negation. From Appendix A, when an inhomogeneous network is represented by the BA model, the fraction of isolated nodes is larger than the fraction of infected nodes. The same is true for other network models with scale-free degree distributions. In general, there is a large fraction of nodes with few neighbors in inhomogeneous networks. While many of these low-degree nodes, for example, $k \in \{1,2\}$, are not susceptible to locally propagating viruses due to their node types, the nodes can easily be isolated by infected neighbors.

Consequently, enough large-degree nodes should be immunized to make the fractions of isolated and infected nodes nearly equal because, at least according to the provided evidence, only then do we obtain a homogeneous subnet of susceptible and infected nodes.

The halting technique's second objective is to ensure that the number of node types $L$ is large enough for the remaining viruses to die out on the homogeneous subnet. Let the subnet be modeled as a generalized random network with equally many nodes of each type. According to Appendix B, the needed number of node types is then lower bounded by

$$L > z^* \cdot \max_l \left\{ \frac{p_l}{q_l} \right\}, \tag{2}$$

where $z^*$ is the average degree of the subnet. From (2), the largest of the spreading rates $p_l/q_l$ essentially determines the required node diversity $L$. Analysis in Appendix B shows that all the infected nodes recover more quickly as $L$ is increased beyond the lower bound in (2).

*5.3. Stochastic Example.* We revisit the second-discussed DH network. Assuming infection probability $p_l = 0.06$ and recovery probability $q_l = 0.04$ for all $l$, we select $L = 7$ node types. The instantaneous fractions of isolated and infected nodes are shown in Figure 5(a). There is a large difference between the fractions until time step one thousand when the 216 largest hubs are immunized. The two fractions then quickly become nearly equal. All remaining infected nodes recover after an additional 2958 steps (not shown).

A real network spanned by viruses is most often embedded in a larger network. If the larger network has adequate diversity $L$, then future virus outbreaks can be halted by immunizing most of the hubs visited by the viruses *before* the actual outbreaks. Figure 5(b) shows the fractions of isolated and infected nodes for the DH network when the 216 largest hubs have been correctly identified and immunized in

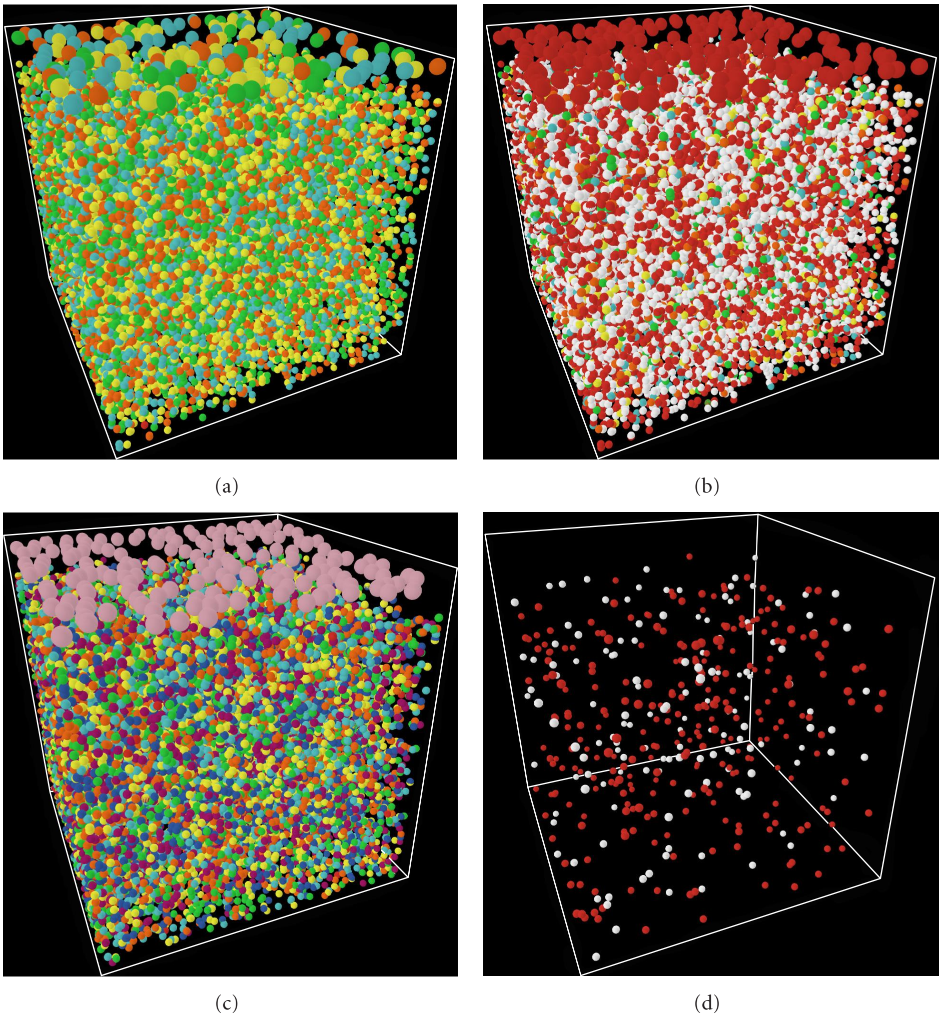


Figure 4: (a) DH network with four-colored node types, 164 enlarged hubs, and twenty seeds per type. (b) After the viruses have spread, all infected nodes are red and all susceptible isolated nodes are white. (c) Same DH network, but now with dark-pink-immunized hubs and six-colored node types. (d) Since the viruses are nearly unable to spread-there are only few red-and white-isolated nodes (other nodes not shown).

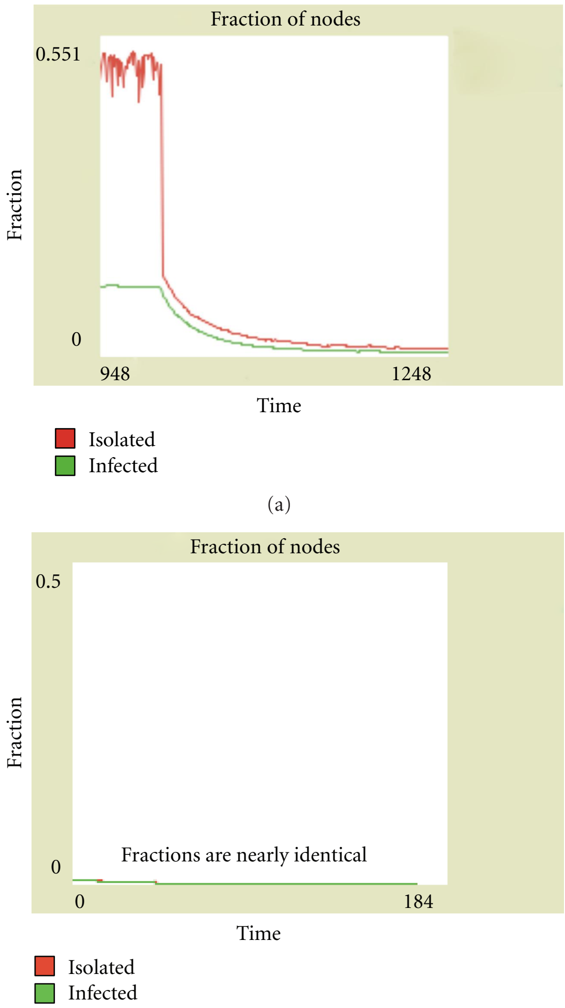
advance. There is very little spreading of the viruses and all infected nodes recover after only 184 steps.

## 6. Generalized Halting

While we do not know the degrees of many nodes in real inhomogeneous networks [14], it is still possible to immunize hubs in advance of virus outbreaks. The acquaintance immunization strategy [15] provides an elegant solution to the problem of immunizing unknown hubs on a monoculture ($L = 1$) infected by viruses: choose a set of nodes uniformly at random and immunize one arbitrary neighbor per node. While the original set of nodes is unlikely to contain the relatively few hubs in an inhomogeneous network, the randomly selected neighbors are much more likely to be hubs, since very many edges are adjacent to high-degree nodes.

We can generalize acquaintance immunization to diverse networks. Assume $N_l = N/L$ nodes per type. For some fraction $0 < f < 1$, choose a set of $f \cdot N_l$ nodes of type $l$ uniformly at random such that each node has at least one neighbor of the same type. Immunize one randomly selected neighbor of type $l$ per node in the set. When the set of all immunized neighbors $fN = \sum_l fN_l$ is large enough, the set $fN$ will contain most of the hubs and the fractions of isolated and infected nodes will be nearly equal.

*6.1. Examples with Unknown Hubs.* We consider the second DH network a last time, assuming unknown node degrees. Let the fraction of immunized neighbors be $f = 0.04$ (4%) and set $p_l = 1$, $q_l = 0$, and $L = 7$. Figure 6(a) shows only the immunized dark-pink nodes and the remaining susceptible multicolored hubs after acquaintance immunization. Note that most of the 216 enlarged hubs are immunized. Figure 6(b) highlights the isolated nodes after the viruses have



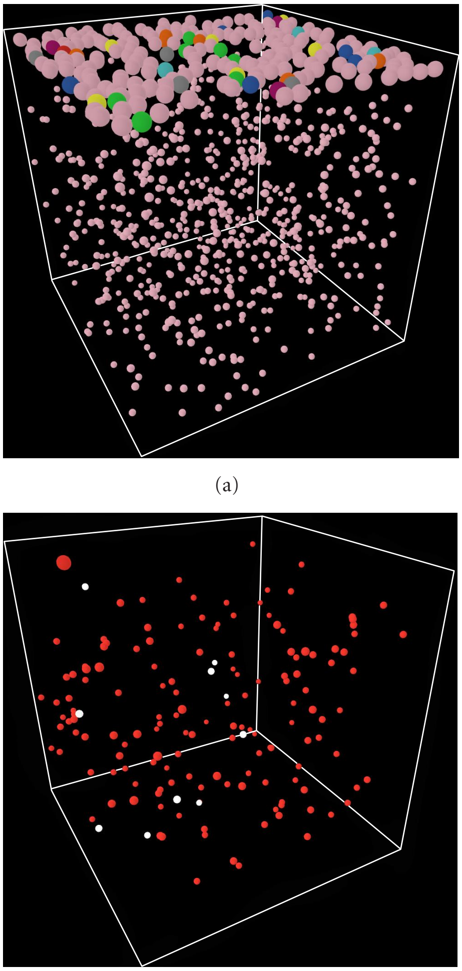
(a)

(b)

Figure 5: Fractions of isolated and infected nodes caused by multiple simultaneous virus outbreaks on DH network. (a) The largest 216 hubs are immunized at time step one thousand. (b) The hubs have been correctly identified and immunized before the virus outbreaks.

spread. The $7 \cdot 20 = 140$ seeds generated 158 isolated nodes or less than 1% of all nodes. Let $p_l = 0.06$ and $q_l = 0.04$. When acquaintance immunization is performed in advance, the fractions of isolated and infected nodes went to zero after only 154 time steps. The plot of the isolated and infected fractions (not shown) is very similar to Figure 5(b).

To verify the usefulness of the halting technique for inhomogeneous networks with unknown hubs, we generated additional model runs for different DH networks, including runs where the infection and recovery probabilities $p_l$ and $q_l$ varied with $l$. After first determining a suitable fraction $f$ of immunized nodes and number of node types $L$, the seeds caused little spreading and all infected nodes recovered. The speed at which the virus outbreaks die out depends on the fraction $f$, diversity $L$, selection of $L \cdot S$ seeds, and spreading rates $p_l/q_l$.



(a)

(b)

Figure 6: Acquaintance immunization of DH network. (a) Immunized dark-pink nodes and remaining susceptible multicolored hubs. (b) The few red and white isolated nodes after the viruses tried to spread.

## 7. Final Discussion

The Internet is best viewed as a large collection of networks. Because each network has different default settings, software patch levels, firewall rules, browser settings, antivirus signature sets, configuration management practices, and diagnostic capabilities, they are not all vulnerable to the same viruses [8]. However, we have seen many examples of large networks with too little software diversity to prevent virus epidemics.

Since the virus writers control the spreading mechanisms of viruses, a practical halting technique must handle viruses with widely different spreading patterns. The reported results indicate that robust halting of viruses is obtainable when application stores with “diversity engines” ensure adequate software diversity on the OS, and application layers of a network and vulnerable hubs are immunized (Appendix C discusses the halting technique’s fragility to clustering of platform types.)

The virus halting technique is of practical interest because it can handle inhomogeneous spreading patterns with unknown hubs. For a reasonable number of node types and nearly equally many nodes per type, the halting technique only needs to immunize a small percentage of all nodes to remove multiple simultaneous virus outbreaks. In contrast, acquaintance immunization of BA networks with a single-node type must immunize roughly a quarter of the nodes [15].

More work, preferably with contributions from practitioners, is needed to transform the halting technique into a practical "tool" to prevent virus epidemics. Initially, there is a need for large-scale network simulations to further verify the applicability of the technique. Mathematical analysis of additional network models would also be useful. The author believes the halting technique is particularly promising for the *mobile Internet* because many users already download OSes and applications to their smartphones from application stores. The technique is also likely to be suitable for the *Internet of Things,* where objects are periodically tethered to smartphones acting as hubs.

## Appendices

## A. Mathematical Analysis

The simulations discussed in Section 4.1 show that the average fractions of isolated and infected nodes differ in the BA network model but not in the WS model. Here, a mathematical analysis of four network models verifies and generalizes these observations.

In the following, an approximate mathematical analysis, based on a special case of the stochastic epidemiological model, establishes a nonzero difference between the average fractions of isolated and infected nodes in two-diverse inhomogeneous network models with scale-free "fat-tail" degree distributions. To confirm that this difference is caused by the network hubs, we initially show that essentially all isolated nodes are infected in two diverse homogeneous network models with "thin-tail" degree distributions.

All virus types in our stochastic model use the same spreading mechanism, that is, the underlying network topology is the same for all viruses, but a virus of a particular type only infects a single type of nodes. Hence, viruses of different types infect distinct subsets of nodes. Let each subset have $N_l = N/L$ nodes of type $l = 1, 2, \ldots, L$, and assume that all $L$ subsets have infection probability $p_l = p > 0$ and recovery probability $q_l = q > 0$. The subsets, thus, have the same fraction of infected nodes when we average over many model runs. Further, the average fraction of infected nodes over all types, denoted $h_L$, can be obtained by considering an arbitrary subset of $N/L$ nodes of the same type.

We consider the stochastic model after the $L$ simultaneous virus outbreaks, one per-node type, have reached a long-term steady state. Let a randomly chosen node have degree $k$ with probability $p_k$. Ignoring short loops of connected nodes [26], the probability that a node is isolated but not infected, that is, the node itself is susceptible and all its $k$ neighbors are infected, is approximated by

$$P(\text{only isolated}) \approx (1 - h_L) \sum_{k=0}^{\infty} p_k (h_L)^k. \qquad \text{(A.1)}$$

*A.1. Small-World Networks.* Initially, we calculate (A.1) for a slight variation on the classical WS model obtained as follows [12]. First, a regular graph is generated by placing $N$ nodes on a circle and then adding edges from each node to its $K$ nearest neighbors in the clockwise direction, $1 \leq K \ll N$. The resulting graph has $NK$ edges and all nodes have degree $2K$.

Next, random edges or "shortcuts," are added to the graph: We view the $N$ nodes as belonging to a random Erdös and Rényi (ER) graph [12] and add edges until the expected number is $NKr$ for $0 < r < 1$. The probability that there is a shortcut between two nodes is then $(NKr)/\binom{N}{2}$, which is equal to $(2Kr)/N$ for large $N$.

The expected total degree of all nodes in the final network is $2(NK+NKr) = 2NK(1+r)$ and the average node degree is $\langle k \rangle = 2K(1+r)$. Since the classical WS model has $\langle k \rangle = 2K$, the increase in average degree is negligible for small $r$.

Each node in the network has degree at least $2K$, due to the edges in the regular graph plus a binomially distributed number of shortcuts. Thus, a node selected uniformly at random has degree $k$ with probability

$$p_k = \binom{N}{k - 2K} \left( \frac{2Kr}{N} \right)^{k-2K} \left( 1 - \frac{2Kr}{N} \right)^{N-k+2K}, \qquad \text{(A.2)}$$

for $k \geq 2K$ [12]. Substituting (A.2) into (A.1), modifying the resulting expression, and using the Binomial Theorem, we have

$$\begin{aligned} P(\text{only isolated}) \approx &(1 - h_L)(h_L)^{2K} \\ &\cdot \sum_{k=0}^{N} \binom{N}{k} \left( \frac{2Kr}{N} h_L \right)^k \left( 1 - \frac{2Kr}{N} \right)^{N-k}, \\ = &(1 - h_L)(h_L)^{2K} \left[ \frac{2Kr}{N} (h_L - 1) + 1 \right]^N. \end{aligned} \qquad \text{(A.3)}$$

The probability estimate in (A.3) is zero for $h_L = 0, 1$. For $0 < h_L < 1$, the expression inside the square parentheses is less than one, and the probability goes to zero for large $N$, regardless the number of node types $L$.

*A.2. Homogeneous Random Networks.* We now calculate (A.1) for the homogeneous ER model [12]. The node degrees have a binomial distribution, which in the limit where the number of nodes $N \gg k$ reduces to to the Poisson distribution

$$p_k = e^{-z} \frac{z^k}{k!}, \qquad k = 0, 1, \ldots, \qquad \text{(A.4)}$$

for $z = \langle k \rangle$ the average degree. Substituting (A.4) into (A.1) and using the definition $e^x = \sum_{n=0}^{\infty} x^n/n!$ give

$$P(\text{only isolated}) \approx \frac{1-h_L}{e^{z(1-h_L)}}. \tag{A.5}$$

While a sparse ER network ($z \ll N$) is very unlikely to have hubs, we have from (A.5) that the average fraction of isolated nodes is still larger than the average fraction of infected nodes for $h_L < 1$. However, as we shall see, this is due to the fraction $p_0 = 1/e^z$ of nodes with degree zero. All these nodes without edges are isolated and cannot become infected as long as they are not seeds.

To estimate the average fraction of infected nodes $h_L$ in (A.5), we extend an analytical technique for ER monocultures ($L = 1$) introduced in [13]. Each virus outbreak in a network with $L > 1$ node types operates on a subset of $N/L$ nodes of the same type. On average, a node has $z/L$ neighbors in the subset because the probability that a node is of type $l$ is $N_l/N = 1/L$. Let the spreading rate be $\rho_L = (pz)/(qL)$ and view $h_L = h_L(t)$ as a continuous-time variable. Writing down a differential equation representing change in the fraction of infected nodes

$$\frac{dh_L}{dt} = p\left(\frac{z}{L}\right)h_L(1-h_L) - qh_L \tag{A.6}$$

and imposing the stationary condition $dh_L/dt = 0$, we find that the average fraction of infected nodes saturates at $h_L = 1 - 1/\rho_L$ for $\rho_L > 1$. The fraction $h_L$ goes to zero in finite time when $\rho_L < 1$.

For fixed infection probability $p$, recovery probability $q$, and average degree $z$, the spreading rate $\rho_L = (pz)/(qL) < 1$ when the number of node types $L > (pz)/q$. Consequently, $h_L$ goes to zero and (A.5) becomes equal to the fraction of nodes without edges $p_0 = 1/e^z$, which shrinks as $z$ grows.

*A.3. Inhomogeneous $\gamma = 3$ Networks.* The BA model with integer parameter $m \geq 1$ grows a scale-free network with power-law exponent $\gamma = 3$, average node degree $\langle k \rangle = 2m$, and minimum degree $m$ [12]. The degree distribution is given by

$$p_k = \frac{2m(m+1)}{k(k+1)(k+2)}, \quad k \geq m. \tag{A.7}$$

Using computing software (e.g., Maple or WolframAlpha) to combine (A.7) and (A.1) gives

$$\begin{aligned} P(\text{only isolated}) &\approx \frac{(1-h_L)}{(h_L)^2}, \\ &\left[h_L(3h_L-2) - 2(h_L-1)^2\ln(1-h_L)\right], \\ &\left[h_L((9-2h_L)h_L-6) - 6(h_L-1)^2\ln(1-h_L)\right], \end{aligned} \tag{A.8}$$

for $m = 1, 2$, respectively.

To estimate the average fraction of infected nodes $h_L$, we extend an analytical technique for BA monocultures ($L = 1$) developed in [27]. Let $h_{k,L}$ denote the fraction of infected nodes of degree $k$ in a subset of nodes with the same type. We then have

$$h_L = \sum_{k=m}^{\infty} h_{k,L} \cdot p_k. \tag{A.9}$$

Since, on average, a node of degree $k$ has $k/L$ neighbors of the same type, the spreading rate for nodes of degree $k$ is $\rho_{k,L} = (pk)/(Lq)$, and the overall spreading rate is

$$\begin{aligned} \rho_L &= \sum_{k=m}^{\infty} \rho_{k,L} \cdot p_k, \\ &= \frac{p}{Lq}\sum_{k=m}^{\infty} kp_k = \frac{p\langle k \rangle}{Lq} = \frac{2mp}{Lq}. \end{aligned} \tag{A.10}$$

The change in fraction of infected nodes with degree $k$ is given by the differential equation

$$\frac{dh_{k,L}}{dt} = p\left(\frac{k}{L}\right)(1-h_{k,L})\Theta - qh_{k,L}, \tag{A.11}$$

where $\Theta$ denotes the probability that an edge from a node connects to an infected node of the same type. Imposing stationary, we obtain

$$h_{k,L} = \frac{pk\Theta}{Lq + pk\Theta}. \tag{A.12}$$

According to (A.12), the higher the degree $k$, the more likely a node, especially a hub, is to be infected.

The probability that an edge connects to an infected node of a particular type is given by

$$\Theta = \frac{\sum_{k=m}^{\infty}(k/L)p_k h_{k,L}}{\langle k \rangle/L} = \frac{\sum_{k=m}^{\infty} kp_k h_{k,L}}{2m}. \tag{A.13}$$

If we view $k$ as a continuous variable, then the sum on the right-hand side of (A.13) can be estimated by an integral. Utilizing (A.12) and the estimate $p_k \approx 2\,\mathrm{m}^2/\mathrm{k}^3$ obtained from (A.7), we get

$$\begin{aligned} \Theta &= mp\Theta \int_m^{\infty} \frac{1}{k}\frac{1}{Lq + p\Theta k}dk \\ &= \frac{Lq}{mp}\left[e^{(Lq)/(mp)} - 1\right]^{-1}, \end{aligned} \tag{A.14}$$

which reduces to the case studied in [27] for $L = 1$.

Using an integral approximation one more time, we have from (A.9) and (A.12) that

$$h_L = 2m^2 p\,\Theta \int_m^{\infty} \frac{1}{k^2}\frac{1}{Lq + p\Theta k}dk. \tag{A.15}$$

Finally, combining (A.14) and (A.15) gives

$$h_L = \frac{2\left[e^{2/\rho_L} - 2/\rho_L - 1\right]}{(e^{2/\rho_L} - 1)^2}, \tag{A.16}$$

where the spreading rate $\rho_L$ is defined by (A.10).

We plot the average fraction of infected nodes $h_L$ given by (A.16) as a function of the average spreading rate $\rho_L$ in Figure 7(a). Unlike the ER model, there is no non-zero value of $\rho_L$ for which $h_L$ drops to zero. The probability in (A.8) that a node is isolated and not infected is plotted as a function of $h_L$ in Figure 7(b). Since the probability is positive for all $h_L > 0$, the hubs in the BA model (at least for $m = 1, 2$) cause the average fraction of isolated nodes to be larger than the average fraction of infected nodes for all spreading rates $\rho_L > 0$.

*A.4. Inhomogeneous $\gamma > 2$ Networks.* Finally, to verify that there is no need to have power-law exponent $\gamma = 3$, we consider a class of inhomogeneous scale-free networks with node degrees given by the Zeta distribution

$$p_k = \frac{1}{\zeta(\gamma)} k^{-\gamma}, \qquad k = 1, 2, \ldots, \tag{A.17}$$

where $\zeta(\gamma)$ is the Riemann zeta function. The average degree $\langle k \rangle = \zeta(\gamma - 1)/\zeta(\gamma)$ is finite for $\gamma > 2$. From (A.1) and (A.17), a node is isolated but not infected with probability

$$\begin{aligned} P(\text{only isolated}) &\approx \frac{1 - h_L}{\zeta(\gamma)} \sum_{k=1}^{\infty} \frac{(h_L)^k}{k^\gamma}, \\ &= \frac{1 - h_L}{\zeta(\gamma)} Li_\gamma(h_L), \end{aligned} \tag{A.18}$$

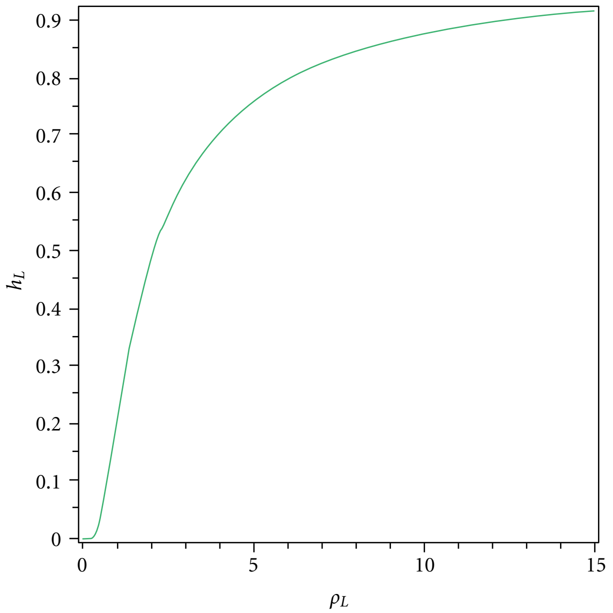
where $Li_\gamma(\cdot)$ denotes the polylogarithm function. The probability in (A.18) is strictly positive for any average fraction of infected nodes $0 < h_L < 1$.

## B. Analysis of Needed Diversity

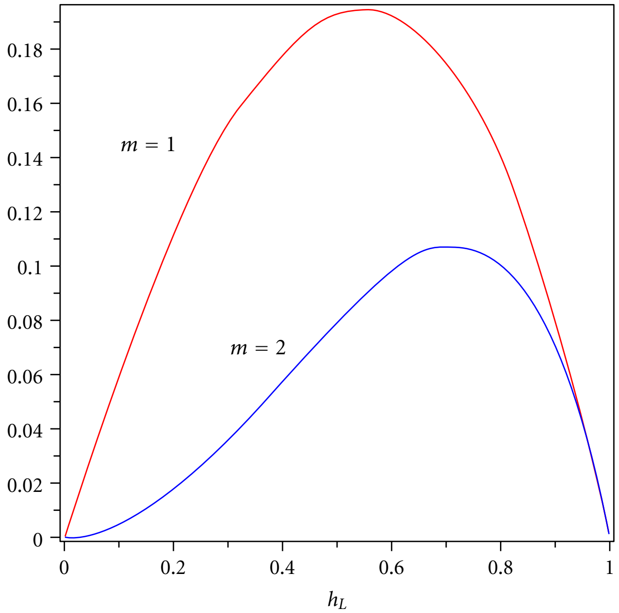
This appendix determines a lower bound on the number of node types needed to eliminate all viruses. Since diverse scale-free networks allow viruses to spread even for very small spreading rates, hubs must be immunized to obtain a homogeneous subnet on which epidemics die out. This subnet, determined by deleting all immunized hubs and their adjacent edges in the original network, is homogeneous when the fractions of isolated and infected nodes are nearly equal. In the following, we determine a lower bound on the number of node types $L$ needed to remove all epidemics from the homogeneous subnet. When the subnet is not connected, we consider its giant component.

Assume roughly $N_l = N/L$ nodes per type and the same infection probability $p$ and recovery probability $q$ for all epidemics. Let $f$ be the fraction of immunized nodes on the original network. A node selected uniformly at random in the subnet is of type $l$ with probability $[N_l(1 - f)]/[N(1 - f)] = 1/L$. On average, a subnet node has $z^*/L$ neighbors of the same type, where $z^*$ is the average node degree of the subnet. Modeling the subnet as a diverse random network and setting (A.6) equal to zero for $z = z^*$, we find that the epidemics die out when the diversity

$$L > \frac{pz^*}{q} \tag{B.1}$$



(a)



(b)

FIGURE 7: Estimates for diverse BA networks with $N_l = N/L$, $p_l = p$, and $q_l = q$ for all $l$. (a) Average fraction of infected nodes $h_L$ as a function of the average spreading rate $\rho_L$. (b) Probability of node being isolated and not infected as a function of $h_L$.

because the spreading rate $\rho_L = (pz^*)/(qL) < 1$. The lower bound in (B.1) also holds when the subnet is modeled as a generalized random network with arbitrary "thin-tail" degree distribution or a random-like small-world network with $r = 1$ because (A.6) is valid for these networks.

As we shall see, how fast the epidemics die out is determined by the infection probability $p$, recovery probability $q$, diversity $L$, and average degree $z^*$. For simplicity, we assume that all hub immunizations occur simultaneously

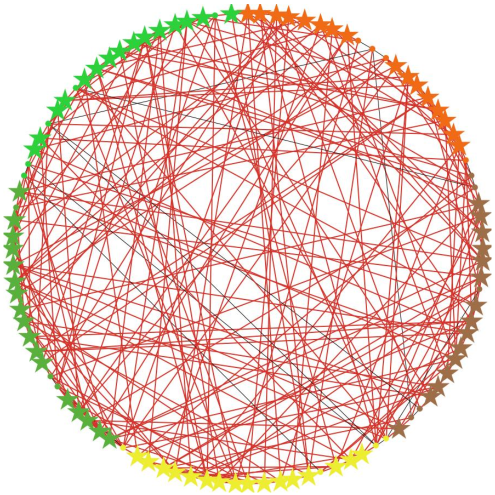


Figure 8: Snapshot of multi-strain global epidemic on modified WS network with five node types of different colors. The stars are infected nodes and the red edges are adjacent to infected nodes.

and instantly. Setting $z = z^*$, we then solve (A.6) to determine the average fraction of infected nodes $h_L = h_L(t)$ as a function of the time $t(\geq 0)$ *after* hubs are immunized:

$$h_L(t) = \frac{-h_0 R e^{Rt}}{p(z^*/L)h_0(1 - e^{Rt}) - R}. \qquad \text{(B.2)}$$

Here, $R = (pz^*)/L - q$ and $h_0 = h(0)$ are the fraction of infected nodes immediately after hub immunizations. For diversity $L > (pz^*)/q$, we have $R < 0$ and $h_L(t)$ go to zero with increasing time $t$ as predicted earlier.

More importantly, the smaller infection probability $p$ and average degree $z^*$, and the larger diversity $L$ and recovery probability $q$, the more negative $R$ becomes and the faster $h_L$ goes to zero. In particular, increasing $L$ beyond the minimum required value or immunizing more hubs to reduce $z^*$ speed up virus eliminations.

We end this appendix with a generalization of the lower bound in (B.1) for varying infection probabilities $p_l$ and recovery probabilities $q_l$. As before, there are $N/L$ nodes per type. Using the above technique, we can show that an epidemic on nodes of type $l$ dies out when $L > (p_l z^*)/q_l$. Let $Q = \max_l\{p_l/q_l\}$, then all epidemics die when $L > z^* \cdot Q$.

## C. Fragility Analysis

The halting technique's performance depends on the pattern of node-type assignments in a network. In general, the technique causes all epidemics to die out when the nodes of each type have a uniform distribution over the network. However, the technique fails in rare cases when most nodes of each type are clustered together.

View the homogeneous diverse subnet obtained by deleting immunized nodes and adjacent edges from the original network as $L$ distinct monocultures, each containing all nodes of type $l$. Model a monoculture as a generalized random network with arbitrary "thin-tail" degree distribution, $N_l$ nodes, average degree $z_l$, and spreading rate $\rho_l = (p_l \cdot z_l)/q_l$. Assume that each monoculture has a giant component, that is, a connected component with size proportional to $N_l$. If $\rho_l > 1$, then a fraction $h_l \approx 1 - 1/\rho_l$ of type $l$ nodes will be infected [13]. The total number of infected nodes is $\sum_l h_l \cdot N_l$ when $\rho_l > 1$ for all $l$. A *multi-strain global epidemic* infecting nearly all nodes occurs when each $h_l \approx 1$.

To illustrate the longevity of a multi-strain global epidemic on the stochastic model, we consider another slight variation on the classical WS model [12]; during network construction let a node's clockwise edges, except the edge to the nearest neighbor, be rewired with probability $r = 1$. Then, for each node type $l$, assign type $l$ to $N_l = N/L$ consecutive nodes on the circle. The result is a modified WS network with $L$ connected monocultures. These monocultures are giant components of size $N_l$ allowing the seeds to infect all $N$ nodes.

Let $p_l = 0.03$ and $q_l = 0.01$ for all $l$. Figure 8 shows a snapshot of a modified WS network with $N = 100$ nodes, $L = 5$ colored node types, and average degree $2K = 6$. Infected nodes are represented by stars. An edge is colored red if at least one adjacent node is infected. The fraction of isolated nodes, averaged over no less than $10^6$ time steps, is 0.9. Since the network is homogeneous, the averaged fraction of infected nodes is nearly the same. The example illustrates that homogeneous networks with large-connected subnets of the same node types are fragile to long-lasting global epidemics even for large diversity $L$. Such clustered patterns of node types should be avoided in real networks.

## References

[1] M. Donner, "Phagocytes in cyberspace," *IEEE Security and Privacy*, vol. 8, no. 5, pp. 3–4, 2010.

[2] D. E. Geer, "Monopoly considered harmful," *IEEE Security and Privacy*, vol. 1, no. 6, pp. 14–17, 2003.

[3] G. Goth, "Addressing the monoculture," *IEEE Security and Privacy*, vol. 1, no. 6, pp. 8–10, 2003.

[4] D. Aucsmith, "Monocultures are hard to find in practice," *IEEE Security and Privacy*, vol. 1, no. 6, pp. 15–16, 2003.

[5] J. A. Whittaker, "No clear answers on monoculture issues," *IEEE Security and Privacy*, vol. 1, no. 6, pp. 18–19, 2003.

[6] M. Stamp, "Risks of monoculture," *Communications of the ACM*, vol. 47, no. 3, p. 120, 2004.

[7] F. B. Schneider and K. P. Birman, "The monoculture risk put into context," *IEEE Security and Privacy*, vol. 7, no. 1, pp. 14–17, 2009.

[8] M. Ranum and B. Schneier, "Is a software monoculture dangerous to computer security?" *Information Security Magazine*, vol. 12, no. 9, pp. 19–23, 2010.

[9] A. J. O'Donnell and H. Sethu, "On achieving software diversity for improved network security using distributed coloring algorithms," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 121–131, Washington, DC, USA, October 2004.

[10] S. P. Gorman, R. G. Kulkarni, L. A. Schintler, and R. R. Stough, "A predator prey approach to diversity based defenses in heterogeneous networks," in *Proceedings of the Winter International Symposium on Information and Communication Technologies*, Cancun, Mexico, January 2004.

[11] J. Balthrop, S. Forrest, M. E. J. Newman, and M. M. Williamson, "Technological networks and the spread of computer viruses," *Science*, vol. 304, no. 5670, pp. 527–529, 2004.

[12] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, no. 2, pp. 167–256, 2003.

[13] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 343–358, Oakland, Calif, USA, May 1991.

[14] Z. Dezsö and A. L. Barabási, "Halting viruses in scale-free networks," *Physical Review E*, vol. 65, no. 5, Article ID 055103, 2002.

[15] R. Cohen, S. Havlin, and D. Ben-Avraham, "Efficient immunization strategies for computer networks and populations," *Physical Review Letters*, vol. 91, no. 24, Article ID 247901, 2003.

[16] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, vol. 65, no. 5, Article ID 056109, pp. 056109/1–056109/14, 2002.

[17] Y. Chen, G. Paul, S. Havlin, F. Liljeros, and H. E. Stanley, "Finding a better immunization strategy," *Physical Review Letters*, vol. 101, no. 5, Article ID 058701, 2008.

[18] C. M. Schneider, T. Mihaljev, S. Havlin, and H. J. Herrmann, "Suppressing epidemics with a limited amount of immunization units," *Physical Review E*, vol. 84, Article ID 061911, 2011.

[19] M. Franz, "E unibus pluram: Massive-scale software diversity as a defense mechanism," in *Proceedings of the New Security Paradigms Workshop (NSPW '10)*, pp. 7–16, Concord, Mass, USA, September 2010.

[20] K. Kravvaritis, D. Mitropoulos, and D. Spinellis, "Cyberdiversity: Measures and initial results," in *Proceedings of the 14th Panhellenic Conference on Informatics (PCI '10)*, pp. 135–140, Tripoli, Greece, September 2010.

[21] A. L. Barabási, R. Albert, and H. Jeong, "Scale-free characteristics of random networks: the topology of the world-wide web," *Physica A*, vol. 281, no. 1, pp. 69–77, 2000.

[22] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[23] S. E. Page, *Diversity and Complexity*, Princeton University Press, 2011.

[24] R. Pastor-Satorras and A. Vespignani, "Immunization of complex networks," *Physical Review E*, vol. 65, no. 3, Article ID 036104, pp. 036104/1–036104/8, 2002.

[25] U. Wilensky, *NetLogo, Center for Connected Learning and Computer-Based Modeling*, Northwestern University, Evanston, Ill, USA, 1999.

[26] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, "Critical phenomena in complex networks," *Reviews of Modern Physics*, vol. 80, no. 4, pp. 1275–1335, 2008.

[27] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Physical Review E*, vol. 63, no. 6, Article ID 066117, 2001.

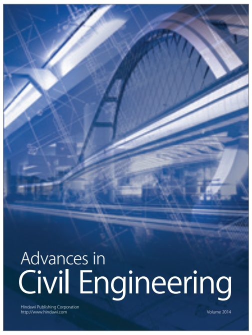
Journal of
Engineering

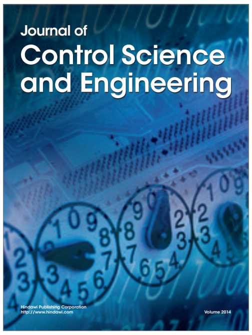
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

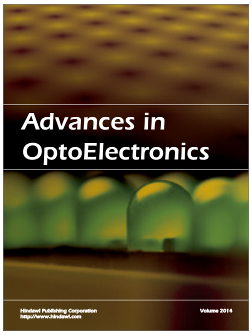
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

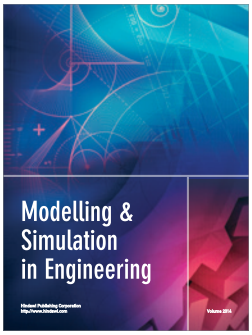
Journal of
Robotics

Journal of
Electrical and Computer Engineering

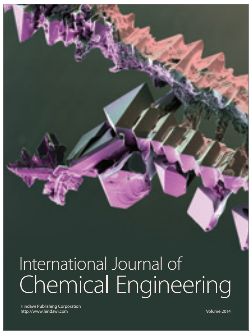

Advances in
OptoElectronics

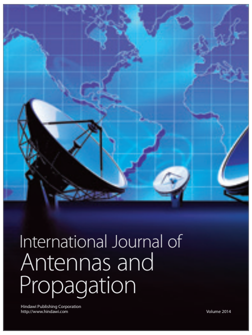
VLSI Design

International Journal of
Navigation and Observation

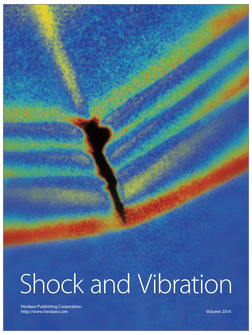

Modelling & Simulation in Engineering

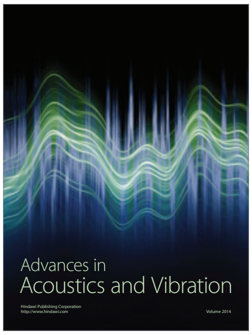
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration