Fall 12-2014

Security Analysis on Network Systems Based on Some Stochastic Models

Xiaohu Li
xli18@uno.edu

Security Analysis on Network Systems Based on Some Stochastic Models

A Dissertation

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of the
requirements for the degree of

Doctor of Engineering and Applied Science
in
Mathematics

by

Xiaohu Li

Ph.D. University of New Orleans, 2014

December, 2014

Acknowledgments

I would like to give my sincere gratitude toward Professor Linxiong Li, who generously spent numerous afternoons in the past two years on discussing lots of details in this dissertation. Professor Li also read through the earlier draft of this dissertation with great patience and presented many valuable suggestions, without which, I believe, there is still a long way for it to take the present form. As a respectable professor, Dr. Li taught me quite a lot in statistical science; As a faith-worthy friend, Dr. Li also helped me to deal with other things in my campus life.

I would like to thank other four committee members,

Professor Tumulesh Solanky Department of Mathematics, College of Sciences, University of New Orleans

Professor Jairo Santanilla Department of Mathematics, College of Sciences, University of New Orleans

Professor Xiaorong Li Department of Electrical Engineering, College of Engineering, University of New Orleans

Associate Professor Nikolas I. Xiros Department of Naval Architecture and Marine Engineering, College of Engineering, University of New Orleans

their advices and suggestions contribute in several aspects to this dissertation. Also

I would like to extend my thank to those faculties who brought me into the world of statistics and engineering through teaching the interesting graduate courses. Besides, I want to address the gratitude to several of graduate students in China, their studious effort to pursue academic excellence is always the main driving force of my research work in reliability, security and risk management.

Finally, I am deeply grateful to my wife, Xiao Zhou, for her continuous support, kind assistance and great patience and to my brother and sisters for taking care of my parents in the past two decades. I dedicate this dissertation to my parents.

Xiaohu Li

Department of Mathematics

University of New Orleans

New Orleans LA 70148

October 12, 2014

Contents

List of Figures

List of Tables

Abstract

Due to great effort from mathematicians, physicists and computer scientists, network science has attained rapid development during the past decades. However, because of the complexity, most researches in this area are conducted only based upon experiments and simulations, it is critical to do research based on theoretical results so as to gain more insight on how the structure of a network affects the security. This dissertation introduces some stochastic and statistical models on certain networks and uses a k-out-of-n tolerant structure to characterize both logically and physically the behavior of nodes. Based upon these models, we draw several illuminating results in the following two aspects, which are consistent with what computer scientists have observed in either practical situations or experimental studies.

Suppose that the node in a P2P network loses the designed function or service when some of its neighbors are disconnected. By studying the isolation probability and the durable time of a single user, we prove that the network with the user's lifetime having more NWUE-ness is more resilient in the sense of having a smaller probability to be isolated by neighbors and longer time to be online without being interrupted. Meanwhile, some preservation properties are also studied for the durable time of a network. Additionally, in order to apply the model in practice, both graphical and nonparametric statistical methods are developed and are employed to a real data set.

On the other hand, a stochastic model is introduced to investigate the security of

network systems based on their vulnerability graph abstractions. A node loses its designed function when certain number of its neighbors are *compromised* in the sense of being taken over by the malicious codes or the hacker. The attack compromises some nodes, and the victimized nodes become accomplices. We derived an equation to solve the probability for a node to be compromised in a network. Since this equation has no explicit solution, we also established new lower and upper bounds for the probability.

The two models proposed herewith generalize existing models in the literature, the corresponding theoretical results effectively improve those known results and hence carry an insight on designing a more secure system and enhancing the security of an existing system.

Key words: Durable time; Exponential distribution; Harmonic mean; Increasing convex order; Isolation probability; Jackknifing; k-out-of-n; NWUE; Pareto distribution; Power law distribution; Stochastic orders; Random graph; TTT plot; U-statistic

AMS 1991 Subject Classification: Primary 60E15, Secondary 60K10

1

Introduction and Preliminaries

1.1 Introduction

Computer and network security has become a rather popular and important topic in the past two decades. A simple Google search based on the keyword "computer and network security" showed 27.8 million items on September 25, 2014. In general, network security mainly aims to protect the entire infrastructure of a network system as well as its corresponding services from unauthorized access. There are several fundamental components in network security:

(i) Security-specific infrastructures, such as hardware- and software-based fire-walls and physical security approaches;

(ii) Security polices, which include security protocols, users authentications, authorizations, access controls, information integrity and confidentiality;

(iii) Detection of malicious programs, including anti-viruses, worms, or Trojan horses, and spyware or malware;

(iv) Intrusion detection and prevention, which encompasses network traffic surveillance and analyzing and profiling user behavior.

Since the topic of network security links a great number of research areas and disciplines, we will investigate the role the infrastructures of a network plays in the system's security based upon some stochastic models. For an overall introduction on network security, including key tools and technologies used to secure network access, please refer to Malik (2003) and Laet and Schauwers (2005).

1.1.1 Peer to peer network

As a decentralized structure, a Peer-to-Peer (P2P) computer network utilizes diverse connectivity among users participating a network and the cumulative bandwidth of them rather than conventional centralized resources where a relatively low number of servers play the key role in providing a service or application.

P2P networks, which are usually used for connecting nodes through largely ad hoc connections, are useful for many purposes. Sharing content files containing audio, video, data or anything in digital format and real time data. P2P networks can be classified by what they can be used for: (i) file sharing, (ii) telephony, (iii) media streaming (audio, video), and (iv) discussion forums etc.

A pure P2P network does not have any clients or servers but only equal peer nodes that function as both "clients" and "servers" simultaneously to the other nodes in the network (see Figure 1.1.1). This structure of network differs from the client-server model where communication is mostly between the node and a central server (see Figure 1.1.1). As a typical example, an FTP server transfers file in a manner totally different from that a P2P network does. Actually, the client and server programs in an FTP server are quite distinct, the clients initiate the download/uploads, and the servers offer the service according to these requests.

Besides the pure P2P network, there are quite a lot of Hybrid P2P networks. For example, as a distributed discussion system, the Usenet news server system also adopts

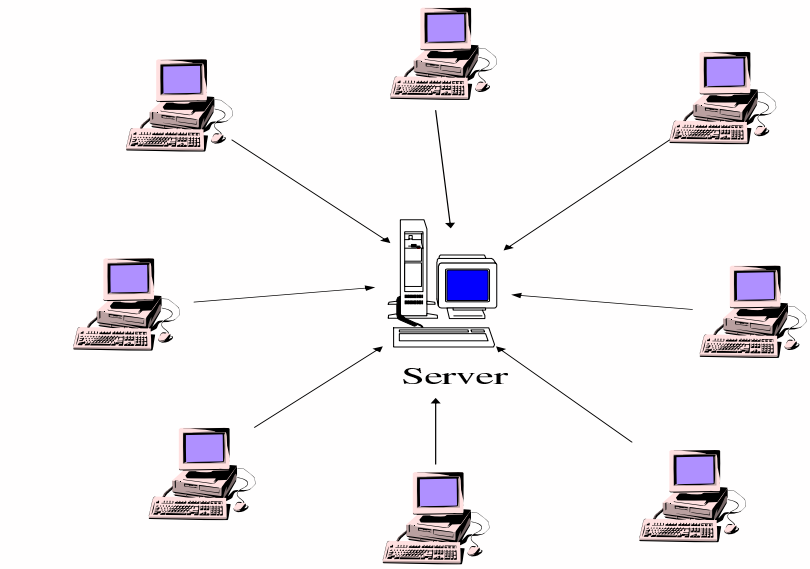


Figure 1.1: A server based network

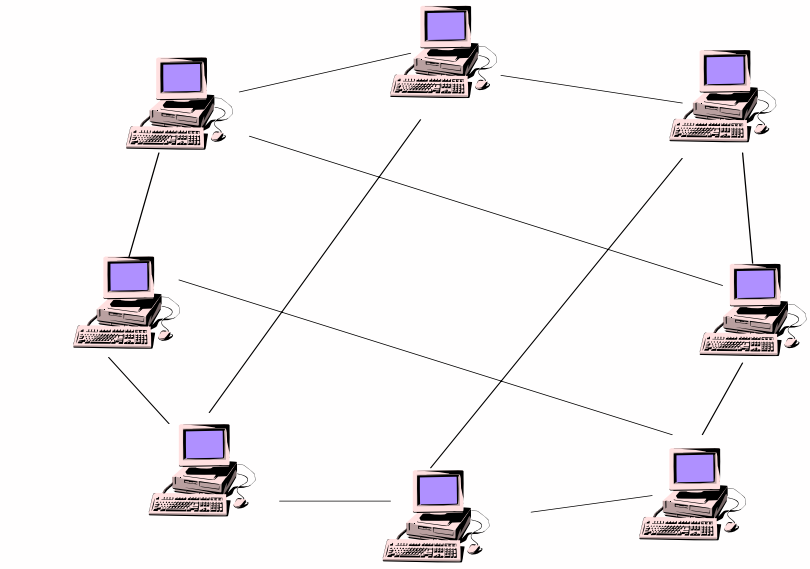


Figure 1.2: A P2P based network

a client-server form. To disseminate Usenet news articles over the entire Usenet network, news servers communicated with each other. However, the news server system acts in a client-server style when individual users access a local news server to deal with news. As another example, in an SMTP email system, the core email relaying network of mail transfer agents from a P2P model while the periphery of Mail user agents and their direct connections is client-server. On the other hand, some other networks, for example, Napster, OpenNAP and IRC, use a client-server structure for some tasks (e.g. searching) and a P2P structure for others.

Currently, P2P structure rapidly evolves and is widely used in distributed networks not only computer to computer but also human to human. Without any server, a node in P2P network mainly relies upon connections from its neighbors to operate correctly and losing some connections implies the failure of this node, it is very important to study its resilience and reliability. Leonard et al (2007) built the lifetime model for a P2P network, it is assumed that the node is isolated when it is physically disconnected from all its neighbors, that is, all connections are broken. In Chapter 2, we study the resilience of the pure P2P network through a new lifetime model, which is a generalization of that proposed by Leonard et al (2007) in the sense that a node loses the function and service if and only if some of its neighbor nodes are disconnected, this enable the new model to include both physical and logical isolation and hence to be more useful in practical situations. We derive the probability for a node to be isolated and the expected dural time, and show that the more heavier the tail of probability of the lifetime is, the more resilient the P2P network is.

1.1.2 Vulnerable network

With the rapid development of computer, this world gets more involved into networks. As a result, any minor failure in a network that you participate may collapse the whole

network and hence result in hazardous loss in business. In fact, the past two decades witnessed numerous such kind of cases. This fundamentally attributes to vulnerability of networks and it is rather urgent to study the network security so as to effectively defense the network from being invaded.

Network security usually consists of those provisions made in an underlying computer network topology, policies adopted by the network administrator to protect the network, the network-accessible resources from unauthorized access, and consistent and continuous monitoring to measure its effectiveness.

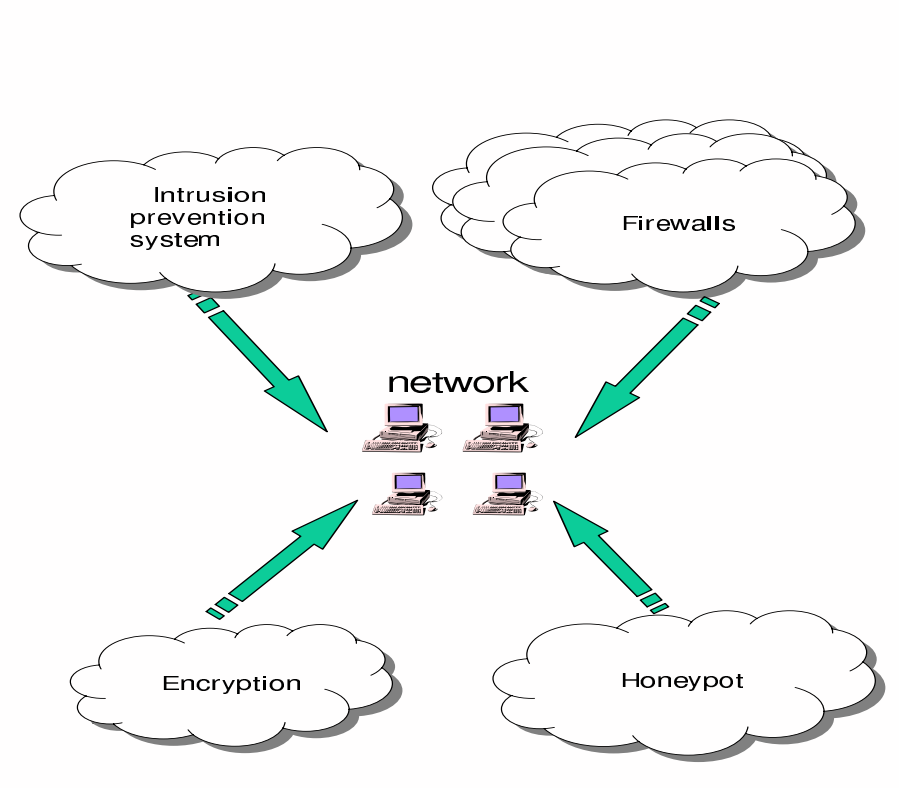


Figure 1.3: A depiction of a vulnerable network with security components

Network security originates from authenticating all user a username and a password. After the authentication, a fire wall is employed to enforce access policies which control legal services to be accessed by all network users. The fire wall may prevent the network

from being accessed without being authorized, however, this component fails to check potentially harmful contents such as computer worms and virus being disseminated over the network. In order to screen these malicious codes, an intrusion prevention system (IPS) (see Mirkovic et al, 2004) is designed to detect and prevent such malware from invading the network. Additionally, IPS also monitors for suspicious network traffic for contents, volume and anomalies so as to protect the network from being attacked by denial of service. On the other hand, to keep privacy, communication between two host nodes in the network is encrypted as well. Meanwhile, all individual events occurred in the network are tracked and audited for a later high level analysis. Besides, as surveillance and early-warning tools, Honeypots (see Grimes, R. A., 2005) essentially decoying network-accessible resources is also deployed in a network. Techniques employed by attackers attempting to compromise any decoy resources are studied during and after an attack to keep an eye on those new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honey pot.

For a comprehensive summary of standard concepts and methods in network security, please refer to Curtin (1997) and Simmonds et al (2004), which presents all notions and techniques in the form of an extensible ontology of network security attacks.

In Chapter 3, the network is abstracted as a vulnerable graph, which is composed of nodes (users) and edges (connections). In order to model the infrastructure of the network, a node of the graph is always assumed to have a random degree representing its neighbors. Since our aim is to investigate how the random degree has an impact on the network security, an attack outside the network is supposed to attempt to compromise nodes all the time and any compromised nodes become his accomplices in the sense of having the capability of compromising their neighbors. On the other hand, due to these security components deployed over the network, the attacker only penetrates the protection system with a certain probability, and the compromised nodes may be detected

after being compromised and hence become secure after being disinfected. Likewise, to make our model more multifunctional, it is also assumed that a node is compromised only when at lease some prefixed number of neighbors are infected. This model is an substantial extension of that studied by Li et al (2011). In effect, we proved that the probability for a node to be compromised is increasing as the random degree grows in the increasing convex order. Among others, new lower and upper bounds are also built for the probability to be compromised, evaluations reveals that they are better than those developed in Li et al (2011). The main result shows that power law graph is more vulnerable than both the random graph and the regular graph.

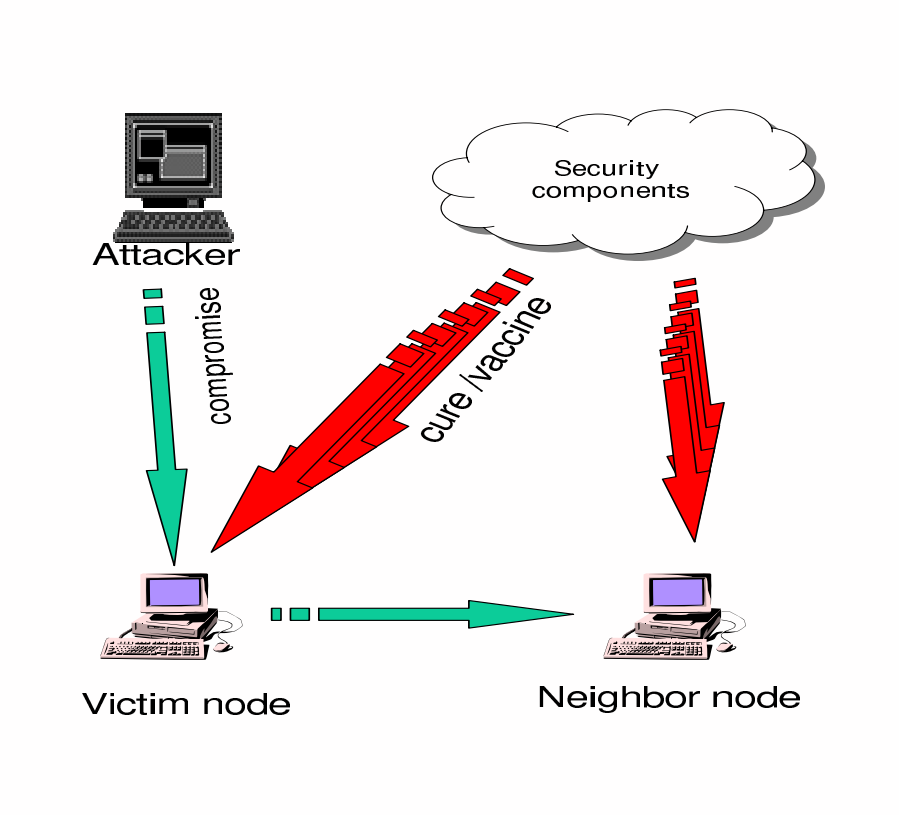


Figure 1.4: A depiction of a vulnerable network with security components

1.2 Preliminaries

For ease of references, let us recall some fundamental yet important concepts on aging property and stochastic ordering, which will be employed to characterize network systems in the following chapters.

Throughout this dissertation, the term *increasing* is used instead of monotone non-decreasing and the term *decreasing* is used instead of monotone non-increasing. We also assume that all random variables under consideration have 0 as the common left end point of their supports, and all random variables are implicitly assumed to be absolutely continuous.

1.2.1 Important notations

1.2.2 Several aging properties

For a nonnegative random variable X with distribution function F and the reliability function $\bar{F} = 1 - F$, let

$$X_t = X - t | X > t$$

be the residual lifetime of X at time $t \geq 0$, the mean residual lifetime

$$\mu_F(t) = \mathsf{E}[X - t | X > t] = \frac{\int_t^\infty \bar{F}(x)\,\mathrm{d}x}{\bar{F}(t)}.$$

Definition 1.2.1 A random lifetime X is said to be of

(i) *increasing failure rate* (IFR) if the cumulative failure rate $-\ln \bar{F}(t)$ is convex with respect to $t \geq 0$;

(ii) *increasing failure rate in average* (IFRA) if the cumulative failure rate $-\ln \bar{F}(t)$ is

star-shaped with respect to $t \geq 0$, that is, $-\frac{1}{t}\log \bar{F}(t)$ is increasing in $t \geq 0$;

(iii) *decreasing mean residual life* (DMRL) if $\mu_F(s) \geq \mu_F(t)$ for all $t \geq s \geq 0$;

(iv) *new better than used in expectation* (NBUE) if $\mu_F(t) \leq \mu_F(0)$ for all $t \geq 0$.

Reversing the monotone property and the inequality above, we get their dual versions: DFR (decreasing failure rate), DFRA (decreasing failure rate in average), IMRL (increasing mean residual life) and NWUE (new better than used in expectation). The following chain of implications is well-known,

$$IFR\,(DFR) \Longrightarrow IFRA\,(DFRA) \Longrightarrow DMRL\,(IMRL) \Longrightarrow NBUE\,(NWUE).$$

For more details on these nonparametric aging properties, please refer Barlow and Proschan (1981), Lai and Xie (2006).

1.2.3 Some stochastic orders

For two nonnegative random variable X and Y with distribution functions F and G, and reliability function $\bar{F} = 1 - F$ and $\bar{G} = 1 - G$, denote F^{-1} and G^{-1} the corresponding right continuous inverses of F and G respectively.

Definition 1.2.2 X is said to be smaller than Y in the

(i) *hazard rate* order (denoted by $X \leq_{\rm hr} Y$) if $\bar{F}(t)/\bar{G}(t)$ is decreasing in $t \geq 0$;

(ii) *stochastic order* (denoted as $X \leq_{\rm st} Y$) if $\Pr(X > t) \leq \Pr(Y > t)$ for all t;

(iii) *increasing convex order* (denoted as $X \leq_{\rm icx} Y$) if

$$\int_t^\infty \Pr(X > x)\,{\rm d}x \leq \int_t^\infty \Pr(Y > x)\,{\rm d}x, \quad \text{for all } t;$$

(iv) *harmonic mean residual life* order (denoted by $X \leq_{\rm hmrl} Y$) if, for all $t \geq 0$,

$$\left[\frac{1}{t}\int_0^t \frac{1}{\mu_F(u)}\,\mathrm{d}u\right]^{-1} \leq \left[\frac{1}{t}\int_0^t \frac{1}{\mu_G(u)}\,\mathrm{d}u\right]^{-1},$$

for which the expectations exist.

(v) *convex order* (denoted by $X \leq_{\rm cx} Y$) if $\mathsf{E}[\phi(X)] \leq \mathsf{E}[\phi(Y)]$ for any convex ϕ.

It holds evidently that

$$X \leq_{\rm hr} Y \Longrightarrow X \leq_{\rm st} Y \Longrightarrow X \leq_{\rm icx} Y \Longrightarrow X \leq_{\rm cx} Y.$$

Kochar and Wiens (1987) proposed a partial order to compare the NBUE-ness of two life distributions. Since NBUE and NWUE are dual with each other, for convenience, we call it the NWUE order.

Definition 1.2.3 X is said to be *more NWUE* than Y (denoted by $X \geq_{\rm nwue} Y$) if

$$\frac{\mu_F\big(F^{-1}(v)\big)}{\mu_G\big(G^{-1}(v)\big)} \geq \frac{\mu_F}{\mu_G}, \quad \text{for all } v \in (0,1). \tag{1.1}$$

As a function of $v \in (0,1)$,

$$\int_0^{F^{-1}(v)} \bar{F}(t)\,\mathrm{d}t$$

is the well-known *total time on test* (TTT) transform of the distribution F of a random lifetime X. The scaled TTT transform

$$\varphi_F^{-1}(v) = \frac{1}{\mu_F}\int_0^{F^{-1}(v)} \bar{F}(t)\,\mathrm{d}t$$

plays an important role in characterizing aging property of random lifetime. One may see Kochar et al. (2002), Li and Shaked (2007) for more on TTT transform.

Recently, Kochar et al. (2002) proposed a new partial order: X is said to be larger than Y in the *total time on test transform* order (denoted by $X \leq_{\text{ttt}} Y$) if

$$\int_0^{F^{-1}(v)} \bar{F}(x)\,\mathrm{d}x \geq \int_0^{G^{-1}(v)} \bar{G}(x)\,\mathrm{d}x, \quad \text{for all } v \in (0,1).$$

These two stochastic orders mentioned above have a close relation in the sense that when $\mathsf{E}[X] = \mathsf{E}[Y]$, $X \geq_{\text{nwue}} Y$ is equivalent to $X \geq_{\text{ttt}} Y$.

Readers may refer to Müller and Stoyan (2002), Shaked and Shanthikumar (2007), and Li and Li (2013) for more details on these stochastic orders.

1.2.4 The k-out-of-n structure

Let $X_1, X_2, \cdots, X_n$ denote n independent component lifetimes with $X_{i,n}$ being the i-th order statistic, here $i = 1, \cdots, n$. A k-out-of-n system of these components functions if and only if at least k components function. When $k = n$, the system has a series structure with lifetime

$$X_{n,n} = \min\{X_1, \cdots, X_n\};$$

whereas for $k = 1$, it reduces to a parallel structure with lifetime

$$X_{1,n} = \max\{X_1, \cdots, X_n\}.$$

Thus, a k-out-of-n system is more general than either a series or a parallel structure. The lifetime of this system is simply given by the order statistic $X_{n-k+1:n}$.

As a fault-tolerant structure, the k-out-of-n system is widely used in many practical situations, including, for example, electronic engineering, manufacturing and defense industry etc. One may refer to Kuo and Zuo (2006) and Lai and Xie (2006) for comprehensive discussions on k-out-of-n structure. In this thesis, we will employ this structure

to describe a network which is tolerant to some compromised neighbors due to anti-virus software.

1.3 Archimedean copula

Mutual independence among multiple random variables is common in reliability and risk management. The interdependence among components' lifetimes, random risks, and potential loss/returns etc. cannot be ignored in practical situations. In classical statistical theory, Pearson's correlation coefficient is usually utilized to measure the dependence among random variables. In Chapter 2 we will instead employ copula, a functional measure, to characterize the association among network users' lifetimes.

For a random vector $\boldsymbol{X} = (X_1, \ldots, X_n)$ with joint distribution function F, survival function $\bar{F}$ and univariate marginal distribution functions $F_1, \ldots, F_n$, its *copula* is defined as

$$C_{\boldsymbol{X}}(u_1, \cdots, u_n) = F\big(F_1^{-1}(u_1), \cdots, F_n^{-1}(u_n)\big), \qquad 0 < u_1, \cdots, u_n < 1.$$

In parallel, the *survival copula* is

$$\widehat{C}_{\boldsymbol{X}}(u_1, \cdots, u_n) = \bar{F}\big(\bar{F}_1^{-1}(u_1), \cdots, \bar{F}_n^{-1}(u_n)\big), \qquad 0 < u_1, \cdots, u_n < 1.$$

Since the copula does not contain any information of marginal distributions, it provides us with a rather convenient way to impose a dependence structure onto predetermined marginal distributions in practice. Actually a large number of excellent applications of copulas can be found in various areas, and so far copula has become more or less a standard tool in risk management, finance, econometrics and actuarial science etc. Recently, Copulas are being used for reliability analysis of complex systems of machine components with competing failure modes in reliability engineering, see for example Pham

and Hong (2003), and copula functions have been successfully applied to the database formulation for the reliability analysis of highway bridges, and to various multivariate simulation studies in civil, mechanical and offshore engineering, see for example Thompson and Kilgore(2011). In literature on statistics, there are a large number of copulas depicting various dependence structures, Hutchinson and Lai (1990) and Nelsen (2006) provide a wide range families of bivariate copulas along with their properties. In the past twenty years, Archimedean copulas became particularly popular because of its mathematical tractability and the capability of capturing wide ranges of dependence. Notably, since the statistical inference on Archimedean copulas has got well developed in this decade, excellent applications are coming to the fore in various areas.

Definition 1.3.1 (McNeil and Nešlehová (2009)) For a non-increasing and continuous function $\phi : [0, +\infty) \mapsto [0, 1]$ such that $\phi(0) = 1$ and $\phi(+\infty) = 0$, let $\psi = \phi^{-1}$ be the pseudo-inverse,

$$C_\phi(u_1, \cdots, u_n) = \phi\big(\psi(u_1) + \cdots + \psi(u_n)\big), \quad \text{for } (u_1, \cdots, u_n) \in [0, 1]^n, \tag{1.2}$$

is called an *Archimedean copula* with the generator ϕ if $(-1)^k \phi^{(k)}(x) \geq 0$ for $k = 0, \ldots, n-2$ and $(-1)^{n-2}\phi^{(n-2)}(x)$ is non-increasing and convex.

The generator ϕ is said to be *strict* if $\phi(+\infty) = 0$. As is well-known, the Archimedean family contains a plenty of useful copulas, including some well-known ones. For example, the independence (product) copula $C_1(\boldsymbol{u}) = \prod_{i=1}^n u_i$ with the generator $\phi(t) = e^{-t}$, the Clayton copula

$$C_2(\boldsymbol{u}) = \left(\prod_{i=1}^n u_i^{-\theta} - n + 1 \right)^{-1/\theta}$$

with the generator $\phi(t) = (\theta t + 1)^{-1/\theta}$ for $\theta \geq 0$, and the Ali-Mikhail-Haq (AMH) copula

$$C_3(\boldsymbol{u}) = \frac{(1-\theta)\prod_{i=1}^{n} u_i}{\prod_{i=1}^{n}(1-\theta+\theta u_i) - \theta\prod_{i=1}^{n} u_i}.$$

with the generator $\phi(t) = \frac{1-\theta}{e^t-\theta}$ for $\theta \in [0, 1)$. For more on copula and its applications, we refer readers to Joe (1997) and Nelsen (2006).

1.4 Summary

Resilience analysis of P2P network

By studying the isolation probability and the durable time of a single user, we conduct resilience and reliability analysis of the P2P network, which is widely used in communication systems in recent several years due to the decentralized property. It is proved that the network with the user's lifetime having more NWUE-ness is more resilient. Both graphical and nonparametric statistical methods are developed to test the NWUE order between two real data sets.

Security analysis of networks

A stochastic model is introduced to investigate security of network systems based on their vulnerability graph abstractions. Instead of doing traditional security analysis, we employ the increasing convex ordering to study the underlying vulnerability graph, the main theoretical results carry an insight on designing a more secure system and enhancing the security of an existing system.

2

Resilience Analysis of P2P Network Systems

2.1 Introduction

Peer-to-Peer (P2P) internet network allows a group of computer users equipped with the same networking program to connect with each other for the purpose of directly accessing files from one another's hard drives. A P2P network functions by connecting individual computers together to share files instead of going through a central server. P2P networks can be classified by what they can be used for, for instance, content delivery, file sharing, telephony, media streaming (audio, video) and discussion forums etc. In the current study of P2P networks, Kaashoek and Karger (2003) and Stoica et al. (2001) investigate the single-node isolation, Aspnes et al. (2002), Ganesh and Massoulie (2003), Gummadi et al. (2003), and Massoulié (2003) etc discuss the disconnection of the entire graph. Bhagwan et al. (2003) is among the first to pay attention to the more realistic P2P failure models, in which the intrinsic behavior of internet users is taken into account and the departments of users depend on more complex factors including their attention span and browsing habits, and so on, other than the traditional simple binary metric. In order to investigate the properties of such systems, Leonard et al. (2005) recently introduces the node-failure

model based on users' lifetimes and studies the stochastic resilience of P2P networks, in which an user stays online for random periods of time till all his neighbors go off line or he leaves the network on his own initiative. In this model, the random lifetime that an arriving user will stay on line reflects both the behavior of the user itself and the duration of its service to the entire P2P network community.

This chapter proposes a more general P2P network model, in which an user is isolated only when a number of its neighbors leave the network and hence the P2P model in Leonard et al. (2005) is included as a special case. We further investigate both the stochastic resilience and reliability properties of this new model. It is proved that the network with the user's lifetime having more NWUE-ness is more resilient. The rest of this paper is organized as below: Section 2 introduces the new P2P network model. Section 3 studies the stochastic resilience by using the isolation probability of a single user, and Section 4 discusses some reliability properties of the available time of a single user in the network. Finally, both graphical and nonparametric methods are developed in section 5 to detect the NWUE order between two data sets. All main conclusions are consistent with those obtained through experiments in the literature.

2.2 Model description

In this section, we describe our P2P network model in details and present its rationality.

For an internet user, let X, a nonnegative random variable, be the lifetime that stays online in the network for his own purpose or providing services to other peers. Saroiu et al. (2002), Bustemante and Qiao (2003) pointed out that the distribution of an user's lifetime in practical P2P network very well accords with Pareto distribution, which possesses of the well-known *new worse than used in expectation* (NWUE) property (they called it the *heavy-tail* property). It is worthwhile mentioning that Harchol-Balter and Downey (1997)

found that the distribution of the lifetime of an UNIX process is also Pareto, it was named there as *used better than new in expectation* (UBNE) instead of NWUE. Here, we assume a general type of the distribution of the user's lifetime other than Pareto law so that the new model not only is suitable for human-based P2P networks but also can be applied to non-human network systems.

For a new internet user with random lifetime X having the distribution function F, assume

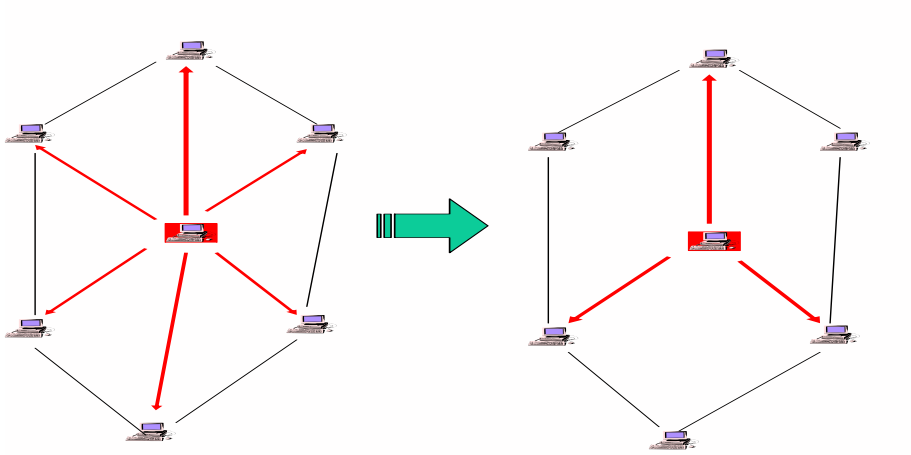


Figure 2.1: A typical depiction of a node with 3-out-of-6 structure

(i) the P2P network system has operated so long that there is no transient effect, that is, the expected lifetime of the new user is negligible in contrast to the age of the whole P2P system;

(ii) when entering the system, the new user randomly (in the sense that each existing user has the same probability to be selected) picks k neighbors from the existing nodes in the system as soon as it enters into the system;

(iii) the selection of neighbors is independent of both the lifetime X and the neighbors' present ages;

(iv) the time that a new user will spend in the system is independent of those of his neighbors.

Since the P2P network has operated for a sufficiently long period when the new user joins the system, it is reasonable to suppose that all those selected neighbors have $\tilde{X}$, the equilibrium renewal excess lifetime of X, as their common residual lifetime, that is,

$$F_{\tilde{X}}(t) = \frac{1}{\mu_F} \int_0^t \bar{F}(x)\, \mathrm{d}x,$$

where $\mu_F = \mathsf{E}[X]$ and $t \geq 0$.

For $1 \leq r \leq k$, denote $\tilde{X}_r$ the residual lifetime of the r-th neighbor. According to David and Nagaraja (2003), the order statistic $\tilde{X}_{r,k}$, which gives the residual lifetime of the r-th failed neighbor, has the reliability function

$$\bar{F}_{\tilde{X}_{r,k}}(t) = \sum_{i=0}^{r-1} \binom{k}{i} \left[F_{\tilde{X}}(t)\right]^i \left[\bar{F}_{\tilde{X}}(t)\right]^{k-i} = r\binom{k}{r} \int_{F_{\tilde{X}}(t)}^1 u^{r-1}(1-u)^{k-r}\, \mathrm{d}u$$

and the probability density function

$$f_{\tilde{X}_{r,k}}(t) = \frac{r}{\mu}\binom{k}{r} \bar{F}(t) \left[F_{\tilde{X}}(t)\right]^{r-1} \left[\bar{F}_{\tilde{X}}(t)\right]^{k-r}.$$

In the study of passive model in Leonard et al. (2005), a node is considered as isolated after its last surviving neighbor fails. However, in many realistic environments, neighbors of a node usually fail to service due to lower performance and in fact it reaches the isolation state only if there are$1 \leq r \leq k$ neighbors in failure. An instantiation of such a case is that this node is sharing an animation file with its neighbors. Under the condition that a fraction of its neighbors (not necessary all its neighbors) fail to service, the display of the animation file is so incoherent that this node can be considered as disconnected. As a result, we adopt the more general P2P model that a node is considered to be isolated

or disconnected only when more than $r-1$ neighbors fail to service. This is in fact the famous r-out-of-k structure and thus the passive model in Leonard et al. (2005) is the special case with $r = k$.

We will investigate the stochastic resilience of this P2P model by using the *isolation probability*

$$\pi_r(X) = \Pr\left(X > \tilde{X}_{r,k}\right), \tag{2.1}$$

which denotes the probability that the new node outlives the residual lifetime of its r-th neighbor before it decides to leave the system. It is obvious that larger isolation probability means worse resilience of the P2P network. On the other hand, we will employ

$$T_r(X) = \min\left\{X, \tilde{X}_{r,k}\right\} \tag{2.2}$$

rather than $\tilde{X}_{r,k}$ to measure the *durable time* of a new node in a P2P network. It should be marked here that Leonard et al. (2005) studies P2P networks by using $\tilde{X}_{k,k}$, the time that all k neighbors of the new node are simultaneously in failure state before it decides to leave the system. However, as a competition between the lifetime X and the lifetime $\tilde{X}_{r,k}$, $T_r(X)$ takes into account both the failure due to neighbors and that due to the new user itself, it is more reasonable to serve as a metric to measure the stochastic resilience of P2P networks.

2.3 Resilience analysis

Resilience analysis of random graphs and various types of deterministic networks has attracted considerable interest of researchers during the past several decades. For more details, please refer to Bollobás (2001), Burtin (1977), and Leighton et al. (1995). Along this line of study, one of the most important problems is that under what failure conditions

the network appears disconnection or demonstrates noticeably lower performance to its users. Assuming uniformly random node failure, Stoica et al. (2001), Bollobás (2001), Gummadi et al. (2003) derive the conditions from different points of view under which the networks stay connected after some nodes fail.

In this section, we study the resilience of P2P network systems by evaluating the isolation probability for any given user. As described in Section 2, a node with lifetime X is forced to disconnect from the system only if X is greater than $\tilde{X}_{r,k}$, $1 \le r \le k$. Then, the isolation probability is

$$\begin{aligned}
\pi_r(X) &= \Pr\left(\tilde{X}_{r,k} < X\right) \\
&= \int_0^\infty \Pr(X > t) f_{\tilde{X}_{r,k}}(x)\,\mathrm{d}t \\
&= \frac{r}{\mu^k}\binom{k}{r}\int_0^\infty \bar{F}^2(t)\left(\int_0^t \bar{F}(u)\,\mathrm{d}u\right)^{r-1}\left(\int_t^\infty \bar{F}(u)\,\mathrm{d}u\right)^{k-r}\mathrm{d}t. \qquad (2.3)
\end{aligned}$$

As illustrations, isolation probabilities corresponding to the three popular lifetime distributions are evaluated in the following examples.

Example 2.3.1 (Pareto distribution) Suppose the user has a lifetime X with probability distribution

$$G(x) = 1 - \left(1 + \frac{t}{\beta}\right)^{-\alpha}, \quad t > 0,\ \alpha > 1,\ \beta > 0.$$

Then, for any $1 \le r \le k$, the isolation probability

$$\begin{aligned}
\pi_r(X) &= r\binom{k}{r}\left(\frac{\alpha-1}{\beta}\right)^k \int_0^\infty \left(1+\frac{t}{\beta}\right)^{-2\alpha}\left[\int_0^t \left(1+\frac{u}{\beta}\right)^{-\alpha}\mathrm{d}u\right]^{r-1}\left[\int_t^\infty \left(1+\frac{u}{\beta}\right)^{-\alpha}\mathrm{d}u\right]^{k-r}\mathrm{d}t \\
&= \binom{k}{r}\frac{r(\alpha-1)}{\beta}\int_0^\infty \left(1+\frac{t}{\beta}\right)^{-2\alpha}\left[1-\left(1+\frac{t}{\beta}\right)^{1-\alpha}\right]^{r-1}\left(1+\frac{t}{\beta}\right)^{(1-\alpha)(k-r)}\mathrm{d}t
\end{aligned}$$

$$
\begin{aligned}
&= \binom{k}{r} \frac{r(\alpha-1)}{\beta} \int_0^\infty \left[1 - \left(1+\frac{t}{\beta}\right)^{1-\alpha}\right]^{r-1} \left(1+\frac{t}{\beta}\right)^{(1-\alpha)(k-r)-2\alpha} \mathrm{d}t \\
&= r\binom{k}{r} \int_0^1 t^{k-r+\frac{\alpha}{\alpha-1}} (1-t)^{r-1} \mathrm{d}t \qquad (2.4) \\
&= \frac{k!}{(k-r)!} \frac{\Gamma\left(k-r+1+\frac{\alpha}{\alpha-1}\right)}{\Gamma\left(k+1+\frac{\alpha}{\alpha-1}\right)}, \qquad \text{for any } 1 \le r \le k.
\end{aligned}
$$

■

Example 2.3.2 (Exponential distribution) Suppose the user has a lifetime Y with distribution

$$F(x) = 1 - e^{-\lambda t}, \qquad t \ge 0.$$

According to (2.3), any new node has the isolation probability

$$
\begin{aligned}
\pi_r(Y) &= r\binom{k}{r} \lambda^k \int_0^\infty \frac{e^{-2\lambda t}}{\lambda^{r-1}} \left(1-e^{-\lambda t}\right)^{r-1} \frac{1}{\lambda^{k-r}} \left(e^{-\lambda t}\right)^{k-r} \mathrm{d}t \\
&= r\binom{k}{r} \lambda \int_0^\infty \left(e^{-\lambda t}\right)^{k-r+2} \left(1-e^{-\lambda t}\right)^{r-1} \mathrm{d}t \\
&= r\binom{k}{r} \int_0^1 t^{k-r+1} (1-t)^{r-1} \mathrm{d}t \qquad (2.5) \\
&= \frac{k!}{(r-1)!(k-r)!} \frac{(r-1)!(k-r+1)!}{(k+1)!} \\
&= \frac{k-r+1}{k+1}, \quad \text{for any } 1 \le r \le k.
\end{aligned}
$$

■

Example 2.3.3 (Uniform distribution) Suppose the user Z has a lifetime with uniform distribution on the interval $(0, 2\mu)$, that is, the distribution function

$$H(x) = \frac{t}{2\mu}, \qquad 0 \le t \le 2\mu,\ \mu > 0.$$

Then, the isolation probability is

$$\begin{aligned}
\pi_r(Z) &= \binom{k}{r}\frac{r}{\mu^k}\int_0^{2\mu}\left(1-\frac{t}{2\mu}\right)^2\left[\int_0^t\left(1-\frac{u}{2\mu}\right)\mathrm{d}u\right]^{r-1} \\
&\quad\cdot\left[\int_t^{2\mu}\left(1-\frac{u}{2\mu}\right)\mathrm{d}u\right]^{k-r}\mathrm{d}t \\
&= \frac{r}{\mu}\binom{k}{r}\int_0^{2\mu}\left(\frac{2\mu-t}{2\mu}\right)^2\left[1-\left(\frac{2\mu-t}{2\mu}\right)^2\right]^{r-1}\left(\frac{2\mu-x}{2\mu}\right)^{2(k-r)}\mathrm{d}t \\
&= r\binom{k}{r}\int_0^1 t^{k-r+\frac{1}{2}}(1-t)^{r-1}\,\mathrm{d}t \qquad (2.6) \\
&= \frac{k!}{(k-r)!}\frac{\Gamma\left(k-r+\frac{3}{2}\right)}{\Gamma\left(k+\frac{3}{2}\right)}, \quad \text{for any } 1\le r\le k.
\end{aligned}$$

■

From (2.4), (2.5) and (2.6), we observe the following:

(i) All of the three probabilities of isolation are independent of the expectation of the user's lifetime. So, it seems that property of the distribution instead of the expectation has direct impact on the isolation probability.

(ii) The isolation probability corresponding to Pareto lifetime is the smallest one, the uniform distribution achieves the largest isolation probability. Thus, we may conclude that the P2P network that users has Pareto lifetime is the most resilient one.

Based upon the above two facts, one may wonder whether the isolation probability preserves some stochastic order on user's lifetime, that is, $\pi_r(X) < \pi_r(Y)$ holds for X smaller than Y in some stochastic sense. As a positive answer, Theorem 2.3.4 below asserts that a P2P network with users' lifetime having a stronger NWUE property is more resilient.

Theorem 2.3.4 *Suppose that X and Y are two nonnegative random variables which represent user lifetimes of two different P2P systems, respectively. Then, $X \geq_{\text{nwue}} Y$ implies $\pi_r(X) \leq \pi_r(Y)$.*

Proof: For any $1 \leq r \leq k$, the isolation probability $\pi_r(X)$ can be rephrased as

$$\begin{aligned}
\pi_r(X) &= \Pr(\tilde{X}_{r,k} < X) \\
&= \int_0^\infty F_{\tilde{X}_{r,k}}(x)\,\mathrm{d}F(x) \\
&= r\binom{k}{r}\int_0^\infty \int_0^{F_{\tilde{X}}(x)} u^{r-1}(1-u)^{k-r}\,\mathrm{d}u\,\mathrm{d}F(x) \\
&= r\binom{k}{r}\int_0^{\varphi_F^{-1}(v)} u^{r-1}(1-u)^{k-r}\,\mathrm{d}u\,\mathrm{d}F(x) \\
&= r\binom{k}{r}\int_0^1 \int_0^{\varphi_F^{-1}(v)} u^{r-1}(1-u)^{k-r}\,\mathrm{d}u\,\mathrm{d}v,
\end{aligned}$$

here the scaled TTT transform

$$\varphi_F^{-1}(v) = \frac{1}{\mu_F}\int_0^{F^{-1}(v)} \bar{F}(t)\,\mathrm{d}t.$$

Likewise, the isolation probability

$$\pi_r(Y) = r\binom{k}{r}\int_0^1 \int_0^{\varphi_G^{-1}(v)} u^{r-1}(1-u)^{k-r}\,\mathrm{d}u\,\mathrm{d}v.$$

Note that $X \geq_{\text{nwue}} Y$ if and only if, for all $v \in (0,1)$,

$$\frac{1}{\mu_F}\int_0^{F^{-1}(v)} \bar{F}(u)\,\mathrm{d}u \geq \frac{1}{\mu_G}\int_0^{G^{-1}(v)} \bar{G}(u)\,\mathrm{d}u,$$

the desired result follows immediately. ∎

For the three distributions in Examples 2.3.2, 2.3.1 and 2.3.3, it is easy to verify that $\mu_G(t) \equiv \mu_G$, $\mu_F(t) = (1 + t/\beta)\,\mu_F \geq \mu_F$ and $\mu_H(t) = \mu_H - t/2 \leq \mu_H$ for all $t \geq 0$.

As a result, it holds that $X \geq_{\text{nwue}} Y \geq_{\text{nwue}} Z$. According to Theorem 2.3.4, we have $\pi_r(X) \leq \pi_r(Y) \leq \pi_r(Z)$, which can also be verified directly in Examples 2.3.1, 2.3.2 and 2.3.3.

2.4 Reliability analysis

The mean durable time of a user entering into a P2P network system is derived as below.

Proposition 2.4.1 *For a P2P network system with user's lifetime X,*

$$\mathsf{E}[T_r(X)] = \frac{r\,\mu_F}{k+1}, \quad \textit{for all } r = 1, \cdots, k.$$

Proof: Since $T_r(X)$ is nonnegative, it holds that

$$\begin{aligned}
\mathsf{E}[T_r(X)] &= \int_0^\infty \Pr\left(\min\left\{X, \tilde{X}_{r,k}\right\} > x\right) \mathrm{d}x \\
&= \int_0^\infty \bar{F}(x)\bar{F}_{\tilde{X}_{r,k}}(x)\,\mathrm{d}x \\
&= r\binom{k}{r}\int_0^\infty \bar{F}(x)\left[\int_{F_{\tilde{X}}(x)}^1 u^{r-1}(1-u)^{k-r}\,\mathrm{d}u\right]\mathrm{d}x \\
&= r\binom{k}{r}\int_0^1 u^{r-1}(1-u)^{k-r}\left[\int_0^{F_{\tilde{X}}^{-1}(u)} \bar{F}(x)\,\mathrm{d}x\right]\mathrm{d}u \\
&= \mu r\binom{k}{r}\int_0^1 u^{r-1}(1-u)^{k-r}\left[\int_0^{F_{\tilde{X}}^{-1}(u)} \mathrm{d}F_{\tilde{X}}(x)\right]\mathrm{d}u \\
&= \mu r\binom{k}{r}\int_0^1 u^{r}(1-u)^{k-r}\,\mathrm{d}u \\
&= \frac{r\,\mu_F}{k+1}, \quad \text{for any } 1 \leq r \leq k.
\end{aligned}$$

■

The above proposition reveals that the durable time of a new user in P2P network is distribution free. More precisely, for a P2P network with any type of user's lifetime

distribution, the expected time it stays online depends upon the user's lifetime distribution only through its expectation.

2.4.1 Preservation of aging properties

The next result asserts that the durable time of the user in P2P system preserves both IFR and IFRA properties of the user's lifetime distribution.

Theorem 2.4.2 *If X is IFR (IFRA), then $T_r(X)$ is also IFR (IFRA).*

Proof: IFR implies DMRL. It is known that the DMRL property of X is equivalent to the IFR property of $\tilde{X}$. Since IFR property is preserved by the k-out-of-n structure with i.i.d units, it follows that $\tilde{X}_{r,k}$ is IFR. On the other hand, IFR property is also preserved by series system with independent components. So, we obtain the preservation of IFR.

Since IFRA property is preserved for coherent structure (see Barlow and Proschan (1981)), the rest proof is the same as before. ■

As an application of Theorem 2.4.2, we build a lower bound of reliability of the durable time of the user in P2P network.

Corollary 2.4.3 *Let X be a nonnegative random variable which represents the user's lifetime of P2P network system. If X is IFRA with mean μ, then, for all $1 \leq r \leq k$,*

$$\bar{F}_{T_r(X)}(x) \geq \left(1 - \frac{(k+1)t}{r\mu}\right)_+, \quad \textit{for all } t \geq 0,$$

where $x_+ = \max\{x, 0\}$.

Proof: Theorem 2.4.2 guarantees that $T_r(X)$ is IFRA and hence NBUE. By Hu et al (2001), it holds that X is NBUE if and only if $\tilde{X} \leq_{\text{st}} X$, which implies

$$F_{T_r(X)}(x) \leq \frac{1}{\mathsf{E}[T_r(X)]} \int_0^t \bar{F}_{T_r(X)}(u)\, \mathrm{d}u \leq \frac{(k+1)t}{r\mu},$$

for all $1 \leq r \leq k$ and $t \geq 0$. This completes the proof. ∎

2.4.2 Stochastic monotonicity

Hu et al. (2001) characterized some stochastic orders in terms of other stochastic orders between their corresponding equilibrium versions. Especially, it is proved that $X \leq_{\mathrm{hr}} (\leq_{\mathrm{st}})Y$ if and only if $\tilde{X} \leq_{\mathrm{hr}} (\leq_{\mathrm{st}})\tilde{Y}$. Based on this and the fact that both the order $\leq_{\mathrm{hr}}$ and the order $\leq_{\mathrm{st}}$ are closed for k-out-of-n structure with independent units (see Shaked and Shanthikumar (2007)), it is easy to obtain the proposition below, which asserts that the durable time of the user in P2P network preserves both the hazard rate order and the stochastic order of the parent distribution.

Proposition 2.4.4 *If* $X \leq_{\mathrm{hr}} (\leq_{\mathrm{st}}) Y$, *then* $T_r(X) \leq_{\mathrm{hr}} (\leq_{\mathrm{st}}) T_r(Y)$.

At the beginning of this section, we have concluded that the durable time of the user in P2P network is distribution free. In other words, we cannot distinguish the difference between P2P network systems with different types of user lifetime distributions by contrasting the mean durable times of users. In this subsection, we will present a convex order result on T_r. Precisely, the durable times of the user of two different P2P network systems are ordered in the sense of the convex order if their respective parent distributions are of common mean and ordered in the sense of the harmonic mean residual life order. Let us first recall a useful lemma due to Shaked and Shanthikumar (2007).

Lemma 2.4.5 *Suppose* $\mathsf{E}[X] = \mathsf{E}[Y]$. *Then,* $X \leq_{\mathrm{cx}} Y$ *if and only if*

$$\int_x^\infty \bar{F}(u)\,\mathrm{d}u \leq \int_x^\infty \bar{G}(u)\,\mathrm{d}u, \quad \textit{for all } x.$$

Now, we get ready to present our main result in this subsection.

Theorem 2.4.6 *Suppose* $\mathsf{E}[X] = \mathsf{E}[Y]$. *If* $X \leq_{\rm hmrl} Y$, *then* $T_r(X) \leq_{\rm cx} T_r(Y)$.

Proof: For all $1 \leq r \leq k$ and $t \geq 0$, it holds that

$$\begin{aligned}\int_t^\infty \bar{F}_{T_r(X)}(x)\,{\rm d}x &= \int_t^\infty \bar{F}(x)\bar{F}_{\tilde{X}_{r,k}}(x)\,{\rm d}x \\ &= \mu r\binom{k}{r}\int_t^\infty \left[\int_{F_{\tilde{X}}(x)}^1 u^{r-1}(1-u)^{k-r}\,{\rm d}u\right]{\rm d}F_{\tilde{X}}(x) \\ &= \mu r\binom{k}{r}\int_{F_{\tilde{X}}(t)}^1 \left[\int_v^1 u^{r-1}(1-u)^{k-r}\,{\rm d}u\right]{\rm d}v.\end{aligned}$$

Similarly, we have, for all $1 \leq r \leq k$ and $t \geq 0$,

$$\int_t^\infty \bar{F}_{T_r(Y)}(x)\,{\rm d}x = \mu r\binom{k}{r}\int_{F_{\tilde{Y}}(t)}^1 \left[\int_v^1 u^{r-1}(1-u)^{k-r}\,{\rm d}u\right]{\rm d}v.$$

In view of the equivalence between $X \leq_{\rm hmrl} Y$ and $\tilde{X} \leq_{\rm st} \tilde{Y}$, it follows from the assumption of $X \leq_{\rm hmrl} Y$ that $F_{\tilde{X}}(x) \geq F_{\tilde{Y}}(x)$ for all $x \geq 0$ and hence

$$\int_t^\infty \bar{F}_{T_r(X)}(x)\,{\rm d}x \leq \int_t^\infty \bar{F}_{T_r(Y)}(x)\,{\rm d}x, \quad \text{for all } t \geq 0.$$

On the other hand, $\mathsf{E}[X] = \mathsf{E}[Y] = \mu$ implies $\mathsf{E}[T_r(X)] = \mathsf{E}[T_r(Y)] = \dfrac{r\mu}{k+1}$. Thus, the desired result $T_r(X) \leq_{\rm cx} T_r(Y)$ can be validated by Lemma 2.4.5 again. ∎

Let X, Y and Z be Pareto, exponential and uniform random variables with a common expectation μ. It is easy to verify that $X \geq_{\rm hmrl} Y \geq_{\rm hmrl} Z$. Thus, from Theorem 2.4.6 it follows immediately that $T_r(X) \geq_{\rm cx} T_r(Y) \geq_{\rm cx} T_r(Z)$.

2.5 Interdependence among users lifetimes

In previous subsections we investigate the resilience and reliability of the P2P network through some discussions on the isolation probability and the durable time. As is seen,

the order statistics $\tilde{X}_{r,k}$ plays the very important role in characterizing both isolation probability (2.1) and the durable time (2.2). Note that the discussion over there is developed under the framework of mutual independence among users' lifetimes. Here we introduce the statistical dependence by equipping the users' lifetimes with the well-known Archimedean copula and then explore the effect due to statistical dependence among users' lifetimes.

Assume $(X_1, \cdots, X_k)$ and $(Y_1, \cdots, Y_k)$ have their Archimedean copulas C_{ϕ_1} and C_{ϕ_2}, respectively. Let $\mathsf{E}[X_i] = \mathsf{E}[Y_i]$, $i = 1, \cdots, k$. Denote W_i the random variable such that

$$\phi_i(t) = \mathsf{E}\big[e^{-tW_i}\big], \quad \text{for } t \geq 0 \text{ and } i = 1, 2.$$

We next present the following theorem to throw a light into our P2P network systems.

Theorem 2.5.1 *Suppose* $W_1 \leq_{\text{st}} W_2$ *and* $\psi_1(\bar{F}_{\tilde{X}}(t)) \leq \psi_2(\bar{F}_{\tilde{Y}}(t))$ *for all* $t \geq 0$. *Then,* $T_r(X) \geq_{\text{st}} T_r(Y)$.

Proof: Note that $W_1 \leq_{\text{st}} W_2$ and $\psi_1(\bar{F}_{\tilde{X}}(t)) \leq \psi_2(\bar{F}_{\tilde{Y}}(t))$ for all $t \geq 0$. From Theorem 3.9 of Rezapour and Alamatsaz (2014) it follows immediately that

$$\tilde{X}_{r,k} \geq_{\text{st}} \tilde{Y}_{r,k}, \quad \text{for } r = 1, \cdots, k. \tag{2.7}$$

Additionally, $W_1 \leq_{\text{st}} W_2$ implies $\phi_1(t) \geq \phi_2(t)$ for all $t \geq 0$ or equivalently,

$$\psi_1 \circ \psi_2(u) \geq u, \quad \text{for all } u \in (0, 1).$$

Also, $\psi_1\big(\bar{F}_{\tilde{X}}(t)\big) \leq \psi_2\big(\bar{F}_{\tilde{Y}}(t)\big)$ for all $t \geq 0$ implies that

$$\psi_1 \circ \psi_2(u) \leq \bar{F}_{\tilde{X}} \circ \bar{F}^{-1}_{\tilde{Y}}(u), \quad \text{for all } u \in (0, 1).$$

As a consequence, we have $\bar{F}_{\tilde{X}} \circ \bar{F}_{\tilde{Y}}^{-1}(u) \geq u$ for all $u \in (0,1)$. Equivalently, $\bar{F}_{\tilde{X}}(t) \geq \bar{F}_{\tilde{Y}}(t)$ for all $t \geq 0$. Take $\mathsf{E}[X] = \mathsf{E}[Y]$ into account we have $\bar{F}_X(t) \geq \bar{F}_Y(t)$ for all $t \geq 0$. That is, $X \geq_{\rm st} Y$. Now, in combination with (2.7) we get

$$T_r(X) = \min\left\{X, \tilde{X}_{r,k}\right\} \geq_{\rm st} \min\left\{Y, \tilde{Y}_{r,k}\right\} = T_r(Y).$$

That is the desired result. ∎

In accordance with Theorem 2.5.1, reliability engineers may improve the reliability of the P2P network system through (i) strengthen the interdependence among users' lifetimes and (ii) choosing much more dispersed lifetime distribution for users. Note that the generator ϕ determines the degree of corresponding dependence, one may naturally wonder whether we can improve the resilience of the network by imposing stronger interdependence among its users. The following example serves as a negative answer.

Example 2.5.2 Consider two 3-dimensional random vectors (U_1, U_2, U_3) and (V_1, V_2, V_3) both with uniform marginals on $[0,1]$. Assume that they have Clayton copulas with generators

$$\phi_1(t) = (2t+1)^{-1/2} \qquad \text{and} \qquad \phi_2(t) = (t+1)^{-1},$$

respectively. Note that $\psi_1 \circ \phi_2(0) = 0$ and $\psi_1 \circ \phi_2 = ((1+t)^2 - 1)/2$ is convex and hence super-additive. However, as is shown in Figure 2.2, $\Pr\big(U_{2:3} \leq t\big) - \Pr\big(V_{2:3} \leq t\big)$ is first positive then negative on the interval $[0,1]$, indicating that there is no stochastic order between $U_{2:3}$ and $V_{2:3}$. ∎

2.6 Identifying the NWUE order

As is seen in previous section, NWUE property of a random lifetime plays an important role in determining both reliability and resilience of a P2P network. In this section, we

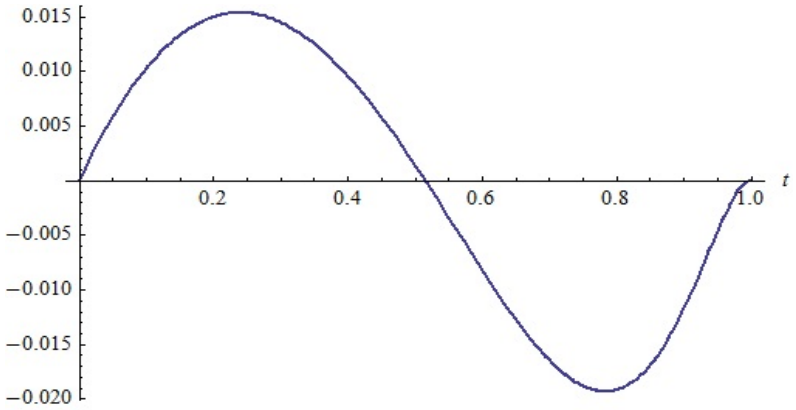


Figure 2.2: $\Pr\big(U_{2:3} \le t\big) - \Pr\big(V_{2:3} \le t\big)$.

build some methods to detect the strict NWUE order based upon two samples

$$\boldsymbol{X}_n = (X_1, \ldots, X_n), \qquad \boldsymbol{Y}_m = (Y_1, \ldots, Y_m)$$

from independent populations X and Y with continuous distributions, respectively.

2.6.1 Graphical method based on TTT plot

Define

$$\varphi_F^{-1}(v) = \frac{1}{\mu_F} \int_0^{F^{-1}(v)} \bar{F}(t)\,\mathrm{d}t, \qquad v \in (0,1),$$

the scaled *total time on test* (TTT) transform (see Barlow and Campo (1975)) of the distribution F of a random lifetime X. Since F and φ_F^{-1} uniquely determine each other, TTT transform is convenient to be used to judge the aging properties of X. Bergman (1979) showed that X is NWUE if and only if $\varphi_F^{-1}(v) \le v$ for all $v \in (0,1)$.

Example 2.6.1 (Pareto distribution) For the distribution in Example 2.3.1, it holds that

$$\int_0^{G^{-1}(v)} \bar{G}(t)\,\mathrm{d}t = \frac{\beta}{\alpha - 1}\left[1 - (1-v)^{1-1/v}\right], \quad v \in (0,1).$$

Thus, the scaled TTT transform

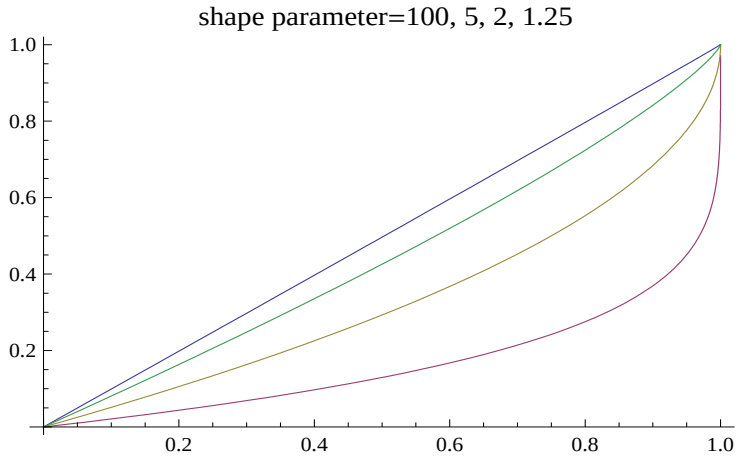


Figure 2.3: Scaled TTT plots of Pareto distributions with $\alpha = 100,\ 5,\ 2,\ 1.25$

$$\varphi_G^{-1}(v) = 1 - (1-v)^{1-1/v}, \quad v \in (0,1).$$

It is evident that shape parameter α has a direct impact on the degree of NWUE property whilst the scaled TTT transform is independent of the scale parameter β. As can be seen in Figure 2.6.1, the smaller the shape parameter α, the more far below the diagonal the scaled TTT transform, and hence the more NWUE the distribution is. ■

Let $F_n(t)$ be the empirical distribution function, $X_{1:n} \leq \cdots \leq X_{n:n}$ be order statistics and $\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$ be the sample mean of $X_1, \cdots, X_n$. Then, for $i = 1, \cdots, n$,

$$\varphi_{F_n}^{-1}\left(\frac{i}{n}\right) = \frac{1}{\bar{X}} \int_0^{F_n^{-1}(i/n)} \bar{F}_n(t)\,\mathrm{d}t = \frac{\displaystyle\sum_{j=1}^{i} X_{j:n} + (n-i)X_{i:n}}{\displaystyle\sum_{j=1}^{n} X_{j:n}},$$

gives the sample version of the scaled TTT transform, which converges to the population version $\varphi_F^{-1}(v)$ as sample size $n \to \infty$. As a result, the data set has the NWUE property

if its scaled TTT plot

$$\left(\frac{i}{n}, \quad \varphi_{F_n}^{-1}\left(\frac{i}{n}\right)\right), \qquad i = 1, \cdots, n,$$

lies below the diagonal line.

Example 2.6.2 (Proschan, 1963) Lifetimes (in hours) of the air-conditioning systems in two different planes are recorded in Table 2.6.2 below. TTT plots based upon these

plane's type	sample
8045	14,14,27,32,34,54,57,59,61,66,67,102,134,152,209,230
7909	10,14,20,23,24,25,26,29,44,44,49,56,59,60,61,62, 70,76,79,84,90,101,118,130,156,186,208,208,310

Table 2.1: Life times of air-conditioning systems of planes

lifetimes are listed in Figure 2.4. Apparently, they both are not below the diagonal line

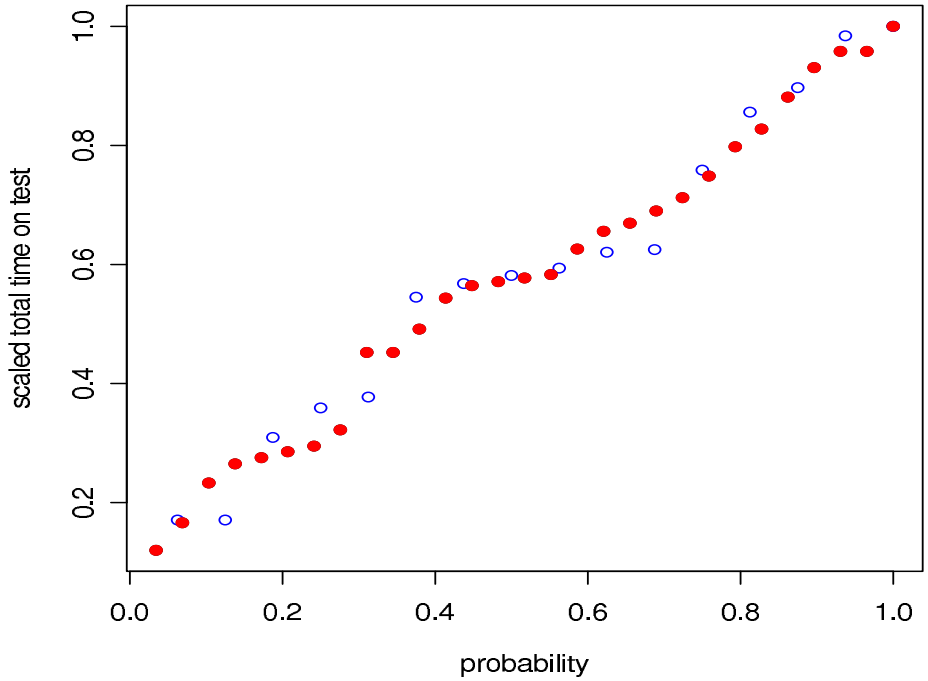


Figure 2.4: TTT plots of air-conditioning systems in airplane: 8045 (○), 7909 (●)

and hence lifetimes of these two systems don't possess the NWUE property. ■

As a matter of fact, it is also quite convenient to identify the NWUE order by comparing the two TTT plots. It may be derived from (1.1) directly that

$$X \geq_{\text{nwue}} Y \quad \text{if and only if} \quad \varphi_F^{-1}(v) \leq \varphi_G^{-1}(v) \quad \text{for all } v \in (0,1).$$

Therefore, it is reasonable to identify the NWUE order through checking whether

$$\left(\frac{i}{n}, \quad \varphi_{F_n}^{-1}\left(\frac{i}{n}\right)\right), \qquad i = 1, \cdots, n,$$

the TTT plot based on $X_1, \cdots, X_n$, lies below

$$\left(\frac{j}{m}, \quad \varphi_{G_m}^{-1}\left(\frac{j}{m}\right)\right), \qquad j = 1, \cdots, m,$$

the TTT plot based on $Y_1, \cdots, Y_m$, here, for $j = 1, \cdots, m$,

$$\varphi_{G_m}^{-1}\left(\frac{j}{m}\right) = \frac{1}{\bar{Y}} \int_0^{G_m^{-1}(j/m)} \bar{G}_m(t)\, \mathrm{d}t = \frac{\sum_{k=1}^{j} Y_{k:m} + (m-j)Y_{j:m}}{\sum_{k=1}^{m} Y_{k:m}},$$

$Y_{1:m} \leq \cdots \leq Y_{m:m}$ are order statistics and $\bar{Y}$ is the sample mean corresponding to $Y_1, \cdots, Y_m$.

Example 2.6.3 (Skype and Yahoo) The users' times (in seconds) of the network chatting systems are recorded in both Skype and Yahoo network chatting systems in Table 2.6.3.

As can be seen in Figure 2.5, the two TTT plots lie far below the diagonal demonstrating the obvious NWUE property. Further, TTT plot of Skype system is below that of Yahoo system and hence showing a stronger NWUE property. ■

System	sample
Yahoo	6,9,13,18,24,28,38,44,48,54,57,69,86,120,150,176, 198,206,234,306,400,447,502,604,708,800,1005,1560
Skype	2,5,8,11,12,15,19,22,26,30,34,36,39,40,41,52,55,57, 56,70,83,108,117,209,306,409,530,602,845,1203,1882

Table 2.2: Times user spend in chatting systems

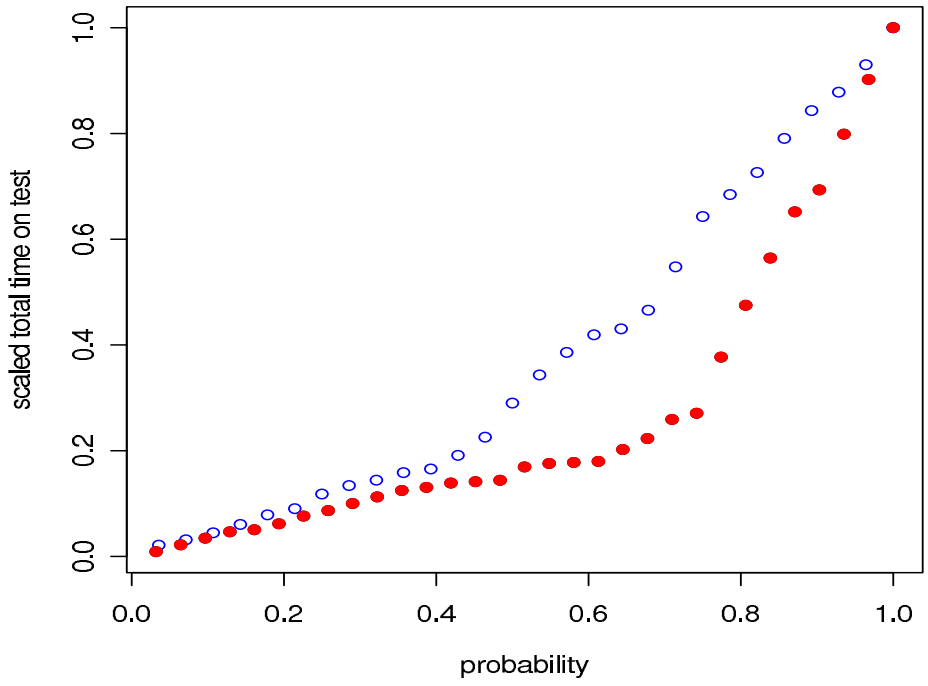


Figure 2.5: TTT plots of network chatting systems: Yahoo (○), Skype (●)

2.6.2 A nonparametric test

In literature, some partial orders were introduced to measure various common aging properties, such as IFR, IFRA, NBU, DMRL and NBUE. However, they can not be accurately detected without the parametric forms of survival functions. As a result, engineers resort to statistical methods in practical applications. In the past decades, nonparametric procedures were proposed to test the IFR order, IFRA order, NBU order and DMRL order, respectively. One may refer Aly (1993), Ahamed and Kochar (1990), Kusum et al (1986), Hollander et al (1982) and Gerlach (1986), and Lai and Xie (2006) for more details. Here, we propose a nonparametric test for the strict NWUE order.

According to Kochar and Wiens (1987), $X \geq_{\text{nwue}} Y$ and $X \leq_{\text{nwue}} Y$ (written as $X \sim Y$) if and only if $\bar{F}(t) = \bar{G}(\theta t)$ for all $t \geq 0$, where $\theta = \mu_G/\mu_F$, $\mu_G = \mathsf{E}[Y]$ and $\mu_F = \mathsf{E}[X]$. That is, two random lives have same degree of NWUE-ness if and only if their survival functions differ by at most a positive scale factor. In order to test the following hypothesis

$$\mathsf{H}: \quad X \sim Y \qquad \text{versus} \qquad \mathsf{K}: \quad X \geq_{\text{nwue}} Y \text{ strictly},$$

it is necessary to build some testing statistic and derive its (asymptotic) null distribution.

Let

$$\beta(Y) = \int_0^\infty \bar{G}^2(t)\,\mathrm{d}t, \qquad \beta(X) = \int_0^\infty \bar{F}^2(t)\,\mathrm{d}t.$$

The following lemma helps to build a testing statistic for H versus K.

Proposition 2.6.4 *If $X \geq_{\text{nwue}} Y$, then*

$$\Delta(X,Y) = \frac{\beta(X)}{\mu_F} - \frac{\beta(Y)}{\mu_G} \geq 0, \tag{2.8}$$

the strict inequality holds when X is strictly more NBUE than Y, that is, $X \geq_{\text{nwue}} Y$ but not $X \sim Y$.

Proof: $X \geq_{\text{nwue}} Y$ implies $\mu_F(F^{-1}(s)) \geq \theta^{-1}\mu_G(G^{-1}(s))$ for all $0 \leq s \leq 1$. Then,

$$\begin{aligned}\int_0^1 \int_{F^{-1}(s)}^{\infty} \bar{F}(y)\,\mathrm{d}y\,\mathrm{d}s &= \int_0^1 \mu_F(F^{-1}(s))\,\mathrm{d}s \\ &\geq \frac{1}{\theta}\int_0^1 \mu_G(G^{-1}(s))\,\mathrm{d}s \\ &= \frac{1}{\theta}\int_0^1 \int_{G^{-1}(s)}^{\infty} \bar{G}(y)\,\mathrm{d}y\,\mathrm{d}s. \end{aligned} \tag{2.9}$$

By *Fubini*'s theorem,

$$\begin{aligned}\int_0^1 \int_{F^{-1}(s)}^{\infty} \bar{F}(y)\,\mathrm{d}y\,\mathrm{d}s &= \int_0^{\infty} \int_0^{F(y)} \bar{F}(y)\,\mathrm{d}s\,\mathrm{d}y \\ &= \int_0^{\infty} \bar{F}(y)F(y)\,\mathrm{d}y \\ &= \mathsf{E}[X] - \int_0^{\infty} \bar{F}^2(y)\,\mathrm{d}y; \end{aligned}$$

Likewise,

$$\int_0^1 \int_{G^{-1}(s)}^{\infty} \bar{G}(y)\,\mathrm{d}y\,\mathrm{d}s = \mathsf{E}[Y] - \int_0^{\infty} \bar{G}^2(y)\,\mathrm{d}y.$$

So, (2.9) implies

$$\int_0^{\infty} \bar{F}^2(y)\,\mathrm{d}y - \frac{1}{\theta}\int_0^{\infty} \bar{G}^2(y)\,\mathrm{d}y \geq \mathsf{E}[X] - \frac{1}{\theta}\mathsf{E}[Y] = 0,$$

irrespective of the two means μ_F and μ_G. ■

According to Proposition 2.6.4, $\Delta(X, Y) = 0$ when $X \sim Y$, and $\Delta(X, Y) > 0$ when $X \geq_{\text{nwue}} Y$ strictly. So, it serves as a reasonable measure for the deviation from the null hypothesis H toward the alternative K.

Let

$$\beta(\boldsymbol{X}_n) = \binom{n}{2}^{-1} \sum_{i \neq j}^{n} \min\{X_i, X_j\}, \qquad \beta(\boldsymbol{Y}_m) = \binom{m}{2}^{-1} \sum_{i \neq j}^{m} \min\{Y_i, Y_j\}.$$

According to the theory of U-statistic (Hoeffding, 1948), if $\mathsf{E}[X^4] < \infty$, then, as $n \to \infty$,

$$\frac{\sqrt{n}\big(\beta(\boldsymbol{X}_n) - \beta(X)\big)}{2\sigma_X} \xrightarrow{L} \mathcal{N}(0,1),$$

where

$$\sigma_X^2 = \mathsf{E}[\mathsf{E}[\min\{X_1, X_2\}|X_1] - \beta(X)]^2.$$

By *Slutsky*'s theorem, it holds that, as $n \to \infty$,

$$\frac{\sqrt{n}\left[\dfrac{\beta(\boldsymbol{X}_n)}{\bar{X}} - \dfrac{\beta(X)}{\mu_F}\right]}{2\dfrac{\sigma_X}{\mu_F}} \xrightarrow{L} \mathcal{N}(0,1). \tag{2.10}$$

Likewise, as $m \to \infty$,

$$\frac{\sqrt{m}\left[\dfrac{\beta(\boldsymbol{Y}_m)}{\bar{Y}} - \dfrac{\beta(Y)}{\mu_G}\right]}{2\dfrac{\sigma_Y}{\mu_G}} \xrightarrow{L} \mathcal{N}(0,1), \tag{2.11}$$

where

$$\bar{Y} = \frac{1}{m}\sum_{i=1}^{m} Y_i, \qquad \sigma_Y^2 = \mathsf{E}[\mathsf{E}[\min\{Y_1, Y_2\}|Y_1] - \beta(Y)]^2.$$

Combining (2.10) and (2.11), we reach the asymptotic distribution of

$$\Delta(\boldsymbol{X}_n, \boldsymbol{Y}_m) = \frac{\beta(\boldsymbol{X}_m)}{\bar{X}} - \frac{\beta(\boldsymbol{Y}_n)}{\bar{Y}}.$$

Proposition 2.6.5 *Suppose* $\mathsf{E}[X^4], \mathsf{E}[Y^4] < \infty$*, and* $\frac{m}{n+m}$ *is bounded away from* 0 *and* 1.

Then, as $\min(n, m) \to \infty$,

$$\sqrt{\frac{nm}{n+m}}\,\frac{\Delta(\boldsymbol{X}_n, \boldsymbol{Y}_m) - \Delta(X, Y)}{\sqrt{\sigma^2(X, Y)}} \xrightarrow{L} \mathcal{N}(0, 1), \tag{2.12}$$

where $\Delta(X, Y)$ *is determined by* (2.8) *and*

$$\sigma^2(X, Y) = \frac{m}{n+m}\frac{\sigma_X^2}{\mathsf{E}^2[X]} + \frac{n}{n+m}\frac{\sigma_Y^2}{\mathsf{E}^2[Y]}.$$

The parameter $\sigma^2(X, Y)$ is unknown and hence needs to be consistently estimated. Set

$$V_i(\boldsymbol{X}_n) = \frac{1}{n-1}\sum_{j \neq i} \min\{X_i, X_j\}, \qquad i = 1, 2, \cdots, n.$$

By Arvesen (1969), as $n \to \infty$, the *jackknifing* estimate

$$S^2(\boldsymbol{X}_n) = \frac{1}{n-1}\sum_{i=1}^{n} \big(V_i(\boldsymbol{X}_n) - \beta(\boldsymbol{X}_n)\big)^2 \xrightarrow{P} \sigma_X^2.$$

Likewise, as $m \to \infty$,

$$S^2(\boldsymbol{Y}_m) = \frac{1}{m-1}\sum_{j=1}^{m} \big(V_j(\boldsymbol{Y}_m) - \beta(\boldsymbol{Y}_m)\big)^2 \xrightarrow{P} \sigma_Y^2.$$

Now, applying *Slutsky*'s theorem to (2.12), we immediately get the following.

Proposition 2.6.6 *Under the assumptions in Proposition 2.6.5, as* $\min\{n, m\} \to \infty$,

$$\sqrt{\frac{nm}{n+m}}\,\frac{\Delta(\boldsymbol{X}_n, \boldsymbol{Y}_m) - \Delta(X, Y)}{\sqrt{S^2(\boldsymbol{X}_n, \boldsymbol{Y}_m)}} \xrightarrow{L} \mathcal{N}(0, 1), \tag{2.13}$$

where

$$S^2(\boldsymbol{X}_n, \boldsymbol{Y}_m) = \frac{m}{n+m}\frac{S^2(\boldsymbol{X}_n)}{\bar{X}^2} + \frac{n}{n+m}\frac{S^2(\boldsymbol{Y}_m)}{\bar{Y}^2}.$$

Since $\Delta(X, Y) = 0$ under the original H, from (2.13), now, we get the following testing

rule with the asymptotic level $0 < \alpha < 1$: H may be reasonably rejected when

$$T(\boldsymbol{X}_n, \boldsymbol{Y}_m) = \sqrt{\frac{nm}{n+m}} \frac{\Delta(\boldsymbol{X}_n, \boldsymbol{Y}_m)}{\sqrt{S^2(\boldsymbol{X}_n, \boldsymbol{Y}_m)}} > z_{1-\alpha},$$

where $z_{1-\alpha}$ is the $1-\alpha$ percentile of the standard normal distribution $\mathcal{N}(0,1)$. Standard arguments give rise to the consistency of the test.

To end this chapter, we apply the above testing method to data sets in Examples 2.6.2 and 2.6.3. Testing statistics observed as well as corresponding p-values are presented in the following table.

data set	sample size (n,m)	$T(\boldsymbol{X}_n, \boldsymbol{Y}_m)$	p-value
air-conditioning systems	(16,29)	0.022	0.5088
Skype/Yahoo chatting	(28,31)	2.2048	0.0237

Table 2.3: Statistics on data sets of air-conditioning and network chatting systems

Apparently,

(i) for the data set on air-conditioning systems, the larger p-value 0.5088 suggests us to accept the original hypothesis. That is, NWUE order between the lifetimes (in hours) of the air-conditioning systems in two different planes is insignificant;

(ii) however by contrast, p-value corresponding to the network chatting is only 0.0237, it is reasonable to reject the original hypothesis. That is, the lifetime of a user in Skype chatting system is more NWUE than that of Yahoo.

2.6.3 Concluding remarks

(i) No NWUE order is detected in lifetimes of air-condition systems in airplanes. Actually, an air-condition system is composed of some mechanical components, which will wear-out (at least during one maintenance cycle) as it is put into operation.

Thus, the two lifetimes of the air-conditioning systems do not have the NWUE property at all.

(ii) NWUE order is detected in chatting times (P2P network) of Yahoo and Skype. As software, both systems will be improved through removing bugs and patching program after being put into use. As a result, the chatting times of Yahoo and Skype inherently possess the NWUE property. Our test detects the NWUE order between the two chatting times.

3

Security Analysis of Compromised-Neighbor-Tolerant Networks

3.1 Introduction

In traditional security analysis of a network system, it usually focuses on cryptographic primitives and protocols, such as how a message is reasonably padded before being encrypted by the RSA (Rivest-Shamir-Adleman) function or how a password-based authentication protocol is properly operated so that the network system is immune to the off-line dictionary attack, etc. Although this approach of analysis works well, it would be more efficient if the knowledge on, for instance, network topology (the specific physical or logical arrangement of elements in a network) and defensive capability, etc, is acquired and properly exploited, since they usually have a significant impact on the security.

In the literature, a lot of epidemic models, for example, Kephart and White (1991), Kephart et al (1993), Aron and Grove (1998), Wierman and Marchette (2004), Li et al (2007), and Piqueira et al (2008), among others, were adopted in succession to study the spreading of computer viruses or worms and to address various aspects on the security of network systems. However, most such models assume that all nodes have equal contact with other nodes and the rate to compromise (a compromised node loses its designed

functionality due to either a successful attack outside the network or an infection from some of its neighbors) is largely determined by the density of the compromised nodes. Other epidemic models, for example, Barabási and Albert (1999), Pastor and Vespignani (2001), Moreno et al (2002), Pastor and Vespignani (2002), Wang et al (2003a,b), etc., considered non-homogeneous graphs (a graph is homogeneous if any isomorphism between finite induced subgraphs extends to an automorphism of the graph) without grasping the fact that computers may get compromised because of their own actions such as downloading or executing a malicious code. Recently, by abstracting the network system as a vulnerability graph of nodes set $\mathcal{V}$ and edges set $\mathcal{E}$, Li et al (2011) built a stochastic model characterizing a network system in which a node is compromised as soon as one of its neighbors is compromised and a compromised node may get secure again by receiving some curing operation. They proved that the probability a node gets compromised is increasing as the random degree (i.e., the random number of edges of a node) increases in the sense of stochastic ordering and obtained a simple lower/upper bound for this probability.

In practical occasions, most network systems equipped with certain security software possess some tolerance when some of its neighbors are compromised, and sometimes a node with a few neighbors being compromised does not stop working in the proper style until the number of compromised neighbors becomes large enough and goes beyond the tolerance level. In view of these, this paper studies a more general stochastic model, which characterizes the mechanism that a system is compromised and gets secure again and analyzes some aspects of network security. This model mainly includes the following several key aspects:

1. A vulnerability graph is used to abstract a network system with vertices representing possible vulnerabilities and edges capturing connections, through which the exploitation of one vulnerability could lead to the exploitation of the other;

2. An alternative renewal process is utilized to model those state changes due to attacks over the vulnerability graph and the endeavor to cure or vaccine compromised nodes;

3. The k-out-of-n fault tolerant structure (see Kuo and Zuo, 2002) is employed to characterize the way a node is compromised due to its neighbors or an intruder from outside the system, this makes the model capable of modeling the network system which is tolerant of compromised neighbors.

In this chapter, we focus on the degree distribution of the vulnerability graph which has an important impact on the security of a network system. In fact, it is shown that the probability for a node to be compromised increases as the degree grows in the increasing convex ordering, which is weaker than the usual stochastic ordering. Further, new upper and lower bounds on the probability for a node to be compromised are obtained and proved to be both more informative in the sense of incorporating more parameters of the system and being sharper than those in Li et al (2011). Besides, we have also conducted some stochastic comparisons among three typical degree distributions: regular graph, random graph, and power-law graph. The results obtained in this paper can help the designer to determine a better degree distribution leading to a more secure system, and can also help the engineer to well orchestrate the system configurations to make the system secure by taking effective actions. Hopefully the results can throw some new light on tuning system parameters so as to enhance the security. Additionally, the model abstracts vulnerability graphs through the degree distributions and hence can handle systems with any topology.

3.2 The model

In practical situations, a network system often faces attacks (malicious codes or hackers, etc.) from outside the system. Initially, all nodes are secure, not compromised. The attacker tries to paralyze the system through continuously launching attacks to any secure

nodes in the system. An attack succeeds if it penetrates the *attack-prevention mechanism* such as virus or fire-wall filters deployed by the corresponding machines. A successful attack may be typically detected after a delay in time, and the system becomes secure again through some *attack-recovery mechanism*. As time elapses, some nodes may get compromised and consequently may compromise its neighbors. Those compromised nodes may either be detected by a software (periodically scanning by the fire wall) and get cured or become secure due to vaccine and immunity. The node that got secure at some previous time may be compromised again after being cured. This process repeats for all nodes. Since a node may get compromised by an attack that is launched from one or multiple neighbors, an important issue is to capture how states of those neighbors have their impact on the state of a node itself. This helps the architect have a better understanding on the structure of a system and achieve a better design of the network system.

For ease of reference, all notations are listed in Table 3.1.

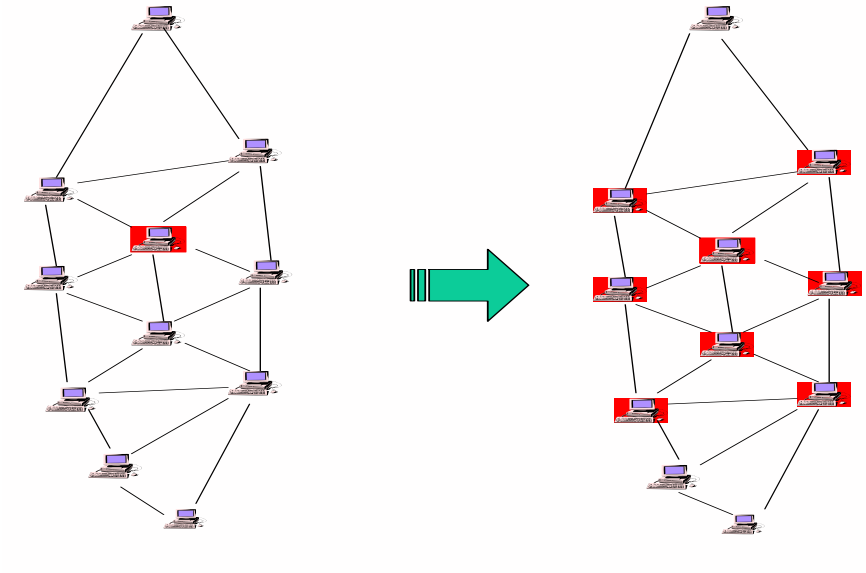


Figure 3.1: A depiction of the evolving process of a vulnerable network

1. Vulnerability graph abstraction Denote $\mathcal{G}$ a finite undirected graph with node set $\mathcal{V}$

α	the rate for a node with all its neighbors secure to be compromised by the attacker;
γ	the rate for a node to be compromised by one compromised neighbor, usually $\gamma > \alpha$;
β	the rate for a compromised node to get secure after being detected;
η	the rate for a compromised node to get secure due to vaccine or immunity;
X	the time interval for a node to be in secure state during a cycle;
Y	the time interval for a node to be in compromised state during a cycle;
W_0	the time for the attacker to compromise a node with all neighbors secure;
W_i	the time for a secure node to be infected by its compromised neighbor i;
$W_{r,k}$	the rth smallest one among $W_1, \cdots, W_k$, $r = 1, \cdots, k$;
V_1	the time for a compromised node to get secure after being detected;
V_2	the time for a compromised node to get secure due to vaccine or immunity;
q	the steady state probability for a node to be compromised;
p	the steady state probability for a node to be secure, $p = 1 - q$;
D	the random degree of a node in the system;
r	the minimal number of compromised neighbors for a secure node to get compromised;
K	number of compromised neighbors of a node with degree D, it has a binomial distribution with number of trials D and the probability of success q;
$\leq_{\text{st}}$	being smaller in the sense of stochastic ordering;
$\leq_{\text{icx}}$	being smaller in the sense of increasing convex ordering;
$\lfloor x \rfloor$	the largest integer which is smaller than or equal to x.
$\lceil x \rceil$	the smallest integer which is not smaller than x.
$\Gamma(\cdot)$	the gamma function;
$I(\cdot)$	the index function, $I(A) = 1$ if A occurs and $I(A) = 0$ otherwise;
$\Pr(\cdot)$	the probability function;
$\mathsf{E}[\cdot]$	the expectation function;

Table 3.1: A list of all notations employed in the model

and edge set $\mathcal{E} \neq \emptyset$, where the size of the graph (i.e., the number of nodes) $|\mathcal{V}| > 0$. Each node $v \in \mathcal{V}$ represents a vulnerability and an edge $(u, v) \in \mathcal{E}$ means that the exploitation of vulnerability u can lead to the exploitation of vulnerability v, and vice versa. Any node $v \in \mathcal{V}$ has a random degree that follows some integer-valued distribution on $\{r, \ldots, |\mathcal{V}| - 1\}$. All nodes in the system are secure (not compromised) at the beginning and are either secure or compromised during the whole process.

2. Compromising mechanism Suppose that an attacker outside the system keeps launching attacks to all secure nodes. Once a node is compromised, it becomes an accomplice of the attacker and then threatens its secure neighbors through logic or physical connections between them. Assume that

   (i) W_0 has an exponential distribution with rate α (or mean $1/\alpha$),

   (ii) W_i has an exponential distribution with rate γ, and

   (iii) each secure node has a compromising tolerance level, say r (See Table 3.1). That is, a node with more than r neighbors becomes compromised (and thus loses the capability of functioning in designed manner) when r of its neighbors are compromised.

3. Attack-detection-recovery mechanism The compromised nodes have a chance to get secure again. Assume that

   (i) V_1 follows an exponential distribution with rate β, and

   (ii) V_2 follows an exponential distribution with rate η.

4. Statistical independence Assume that

   (i) the attacker and his accomplices independently launch their respective attacks to secure nodes (neighbors),

(ii) the attack-detection system and the vaccine/immune system work independently, and

(iii) getting compromised and getting back to secure state are independent. That is, random variables D, W_0, V_1, V_2, and W_i are mutually independent. It should be noted that this by no means implies that a node to get compromised is independent of other nodes to get compromised. By contrast, the events that nodes get compromised are highly correlated.

3.3 Main analytical results

This section devotes to studying the probability for a node in a network system to get compromised. We discuss its monotonicity with respect to the random degree and derive upper and lower bounds through an implicit equation for this important security index.

3.3.1 Equation of the probability to be compromised

The state evolution of a node in the system forms an *alternating renewal process* (see Ross, 1996). Each cycle of the process is composed of the time interval X corresponding to the secure state and the time interval Y corresponding to the compromised state. In order to measure the security of the system, we consider q, the probability for a node to be compromised when the system enters its steady state. Intuitively, the smaller the q is, the more secure the system is. The following theorem provides an implicit equation for q, which is useful in the sequel to study the security mechanism of the system.

Theorem 3.3.1 *For an arbitrary graph $\mathcal{G}$ with random degree D, the steady state probability for a node to be compromised, q, satisfies*

$$\frac{1}{q} - 1 = \frac{\beta + \eta}{\alpha} \mathsf{E}\left[1 - \frac{\Gamma(K+1)\Gamma(\alpha/\gamma + K - r + 1)}{\Gamma(K - r + 1)\Gamma(\alpha/\gamma + K + 1)}\right]. \tag{3.1}$$

Proof: First, denote $W_{r,k}$ the r-th order statistic based upon $W_1, \cdots, W_k$, which is the time for a node v to get compromised due to its compromised neighbors, say, $1, \cdots, k$. Then, the time interval for v to be secure in a cycle is $[0, X]$ with $X = \min\{W_0, W_{r,K}\}$. Given $K = k$, $W_1, \cdots, W_k$ are independent and have a common exponential distribution function

$$F(x) = 1 - \mathrm{e}^{-\gamma x}, \qquad \text{for } x \geq 0.$$

Given $K = k$, $W_{r:k}$ has distribution function

$$F_{r:k}(x) = \frac{k!}{(r-1)!(k-r)!} \int_0^x F^{r-1}(t)(1 - F(t))^{k-r} \, \mathrm{d}F(t), \quad x \geq 0.$$

By the assumption, W_0 has exponential distribution

$$G(x) = 1 - \mathrm{e}^{-\alpha x}, \quad \text{for } x \geq 0 \text{ and } \alpha > 0.$$

Since W_0 is independent of $\{W_1, \cdots, W_k\}$, the series structure $\min\{W_0, W_{r:k}\}$ has distribution function $1 - \bar{G}(x)\bar{F}_{r:k}(x)$, and then by Fubini's theorem, we have

$$\begin{aligned}
& \mathsf{E}\big[\min\{W_0, W_{r:k}\}\big] \\
= & \int_0^\infty \bar{G}(x)\bar{F}_{r:k}(x) \, \mathrm{d}x \\
= & \int_0^\infty \mathrm{e}^{-\alpha x} \left[\frac{k!}{(r-1)!(k-r)!} \int_x^\infty F^{r-1}(t)(1 - F(t))^{k-r} \, \mathrm{d}F(t) \right] \mathrm{d}x \\
= & \int_0^\infty \frac{1 - \mathrm{e}^{-\alpha t}}{\alpha} \frac{k!}{(r-1)!(k-r)!} F^{r-1}(t)(1 - F(t))^{k-r} \, \mathrm{d}F(t) \\
= & \frac{1}{\alpha} \frac{k!}{(r-1)!(k-r)!} \int_0^1 y^{k-r}(1-y)^{r-1}(1 - y^{\alpha/\gamma}) \, \mathrm{d}y \qquad (y = e^{-\gamma t}) \\
= & \frac{1}{\alpha} \left[1 - \frac{\Gamma(k+1)\Gamma(\alpha/\gamma + k - r + 1)}{\Gamma(k-r+1)\Gamma(\alpha/\gamma + k + 1)} \right].
\end{aligned}$$

As a result, it follows that

$$\begin{aligned} \mathsf{E}[\min\{W_0, W_{r,K}\}] &= \mathsf{E}\big[\mathsf{E}[\min\{W_0, W_{r,K}\}|K]\big] \\ &= \frac{1}{\alpha}\,\mathsf{E}\left[1 - \frac{\Gamma(K+1)\Gamma(\alpha/\gamma + K - r + 1)}{\Gamma(K-r+1)\Gamma(\alpha/\gamma + K + 1)}\right]. \end{aligned} \tag{3.2}$$

On the other hand, the length of the time for a node to be compromised in a cycle, $Y = \min\{V_1, V_2\}$, follows an exponential distribution with rate $\beta + \eta$. So,

$$\mathsf{E}[Y] = \mathsf{E}\big[\min\{V_1, V_2\}\big] = \frac{1}{\beta + \eta}. \tag{3.3}$$

Now, by Blackwell's theorem (Ross, 1996), the steady state probability that a node is secure equals

$$p = \frac{\mathsf{E}\big[\min\{W_0, W_{r,K}\}\big]}{\mathsf{E}\big[\min\{W_0, W_{r,K}\}\big] + \mathsf{E}\big[\min\{V_1, V_2\}\big]}, \tag{3.4}$$

and thus $q = 1 - p$ satisfies

$$\frac{1}{q} = 1 + \frac{\mathsf{E}[\min\{W_0, W_{r,K}\}]}{\mathsf{E}[\min\{V_1, V_2\}]}.$$

Plugging (3.2) and (3.3) into (3.4), we immediately reach the desired equation (3.1). ■

Intuitively, the security of a system can be improved by deploying some reactive security mechanisms such as intrusion detection systems to increase $\beta + \eta$ and/or by deploying some proactive security mechanisms such as virus filters to decrease α and γ. This is justified by the following Proposition 3.3.2

Proposition 3.3.2 *The probability q for a node to be compromised is*

(i) decreasing with respect to $\beta + \eta \geq 0$, and

(ii) increasing with respect to $\alpha > 0$ and $\gamma > 0$.

Proof: (i) For any fixed α and γ, note that

$$0 < \frac{\Gamma(K+1)\Gamma(\alpha/\gamma + K - r + 1)}{\Gamma(K-r+1)\Gamma(\alpha/\gamma + K + 1)} < 1,$$

and the right hand side of (3.1) increases when $\beta + \eta$ increases. Hence q decreases with respect to $\beta + \eta \geq 0$.

(ii) By $\Gamma(x+1) = x\Gamma(x)$ for any $x > 0$, it holds that

$$\begin{aligned} g(\alpha,\gamma) &= \frac{1}{\alpha}\left[1 - \frac{\Gamma(K+1)\Gamma(\alpha/\gamma + K - r + 1)}{\Gamma(K-r+1)\Gamma(\alpha/\gamma + K + 1)}\right] \\ &= \frac{1}{\alpha}\left[1 - \frac{\prod_{i=1}^{r}(K-i+1)}{\prod_{i=1}^{r}(\alpha/\gamma + K - i + 1)}\right] \end{aligned}$$

is decreasing in $\gamma > 0$. This guarantees that q increases in $\gamma > 0$.

Since

$$\begin{aligned} & \prod_{i=1}^{r}(K-r+i)\left(1 + \frac{\alpha}{\gamma}\sum_{j=1}^{r}\frac{1}{\frac{\alpha}{\gamma} + K - r + j}\right) \\ < & \prod_{i=1}^{r}(K-r+i)\left(1 + \frac{\alpha}{\gamma}\sum_{j=1}^{r}\frac{1}{K-r+j}\right) \\ = & \prod_{i=1}^{r}(K-r+i) + \frac{\alpha}{\gamma}\sum_{j=1}^{r}\prod_{i=1, i\neq j}^{r}(K-r+i) \\ < & \prod_{i=1}^{r}\left(\frac{\alpha}{\gamma} + K - r + i\right), \end{aligned}$$

by taking the partial derivative, we have

$$\frac{\partial}{\partial\alpha} g(\alpha,\gamma)$$

$$
\begin{aligned}
&= \frac{-1}{\alpha^2}\left(1-\frac{\prod_{i=1}^{r}(K-i+1)}{\prod_{i=1}^{r}(\alpha/\gamma+K-i+1)}\right)+\frac{\prod_{i=1}^{r}(K-i+1)\cdot\sum_{j=1}^{r}\prod_{i=1,i\neq j}^{r}\left(\frac{\alpha}{\gamma}+K-r+i\right)}{\alpha\gamma\prod_{i=1}^{r}(\alpha/\gamma+K-i+1)^2}\\
&= \frac{1}{\alpha^2}\left(\frac{\prod_{i=1}^{r}(K-i+1)}{\prod_{i=1}^{r}\left(\alpha/\gamma+K-i+1\right)}-1\right)+\frac{1}{\alpha\gamma}\frac{\prod_{i=1}^{r}(K-i+1)\cdot\sum_{j=1}^{r}\left(\frac{\alpha}{\gamma}+K-r+j\right)}{\prod_{i=1}^{r}(\alpha/\gamma+K-i+1)}\\
&= \frac{1}{\alpha^2}\left[\frac{\prod_{i=1}^{r}(K-i+1)}{\prod_{i=1}^{r}\left(\alpha/\gamma+K-i+1\right)}\left(1+\frac{\alpha}{\gamma}\sum_{j=1}^{r}\frac{1}{\frac{\alpha}{\gamma}+K-r+j}\right)-1\right]\\
&= \frac{1}{\alpha^2}\left[\frac{\prod_{i=1}^{r}(K-r+i)}{\prod_{i=1}^{r}\left(\alpha/\gamma+K-r+i\right)}\left(1+\frac{\alpha}{\gamma}\sum_{j=1}^{r}\frac{1}{\frac{\alpha}{\gamma}+K-r+j}\right)-1\right]\\
&< 0.
\end{aligned}
$$

That is, the right hand side of (3.1) decreases and hence q increases when α increases. ■

3.3.2 Impact of topology on vulnerability graph

Before proceeding to investigating how the topology (i.e., the degree distribution) of a vulnerability graph affects the probability for a node to be compromised, let us first introduce the following lemma.

Lemma 3.3.3 *The function*

$$H_r(k,\omega)=1-\frac{\Gamma(k+1)\Gamma(\omega+k-r+1)}{\Gamma(k-r+1)\Gamma(\omega+k+1)}$$

(i) decreases in $k=r,r+1,\cdots$, for any $\omega>0$, and

(ii) is convex with respect to $k = r, r+1, \cdots$, for any $\omega \leq \frac{3+r}{r-1}$.

Proof: (i) For any $k \geq r$,

$$\begin{aligned} & H_r(k,\omega) - H_r(k+1,\omega) \\ = & \frac{\Gamma(k+2)\Gamma(\omega+k-r+2)}{\Gamma(k-r+2)\Gamma(\omega+k+2)} - \frac{\Gamma(k+1)\Gamma(\omega+k-r+1)}{\Gamma(k-r+1)\Gamma(\omega+k+1)} \\ = & \frac{\Gamma(k+1)\Gamma(\omega+k-r+1)}{\Gamma(k-r+1)\Gamma(\omega+k+1)} \left[\frac{(k+1)(\omega+k-r+1)}{(k-r+1)(\omega+k+1)} - 1\right]. \end{aligned}$$

Since, for $\omega > 0$,

$$(k+1)(\omega+k-r+1) - (k-r+1)(\omega+k+1) = r\omega > 0,$$

it is concluded that $H_r(k,\omega)$ is decreasing in $k \geq r$.

(ii) Let the increment $\Delta_r(k,\omega) = H_r(k+1,\omega) - H_r(k,\omega)$. Then,

$$\begin{aligned} & \Delta_r(k+1,\omega) - \Delta_r(k,\omega) \\ = & H_r(k+2,\omega) - 2H_r(k+1,\omega) + H_r(k,\omega) \\ = & \left[1 - \frac{\Gamma(k+3)\Gamma(\omega+k-r+3)}{\Gamma(k-r+3)\Gamma(\omega+k+3)}\right] - 2\left[1 - \frac{\Gamma(k+2)\Gamma(\omega+k-r+2)}{\Gamma(k-r+2)\Gamma(\omega+k+2)}\right] \\ & + \left[1 - \frac{\Gamma(k+1)\Gamma(\omega+k-r+1)}{\Gamma(k-r+1)\Gamma(\omega+k+1)}\right] \\ = & \left[\frac{2(k+1)(\omega+k-r+1)}{(k-r+1)(\omega+k+1)} - \frac{(k+2)(k+1)(\omega+k-r+2)(\omega+k-r+1)}{(k-r+2)(k-r+1)(\omega+k+2)(\omega+k+1)} - 1\right] \\ & \cdot \frac{\Gamma(k+1)\Gamma(\omega+k-r+1)}{\Gamma(k-r+1)\Gamma(\omega+k+1)} \\ = & \frac{r\omega(3+2k-r+\omega-r\omega)}{(k-r+2)(k-r+1)(\omega+k+2)(\omega+k+1)}. \end{aligned}$$

Note that, for $r \leq k$, when $0 < \omega \leq 1$,

$$3 + 2k - r + \omega - r\omega \geq 3 + r + \omega - r\omega \geq 3 + \omega > 0,$$

and when $1 < \omega \leq \frac{3+r}{r-1}$,

$$3 + 2k - r + \omega - r\omega \geq 3 + k - \omega(r-1) \geq 0,$$

it follows that, for any $\omega \geq 0$, $\Delta_r(k, \omega)$ is increasing in $k \geq r$ and hence $H_r(k, \omega)$ is convex with respect to $k \geq r$. ■

Recall for $r = 1$, Li et al (2011) proved that the probability for a node to be compromised increases as D grows in the sense of the stochastic order. Theorem 3.3.4 below presents a more general result than Li et al (2011) regarding the effect of the degree distribution on the security of network systems.

Theorem 3.3.4 *For any arbitrary graph $\mathcal{G}$ with random degree D, the probability for a node to be compromised, q, increases as D increases in the sense of the increasing convex order.*

Proof: Denote $\omega = \alpha/\gamma$ and let $K = \sum_{i=1}^{D} I(A_i)$, here A_i is the event that neighbor i of a node is compromised (with probability q), $i = 1, 2, \cdots$. Since (i) K is stochastically increasing as D stochastically increases, and (ii) $\frac{1}{q} - 1$ in (3.1) is decreasing with respect to q, it suffices to show that $\mathsf{E}[H_r(K, \omega)]$ is decreasing as K increases in the increasing convex order.

By Lemma 3.3.3, $H_r(k, \omega)$ is both decreasing and convex in $k = r, r+1, \cdots$. Note that the expectation of any increasing and convex function preserves the increasing convex order. It follows immediately that $\mathsf{E}[H_r(K, \omega)]$ is decreasing as K increases in the increasing convex order. This completes the proof. ■

Remark 3.3.5 Theorem 3.3.4 simply claims that the steady state probability for a node to be compromised becomes larger if the degree of a network topology becomes larger. This could provide the engineer with an insight to improve the security of an existing

system: amend the system's topology and choose a topology with smaller random degree in the sense of the increasing convex order.

As an example of Theorem 3.3.4, let us now look at three topologies, which are very common in practice. Here, the degree of a node is the number of its neighbors, an integer-valued random variable. Readers may refer to Bollobás (2001) and Caldarelli (2007) for more details.

- *Regular graph*: The degree D_κ of a node follows a degenerate distribution

$$\Pr(D_\kappa = \kappa) \equiv 1, \qquad \text{for some integer } \kappa < |\mathcal{V}|;$$

- *Random graph*: The degree D_τ of a node follows a binomial distribution

$$\Pr(D_\tau = d) = \binom{|\mathcal{V}| - 1}{d} \tau^d (1-\tau)^{|\mathcal{V}|-d-1},$$

  for $d = 0, 1, \cdots, |\mathcal{V}| - 1$, here τ is the edge probability and all edges in the graph are mutually independent;

- Truncated *power law graph*: The degree $D_{\ell,\nu}$ of a node follows the distribution

$$\Pr(D_{\ell,\nu} = d) = \frac{(d+1)^{-(\nu+1)}}{\sum_{k=\ell}^{|\mathcal{V}|-1} (k+1)^{-(\nu+1)}},$$

  for $d = \ell, \ell+1, \cdots, |\mathcal{V}| - 1$, here the power-law exponent $\nu \geq 1$, and ℓ (≥ 0) is the minimum possible degree. This is actually a transformation (one unit to the left) of the truncated version of the ordinary power law distribution with

$$\Pr(D = d) = \frac{\nu \ell^\nu}{d^{\nu+1}}, \qquad \text{for } d = \ell, \ell+1, \cdots.$$

Proposition 3.3.6 below can be easily proved and hence is stated without proof.

Proposition 3.3.6 (i) $D_{\ell,\nu}$ decreases in the increasing convex ordering with respect to ν;

(ii) D_κ and D_τ increase in the increasing convex ordering with respect to κ and τ, respectively.

To make a stochastic comparison among the above three topologies, we need the following lemma.

Lemma 3.3.7 (Denuit et al., 2005, pp. 154) *Suppose two integer-valued random variables N and M such that $\mathsf{E}[N] = \mathsf{E}[M]$. Denote*

$$h_N(d) = \frac{\Pr(N = d)}{\Pr(N = d-1)}, \qquad \text{for } d = 1, 2, \cdots .$$

Then, $N \leq_{\text{icx}} M$ if there exists a constant c such that $h_M(d) \leq h_N(d)$ for $d \leq c$ and $h_M(d) \geq h_N(d)$ for $d > c$.

Proposition 3.3.8 *Suppose $\mathsf{E}[D_\kappa] = \mathsf{E}[D_\tau] = \mathsf{E}[D_{\ell,\nu}]$. Then,*

(i) $D_\kappa \leq_{\text{icx}} D_\tau$ for any $0 < \tau < 1$ and $D_\kappa \leq_{\text{icx}} D_{\ell,\nu}$ for any $\ell \geq 1$ and $\nu \geq 1$;

(ii) $D_\tau \leq_{\text{icx}} D_{0,\nu}$ for $\nu \geq 1$ and $0 < \tau \leq 0.484$.

Proof: (i) It follows directly from the equation (3.A.48) of Shaked and Shanthikumar (2007).

(ii) For $d = 1, \cdots, |\mathcal{V}| - 1$,

$$h_{D_\tau}(d) = -\frac{\tau}{1-\tau} + \frac{|\mathcal{V}|\tau}{d(1-\tau)}, \quad h_{D_{0,\nu}}(d) = \left(1 + \frac{1}{d}\right)^{-(\nu+1)}.$$

It is easy to verify that

$$\Delta(x) = h_{D_\tau}(x) - h_{D_{0,\nu}}(x) = -\frac{\tau}{1-\tau} + \frac{|\mathcal{V}|\tau}{x(1-\tau)} - \left(1+\frac{1}{x}\right)^{-(\nu+1)}$$

is continuous and strictly decreasing in $x \in [1, |\mathcal{V}|-1]$.

Since $0 < \tau < 1$ and $\nu \geq 1$, it holds that

$$\frac{\tau^{(1-\nu)}}{1-\tau} \geq \tau^{(1-\nu)} \qquad \text{and} \qquad \tau > \tau^\nu 2^{-(\nu+1)},$$

which is equivalent to $\tau^{(1-\nu)} > 2^{-(\nu+1)}$. Note that $|\mathcal{V}| - 1 \geq \tau^{-\nu}$, we have

$$\frac{(|\mathcal{V}|-1)\tau}{1-\tau} \geq \frac{\tau^{(1-\nu)}}{1-\tau} \geq \tau^{(1-\nu)} > 2^{-(\nu+1)}.$$

This implies, for $0 < \tau < 1$ and $\nu \geq 1$,

$$\Delta(1) = (|\mathcal{V}|-1)\frac{\tau}{1-\tau} - 2^{-(\nu+1)} > 0.$$

On the other hand, one can verify that $\tau(1+\tau) < (1-\tau)^{1/2}$ for $0 < \tau \leq 0.484$. Since

$$\tau(1+\tau^\nu) \leq \tau(1+\tau) \quad \text{and} \quad (1-\tau)^{1/2} \leq (1-\tau)^{1/(\nu+1)}, \quad \text{for } \nu \geq 1,$$

it holds that, for $0 < \tau \leq 0.484$, $\tau(1+\tau^\nu) < (1-\tau)^{1/(\nu+1)}$, or equivalently

$$\frac{\tau^{(\nu+1)}}{1-\tau} < (1+\tau^\nu)^{-(\nu+1)}.$$

Thus, for $0 < \tau \leq 0.484$,

$$\Delta(|\mathcal{V}|-1) \;=\; \frac{\tau}{(|\mathcal{V}|-1)(1-\tau)} - \left(1+\frac{1}{(|\mathcal{V}|-1)}\right)^{-(\nu+1)}$$

$$\leq \frac{\tau^{(1+\nu)}}{(1-\tau)} - (1+\tau^{\nu})^{-(\nu+1)} < 0.$$

Now, due to the strict decreasing property of $\Delta(x)$, there exists some constant $c \in (1, |\mathcal{V}|-1)$ such that $h_{D_{0,\nu}}(d) \leq h_{D_\tau}(d)$ for $d \leq c$ and $h_{D_{0,\nu}}(d) \geq h_{D_\tau}(d)$ for $d > c$. Taking $\mathsf{E}[D_\tau] = \mathsf{E}[D_{\ell,\nu}]$ into account, it follows from Lemma 3.3.7 that $D_\tau \leq_{\text{icx}} D_{0,\nu}$. ■

Remark 3.3.9 (i) Proposition 3.3.8(i) actually holds for a random graph without the restriction of independence among all edges.

(ii) Note that the stochastic order implies the increasing convex order. By Theorem 3.3.4 and Proposition 3.3.6, we have the following insights: For a network system, the smaller the degree of a node (the edge probability, the exponent) of a regular graph (random graph, power law graph) is, the more secure the system is. It should be pointed out here that the larger the exponent of a power law graph, the lighter the tail of the node distribution.

(iii) For a network with a moderate number of neighbors, according to Theorem 3.3.4 and Proposition 3.3.8, the regular graph is more secure than the random graph (even without the restriction of independence among all edges), and if the network is large, the random graph is more secure than the power-law graph. Thus, to attain more security, it is sensible to decentralize a network, i.e., to avoid having too many edges on one node.

3.4 Probability bounds

Since the probability q for a node to be compromised is determined by the implicit equation (3.1), which is not computable because of the expectation of gamma functions, we in this section provide lower and upper bounds for this probability.

Proposition 3.4.1 *For an arbitrary graph $\mathcal{G}$ with a random degree D,*

$$\frac{\alpha}{\alpha+(\beta+\eta)\left[1-(\mathsf{E}[D]+1)^{-\lfloor\frac{\alpha}{\gamma}\rfloor-1}\right]}<q<\frac{\alpha(\alpha+(\mathsf{E}[D]+1)\gamma)}{\alpha(\alpha+(\mathsf{E}[D]+1)\gamma)+(\alpha+\gamma)(\beta+\eta)}. \quad (3.5)$$

Proof: According to Theorem 3.3.4, for a given threshold r and D, it holds that $q \geq (r+1)/\mathsf{E}[D]$ and hence $\mathsf{E}[K] = q\mathsf{E}[D] \geq r+1$. $D \geq K$ guarantees

$$\mathsf{E}\left[\frac{K-r}{K+1}\right] > \mathsf{E}\left[\frac{K-r}{D+1}\right] \geq \mathsf{E}\left[\frac{1}{D+1}\right]. \quad (3.6)$$

Note that

$$\frac{k+s-r+1}{k+s+1} \leq \frac{k-r+1}{k+1}, \quad \text{for any } s \geq 0,$$

we have, for any $k = 1, 2, \cdots, |\mathcal{V}|$ and the threshold r,

$$\begin{aligned}
& \frac{\Gamma(k+1)\Gamma\big(\alpha/\gamma+k-r+1\big)}{\Gamma(k-r+1)\Gamma\big(\alpha/\gamma+k+1\big)} \\
\geq\ & \frac{\Gamma(k+1)\Gamma\big(\lfloor\alpha/\gamma\rfloor+k-r+1\big)}{\Gamma(k-r+1)\Gamma\big(\lceil\alpha/\gamma\rceil+k+1\big)} \qquad \big(\lfloor x\rfloor \leq x \leq \lceil x\rceil\big) \\
=\ & \frac{\big(k-r+\lfloor\alpha/\gamma\rfloor+1\big)\cdots(k-r+1)}{\big(k+\lfloor\alpha/\gamma\rfloor+1\big)\cdots(k+1)} \\
\geq\ & \left(1-\frac{r}{k+1}\right)^{\lfloor\alpha/\gamma\rfloor+1}.
\end{aligned}$$

Then, by (3.1), we have

$$\begin{aligned}
\frac{1}{q}-1 &< \frac{\beta+\eta}{\alpha}\,\mathsf{E}\left[1-\left(1-\frac{r}{K+1}\right)^{\lfloor\alpha/\gamma\rfloor+1}\right] \\
&\leq \frac{\beta+\eta}{\alpha}\left[1-\left(1-\mathsf{E}\left[\frac{r}{K+1}\right]\right)^{\lfloor\alpha/\gamma\rfloor+1}\right] \qquad \text{(Jensen's inequality)} \\
&< \frac{\beta+\eta}{\alpha}\left[1-\left(\mathsf{E}\left[\frac{1}{D+1}\right]\right)^{\lfloor\alpha/\gamma\rfloor+1}\right] \qquad \text{(the inequality (3.6))}
\end{aligned}$$

$$\leq \frac{\beta+\eta}{\alpha}\left(1-\frac{1}{(\mathsf{E}[D]+1)^{\lfloor\alpha/\gamma\rfloor+1}}\right). \qquad \text{(Jensen's inequality)}$$

Thus, it follows that

$$q > \frac{\alpha}{\alpha+(\beta+\eta)\left[1-\frac{1}{(\mathsf{E}[D]+1)^{\lfloor\alpha/\gamma\rfloor+1}}\right]}.$$

On the other hand, the expectation of (3.1),

$$\begin{aligned}
& \mathsf{E}\left[1-\frac{\Gamma(K+1)\Gamma(\alpha/\gamma+K-r+1)}{\Gamma(K-r+1)\Gamma(\alpha/\gamma+K+1)}\right] \\
= \;& \mathsf{E}\left[1-\frac{K\cdots(K-r+1)}{(K+\alpha/\gamma+1)\cdots(K+\alpha/\gamma-r+1)}\right] \\
> \;& \mathsf{E}\left[1-\left(\frac{K}{K+\alpha/\gamma+1}\right)^r\right] \\
> \;& \mathsf{E}\left[\frac{\alpha/\gamma+1}{K+\alpha/\gamma+1}\right] \\
> \;& \frac{\alpha/\gamma+1}{\mathsf{E}[K]+\alpha/\gamma+1} \qquad \text{(Jensen's inequality)} \\
\geq \;& \frac{\alpha/\gamma+1}{\mathsf{E}[D]+\alpha/\gamma+1}. \qquad (K\leq D)
\end{aligned}$$

Then, from

$$\frac{1}{q}-1 > \frac{\beta+\eta}{\alpha}\frac{\frac{\alpha}{\gamma}+1}{\mathsf{E}[D]+\alpha/\gamma+1},$$

it follows immediately that

$$q < \frac{\alpha[\alpha+\gamma(\mathsf{E}[D]+1)]}{\alpha[\alpha+(\mathsf{E}[D]+1)\gamma]+(\alpha+\gamma)(\beta+\eta)},$$

as is just the desired. ■

Now, we focus on the special case with $r=1$.

In view of $q \equiv 1 - p$, setting $r = 1$ in (3.1) reduces to the following equation in Li et al (2011),

$$\frac{p}{q} = \mathsf{E}\left[\frac{\beta + \eta}{\alpha + \gamma K}\right] = \frac{\beta + \eta}{\left(\mathsf{E}\left[\frac{1}{\alpha+\gamma K}\right]\right)^{-1}}. \tag{3.7}$$

Since the denominator

$$\left(\mathsf{E}\left[\frac{1}{\alpha + \gamma K}\right]\right)^{-1}$$

is the *harmonic mean* of $\alpha + \gamma K$, the rate for a node to be compromised, the equation in (3.7) tells that *the odds for a node to be safe are just the ratio of the rate for a compromised node to become secure to the harmonic mean of the rate for a secure node to be compromised.*

The following proposition presents an upper bound for q.

Proposition 3.4.2 *For a graph $\mathcal{G}$ with any arbitrary degree distribution D and $r = 1$, it holds that*

$$q \leq \frac{\sqrt{s^2(\alpha, \beta, \eta, \gamma) + 4\alpha\gamma\mathsf{E}[D]} - s(\alpha, \beta, \eta, \gamma)}{2\gamma\mathsf{E}[D]}, \tag{3.8}$$

where

$$s(\alpha, \beta, \eta, \gamma) = \alpha + \beta + \eta - \gamma\mathsf{E}[D].$$

Proof: Since the harmonic mean is less than or equal to the usual mean, it follows that

$$\left(\mathsf{E}\left[\frac{1}{\alpha + \gamma K}\right]\right)^{-1} \leq \mathsf{E}[\alpha + \gamma K] = \alpha + \gamma\mathsf{E}[K] = \alpha + q\gamma\mathsf{E}[D].$$

Then, by (3.7), we have

$$\frac{1 - q}{q} \geq \frac{\beta + \eta}{\alpha + q\gamma\mathsf{E}[D]}.$$

Equivalently,

$$\gamma\mathsf{E}[D]q^2 + (\alpha + \beta + \eta - \gamma\mathsf{E}[D])q - \alpha \leq 0.$$

By some algebra, we obtain

$$q \leq \frac{\sqrt{(\alpha+\beta+\eta-\gamma\mathsf{E}[D])^2+4\alpha\gamma\mathsf{E}[D]}-(\alpha+\beta+\eta-\gamma\mathsf{E}[D])}{2\gamma\mathsf{E}[D]}.$$

This completes the proof. ■

To illustrate the bounds in Proposition 3.4.1, we now consider some particular values of α, γ, $\mathsf{E}[D]$ and $\beta+\eta$. Three dimensional plots of segments of new bounds are displayed in Figure 3.2.

Remark 3.4.3 Li et al (2011) derived the following bounds on the probability for a node to be compromised,

$$\frac{\alpha}{\alpha+\beta+\eta} \leq q \leq \frac{\alpha+\gamma\mathsf{E}[D]}{\alpha+\beta+\eta+\gamma\mathsf{E}[D]}. \tag{3.9}$$

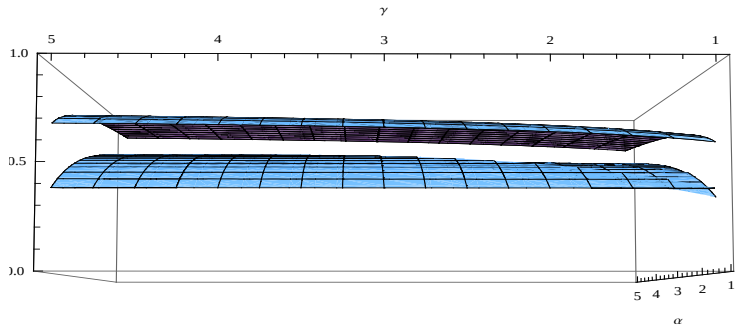
To compare (3.9) with (3.5) and (3.8), one can verify that

$$\frac{\alpha}{\alpha+(\beta+\eta)\left[1-(\mathsf{E}[D]+1)^{-\lfloor\frac{\alpha}{\gamma}\rfloor-1}\right]} \geq \frac{\alpha}{\alpha+\beta+\eta},$$

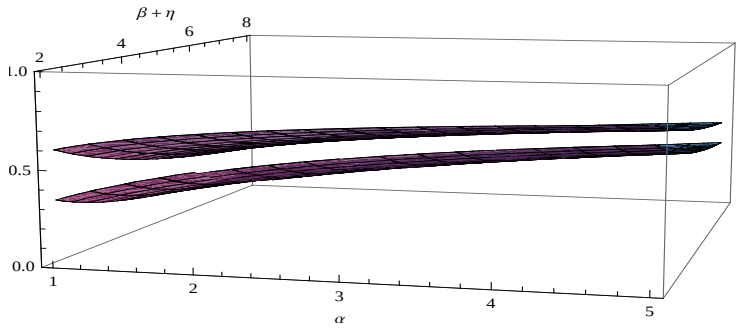
$$\frac{\sqrt{s(\alpha,\beta,\eta,\gamma)^2+4\alpha\gamma\mathsf{E}[D]}-s(\alpha,\beta,\eta,\gamma)}{2\gamma\mathsf{E}[D]} \leq \frac{\alpha+\gamma\mathsf{E}[D]}{\alpha+\beta+\eta+\gamma\mathsf{E}[D]}.$$

Thus the lower bound in (3.5) and the upper bound in (3.8) perform better than the corresponding ones in (3.9), respectively.

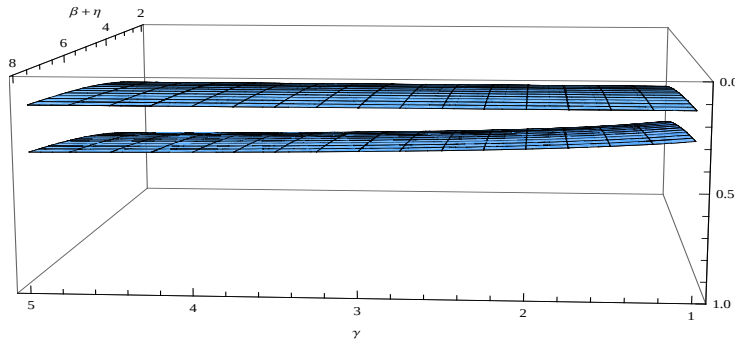
To compare the upper bounds in (3.5) and (3.8), we consider the difference between the upper bound in (3.8) and that in (3.5), i.e., (3.8)-(3.5). Two graphs of the difference for certain parameter values are provided in Figure 3.3. As can be seen, in most area, the difference is positive, i.e., the upper bound in (3.5) is smaller than the one in (3.8); however, there are areas where the difference is negative. See Figure 3.3(b) for instance. This implies that out of these two upper bounds no one is superior to another.



(a) $\beta + \eta = 2, \mathsf{E}[D] = 4$

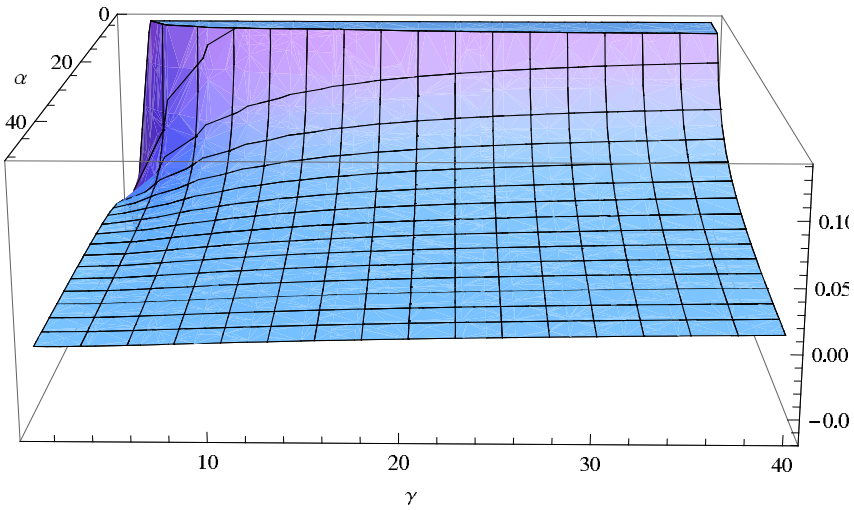


(b) $\gamma = 1, \mathsf{E}[D] = 4$

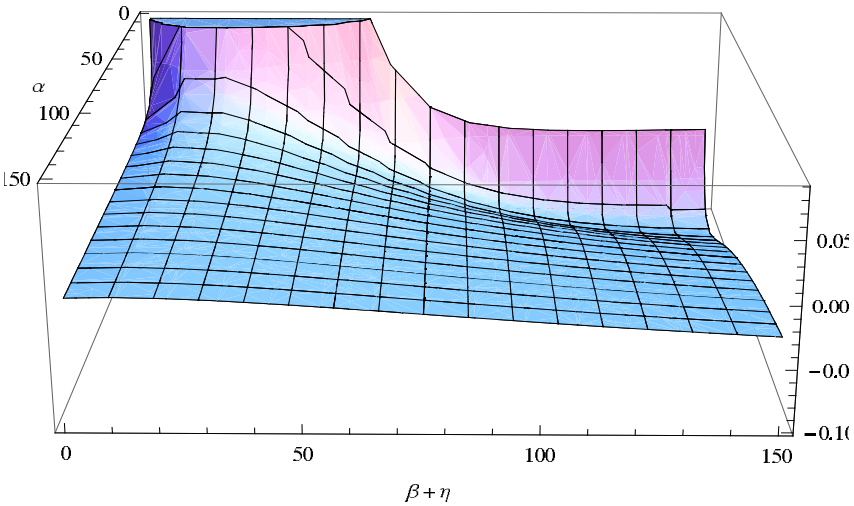


(c) $\alpha = 1, \mathsf{E}[D] = 4$

Figure 3.2: Upper bound (top) and lower bound (bottom) by (3.5)



(a) $\beta + \eta = 1, \mathsf{E}[D] = 4$



(b) $\gamma = 16, \mathsf{E}[D] = 4$

Figure 3.3: The difference between the upper bound in (3.8) and that in (3.5)

3.5 Concluding remarks and future work

By taking the tolerance of compromised neighbors into consideration, we studied the probability for a node to be compromised. This probability is proved to be increasing as the random degree grows in the sense of the increasing convex order. Based on this study, one can conduct comparisons among network systems with certain topology such as, for example, regular graph, random graph and power law graph. Furthermore, the established lower and upper bounds can be used to estimate and improve the security indices. Of course, more studies on the proposed model remain to be done. They include the following several aspects.

(i) After a compromised node is detected, it will get secure again when a software patch is applied. However, if the recovery is broken, then, the software may proceed without re-starting the repair task from the beginning again. That is, the recovery procedure is accumulative and hence the time V_1 for a compromised node to become secure again should not be memoryless. As a result, the assumption that V_1 follows an exponential distribution is inappropriate. Some other distributions with positive aging property may serve as a better alternative.

(ii) The abstraction of a network as a graph with certain random degree and concentrating on local quantities like the node's degree is a significant step to describe a system both empirically and analytically in realistic situations. However, this approach relies heavily on the degree distribution, which is a very local property of graphs. From a graph-theoretic standpoint, it is relatively easy to exhibit very different graphs having the same degree distribution (Aiello et al., 2001). Recently, the page rank function (Brin and Page, 1998) is employed to model a network. It is of interest to consider the model based on the page rank and parallel to the random

degree model so that some further insights may be obtained. In addition, when it comes to global vulnerabilities related to failure spreading and cascades, more global approaches like the spectral analysis of a graph are required. For example, Castellano and Pastor-Satorras (2010) and D'Agostino et al (2011) recently showed how even in random graph there could be a zero epidemic threshold for disease spreading and how the assortativity changes the severity of damage spreading, respectively. Although computationally heavy, global methods complement and compete the local approach when more complete data on the network is available.

(iii) It is assumed that the degree of a vertex is fixed once the network is configured. However, in real world networks, it may change as time elapses, because the number of compromised neighbors varies due to the history (compromised, ever being compromised or never being compromised) of the vertex itself. So, it is interesting to study in future work how the theoretical results are affected by the changing degree. This would bring further information on how effective various reactions to the attack might be. In addition, the dependence among edges is an important aspect if the focus is the statistics on the number of compromised nodes or the probability for an infection to die out, stable regimes for the infection, or similar quantities.

(iv) Theorems in Section 3.3 do not take the following two issues into account: (i) the degree distribution actually does not fully describe a network, and the correlation between neighboring nodes may lead to quite different random networks; and (ii) each realization of a random graph is not a homogeneous object and can contain fluctuations growing monotonically with the size of the network. Thus, infections will not spread in a uniform way. These issues deserve to be studied in the future.

A

R codes

A.1 Codes to produce TTT plot in Figure 2.4

```
##Define a function to get scaled TTT plot!##


Ustat<-function(data){
            value=NULL
            n=length(data)
            for (i in 1:n-1){
                 for (j in i+1:n){
                     if (isTRUE(data[i]<data[j])) {
                                    value=value+data[i]}
                                    else {value=value+data[j]}
                                                  }
                                 }
                    value=2*value/(n*(n-1))
                    return(value)
                    }
```

```
##Air-conditioning data (Proschan,1963)!##
x=c(14,14,27,32,34,54,57,59,61,66,67,102,134,152,209,230)
y=c(10,14,20,23,24,25,26,29,44,44,49,56,59,60,61,62,70,
76,79,84,90,101,118,130,156,186,208,208,310)

x=sort(x); y=sort(y); tttx=triplet(x); ttty=triplet(y)

 plot(tttx)
 plot(ttty, xlab="probablity", ylab="scaled total time on test")

points(tttx, col="blue")
points(ttty, col="red", pch=19)
```

A.2 Codes to produce TTT plot in Figure 2.5

```
##Define a function to get scaled TTT plot!##

Ustat<-function(data){
           value=NULL
           n=length(data)
           for (i in 1:n-1){
                for (j in i+1:n){
                    if (isTRUE(data[i]<data[j])) {
                                   value=value+data[i]}
                                   else {value=value+data[j]}
                                                 }
```

```
                    }
                value=2*value/(n*(n-1))
                return(value)
                }

##Skype and yahoo data!
x=c(6,9,13,18,24,28,38,44,48,54,57,69,86,120,150,176,198,
206,234,306,400,447,502,604,708,800,1005,1560)
y=c(2,5,8,11,12,15,19,22,26,30,34,36,39,40,41,52,55,57,
56,70,83,108,117,209,306,409,530,602,845,1203,1882)

x=sort(x); y=sort(y); tttx=triplet(x); ttty=triplet(y)

 plot(tttx)
 plot(ttty, xlab="probablity", ylab="scaled total time on test")

points(tttx, col="blue")
points(ttty, col="red",pch=19)
```

B

Mathematica codes

B.1 Codes to plot upper/lower bounds in Figure 3.2

lower[a_, b_, c_, d_]:=$\frac{a}{a+b\left(1-\frac{1}{(1+d)^{1+\text{Floor}[\frac{a}{c}]}}\right)}$

upper[a_, b_, c_, d_]:=$\frac{a(a+c(d+1))}{a(a+c(d+1))+(a+c)*b}$

f1 = Plot3D[lower[$a, 2, c, 4$], $\{a, 1, 5\}$, $\{c, 1, 5\}$, AxesLabel → $\{\alpha, \gamma\}$, PlotRange → $\{0, 1\}$]

f2 = Plot3D[upper[$a, 2, c, 4$], $\{a, 1, 5\}$, $\{c, 1, 5\}$, AxesLabel → $\{\alpha, \gamma\}$, PlotRange → $\{0, 1\}$]

Show[f1, f2]

f3 = Plot3D[lower[$a, b, 1, 4$], $\{a, 1, 5\}$, $\{b, 2, 8\}$, AxesLabel → $\{\alpha, \beta + \eta\}$, PlotRange → $\{0, 1\}$]

f4 = Plot3D[upper[$a, b, 1, 4$], $\{a, 1, 5\}$, $\{b, 2, 8\}$, AxesLabel → $\{\alpha, \beta + \eta\}$, PlotRange → $\{0, 1\}$]

Show[f3, f4]

f5 = Plot3D[lower[$1, b, c, 4$], $\{b, 2, 8\}$, $\{c, 1, 5\}$, AxesLabel → $\{\beta + \eta, \gamma\}$, PlotRange → $\{0, 1\}$]

f6 = Plot3D[upper[$1, b, c, 4$], $\{b, 2, 8\}$, $\{c, 1, 5\}$, AxesLabel → $\{\beta + \eta, \gamma\}$, PlotRange → $\{0, 1\}$]

Show[f5, f6]

B.2 Codes to plot lower bounds in Figure 3.2

lower1[a_, b_, c_, d_]:=$\frac{a}{a+b+c}$

lower2[a_, b_, c_, d_]:=$\frac{a(a+c)(a+2c)}{(a+b)(a+c)(a+2c)+b*d}$

f1 = Plot3D[lower1[$a, 2, c, 4$], $\{a, 1, 5\}, \{c, 1, 5\}$, AxesLabel → $\{\alpha, \gamma\}$, PlotRange → $\{0, 1\}$]

f2 = Plot3D[lower2[$a, 2, c, 4$], $\{a, 1, 5\}, \{c, 1, 5\}$, AxesLabel → $\{\alpha, \gamma\}$, PlotRange → $\{0, 1\}$]

Show[f1, f2]

f3 = Plot3D[lower1[$a, b, 1, 4$], $\{a, 1, 5\}, \{b, 2, 8\}$, AxesLabel → $\{\alpha, \beta + \eta\}$, PlotRange → $\{0, 0.8\}$]

f4 = Plot3D[lower2[$a, b, 1, 4$], $\{a, 1, 5\}, \{b, 2, 8\}$, AxesLabel → $\{\alpha, \beta + \eta\}$, PlotRange → $\{0, 0.8\}$]

Show[f3, f4]

f5 = Plot3D[lower1[$1, b, c, 4$], $\{b, 2, 8\}, \{c, 1, 5\}$, AxesLabel → $\{\beta + \eta, \gamma\}$, PlotRange → $\{0, 0.8\}$]

f6 = Plot3D[lower2[$1, b, c, 4$], $\{b, 2, 8\}, \{c, 1, 5\}$, AxesLabel → $\{\beta + \eta, \gamma\}$, PlotRange → $\{0, 0.8\}$]

Show[f5, f6]

B.3 Codes to plot upper bounds in Figure 3.3

upper1[a_, b_, c_, d_]:=$\frac{a+c*d}{a+b+c*d}$

upper2[a_, b_, c_, d_]:=$\frac{\sqrt{(a+b-c*d)^2+4a*c*d}-(a+b-c*d)}{2c*d}$

f1 = Plot3D[upper1[$a, 2, c, 4$], $\{a, 1, 5\}, \{c, 1, 5\}$, AxesLabel → $\{\alpha, \gamma\}$, PlotRange → $\{0.2, 1\}$]

$\mathrm{f2} = \mathrm{Plot3D}[\mathrm{upper2}[a, 2, c, 4], \{a, 1, 5\}, \{c, 1, 5\}, \mathrm{AxesLabel} \to \{\alpha, \gamma\}, \mathrm{PlotRange} \to \{0.2, 1\}]$

$\mathrm{Show}[\mathrm{f1}, \mathrm{f2}]$

$\mathrm{f3} = \mathrm{Plot3D}[\mathrm{upper1}[a, b, 1, 4], \{a, 1, 5\}, \{b, 2, 8\}, \mathrm{AxesLabel} \to \{\alpha, \beta + \eta\}, \mathrm{PlotRange} \to \{0, 1\}]$

$\mathrm{f4} = \mathrm{Plot3D}[\mathrm{upper2}[a, b, 1, 4], \{a, 1, 5\}, \{b, 2, 8\}, \mathrm{AxesLabel} \to \{\alpha, \beta + \eta\}, \mathrm{PlotRange} \to \{0, 1\}]$

$\mathrm{Show}[\mathrm{f3}, \mathrm{f4}]$

$\mathrm{f5} = \mathrm{Plot3D}[\mathrm{upper1}[1, b, c, 4], \{b, 2, 8\}, \{c, 1, 5\}, \mathrm{AxesLabel} \to \{\beta + \eta, \gamma\}, \mathrm{PlotRange} \to \{0, 1\}]$

$\mathrm{f6} = \mathrm{Plot3D}[\mathrm{upper2}[1, b, c, 4], \{b, 2, 8\}, \{c, 1, 5\}, \mathrm{AxesLabel} \to \{\beta + \eta, \gamma\}, \mathrm{PlotRange} \to \{0, 1\}]$

$\mathrm{Show}[\mathrm{f5}, \mathrm{f6}]$

Bibliography

[1] Ahamed, I. A. and Kochar, S. C. (1990) Testing whether F is more IFR than G. *Metrika* 37, 45-58.

[2] Aiello, W. Chung-Graham, F. and Lu, L. (2001) A random graph model for massive graphs. *Experimental Mathematics* 10, 53-66.

[3] Aly, E. E. (1993) On Testing for Mean Residual Life Ordering. *Naval Research Logistics* 40, 633-642.

[4] Aron, J. L. and Gove, R. A. (1998) Application of models from epidemiology to metrics for computer virus risk. *Proceedings of the IFIP TC11 Working Group 11.5, Second Working Conference on Integrity and Internal Control in Information Systems* 136, 131-145.

[5] Arvesen, J. N. (1969) Jackknifing U–statistics. *The Annals of Mathematical Statistics* 40, 2076-2100.

[6] Aspnes, J., Diamadi, Z. and Shah, G. (2002) Fault tolerant routing in Peer to Peer systems. *ACM PODC*.

[7] Barabási, A. and Albert, R. (1999) Emergence of scaling in random networks. *Science* 286, 509-512.

[8] Barlow, R.E. and Campo, R. (1975) Total Time on Test processes and applications to failure data analysis, in *Reliability and Fault Tree Analysis*, pp 451-481, R.E. Barlow, J. Fussell and N.D. Singpurwalla (eds.). SIAM, Philadelphia.

[9] Barlow, R. E. and Proschan, F. (1981) *Statistical Theory of Reliability and Life Testing: Probability Models*. To Begin with, Silver Spring, MD.

[10] Bergman, B. (1979) On age replacement and total time on test concept. *Scandinavian Journal of Statostics* 6, 161-168.

[11] Bollobás, B. (2001) *Random Graphs*. 2nd Edition, Cambridge University Press.

[12] Brin, S. and Page, L. (1998) The anatomy of a large-scale hypertexual Web search engine. *Proceedings of the Seventh International World-Wide Web Conference*, special issue of *Computer Networks and ISDN Systems* 30, 1-7.

[13] Burtin, Y. D. (1977) Connection probability of a random subgraph of an n-dimensional cube. *Probl. Pered. Inf.* **13**, April-June.

[14] Bustemante, F. E. and Qiao, Y. (2003) Friendships that last: Peer lifespan and its role in P2P protocols. *Intl. Workshop on Web Caching and Distribution*.

[15] Caldarelli, G. (2007) *Scale-free Networks*. Oxford University Press, Oxford.

[16] Castellano, C. and Pastor-Satorras, R. (2010) Thresholds for epidemic spreading in networks. *Physical Review Letters* 105, 218701-218704.

[17] Curtain, M. (1997) *Introduction to Network Security*. Kent Information Services, Inc.

[18] D'Agostino, G., Scala, A., Zlatić, V. and Caldarelli, G. (2011) Assortativity effects on diffusion-like processes in scale-free networks. arXiv:1105.3574v2 [physics.soc-ph].

[19] David, H. A. and Nagaraja, H. N. (2003) *Order Statistics*, 3rd edition. New York: Wiley.

[20] Denuit, M., Dhaene, J., Goovaerts, M. and Kaas, R. (2005) *Actuarial Theory for Dependent Risks*. Wiley: New York.

[21] Erdös, P. and Rényi, A. (1960) On the evolution of random graphs. *Publications of the Mathematical Institute of Hungarian Academic of Scieces* 5, 17-61.

[22] Ganesh, A. and Massoulie, L. (2003) Failure resilience in balanced overlay networks. *Allerton Conference on Communication, Control and computing.*

[23] Gerlach, B., (1986) A new test for whether F is "more NBU" than G. *Statistics* 17, 79-86.

[24] Grimes, R. A. (2005) *Honeypots for Windows* (The Experts Voice). New York: Academic Press.

[25] Gummadi, K., Gummadi, R., Gribble, S., Ratnasamy, S., Shenker, S. and Stoica, I. (2003) The impact of DHT routing geometry on resilience and proximity. *ACM SIGCOMM.*

[26] Harchol-Balter, M. and Downey, A. B. (1997) Exploiting process lifetime distributions for dynamic load balancing. *ACM Transactions on Computer Systems* 15, 253-285.

[27] Hoeffding, W. (1948) A class of statistics with asymptotically normal distribution. *The Annals of Mathematical Statistics* 19, 91-95.

[28] Hollander, M., Park, D. H. and Proschan, F. (1982) Testing whether F is "more NBU" than G. *Florida State University Statistics Report M 626.*

[29] Hu, T., Kundu, A. and Nanda, A. K. (2001) On generalized ordering and aging properties with their implications. In: Hayakawa Y, Irony T, Xie M (eds) *System and Bayesian Reliability*. Singapore: World Scientific Press.

[30] Hutchinson, T. P. and Lai, C. D. (1990) *Continous bivariate distributions, emphasising applications*. Sydney: Rumsby.

[31] Kaashoek, M. F. and Karger, D. (2003) Koorde: A simple degree-optimal distributed hash table. *IPTPS*.

[32] Joe, H. (1997) *Multivariate models and dependence concepts*. London: Chapman & Hall.

[33] Kephart, J. O. and White, S. R. (1991) Directed-graph epidemiological models of computer viruses. *IEEE Computer Society Symposium on Research in Security and Privacy* 343-359.

[34] Kephart, J. O., Chess D. M. and White S. R. (1993) Computers and epidemiology. *IEEE Spectrum* 30, 20-26.

[35] Klefsjö, B. (1983) Some tests against aging based on total time on test transform. *Communication in Statistics-Theory and Methods* 12, 907-927.

[36] Kochar, S. C., Li, X. and Shaked, M. (2002) The total time on test transform and the excess wealth stochastic order of distributions. *Advances in Applied Probability* 34, 826-845.

[37] Kochar, S. C. and Wiens, D. P. (1987) Partial ordering of life distributions with respect to their aging properties. *Naval Research Logistics* 34, 823-829.

[38] Kuo, W. and Zuo, M. J. (2002) *Optimal Reliability Modeling: Principles and Applications*. New York: Wiley.

[39] Laet, G. D. and Schauwers, G. (2005) *Network security fundamentals*. Cisco Press fundamentals series. Indianapolis, Ind: Cisco.

[40] Lai, C-D. and Xie, M. (2006) *Stochastic Ageing and Dependence for Reliability*. Springer: Wiley.

[41] Leighton, F. T., Maggs, B. M. and Sitamaran, R. K. (1995) On the fault tolerance of some popular bounded-degree networks. *IEEE FOCS*.

[42] Leonard, D., Yao, Z., Rai, V. and Loguinov, D. (2007) On lifetime-based node failure and stochastic resilience of decentralized peer-to-peer networks. *IEEE/ACM Transactions on Networking* 15, 644 - 656.

[43] Li, H. and Li, X. (2013) *Stochastic Orders in Reliability and Risk*. Springer: New York.

[44] Li, X. and Li, L. (2011) Security analysis of compromised-neighbor-tolerant networks using stochastics. *IEEE transactions on Reliability* 61, 749-757.

[45] Li, X., Parker, P. and Xu, S. (2007) Towards an analytic model of epidemic spreading in heterogeneous systems. *The 4th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*.

[46] Li, X., Parker, P. and Xu, S. (2011) A stochastic model for quantitative security analysis on networked systems. *IEEE transactions on Dependable Computing and Security* 8, 28-43.

[47] Li, X., Zhao, P. and Li, L. (2009) Resilience and reliability analysis of P2P network systems. *Operations Research Letters* 37, 20-26.

[48] Li, X. and Shaked, M. (2007) A general family of univariate stochastic orders. *Journal of Statistical Planning and Inferences* 137, 3601-3610.

[49] Li, X. and Shaked, M. (2004) The observed TTT transform and the observed excess wealth transform. *Statistics and Probability Letters* 68, 247-258.

[50] Maiwald, E. (2003) *Network security: a beginners guide*, 2nd Edition. California: McGraw-Hill.

[51] Massoulié, L., Kermarrec, A. M. and Ganesh, A. (2003) Network awareness and failure resilience in self-organising overlay networks. *IEEE Symposium on Reliable and Distributed Systems*.

[52] McNeil, A. J. and Nešlehová, J. (2009) Multivariate Archimedeaen copulas, D-monotone functions and ℓ_1-norm symmetric distributions. *The Annals of Statistics* 37, 3059-3097.

[53] Mirkovic, J., Dietrich, S., Dittrich, D. and Reiher, P. (2004) *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)*. New York: Prentice Hall.

[54] Mitzenmacher, M. (2001) Dynamic models for file sizes and double pareto distributions. *Internet Mathematics* 1, 305-333.

[55] Moreno, Y., Pastor-Satorras, R. and Vespignani, R. (2002) Epidemic outbreaks in complex heterogeneous networks. *European Physical Journals B* 26, 521-529.

[56] Müller, A. and Stoyan, D. (2002) *Comparison methods for stochastic models and risks*. New York: Wiley.

[57] Nelsen, B. R. (2006) *An introduction to copula*. New York: Springer.

[58] Pandurangan, G., Raghavan, P. and Upfal, E. (2004) Using pagerank to characterize Web structure. *Internet Mathematics* 3, 1-20.

[59] Pastor-Satorras, R. and Vespignani, R. (2001) Epidemic dynamics and endemic states in complex networks. *Physical Reviews E* 63, 1-8.

[60] Pastor-Satorras, R. and Vespignani, R. (2002) Epidemic dynamics in finite size scale-free networks. *Physical Reviews E* 65, 035108.

[61] Pham, H. (2003) *Handbook of reliability engineering*. New York: Springer.

[62] Piqueira, J. R. C., Vasconcelosa, A. A., Gabriela, C. E. C. J. and Araujo, V. O. (2008) Dynamic models for computer viruses. *Computer and Security*, doi:10.1016/j.cose.2008.07.006.

[63] Proschan, F. (1963) Theoretical explanation of observed decreasing failure rate. *Technometrics* 5, 375-383.

[64] Rezapour, M. and Alamatsaz, M. H. (2014) Stochastic comparison of lifetimes of two (n-k+1)-out-of-n systems with heterogeneous dependent components. *Journal of Multivariate Analysis* 130, 240-251.

[65] Ross, S. M. (1996) *Stochastic Processes*. New York: Wiley.

[66] Saroiu, S., Gummadi, P. K., and Gribble, S. D. (2002) A measurement study of Peer-to-Peer file sharing systems. *MMCN*.

[67] Simmonds, A., Sandilands, P. and van Ekert, L. (2004) *An Ontology for Network Security Attacks*. Lecture Notes in Computer Science 3285: 317-323.

[68] Shaked, M. and Shanthikumar, J. G. (2007) *Stochastic Orders*. New York: Springer.

[69] Stoica, I., Morris, R., Karger, Kaashoek, M. F. and Balakrishnan, H. (2001) Chord: A scalable Peer-to-Peer lookup service for internet applications. *ACM SIGCOMM*.

[70] Thompson, D. and Kilgore, R. (2011) Estimating joint flow probabilities at stream confluences using copulas. *Transportation Research Record* 2262, 200-206.

[71] Wang, J., Lu, L. and Chien, A. (2003) Tolerating denial-of-service attacks using overlay networks - impact of topology. *Proceeding of ACM Workshop on Survival and Self-regenerative Systems* 14, 4-4.

[72] Wang, Y., Chakraberti, C., Wang, C. and Faloutsos, C. (2003) Epidemic spreading in real networks: an eigenvalue viewpoint. *Proceeding of 22nd IEEE Symposium on Reliable Distributed Systems* 25-34.

[73] Wierman, J. C. and Marchette, D. J. (2004) Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction. *Computational Statistics & Data Analysis* 35, 3-23.

[74] Xu, S., Li, X., Parker, P. and Wang, X. (2011) Exploiting trust-based social networks for distributed protection of sensitive data. *IEEE Transactions on Information Forensics and Security* 6, 39-52.

Index

Vita

Xiaohu Li, registered as a graduate student in Department of Mathematics, University of New Orleans in 2007 to pursue doctoral degree of Engineering and Applied Science. Before that, he worked as a Research Associate in the Department of Computer Science, University of Texas at San Antonio, USA (2005 - 2007) and in the Department of Mechanical Engineering, University of Alberta, Canada (2003 - 2004). His main research interests include

- Network security,
- Theory of reliability,
- Risk management,
- Statistical dependence,
- Stochastic order,
- Non-parametric life-testing.