Information Knowledge Systems Management 10 (2012) 1–23 1
DOI 10.3233/IKS-2012-0189
IOS Press

Chapter 7

Management of systemic risks and cascade failures in a networked society

Akira Namatame* and Takanori Komatsu
Department of Computer Science, National Defense Academy, Japan

1. Introduction

The qualification of risks lies in their systemic nature. A risk to one subsystem may present an opportunity to another subsystem. A systemic risk is the possibility that an event will trigger a loss of confidence in a substantial portion of the system serious enough to have adverse consequences on system performance. A systemic risk therefore impacts the integrity of the whole system.

In this chapter, we use networks to address risks. A network, which is a collection of nodes with links between them, can be a useful representation of a system. For instance, network analysis can explain certain systemic risks in financial systems by modeling interactions among financial institutions. A network approach is also useful in mitigating large blackouts caused by cascade failure. In this case, instead of looking at the details of particular blackouts, we investigate the cascade dynamics as a series of blackouts using risk propagation models.

We use a general framework of diffusion or contagion models to describe risk propagation in networks and investigate how network topology impacts risk propagation patterns. At the macroscopic level, systemic risk is measured as the fraction of failed nodes. We divide our discussion into two classes of diffusion. First, we discuss so-called progressive diffusion processes. Many diffusion processes are progressive in the sense that once a node switches from one state to another, it remains in that state in all subsequent time steps. The second class is non-progressive diffusion where, as time progresses, nodes can switch back and forth from one state to the other, depending on the states of their neighbors.

Networks increase interdependency, creating challenges for managing risks. This is especially apparent in areas such as financial institutions and enterprise risk management, where the actions of a single actor in an interconnected network can impact all the other actors in the network.

The network is only as strong as its weakest link, and trade-offs are most often connected to a function that models system performance management. In this context, there is a class of problems, ranging from risk spreading to the control of cascade failure, that are naturally defined as network optimization problems. Other efforts like improving the robustness of systems also involve optimization problems and reveal enhanced system properties shaped by optimizing the underlying network topology.

*Corresponding author: Akira Namatame, Department of Computer Science, National Defense Academy, Japan. E-mail: nama@nda.ac.jp.

2. The nature of risks: Emergence, interdependence, and endogenous vs. exogenous effects

Our society consists of individuals and the social systems in which they interact. Decision-making and the behavior of individuals also depend on their social contexts. On the other hand, individuals' behavior creates the social system of which the individuals are parts. Therefore, many social systems are characterized using feedback mechanisms or micro-macro loops between individuals and the whole system.

Emergent properties can appear when a number of simple entities operate in an environment, collectively forming more complex patterns. Emergence is not a property of any single entity, nor can it be easily predicted or deduced from the behavior of lower-level entities. A set of behavioral rules at the individual level can result in emergent properties on the system level, and these properties, in turn, influence individual behaviors and interactions among individuals. A system may need to reach a certain critical point before it can self-generate emergent properties.

Social systems also have emergent properties that cannot be trivially derived from the properties of their components. Understanding and shaping emergence may be essential to the survival of social systems. Unintended consequences and side effects relate closely to emergent properties. In other words, the macroscopic functionality of a system is the sum of the consequences and side effects of emergent properties.

In turn, regularities observed at the macroscopic level also influence individual elements. This bi-directional causal relationship is an essential component of the study of systemic risks. Understanding the relationship between the different levels at which macroscopic phenomena can be observed as compound risks can be made possible by the tools and insights generated in network research.

In a networked world, the risks faced by any one actor depend not only on that actor's actions but also on those of others. The fact that the risk one actor faces is often determined in part by the activities of others gives a unique and complex structure to the incentives that agents face as they attempt to reduce their exposure to these interdependent risks. The term interdependent risks refers to situations in which multiple actors decide separately whether to adopt protective management strategies such as protecting against earthquakes or terrorism, and where each actor has a decreasing incentive to choose protection if others fail to do so.

Protective management strategies can reduce the risk of a direct loss to a country, firm or individual, but there is still some chance of suffering damage from others who do not take similar actions. The fact that the risk is often determined in part by the behavior of others imposes independent risk structures on the incentives that individuals or firms face for reducing risk or investing in risk mitigation measures.

Kunreuther and Heal were initially led to analyze such situations by focusing on the interdependence of security problems (Kunreuther & Heal, 2003). An interdependent security setting is one in which each individual or firm that is part of an interconnected system must decide independently whether to adopt protective strategies that mitigate future losses. The analysis focused on protection against discrete, low-probability events in a variety of protective settings with somewhat different cost and benefit structures: airline security, computer security, fire protection, and vaccination.

Under some circumstances, the interdependent security problem resembles the familiar dilemma in which the only equilibrium is the decision by all actors not to invest in protection even though everyone would be better off if they had decided to incur this cost. In other words, a protective strategy that would benefit all actors if widely adopted may not be worth its cost to any single actor, even if all the other actors were to adopt it; any single actor is better off simply taking a free ride on the others' investments.

In other circumstances, however, a protective measure is cost-effective for each actor provided enough other actors also invest in risk reduction. Independent security problems, though, have the potential for

tipping (Schelling, 1978), where one or several actors' decisions can determine the outcome, and for cascading, in which there is a set of actors for whom the first change in strategy toward or away from protection triggers others to follow suit. Therefore, a key policy issue is to provide incentives for a group of agents to take action with respect to exposure to risks, prompting a move beyond the tipping point.

If one actor believes others will not invest in security, his or her incentive to do so is reduced. The end result may be that no one invests in protection, although all would have been better off if they had incurred the cost of a protection strategy. On the other hand, should each decision maker believe others will also undertake mitigation measures, his or her optimal strategy will be to do the same.

Kunreuther also notes two fundamental aspects of interdependent risks: first, interdependency, and second, heuristic biases and human mistakes (Kunreuther, 2009). The first provides an insight into the nature of interdependency and provides an example of how interdependency affects the way in which we manage and mitigate global risks. The second reflects a human approach to risk in general. Humans operate with incomplete information through the use of heuristics.

From a dynamics point of view, the decision to take action depends on how many others have taken similar steps. With respect to protection and risk-reducing measures, there is evidence from controlled field studies and laboratory experiments that many individuals are not willing to invest in security for a number of reasons that include myopia, high discount rates and budget constraints. In the models considered above there were also no internal positive effects associated with protective measures. Many individuals invest in security to relieve the anxiety and worry they feel about what they perceive might happen to them or to others, and thus gain peace of mind.

A more realistic model of interdependent security that incorporates these behavioral factors as well as people's misperceptions of the risk may suggest a different set of policy recommendations than a rational model of choice. For example, if a country was reluctant to invest in protection because it was myopic, then some type of loan may enable it to discern the long-term benefits of the protective measure. A long-term loan would also help relieve budget constraints that may deter some individuals, firms or nations from incurring the upfront costs of risk-reducing measures.

We tend to use the terms risk and uncertainty interchangeably. However, risk describes a system in which we may not know the outcomes, but we do know what the underlying probability distribution of outcomes looks like. We can model risk using probability calculus. In contrast, uncertainty reflects a situation where we do not know the outcome, nor do we know the distribution of the underlying systems. It is not hard to see that most systems we deal with in the real world are really uncertain, not risky, events.

In summary, we are still not very good at dealing with risk. Psychologists have demonstrated that events that are not vivid in our minds get assigned very low probabilities – much lower than the facts warrant. We are also still linear thinkers with a nearly insatiable need to link cause and effect, and we assess probabilities poorly. However, now we do understand some of the mechanisms that underlie complex systems better than we have in the past, and that knowledge can be very helpful in preparation for future catastrophic events (Mauboussin, 2006).

3. Systemic risk concepts

Risks are idiosyncratic – a risk to one system may present an opportunity for another system. Their consequences are hard to predict and present challenges to us all. The qualification of risks lies in their systemic nature and their impacts challenge the integrity of the system.

When we discuss the mechanisms behind risks, it is important to distinguish between endogenous and exogenous sources of risk. Endogenous risk arises within the system; it is inherent to a social system,

yet remains poorly understood. Endogenous risk also has the potential to do the greatest damage. This is the topic of the chapter, and we will try to elucidate this aspect of risk and its management.

Exogenous risk comes from outside a system, and is basically a condition imposed on it. Most natural and social systems are continuously subjected to external stimulation, noise, or shocks that can vary widely in amplitude. It is thus not clear a priori if a given large event is due to a strong exogenous shock or to the internal dynamics of the system. In most cases it may be due to a combination of both. Many socio-economic systems involving human decision-making are subject to both types of risk.

We will place a particular emphasis on differentiating between systems in which risk is endogenous or internal versus situations in which risk is due to exogenous or external factors. The mechanisms behind risk can really only help describe what is going on, and are of limited predictive value. These mechanisms provide insights into how complex adaptive systems work, and gaining those insights is a first step toward dealing with risk.

Network theory bears on a wide variety of phenomena, including networks of friends, transmitters on the power grid, and the spread of disease. In recent years, scientists have made major advances in understanding the nature of networks. We now know that the structure of a network is important in understanding how things can be transmitted over it.

Networks increase interdependence, which creates challenges for managing risks. This is especially apparent in areas such as financial institutions and enterprise risk management, where the actions of a single node (actor) in an interconnected network can impact all the other nodes in the network.

The concept of a systemic risk is that something bad can happen in a system that is a good deal bigger and worse than the failure of any single node or subsystem. A systemic risk is also defined as the risk of a phase transition from one equilibrium condition to another, less favorable equilibrium. This transition is also characterized by self-reinforcing and feedback mechanisms that make it difficult to reverse.

When studying systemic risks that can trigger unexpected large-scale changes in a system or imply uncontrollable large-scale threats to it, scientific research has often focused on natural disasters such as earthquakes or on failures of engineered systems such as electric power grid blackouts. However, many major disasters affecting human societies relate to the insides of social systems. Periods of financial instability and economic crises are typical examples of systemic risks (Helbing, 2010).

In banking systems, there is a tendency for crises to spread from one institution to another. This tendency is referred to as systemic risk and, at a large enough scale, leads to systemic failure. Some sources for systemic failure have been noted in the literature to explain the mechanism of bank failures during financial crises. For example, Allen and Gale introduced the use of network theories to enrich our understanding of financial systems and studied how the financial system responds to contagion when financial institutions are connected with different network topologies (Allen & Gale, 2000).

They explored critical issues in the study of systemic risks by exploring fundamental questions such as how resilient financial networks are to contagion and how financial institutions form connections when exposed to the risk of contagion. They showed that increasing connections between banks might reduce the risk of contagion. While the risk of contagion may be expected to be larger in a highly interconnected banking system, research indicates that shocks may have such complex effects that the more complete the set of links among financial institutions is, the lower the risk of contagion in the system.

Network interdependencies are another reason for failure event cascades. Examples include disease epidemics, traffic congestion, and electrical power system blackouts. These phenomena are known as cascade failures, chain reactions, avalanches or domino effects. The most common feature of cascade failures is that a local failure event results in a global failure on a larger scale. Such systemic risks are typical cases of non-linear interactions, which are ubiquitous in socio-economic systems.

The basic mechanism behind cascade failure is a feedback loop or vicious circle that often induces undesired side effects. A large blackout may start with a fairly routine problem in a particular area. This type of a problem may even happen relatively frequently all over the system, and usually such a failure in one spot is absorbed by a neighboring area. Such a problem may, however, propagate to other regions under certain conditions. When that happens, things worsen all along the chain until the system ends up with a widespread failure.

Another mechanism behind cascade failure is explained as follows: there is a critical load at which risk sharply increases toward a threshold for cascade failure. We will discuss a modeling and simulation approach to computing the proximity to cascade failure. Modeling cascade failure as a dynamic process suggests the quantitative methods to use to compute and monitor criticality by quantifying how failures propagate.

People usually seek to understand causes and effects and to fix problems when they face failure. However, there is no simple way to understand cause and effect. Systemic risks are idiosyncratic and are an inherent part of networked systems. Although networked systems bring many benefits to society, these systems are vulnerable to cascade failures.

Another aspect of social systems is that they face exogenous risks. When we think about disaster preparedness, we are often thinking of exogenous risks. Examples include the threats of avian flu, terrorism, and hurricanes. Each of these risks can be treated as an exogenous threat, and we often think of risky events happening to us exogenously rather than arising endogenously from our day-to-day activities.

Endogenous risk, referring to the risk from shocks that are generated and amplified within the system, stands in contrast to exogenous risk, which refers to shocks that arrive from the outside (Danielsson, 2000). Extreme events are seen to be endogenous, but how can we be confident that a given extreme event is really due to an endogenous self-organization of the system rather than being a response to an external shock?

The outcomes of social systems often have a signature known as a power law. Power laws describe a wide range of phenomena from casualties in wars to earthquake magnitudes, the size of blackouts, stock price changes, and city population size distributions. What is elegant about power laws is that large events happen infrequently and small events happen frequently.

4. Modeling progressive diffusion in networks

Important processes that take place within social networks, such as the spreading of opinions and innovations, are influenced by the topological properties of those networks. In turn, the opinions and practices of individuals can have a clear impact on network topology. In practice, it is desirable to compose an inventory of the types of microscopic dynamics that have been investigated in network research and their impacts at the network level. Such an inventory could enrich research concerning the kinds of cascading and diffusion phenomena that exist.

Technologies, ideas, and illnesses tend to diffuse following a well-known S-curve pattern. For example, a new technology will start with only a few adopters and grow at a relatively slow rate early on. The rate then accelerates, and the diffusion process takes off. This kind of diffusion pattern has been studied in detail and is of prime interest to the studies of epidemics and technology innovation. The key point is that the diffusion process is nonlinear and is very slow at the start, then rises rapidly, and slows down again. It is also important to note that most technologies or ideas do not successfully diffuse, they simply sputter out.

In this section, we investigate how the structure of social network impacts diffusion patterns. The discussions are divided into two classes of diffusion processes. First, we discuss what is called a progressive diffusion process. Many diffusion processes are progressive in a sense that once a node switches from one state to another, it remains in the same state in all subsequent time steps. For this type of progressive diffusion, we focus on the observable systemic risk at the macroscopic level by focusing on the interplay between the network topology and the transmission rate at the individual level.

In the next section, we discuss the second class of diffusion processes, non-progressive diffusion, where as time progresses, nodes can switch back and forth from one state to the other depending on the states of their neighbors. For non-progressive diffusion processes, we focus on the internal process within the node or decision making at the individual level. This class of non-progressive diffusion has a problem structure similar to a social influence process, and is characterized as a threshold-based model.

The spread of information underlies societies. Information diffuses from one individual to others. An individual who knows new information will, with a certain probability, share this information with colleagues. This form of information transmission is a typical example of a diffusion process. The most fundamental question is under what conditions the information will penetrate the society. Information diffusion has a problem structure similar to the process by which epidemics spread, and the properties of that process are well understood.

Whether the information will penetrate a society depends primarily on the probability that it will be passed from the individual who knows it on to other partners. This transmission relationship determines the social network structure. In the spread of opinions, for instance, hearing the same opinion from a number of colleagues or sources results in a higher probability of adopting it than does hearing an opinion from a single source. The status of the individuals from whom the information comes also affects adoption. The dynamics of information transmission is also a threshold phenomenon, where below a certain probability the information will spread within a limited group and above that threshold it will penetrate society.

We begin by discussing several examples of studies that illustrate how network structure impacts macroscopic diffusion patterns. The diffusion of information, rumors, or gossip through social networks can be modeled after the spread of infectious diseases.

The basic diffusion model is the SIR model, in which nodes are initially susceptible to the disease and can become infected from infected neighbors. In the spread of a disease, some nodes (individuals) initially become infected by exogenous sources. Consequently, some of these individuals' neighbors are infected by contact. Once infected, a node continues to infect its neighbors until it is randomly removed from the system. Infected nodes can either recover and stop transmitting the disease or die and completely disappear from the network. There is a possibility that a given node is immune, but if it is not, it is sure to catch the disease if one of its neighbors is infected.

Another model is the SIS model, in which nodes, once infected, can randomly recover; however, after recovery, they are once again susceptible to infection. The SIS model corresponds well with many real-world viral infections that may cause individuals to go back and forth between health and illness.

Below, we model risk propagation as a dynamic birth-death process with self-recovery. An agent propagates the risk to other agents in a single step with some probability β, while at the same time this propagating agent may recover or be relieved of the risk with probability δ. The ratio of the two parameters $\lambda = \beta/\delta$ defines the relative propagation rate.

Epidemic diffusion can be characterized using an epidemic threshold (ρ_c). If the relative infection ratio (β/δ) is greater than this threshold, the epidemic may spread and a large portion of agents will

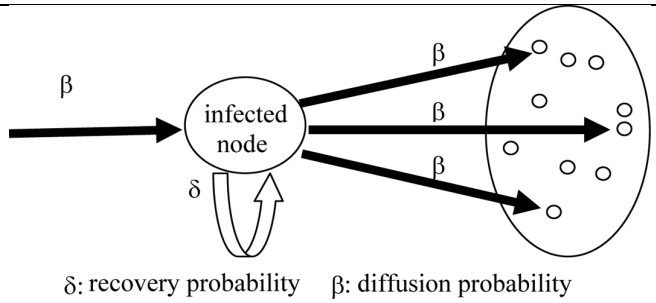

Fig. 1. Risk propagation process.

be infected; otherwise, it may die out. Many studies have been done to obtain and characterize the thresholds in various network topology settings. The threshold of a random network (graph) is given by

$$\rho_{ER} \cong 1/ < k > \tag{1}$$

where $< k >$ is the average degree of the graph. The threshold of a scale-free network is given as

$$\rho_{SF} \cong < k > / < k^2 > \tag{2}$$

where $< k^2 >$ is the average degree of the graph squared.

A network G can be represented by its adjacency matrix A = (a_{ij}), a real symmetric matrix where $a_{ij} = a_{ji} = 1$ if agent i and agent j are connected and are 0 if they are not.

We denote the probability that agent i is aware of the information at time t as $p_i(t)$. The column vector $p(t) = (p_1(t) \cdot p_2(t), \ldots, p_N(t))$ represents the awareness probabilities of the agent population. The transitions of these awareness probabilities are described as

$$p(t+1) = (\beta A \ + \ (1-\delta)I)p(t) \tag{3}$$

where *I* is an *NxN* identity matrix (Wang, 2003). The long run behavior of the dynamic process described by Eq. (3) is determined by the system matrix, defined as S = βA + $(1-\delta)I$.

The spectrum of a network G is the set of eigenvalues of its adjacency matrix A. The spectrum of the system matrix S (the distribution of eigenvalues of S) is closely related to the spectrum of the adjacency matrix A. In particular, we have

$$\lambda_\iota(S) = \beta\lambda_\iota(\mathrm{A}) + (1-\delta), i = 1, 2, \ldots, N. \tag{4}$$

where λ_ι(S) is the i-th largest eigenvalue of the system matrix S.

The largest eigenvalue λ_ι(S) is also called the principal eigenvalue of the system matrix S, which is denoted by λ_1(S). The convergence condition of the diffusion dynamics in Eq. (3) is then given as follows:

$$\text{If } \lambda_1(S) < 1, \text{then } p(t) \text{ converges to the zero vector.} \tag{5}$$

From the relation in Eq. (4), the condition in Eq. (5) in terms of the principal eigenvalue of the system matrix S can be also expressed in term of the principal eigenvalue of the adjacency matrix A. That is,

$$\text{If } \beta/\delta < 1/\lambda_1(\mathrm{A}), \text{then } p(t) \text{ converges to the zero vector.} \tag{6}$$

The principal eigenvalue of the adjacency matrix A also provides useful information for determining how quickly a society may recover from epidemic diffusion. The number of infected nodes decays exponentially over time if the principal eigenvalue of the adjacency matrix A is small.

From the discussion above, we know that the risk diffusion process can be also characterized as a threshold phenomenon. From Eq. (6), the threshold is characterized by the inverse of the largest eigenvalue

$$\rho_{op} \cong 1/\lambda_1(A) \tag{7}$$

Our basic question is how network structure impacts macroscopic diffusion patterns, especially the ratio of infected nodes. This question can be investigated by obtaining epidemic thresholds of various network topologies. Diffusion only starts when there is a high relative propagation rate β/δ in a network that has a sizeable largest eigenvalue.

Different networks exhibit different features with different eigenvalues. We can optimize a network topology using an evolutionary approach, where we select a proper fitness function. To maximize diffusion, for instance, we should have a network (adjacency matrix) with the largest possible eigenvalue. It is obvious that a fully connected complete network fulfills that requirement. Since this is rare, we should consider optimization where the network is influenced by average constraints.

Our basic question is to investigate how the network structure impacts on macroscopic diffusion patterns, especially the ratio of infected nodes. This question can be investigated through by obtaining epidemic thresholds of various network topologies. The diffusion only starts with high the relative propagation rate β/δ in a network with a higher largest eigenvalue.

Different networks exhibit different features with different eigenvalues. We can optimize a network topology through the evolutionary approach with selection of a proper fitness function. For maximizing diffusion, for instance, we should obtain the network (the adjacency matrix) with the largest eigenvalue. It is obvious that the network fully connected complete network has the largest eigenvalue. Therefore, we should consider the optimization under constraint of the average degree.

We compare the largest eigenvalues of a random network of a scale-free network and of the evolutionary optimized network with the same average degree and we have the following relation:

$$\lambda_1(A_{ER}) < \lambda_1(A_{SF}) < \lambda_1(A_{op}) \tag{8}$$

where $\lambda_1(A_{ER})$ and $\lambda_1(A_{SF})$ are the largest eigenvalues of a random network and a scale-free network respectively and $\lambda_1(A_{op})$ is the largest eigenvalue of the optimized network (Komatsu, Namatame, 2010). Chakrabarti introduced the score s of an epidemic on a graph which is defined as (2008)

$$s = \lambda_1(A)(\beta/\delta) \tag{9}$$

The Eq. (6) provides the conditions under which an epidemic dies out ($s < 1$) or survives ($s > 1$). Figure 2 shows the diffusion rates ($\rho = \sum_{i=1}^{N} p_i/N$) over time for various values of the score s in log – log scales. The dotted lines shows the case for $s = 1$. We observe a clear trend and the below the threshold ($s = 1$), the diffusion dies out while the diffusion starts above the threshold ($s-1$) on the optimized network with a higher largest eigenvalue. However the diffusion only starts with a higher score in a scale free-network and it requires a much higher score to diffuse in a random network.

Therefore we can observe that diffusion is easier to start with a lower relative propagation rate β/δ in a network with a higher largest eigenvalue.

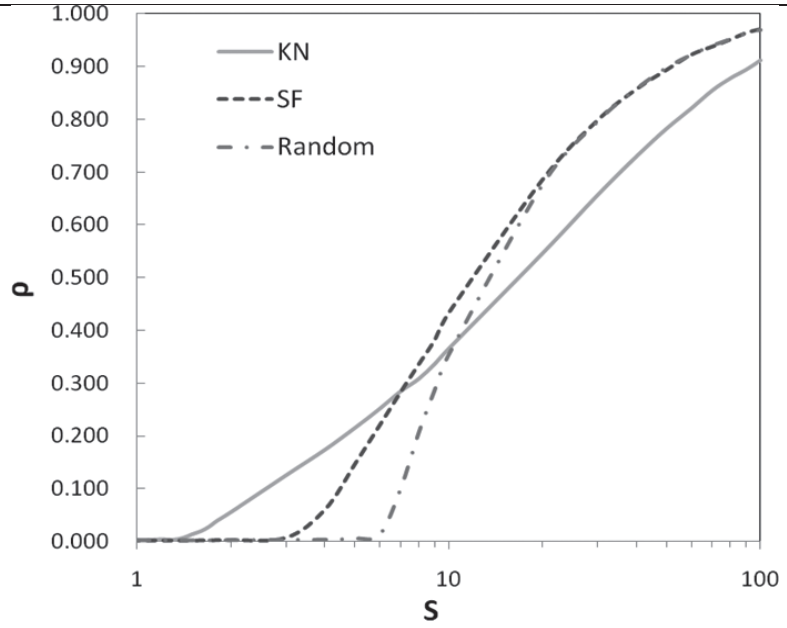

Fig. 2. The ratios of diffused nodes ($\rho = \sum_{i=1}^{N} p_i / N$) as a function of relative propagation rate $s=\lambda_1(A_{OP})(\beta/\delta)$ in different network topologies, random network, scale-free network (SF) and the network with the maximum eigenvalue (KN).

5. Modeling non-progressive diffusion in networks

In this section, we develop a framework to describe non-progressive risk diffusion in a network. This framework will be contrasted with the model discussed in the previous section representing progressive stochastic diffusion. In a non-progressive diffusion process, as time progress, a node can switch back and forth from one state to the other depending on the status of its neighbors. With non-progressive diffusion, we focus on internal node processes or decision-making processes at the individual node level.

For simple diffusion like the spread of disease or rumors – in which a single active node is sufficient to trigger the activation of its neighbors – hub nodes with many connections or random links connecting distant nodes can produce dramatic diffusion. However, not all propagation occurs by the simple activation of nodes after exposure to multiple active neighbors. This can be described by a threshold model in which diffusion at a node is only triggered when the proportion of the node's neighbors that have become active reaches a certain threshold.

Lorenz and colleagues introduced a general framework for network cascade or contagion models to describe various approaches to non-progressive diffusion and identify their commonalities and differences (Lorenz et al., 2009). To unify the various approaches, they define the net fragility of a node, which is the difference between its fragility and the threshold that determines its failure. Nodes fail if their net fragility rises above zero and their failure increases the fragility of neighboring nodes, thus possibly triggering a cascade.

In this framework, Lorenz and colleagues define classes of models according to how the fragility of a node is increased by the failure of a neighbor. At the microscopic level, they show that the failure-spreading pattern varies with the node triggering the cascade, depending on its position in the network. At the macroscopic level, the global failure level is measured as the fraction of nodes that have failed.

On the microscopic side, we denote the binary state of each node i at time t by the dynamic variable $x_i(t)\varepsilon\{0,1\}, i = 1,2,\ldots,N$, where the node can be functional (healthy) or have failed. The status of each node $x_i(t)$ is determined by two factors: tolerance to failure p_i and the external shock h_i to node I. A continuous variable $p_i - h_i$ represents the net fragility of node i. Therefore, node i remains healthy as long as the threshold $\theta_i = p_i(t) - h_i(t)$ is positive, where θ_i represents the threshold above which the fragility produces failure.

Embedding these two parameters, we see that each node is influenced by other failed nodes, so we must consider both in-node failure and failure induced by the external influence from other failed nodes. An individual node, isolated from other nodes' influence, may fail once its net fragility ($p_i - h_i$) becomes negative, or it may fail if the influence of other failed nodes on it exceeds a certain level. Combining these two factors, we define each node's failure function $y_i(t)$, i = 1,2,. . . ,N, as

$$y_i(t) = p_i - h_i + \kappa_i \sum_{i \in N_i} a_{ij} x_i(t) \tag{10}$$

where k_i is a constant, N_i represents the set of nodes to which node i is linked. The coefficient a_{ij} represents the connection relation between two nodes i and j, where

$$a_{ij} = \begin{cases} 1 & \textit{if} \quad \textit{node } i \textit{ is connected to node } j, \\ 0 & \textit{otherwise.} \end{cases} \tag{11}$$

From Eq. (10), each node i is endowed with its own idiosyncratic net fragility θ_i, and fails if the average of its neighboring nodes that have failed becomes greater than its net fragility. That is,

$$x_i = \begin{cases} 1 & if \quad k_i \sum_{k \in N_i} a_{ik} x_k \geqslant h_i - p_i \equiv \theta_i \\ 0 & \textit{otherwise.} \end{cases} \tag{12}$$

Therefore, this class of diffusion is characterized as a threshold-based diffusion process, which is explicitly explained as follows: an individual node is influenced by the status of other nodes. This interdependence is expressed as the threshold rule given by Eq. (12).

On the macroscopic side, the system state at time t is encoded in the N-dimensional state vector x(t) $= \{x_i(t), i = 1,2,\ldots,N\}$, with N being the number of nodes. To fully represent the network dynamics, we extend an individual decision to a collective decision as

$$x(t+1) = F(\ KAx(t) - h\ + p) \tag{13}$$

where F is a set of binary functions such that $F_i(z) = 0$ if $z < 0$ and $F_i(z) = 1$ if $z \geqslant 0$, i = 1,2,. . . ,N. The column vector $x(t)$ stacks up the state variables of all the nodes. The column vector h similarly stacks up all the nodes' idiosyncratic tolerances to failure, and the column vector p stacks up the external shocks they experience. K is the diagonal matrix with a constant k_i.

The macro dynamic variable of interest for systemic risk is the total fraction of failed nodes in the system. We define the total failure rate X(t) at time period t as the percentage of failed nodes as in Eq. (14).

$$X(t) = \sum_{i-1}^{N} x_i(t)/N \tag{14}$$

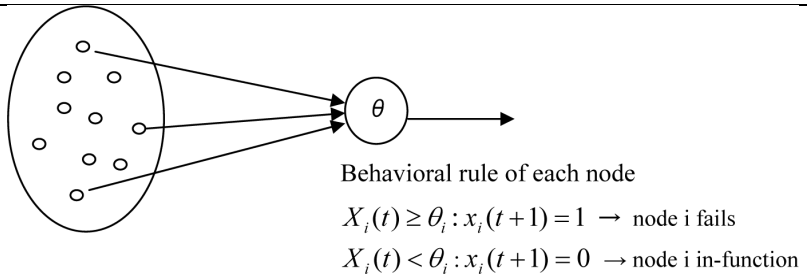

Fig. 3. Threshold rule for each node.

Similarly, we define the failure rate of the neighbors of node i by $X_i(t)$ at time period $t$as a percentage of failed nodes as in Eq. (15).

$$X_i(t) = \sum_{i \in N_i} x_i(t)/N_i \tag{15}$$

The corresponding threshold rule for a node switching to failure state based on its local neighbors is described by Eq. (16).

$$x_i(t+1) = \begin{cases} 1 & \textit{if} \quad X_i(t) \geqslant \theta_i \\ 0 & \textit{otherwise.} \end{cases} \tag{16}$$

Let us suppose that initially almost all nodes are functioning. Thereafter, a few nodes begin to fail. If we apply the update rule in Eq. (12) to nodes in the network, then nodes will, in effect, be repeatedly applying the following threshold rule: a node switches to failure state if the proportion of its neighbors who have failed is larger than the threshold θ_i.

If the trajectories of X(t) stay close to zero, then the system is free of systemic risk, but as the value of X(t) approaches one, the system is prone to systemic risk. We can investigate the phase transition in systemic risk, i.e., situations where small changes in initial conditions result in global failure.

6. A compound propagation model of endogenous and exogenous risks

There are two types of extreme events: endogenous and exogenous shocks. But how can we be confident that a given extreme event is really due to an endogenous (or exogenous) shock? Most natural systems are continuously subjected to external stimulation, noise, shocks, and forcing that can vary widely in amplitude. It is thus not clear a priori if a given large event is due to a strong exogenous shock, to the internal dynamics of the system, or a combination of both. Addressing this question is fundamental for understanding the relative importance of self-organization versus external forcing in complex systems.

This question of whether distinguishing properties characterize endogenous versus exogenous shocks permeates many systems. Sornette provides the following examples where both endogenous and exogenous factors exist: the progressive cascade of reputation versus the result of a well-prepared strategic advertisement, immune system deficiencies to external infections versus internal cascades of regulatory breakdown, domestic economic recession due to global economy recession versus structural domestic and endogenous problems, serendipitous discoveries versus the outcome of a slow endogenous maturation learning process, and the role of external inputs versus internal reinforcements in cognition and brain learning processes (Sornette, 2006).

Johansen and Sornette investigated the precursory and recovery signatures accompanying shocks in the Amazon sales ranking of books (Johansen & Sornette, 2007). They find clear distinguishing signatures classifying two types of sales peaks. Exogenous peaks occur abruptly and are followed by a power law relaxation, while endogenous sales peaks occur after a progressively accelerating power law growth, after which sales follow an approximately symmetrical power law relaxation that is slower than for exogenous peaks. The slow relaxation of sales implies that sales dynamics are dominated by cascades rather than by the direct effects of news or advertisements, indicating that the social network is close to critical. Their analysis suggests a subtle interplay between exogenous and endogenous shocks, casting new light on this debate.

Endogenous risk refers to the risk from shocks generated and amplified within the system, whereas exogenous risk refers to shocks that arrive from outside (Danielsson, 2000). Many socio-economic systems involving human decision-making are subject to both types of risk. However, the greatest damage is caused by endogenous risk.

In this section, we propose a compound propagation model for endogenous and exogenous risks. Each node in the network has two states, normal and failed, and it fails under the influence of two factors, endogenous and exogenous events.

We show that collective dynamics leads to outcomes that seem deterministic in spite of being governed by a stochastic model at the microscopic level. We also investigate the size of cascades observed in collective dynamics and find the relationship between inside failure (endogenous event) and outside failure (exogenous event) and cascade size. When social pressure is strong, the evolution of the collective process is based on a fraction of failure nodes and is not predetermined by each node's characteristics. In this case large-scale cascades occur easily. However, when social pressure is relatively weak, the failure level is determined statistically.

An externality occurs when a failure of one node affects other nodes. As stated above, we assume that there are two factors governing each node's status. The first is based on internal factors at each node and the second on external influences from other nodes. Regarding the first (endogenous) factor, we assume that if each node is isolated from other nodes and does not receive any external influence from them, it may fail with some probability p, which may take a random value between 0 and 1.

There are two node types, A and B. The first type, an α-node, may fail with some probability p_A, which may take a random value between 0 and 0.5 if it is isolated from other nodes and does not receive any external influence. The second type, a β-node, may fail with a higher probability p_B, which may take a random value between 0.5 and 1. The proportion of α-nodes is denoted by μ, which may range from 0 to 1.

Regarding the second endogenous factor, we assume that external influence linearly increases in proportion to the number of the failed nodes. Here A_t denotes the number of failed nodes by period t and B_t denotes the number of nodes that continue to function normally. The external pressure on a normal node to fail at period $t+1$ is simply the proportion of failed nodes, given as $F_t = A_t/(A_t + B_t)$.

We assume that the combined failure probability of a node in period $t+1$ is simply a weighted average and its failure probability is:

$$p[\text{node in period } t+1 \text{ fails}] = q_{t+1} = (1-\alpha)p + \alpha F_t \tag{17}$$

where α ($0 < \alpha < 1$) is the relative impact of external pressure on node failure.

We next investigate the properties of a cascade failure when a large number of nodes (N = 1,000) are located in a line and each node determines the node status sequentially using the rule in Eq. (17). We consider how a failure at some node diffuses to other nodes in sequence. In every period one node

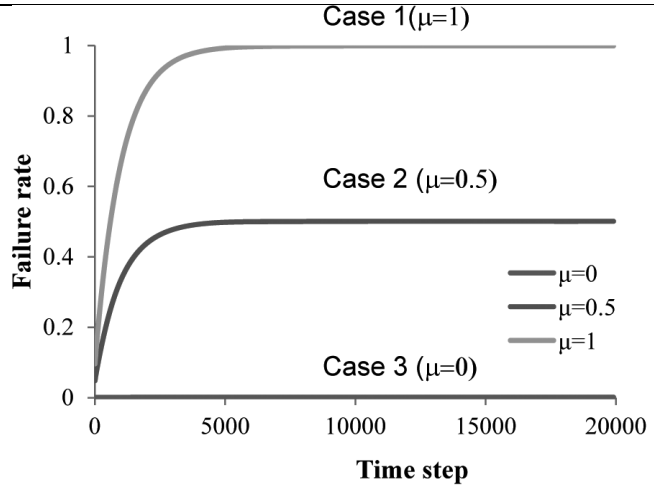

Fig. 4. Simulations of sequential cascade processes after 8,000 rounds. We consider three cases: (Case 1) $\mu = 1$ where all nodes are type α with failure probabilities between 0.5 and 1; (Case 2) $\mu = 0.5$ where half the nodes are type α and the other half are type β, with failure probabilities between 0 and 0.5; and (Case 3) $\mu = 0$ where all nodes are β-type. As can be seen, the failure ratio in Case 3 is simply determined by statistical summation of all nodes. (Colours are visible in the online version of the article; http://dx.doi.org/10.3233/IKS-2012-0189)

examines its status, and in this sense the formulation resembles most contagion models. In a more general situation, at each time period one node is chosen from the network as a target node, and this target node, which has not failed, may fail with the combined probability of failure expressed by Eq. (17), which reflects internal factors and external influences. If the target node has already failed, we select another target node from the network. The diffusion continues until every node in the network has failed.

First, let us examine how a failure of one node propagates over the network by considering the two extremes: $\alpha = 0$ and $\alpha = 1$.

(1) $\alpha = 0$ (independent nodes without external influence)

In this case, the sequential decision process becomes simply an accumulation of independent decisions. The simulation results with 1,000 nodes are shown in Fig. 2. For every value of λ, all nodes eventually fail.

When failure conditions for each node (or subsystem) depend on other nodes, the risk diffusion process is not predetermined by how node tolerances are distributed. Even when the internal tendency toward failure is strong, no particular path that the risk propagation process will follow is predetermined by the initial conditions, and every outcome is just as likely as every other.

(2) $\alpha = 1$ (mutually dependent nodes with full external influence)

In this case, the sequential diffusion process resembles the well-known Polya's urn process. That is, the expected proportion of failed nodes exactly equals the current proportion of failed nodes under full external influence ($p = 1$). Some samples of possible cascade failure paths are shown in Fig. 2. It is easy to show that the martingale property generally holds; that is, the cascade process under pure external influence is strongly path dependent and will most likely stay wherever it is.

If we compare the two factors of the diffusion process, the pure social process is less predictable when measured by the penetration rate F_t. In one situation, the diffusion speed is relatively high, but in the other case it is extremely slow. Thus, every feasible outcome is equally likely at every time; the process

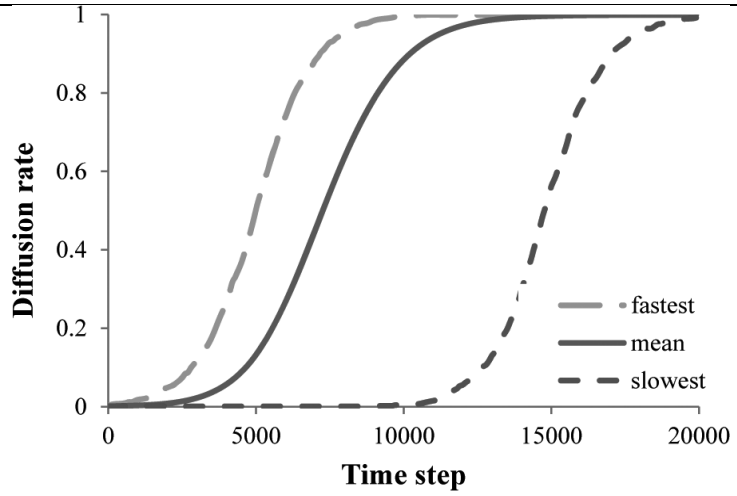

Fig. 5. Simulation results of the cascade process for 20,000 rounds for the fastest, slowest and average diffusion rates. As can be seen, the diffusion process becomes slow and unpredictable under pure external influence ($\alpha = 1$). (Colours are visible in the online version of the article; http://dx.doi.org/10.3233/IKS-2012-0189)

is completely blind when pure social pressure is in action, and the diffusion process becomes completely unpredictable. If diffusion is purely a matter of an external influence, every feasible outcome is equally likely; intuitively, this is a very random process.

(3) $0 < \alpha < 1$ (each node may fail, and nodes experience partial external influence)

Here, the sequential diffusion process becomes a mix between the two extreme cases of $\alpha = 0$ and $\alpha = 1$. If we calculate the expected number of adopters at a given time, the aggregate model displays a cumulative S curve of adopters.

When the innovation is a good whose consumption is individual, single consumers can decide whether to adopt it. We can derive an individual decision rule from the Bass model: the number of individuals who adopt at a given time is a function of the number of individuals who have already adopted. The probability that an individual adopts increases as a function of the number of its neighbors who have already adopted. Naturally, if a person has more friends already using a certain service or product, he or she will have a higher probability of adopting it.

A large number of interactions is not sufficient to guarantee emergent patterns in a system. In some cases, a critical mass must be reached before emergent patterns can be generated; that is, a system must reach a combined threshold of diversity, organization, and connectivity before emergent properties appear. Topological network properties should be derived from the dynamics by which the networks are created.

As examples, we consider three network topologies: (a) regular networks where all agents are connected to 10 neighbors, (b) complete networks where all agents are connected to all other agents, and (c) scale-free networks, where some agents connect to many agents but the rest are connected to only a few agents. The dynamics of the diffusion process according to the penetration rates is shown in Fig. 5. Comparing these results, the fastest diffusion occurs when agents are locally connected. In contrast, when agents are fully connected, the diffusion process is the slowest and the process is unstable: in some cases it is relatively fast, but in others it is extremely slow. In the scale-free network, the diffusion pattern is the mean.

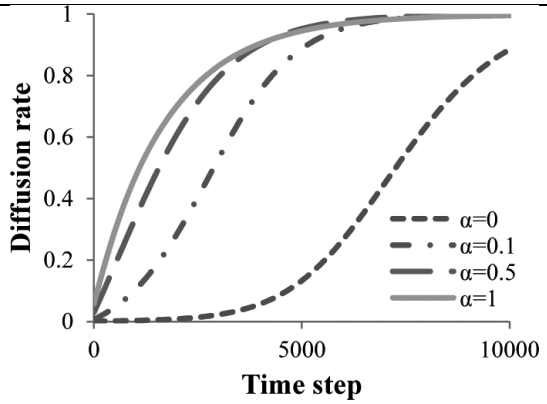

Fig. 6. Simulations of the cascading process after 15,000 rounds. With $\alpha = 0.1$ and $\alpha = 0.5$ we set $\mu = 1$. The diffusion process is faster when α is large, with each node experiencing greater external influence. (Colours are visible in the online version of the article; http://dx.doi.org/10.3233/IKS-2012-0189)

7. Network design to reduce systemic risks

Networks increase interdependencies and this creates challenges for managing risks. This is especially apparent in areas such as financial institutions and enterprise risk management, where the actions of a single actor in an interconnected network can impact all the other actors in the network, making the network is only as strong as its weakest link.

Allen and Gale studied how the financial system responds to contagion when financial institutions are connected under different network topologies (Allen & Gale, 2000). They also explored several critical issues of the study of systemic risks by studying two questions: how resilient financial networks are to contagion, and how financial institutions form connections when exposed to the risk of contagion.

While more links between banks might be expected to increase the risk of contagion, Allen and Gale showed that densely connected banking systems may be less susceptible to contagion than those with a sparse network structure with few connections. They also showed that incomplete networks are more prone to contagion than complete structures. For instance, better-connected networks are more resilient, since the proportion of losses in one bank's portfolio is transferred to more banks through interbank agreements. On the other hand, in the case of an incomplete network, the failure of one bank may trigger the failure of the entire network.

A major line of network research focuses on the dynamics of networks. Here, each node of a network represents a dynamical subsystem. Individual subsystems are coupled according to the network topology. Thus, the topology of the network may remain static while the states of the nodes change dynamically. Important processes studied within this framework include synchronization of the individual dynamical systems and contact processes such as epidemic spreading. Studies like these have clarified that certain topological properties have strong impacts on the dynamics of networks.

Many real-world processes are diffusive in nature, giving rise to optimization problems where the goal is to maximize or minimize the spread of some entity through a network. For example, in epidemiology, the spread of infectious diseases should be minimized. One individual's adoption of a certain marketed product may trigger his or her friends or fans to adopt that product as well. In this case diffusion should be maximized in the social network.

In this context, there are entire classes of problems, ranging from epidemic spreading to the control of cascade failures, which are naturally defined as optimization problems. Others, such as the unexpected

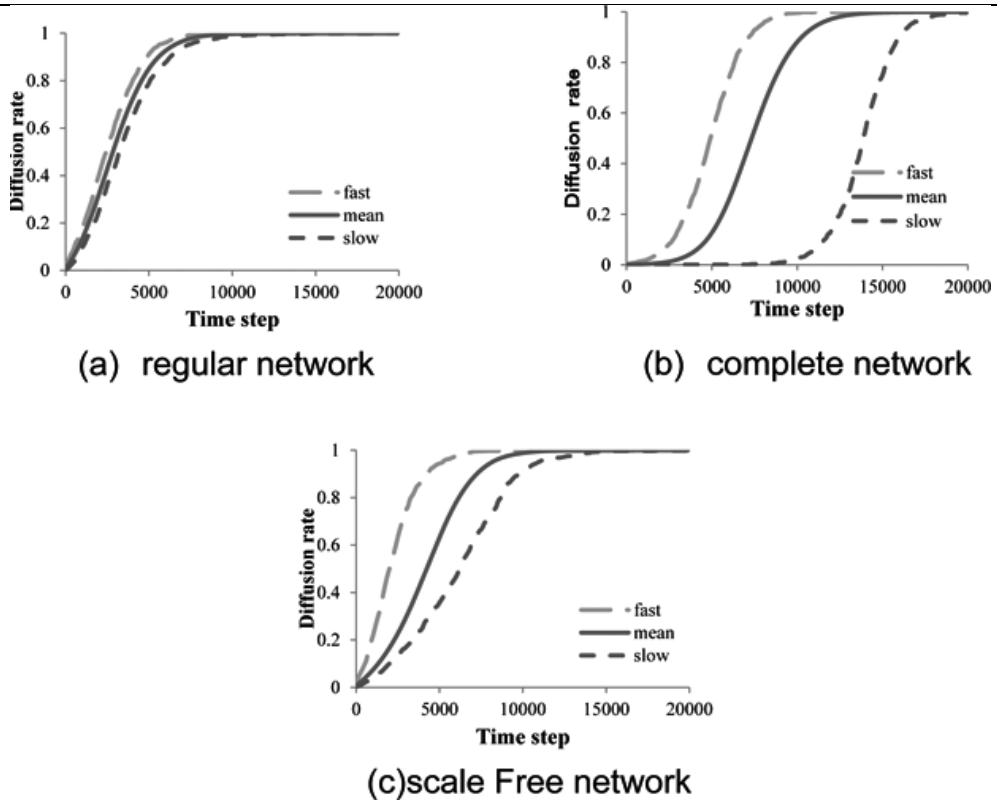

Fig. 7. Simulations of the collective decision process after 1000 rounds under three different agent network topologies: (a) regular network, (b) complete network, and (c) scale-free network. We set $\alpha = 1$ and $\mu = 1$ in Eq. (17) for all three topologies. As can be seen, the diffusion process is slow and unpredictable if all agents are connected to each other (complete network). (Colours are visible in the online version of the article; http://dx.doi.org/10.3233/IKS-2012-0189)

robustness observed in some systems, involve no a priori optimization conditions and yet reveal enhanced properties shaped by the evolution of the system. Optimal behavior is most often connected to a function that the system performs.

Traditionally, optimization has a particular mathematical definition that focuses on obtaining solutions that strictly optimize a well-defined function. Here we adopt a looser definition of the word by extending it to include a tendency of the system to improve its behavior as a result of a natural or artificially imposed selection pressure. Many real-world problems are complex. Accordingly, most quests to find the optimum solution are not realistic. Finding a "good enough" solution or a "better" solution in an iterative manner is a workable alternative.

Optimizing a network requires the selection of a proper object function. There is a tradeoff between risk contagion and risk sharing. More interconnections means higher levels of insurance, but also higher risk of contagion, and large shocks can wipe out large parts of the whole system.

Management strategies can be risk-reducing as well as risk-sharing measures. To illustrate, we consider optimization under link constraints. The average degree of a network with the adjacency matrix $A = (a_{ij})$ is defined as

$$\langle k \rangle = \frac{2}{n} \sum_{k=1}^{n} a_{ij} \tag{18}$$

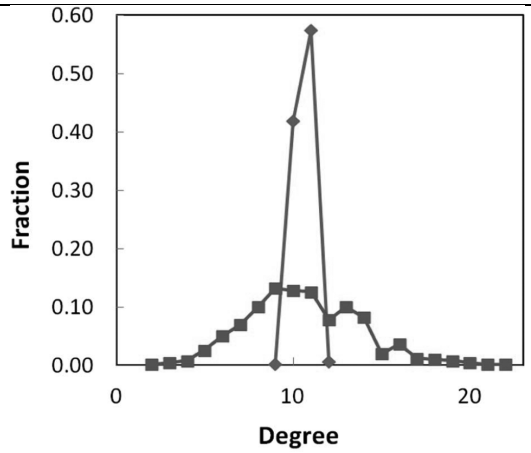

Fig. 8. The degree distribution of the evolutionary optimized network for $\omega = 0.3$: is shown in blue, while a random network with the same number of links is shown in red. (Colours are visible in the online version of the article; http://dx.doi.org/10.3233/IKS-2012-0189)

The object function to be minimized is defined as

$$E(\omega) = \omega(\lambda_1(A)/(N-1)) + (1-\omega)1/\langle k \rangle \tag{19}$$

where ω ($0 \leqslant \omega \leqslant 1$) is a parameter controlling the two objects.

Initially, we prepare 10 undirected graphs, each with a fixed number of nodes and links defined by the binary adjacency matrix $A = (a_{ij})$, $1 \leqslant i, j \leqslant n$.

We use a generic algorithm (GA) by applying mutation and crossover to the binary coded adjacency matrices. The most suitable matrices from among the parent and child matrices are chosen, and the others are eliminated. After long generations have passed, we can obtain an optimal network that minimizes the object function defined in Eq. (19).

Designing desirable networks is complex and may pose multi-constraint and multi-criterion optimization problems. Above, we presented a genetic optimization approach to designing an optimal network, for minimizing risk contagion and for risk sharing. When we increase the weight parameter ω by putting emphasis on minimizing the spread (i.e., minimizing largest eigenvalue $\lambda_1(A)$), we obtain a dense network of a high degree.

The degree distribution of an evolutionary optimized network and that of a random network with same average degree are shown in Fig. 8. The optimized network is characterized as a homogeneous network where each node has almost the same.

The optimized network is homogeneous having almost the same degree and node-to-node distance and this kind of network is known as Ramanujan graph or random regular network in which all nodes have the same degree.

As comparison we consider three network topologies: an evolutionary optimized network with the object function in Eq. (19), a random network and a scale-free network with the same average degree. We describe the trajectories of X(t) defined in Eq. (14) of these networks in Fig. 9 (horizontal-axis). The network system is free of systemic risk, but as the value of X(t) approaches one, the system is prone to systemic risk.

Initially a small portion of nodes fail (the initial condition), and we apply the update rule in Eq. (16) to nodes in the network. By repeatedly applying the threshold rule, a node switches to failure state if the proportion of its neighbors who have failed is larger than the threshold θ_i.

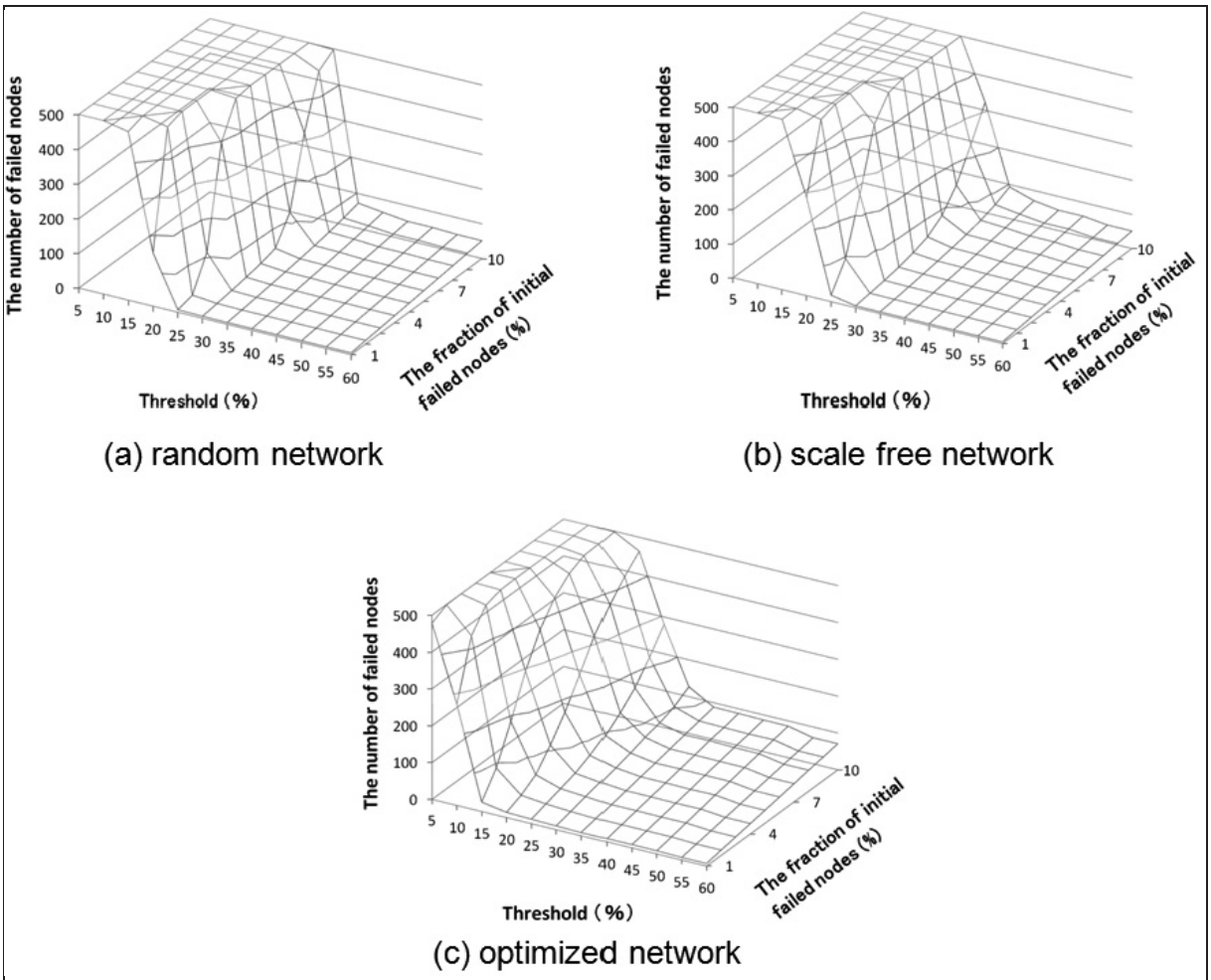

Fig. 9. Trajectories of X(t) (the horizon-axis): If the trajectories of X(t) stay close to zero, then the system is free of systemic risk, but as the value of X(t) approaches one, the system is prone to systemic risk. The phase transitions in systemic risk, i.e., situations where small changes in initial conditions result in global failure are observed in three different topologies, however, the trajectories of X(t) stay close to zero in a wide area of thresholds (x-axis) and initial failure ratios (y-axis). (Colours are visible in the online version of the article; http://dx.doi.org/10.3233/IKS-2012-0189)

From Fig. 9, we can observe the phase transitions in systemic risk in three network topologies, i.e., situations where small changes in initial conditions result in global failure, however, the trajectories of X(t) stay close to zero in a wide area of thresholds (x-axis) and initial failure ratios (y-axis) implying that an evolutionary optimized network is the most risk prone compared with a random network and a scale-free network.

Optimization of performance and robustness are common property of socio-economic systems. Evidence of this has generated increasing interest in dynamical processes in complex networks and how the interplay between processes and network structure influences the performance and robustness of the networked system. The structure of the interconnections is one factor that certainly influences system performance.

In this context, there are entire classes of problems, ranging from the spread of disease epidemics to the control of cascade failures that fall naturally under the definition of optimization problems. As noted

earlier, optimization has a strict mathematical definition that concerns obtaining solutions to well-defined problems. Here again, we loosen this definition by extending it to include the tendency of a system to improve its behavior as a result of natural or artificially imposed selection pressure. Thus, under the expanded definition, evolutionary computation provides a unified approach for optimizing networked systems.

8. Managing risks and wisdom of collectives

Synchronization is the most prominent example of coherent behavior, and is a key phenomenon in systems of coupled oscillators, which is how we characterize most biological networks or physiological functions [3]. Many studies have been done to investigate how synchronous behavior is affected by network structure. The range of stability of a synchronized state is a measure of the system's ability to yield a coherent response and to distribute information efficiently among its elements, while a loss of stability fosters pattern formation (Wang & Che, 2001).

This prompts the following question: what topology maximizes network synchronization? Initial efforts were put into understanding the topological properties of a network, and interest gradually shifted toward the analysis of the interplay between topology and the dynamics of network components. In general, each element node in a network undergoes a dynamical process while coupled to other nodes. The system's collective behavior depends strongly on the efficiency of communication paths, which is in turn dictated by the underlying network topology. In this way, the network structure determines, to a large extent, the network's ability to respond coherently.

The consensus problem is another topic related to the problem of synchronization. Consensus problems have a long history in computer science and control theory. In networks of agents, consensus means reaching an agreement regarding a certain item of interest. It thus depends on the state of all the agents. A consensus algorithm is an interaction rule that specifies the information exchange between an agent and all of its neighbors on the network. The theoretical framework for solving consensus problems for networked systems was introduced by Olfati-Saber et al. (2007).

In recent studies, the reason synchronized networks occur has become clear, and we have learned that the underlying network topology is important. The consensus problem is formulated as follows. All actors are required to obtain the average value when each has a different initial value. They are only allowed to communicate with the neighbors to whom they are connected, and each actor updates its initial value by observing the values of its neighbors. To date, little is known about what network topology is the best for synchronization. Recently it has been shown that improved consensus or synchronization occurs on a Ramanujan graph (Donetti et al., 2007).

In this setting, we now share some thoughts about managing interdependent risk. The first framework is the wisdom of crowds (collective) (Surowiecki, 2007). The basic idea of Surowiecki is simple and somewhat counterintuitive: if we get a diverse group of people together to solve a problem, the group's answer will typically be better than that of any individual, even an expert. The key is that the crowd is only wise under certain conditions. We need agent diversity, an aggregation mechanism, and some sort of incentives. When one or more of these conditions is violated, all bets are off.

A collective system is a large system of systems (or agents), where each system has its performance measure to optimize, along with global performance measures of the full system. The envisioned object is to study the mechanism of inducing desirable collective outcomes to optimize a global performance measure. This aim is quite novel, since a collective system need to establish coordinated and synchronized behavior from the bottom-up (Namatame, 2006).

We can relate the risk-reduction and risk-sharing problem and the wisdom of collective in a more common way to design proper relationships as a network. In human systems, diversity is the most likely condition to be violated. When we take away diversity, the complex system can become fragile. In some cases, this leads to large-scale changes. Along with diversity, we need a proper mechanism for aggregating diverse opinions and ideas. In this framework, the design of the network of humans (or nodes) is essential.

We also have shown that for synchronization and consensus problems, the optimal network design for risk-reduction as well as for risk sharing displays a dual optimal network design. As a result, we now have a better understanding of the emergent properties of desirable aggregate processes. We have shown that optimal networks for risk-reduction as well as for risk-sharing display common features with a wide class of optimal networks for better synchronization and consensus formation. Each node should be connected with almost the same number of other nodes.

Summing up, optimization of risk-reduction and risk sharing is a common property of naturally evolved systems and is desirable in most man-made systems. The interplay between dynamic diffusion processes and network structure influences the performance and robustness of the system. Notably, we have evidence from fields such as epidemic spreading, communications, synchronization dynamics, cascade failures and risk management, and these issues are at the leading edge of current research on network optimization.

In the case of progressive diffusion, scale-free networks with hub nodes foster diffusion as demonstrated by the epidemic and rumor models. On the other hand, in the case of risk-reduction and risk sharing, a random, balanced network where each node is well and equally connected without hub nodes fosters consensus and synchronization. This feature relates to the emergence of coherent behaviors like the wisdom of crowds.

9. Conclusion and further research

In this chapter we used networks to address risks. Research in these areas can improve our understanding of the nature of systemic risks and the effectiveness of strategies to reduce them. These risks arise in the context of networks, so we need to understand network relationships and interactions to understand the true nature of the risks.

Many diffusion processes are progressive in the sense that once a node switches from one state A to another state B, it remains in state B in all subsequent time steps. We showed that scale-free networks with hub nodes foster diffusion. The other type of diffusion is a non-progressive process in which, as time progresses, nodes can switch back and forth from state A to B or from B to A, depending on the states of their neighbors.

In the case of a non-progressive process such as innovation, diffusion processes largely determine individual decisions. In this case, exponential networks with many midsize hub nodes foster diffusion, as demonstrated by the epidemic and rumor models. We also gave a brief overview of the consensus and synchronization processes that relate to the emergence of coherent patterns to emphasize the importance of underlying network topology. We saw that a network with a balanced underling network topology is necessary for the emergence of coordination.

The challenges systemic risks pose are based in network interactions. It is therefore not surprising that efficient solutions to interdependency problems require understanding and harnessing the power of the network itself. We conclude that topological properties of networks should be derived from the dynamics from which the networks were created. A large number of interactions is not enough to

guarantee emergence of a desirable property (risk prone). In some cases, the diffusion process may need to reach a certain critical mass, a combined threshold of diversity and connectivity, before desirable properties emerge.

With respect to protection and risk-reducing measures, there is evidence that we need to assess the risks of individuals and how their actions affect one another. Since these risks arise within interdependent networks, effective solutions usually demand looking beyond an individual firm or division. The fact that the risk is often determined in part by the behavior of others gives a complex structure to the incentives that individuals or firms face in reducing risk or investing in risk-mitigation measures.

The solution for an interdependent security problem may involve coordinating efforts to decrease collective risk. These coordinating efforts and collective incentives can push the network to a tipping point or cascade that then reinforces behavior that benefits the entire system. With the right incentives, the system itself can encourage actions by individuals that reduce collective risk.

A more realistic model of systemic risk that incorporates these behavioral factors as well as people's misperceptions of the risk may suggest a different set of policy recommendations. Psychologists contend that when faced with choices, people often use a reasonable heuristic method, such as following a social trend.

We presented a model of diffusion that combines the heuristic methods with agents' efforts to make rationally grounded decisions. We then established stochastic dynamic processes that exhibit clear properties of individual decisions combined with the cascade dynamics, leading to deterministic outcomes that appear to be very fragile.

We can also share some thoughts about managing interdependent risk with the framework of the wisdom of crowds (Surowiecki, 2007). The key is that the crowd is only wise under certain conditions, which include diversity and an aggregating mechanism. When any of the necessary conditions is violated, the network becomes unpredictable. In human systems, diversity is the most likely condition to be violated. When diversity is lost, a complex system can become fragile and may tend to experience large-scale changes. Booms and crashes are good examples of diversity breakdowns in markets. Fads and fashions also illustrate this concept.

There are two features of these frameworks that are worth emphasizing in relation to risk management. The first is that nonlinear thinking is necessary. For example, in the case of the wisdom of crowds, we can reduce diversity, then reduce it more, and nothing happens; however, if you reduce it a bit more, the system reacts violently – the proverbial straw that broke the camel's back. This is the idea of the tipping point, which leads to another nonlinear feature: lack of proportionality. The size of the perturbation and the outcome are not always linked. Sometimes small perturbations lead to large outcomes, and vice versa. When you combine a lack of linearity with a lack of proportionality, it is not hard to see that predictions are difficult and cause and effect thinking is often futile.

The second feature is that we need a mechanism to handle aggregation of diversity, some sort of individual incentive to encourage actors to reach agreement or consensus. We have shown that the optimal network design for risk-reduction and risk-sharing displays common features with a wide class of optimal network problems for improving synchronization and consensus formation.

References

Allen, F., Gale, D. (2000). Financial Contagion, Journal of Political Economy, 108 (1), 1-33.

Ball, P. (2004). Critical Mass, Farrar, Straus and Giroux.

Banerjee, A. (1992). A Simple Model of Herd Behavior, Quarterly Journal of Economics, 110, 797-817.

Bendor J., Huberman, B., Wu. F. (2006). Management Fads, Pedagogies, and other Soft Technologies, http://www.hpl.hp.com/research/idl/2006.

Chakravorti, B. (2003). The Slow Pace of Fast Change: Bringing Innovations to Market in a Connected World. Boston, Harvard Business School Press.

Chakrabarti, D., Wang, Y, Wang, Y., Leskovec, J., Faloutsos, C. (2008). Epidemic Thresholds in Real Networks. ACM Transactions Information and System Security, Vol. 10, No. 4, 131-152.

Colizza, B., Barrat, A., Barthelemy, M., Vespignamic, D. (2006). The role of the airline transportation network in the prediction and predictability of global epidemics, PNAS, 103, 2015-2020.

Danielsson, J., Shin, H. (2003). Endogenous Risk, in Modern risk management: a history, Risk Books.

Donetti, L., Neri, F., Munoz, M. (2006). Optimal network topologies: expanders, cages, Ramanujan graphs, entangled networks and all that. J. Stat. Mech. vol. 26, pp. 134-144.

Geoffrey M. Heal, Howard Kunreuther. (2003). You only die once: managing discrete interdependent risks, NBER Working Paper 9885, Cambridge, MA.

Helbing, D. (2010). Systemic Risks in Society and Economics, RGC – Emerging Risks.

Jackson, M., Yariv, L. (2008). Diffusion, Strategic Interaction and Social Structure, TR-Stanford University.

Johansen, A., Sornette, D. (2006). Shocks, Crashes and Bubbles in Financial Markets, Brussels Economic Review, 49 (3/4).

Komatsu, T., Namatame, A. (2010). Dynamic diffusion process in evolutionary optimized networks, Proceeding of The 14th Asia Pacific Symposium on Intelligent and Evolutionary Systems, pp. 263-274.

Kunreuther, H., Heal, G. (2003). Interdependent Security, Journal of Risk and Uncertainty 26: 231-49.

Kunreuther, H. (2009). The Weakest Link: The Network Challenge in Strategy, Profit and Risk in an Interlinked World, Kleindorfer, P and Yoram W (eds). Wharton School Publishing.

Lopetz-Pintado, D. (2006). Contagion and coordination in random networks. Int. Journal of Game Theory, 34, 371–382.

Lorenza, J., Battiston, S. (2009). Schweitzer. F., Systemic risk in a unifying framework for cascading processes on networks, Eur. Phys. J. B71, 441–460.

Meyers, L., Pourbohloul, D., Newman, M.E.J. (2005). Network Theory and SARS: prediciting outbreak diversity. Journal of Theoretical Biology 232, 71–81.

Mauboussin, M.J. (2006). Interdisciplinary Perspective on Risk, Mauboussin on Strategy.

Motter, A., Zhou, C., Kutth, J. (2005). Network synchronization, Diffusion, and the Paradox of Heterogeneity, Physical Review E, 71, 016116-1-9.

Namatame, A. (2006). Adaptation and Evolution in Collective Systems, World Scientific Olfati-Saber, R., Fax, J.A., Murray, R.M. (2007). Consensus and cooperation in networked multi-agent systems, Proceedings of the IEEE, vol. 95, no.1, pp. 215-233.

Pikovsky, A., Rosenblum, M., Kurths, J. (2003). Synchronization, A Universal Concept in Nonlinear Sciences, Cambridge University Press.

Sornette, D. (2006). Critical Phenomena in Natural Sciences: Chaos, Fractals, Self-organization and Disorder. Springer, Berlin.

Surowiecki, J. (2004). The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, and Nations, New York: Random House.

Rogers, E.M., Medina, U.E., Rivera, M.A., Wiley, C.J. (2005). Complex Adaptive Systems and the Diffusion of Innovations, The Innovation Journal, 10(3), 1-26.

Wang, X.F., Chen G. (2001). Synchronization in scale-free dynamical networks: Robustness and fragility.

Wang, Y., Chakrabarti, D. (2003). Epidemic Spreading in real Networks: An Eigenvalue Viewpoint. Proceedings of the 22nd Symposium on Reliable Distributed Computing, pp. 242-262.

Watts, D. (2007). Influentials, Networks, and Public Opinion Formation. Journal of Consumer Research, 34(4), 441-458.

Authors' Bios

Dr. Akira Namatame is a Professor of Computer Science Department and Academic Dean at National Defense Academy of Japan. He is well-known as an international research leader in the field of multi-agent modeling and complex systems, and in the past ten years he has given over 30 invited talks in these areas. His research interests include multi-agent systems, complex networks, evolutionary computation, and game theory. He is the editor-in-chief of Springer's Journal of Economic Interaction and Coordination. He has published more than 230 refereed scientific papers, together with eight books on multi-agent systems, collective systems and game theory.

Mr. Takanori Komatsu (Captain of Japan Air-self Defense Force) holds the bachelor's degree of Science in Electrical and Electronic Engineering at Tokyo University of Agriculture and Technology in Japan and master's degree of Science in Computer Science and Engineering at National Defense Academy of Japan. Currently he is doing his PhD in Computer Science at National Defense Academy of Japan. His research interests include network design, network security and Multi-agents.