Understanding Complex Systems: A Communication Networks Perspective

Article · March 2007

2 authors:

Pavlos Antoniou
University of Cyprus
18 PUBLICATIONS **223** CITATIONS

SEE PROFILE

Andreas Pitsillides
University of Cyprus
333 PUBLICATIONS **3,669** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Social Internet of Things View project

Urban Web of Things View project

Understanding Complex Systems: A Communication Networks Perspective

Pavlos Antoniou and Andreas Pitsillides

Networks Research Laboratory, Computer Science Department, University of Cyprus

75 Kallipoleos Street, P.O. Box 20537, 1678 Nicosia, Cyprus

Telephone: +357-22-892687, Fax: +357-22-892701

Email: paul.antoniou@cs.ucy.ac.cy, andreas.pitsillides@ucy.ac.cy

Abstract

Recent approaches on the study of networks have exploded over almost all the sciences across the academic spectrum. Over the last few years, the analysis and modeling of networks as well as networked dynamical systems have attracted considerable interdisciplinary interest. These efforts were driven by the fact that systems as diverse as genetic networks or the Internet can be best described as complex networks. On the contrary, although the unprecedented evolution of technology, basic issues and fundamental principles related to the structural and evolutionary properties of networks still remain unaddressed and need to be unraveled since they affect the function of a network. Therefore, the characterization of the wiring diagram and the understanding on how an enormous network of interacting dynamical elements is able to behave collectively, given their individual non linear dynamics are of prime importance.

In this study we explore simple models of complex networks from real communication networks perspective, focusing on their structural and evolutionary properties. The limitations and vulnerabilities of real communication networks drive the necessity to develop new theoretical frameworks to help explain the complex and unpredictable behaviors of those networks based on the aforementioned principles, and design alternative network methods and techniques which may be provably effective, robust and resilient to accidental failures and coordinated attacks.

Index Terms

Complex systems, random networks, small-world networks, scale-free networks, communication networks.

I. Introduction

It is becoming apparent that our environment may be viewed as networked world. From the Internet to the global ecosystem, from the road traffic network to the stock markets, from biological to social systems, massively interconnected, interacting, components make up our vital systems in this world. These systems can be classified as Complex systems.

Complex systems is a new field of science studying how elements of a system give rise to the collective behaviors of the system, and how the system interacts with its environment. Qualitatively, to understand the behavior of a complex system one must understand not only the behavior of the constituent elements but how they act together to form the behavior of the whole.

Complex systems and their desired behavior usually involve references to emergence, adaptability, self-organization, resilience, robustness, decentralization, flexibility, and speed. However, recently there has been more focus in the literature on the structural characteristics of complex systems. Increasingly, these systems are described as 'networks' characterized as decentralized, non-hierarchical, flat, amorphous, dispersed, and distributed.

Complex systems, as networks of interacting entities, are studied empirically through the rapidly increasing mass of data which has become available in many different domains. At the same time, these different domains also appear to share many new and fundamental theoretical questions. These circumstances should encourage the interdisciplinary development of a new science of complex systems. Social systems formed (in part) out of people connected by social relationships, the brain formed out of neurons connected by synapses, molecules formed out of atoms connected by bonds, the Internet formed out of routers and computers linked by various wired or wireless links, the World Wide Web formed out of hypertext documents (web pages) connected by hyperlinks are all examples of complex systems. The field of complex systems cuts across many diverse disciplines including mathematics, engineering, computer science, chemistry, physics, philosophy, psychology, sociology, economics, management, medicine, molecular biology and anthropology. This new field focuses on certain questions about elements, wholes and relationships. These questions are relevant to all traditional fields.

The study of complex systems is about understanding indirect effects. Problems that are difficult to solve are often hard to understand because the causes and effects are not obviously related. Towards this direction, complexity theory studies how patterns emerge through the interaction of many elements. In this space, emergent patterns can be perceived but not predicted. Patterns may indeed repeat for a time, but we cannot be sure that they will continue to repeat, because the underlying sources of the patterns are not open to inspection (and observation of the system may itself disrupt the patterns) [1].

According to [2], there are three interrelated approaches to the modern study of complex systems which are: (a) find statistical properties, such as path length and degree distribution that characterize the structure and dynamic behavior of networked systems, (b) build models of networks that explain and help understand how they are created and how they evolve, and (c) predict the behavior of networked systems based on the measured statistical properties of the structure and the local properties of given vertices (study pattern formation and evolution), e.g., what will happen to the equilibrium of an ecological network if a certain species disappears. The modeling of patterns formed in a complex environment is further discussed in Section V.

Nowadays, systems become increasingly larger acquiring even more components while the information flow in the system increases at a fast pace. Mastering their complexity (the high level of interdependence between their often very heterogeneous components), becomes a major hurdle threatening to slow down the information revolution. Designing, controlling, modeling and monitoring behavior of such systems are the fundamental challenges that should be addressed. We need new paradigms as we are rapidly moving from systems based on closed hierarchical or semi-hierarchical structures to open and distributed, networked organizations. Recent studies of complex systems as they occur in nature, society or even engineering (whether these are living organisms, animal societies, ecosystems, markets, cultural groupings, or the Internet) suggest that we can learn lessons from these systems on how to design and control a new generation of complex IT systems.

From real communication networks perspective, the key challenge is to learn how to design such networks that can self-organize, self-adapt and optimize their interactions and functions in a continuous and robust manner to satisfy user demand. Complex Systems field can provide models, theories, mechanisms and approaches that allow for a principled design method to be developed to address this key challenge. In addition, complex systems science provide a number of sophisticated tools, some of them concepts that help us think about these systems, some of them analytical for studying these systems in greater depth, and some of them computer based for describing, modeling or simulating these systems.

This rest of this technical report is organized as follows: Section II deals with some basic concepts of complex systems. Section III focuses on complex adaptive systems and their properties. Section IV refers to network modeling paradigms. Section V investigates real communication networks from complex system's perspective. Section VI concentrates on real network paradigms. Section VII concludes the technical report.

II. Basic Concepts of Complex Systems

It is beyond any doubt that Physics, a traditional science discipline, has developed many successful tools for predicting the behavior of a system as a whole from the properties of its constituents. The success of this modeling is based on the simplicity of the interactions between the elements according to which there is no ambiguity as to what interacts with what, and the interaction strength is uniquely determined by the 'physical distance'.

On the other hand, for many complex systems with nontrivial network topology such ambiguity is naturally present. In the past few years many researchers studied the structure and function of complex networks [2] and they have increasingly recognized that the tools of statistical mechanics offered a framework for describing these interwoven systems [3].

Nowadays, there is an increasing need to move beyond physics-based approaches and try to understand the behavior of the system as a whole. Towards this direction, understanding the topology of the interactions between the components is unavoidable. In accordance with [3], there are three basic concepts that occupy a prominent place in contemporary thinking about complex systems, which are defined below:

- **Small world:** The small-world concept in simple terms describes the fact that despite their often large size, in most networks there is a relatively short path between any two nodes. The distance between the two nodes is defined as the number of edges along the shortest path connecting them. The concept gave rise to the famous phrase 'six degrees of separation' after a 1967 small world experiment by social psychologist Stanley Milgram which suggested that two random US citizens were connected on average by a chain of six acquaintances. 'Six degrees of separation' arises from the existence of cliques and a few popular individuals who provide connections between these cliques.
- **Clustering:** A common property of social networks is that clique's form, representing circles of friends or acquaintances in which every member knows every other member. The inherent tendency to cluster is quantified by the clustering coefficient (Watts and Strongatz, 1998 in [12]), a concept that has its roots in sociology. The clustering coefficient of node i is the ratio of actual number of edges connecting the nodes with their immediate k neighbors to the number of edges in a fully connected network of those k nodes, denoted by C_i:

$$C_i = \frac{2E_i}{k_i(k_i - 1)}, \tag{1}$$

  where E_i is the number of edges leaving from node i towards its k_i neighbours. The clustering coefficient of the entire network is the average of all individual C_i's.
- **Degree distribution:** Not all nodes in a network have the same number of edges (same node degree). The spread in the node degrees is characterized by a distribution function $p(k)$, which gives the probability that a randomly selected node has exactly k edges. Based on the aforementioned attributes, the three robust measures that are used to analyze a network topology are: average path length, clustering coefficient and degree distribution.

III. COMPLEX ADAPTIVE SYSTEMS (CAS) PROPERTIES

Complex adaptive systems can be seen as subsets of complex systems. They are complex in the sense that they are diverse and made up of multiple interconnected elements and adaptive in that they have the capacity to learn and change over time based on experience. Organized behavior emerges from the simultaneous interactions of elements without any global plan.

Stock market, social insect and ant colonies, the biosphere and the ecosystem, the brain and the immune system, the cell and the developing embryo, manufacturing businesses and any human social group-based endeavor in a cultural and social system such as political parties or communities are all examples of complex adaptive systems. Complex adaptive systems encompass many properties and the most important of them are listed below:
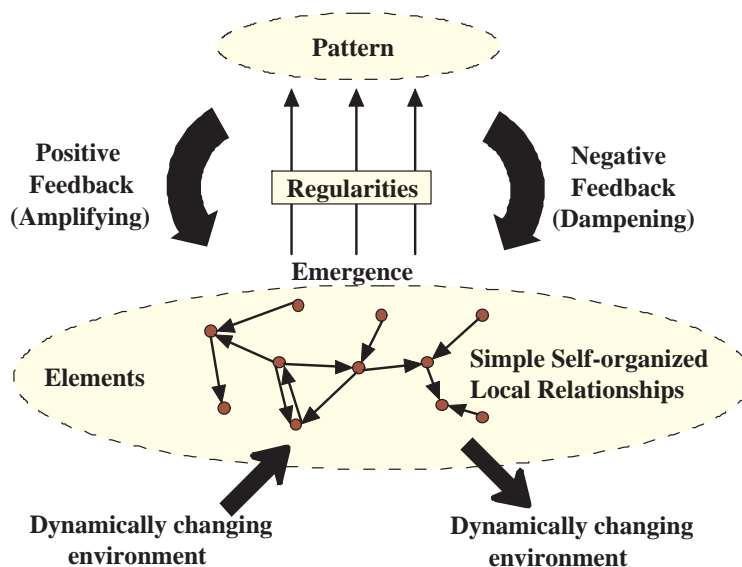

Fig. 1. Complex adaptive system (CAS).

- **Many interacting parts:** The sole components of a system are known as elements as, for example, the air and water molecules in a weather system, the flora and fauna in an ecosystem, which are arbitrarily interconnected. These elements interact with each other as well as with their environment in unpredictable and unplanned ways. But from this mass of interactions regularities emerge and start to form a pattern which feeds back on the system and informs the interactions of the elements. For example, in an ecosystem if a virus starts to deplete one species, this results in a greater or lesser food supply for others in the system which affects their behavior and their numbers. A period of flux occurs in all the populations in the system until a new balance is established. For clarity, in Fig. 1 the regularities, pattern and feedback are shown outside the system but in reality they are all intrinsic parts of the system.

- **Evolution and Cooperation:** A complex system consists of many interacting elements that may compete or cooperate in different times. This behavior is primarily based on the heterogeneity of the constituent components that have different attributes and capabilities and therefore depending on the particular cooperative links can potentially perform multiple and diverse tasks. Under these circumstances evolution results from the process of creating linkages between elements so that the result will be successful in the environment. Therefore, the essential ability of an evolutionary network appears to be its capability to create cooperative links that lead to an overall successful result in the environment. Individuals are therefore searching for a situation in which they fit into the 'inner' environment made up of the particular partners to which they are linked in the network, and also in which the overall effect of the partners working together fulfil some requirements in the external environment. Stability arises when each individual fits successfully in the alliance, and the alliance fits successfully in the wider environment. In case of external perturbations causing a change in the stable state of the environment, then the alliance as well as each individual that may participate within the alliance will need to evolve. This discussion sheds light on the aspects concerning the interactions of individuals within a system which are bound to change the environments these individuals live in. By closing the feedback loop in the evolutionary explanation, a new mathematical theory of the evolution of complex adaptive systems arises. It is this general theoretical option that lies at the core of the emerging field of complex adaptive systems. Consequently, a major promise in the study of complex adaptive systems is to elucidate the long-term effects of the interactions among the evolutionary complex processes and provide causal explanations for phenomena that are highly improbable in common sense.

- **Emergent Behavior:** Emergence is the process of deriving some new and coherent structures, patterns and properties in a complex system which were not previously observed. Emergent phenomena occur due to the pattern of interactions (non-linear and decentralized) between the elements of the system over time. More generally, it refers to how behavior at a larger scale of the system arises from the detailed structure, behavior and relationships on a finer scale. One of the main points about emergent phenomena is that they are observable at a macro-level, even though they are generated by micro-level elements. In the extreme, it is about how macroscopic behavior arises from microscopic behavior.

- **Adaptability:** In the most general sense, adaptation is a feedback process in which external changes in an environment are mirrored by compensatory internal changes in an adaptive system. In the simplest case, an adaptive system may act in a regulatory manner, like a thermostat, so as to maintain some property of the system at a constant level. An interesting type of adaptation is found in complex systems in which the interactions among the constituent elements are allowed to change. This process is very similar to a self-modifying program, since the actions of the adaptive unit can affect the environment, which, in turn, feeds information back to the adaptive system. Thus, adaptation can be seen as a computation of the most complex form that emerges through the multiplicity and recursion of simple elements or subsystems.

- **Self-Organization:** Self-organization is the evolution of a system into an organized form in the absence of external direction, manipulation or control. In other words, the constraints on the organization of the system are internal phenomena, resulting from the interactions among the components and usually independent of their physical nature. The dynamics of a self-organizing system is typically non-linear, because of circular or feedback relations between the components (Fig. 1). Two types of feedback loops exist, positive feedback loop and negative feedback loop. In a positive feedback loop the system responds in the same direction as the perturbation. The end result of a positive feedback is often amplifying and 'explosive'. That is, a small perturbation will result in big changes. This feedback, will drive the system even further away from its own original setpoint, thus amplifying the original perturbation signal, and eventually become explosive because the amplification often grows exponentially (with the first order positive feedback), or even hyperbolically (with the second order positive feedback). On the other hand, in negative feedback loop the system responds in an opposite direction to the perturbation. It is a process of feeding back to the input a part of a system's output, so as to reverse the direction of change of the output. This tends to keep the output from changing, so it is stabilizing and attempts to maintain constant conditions. This often results in equilibrium (in physical science) or homeostasis (in biology) such that the system will return to its original setpoint . While self-organization will often be in response to the system's environment, it will not be directly controlled by either the environment nor have been designed by someone outside the system. A complex adaptive system is continually self-organizing through the process of emergence and feedback. The research on self-organization tries to find general rules about the growth and evolution of systemic structures, the forms it might take, and seeks for methods that may predict the future results of self-organizing processes.

- **Decentralization:** Decentralized operation can provide a degree of scalability and robustness that cannot be achieved with centralized architectures. Decentralization achieves modularity and increases reliability by reducing explicit dependence

on a few central nodes. In particular, it can permit a network of nodes to exchange information and coordinate activities in a flexible and scalable architecture that would be impractical or impossible to achieve with a single, monolithic systems platform. Moreover, decentralized systems provide adaptability and intelligence as systems can be 'smarter' than smartest element. It is worth to mention that decentralized and distributed systems are two different approaches (Fig. 2). In distributed systems, the decision is made by a negotiation process between the executive components and executed by them. In decentralized systems each executive component makes its own decisions and executes only these decisions.

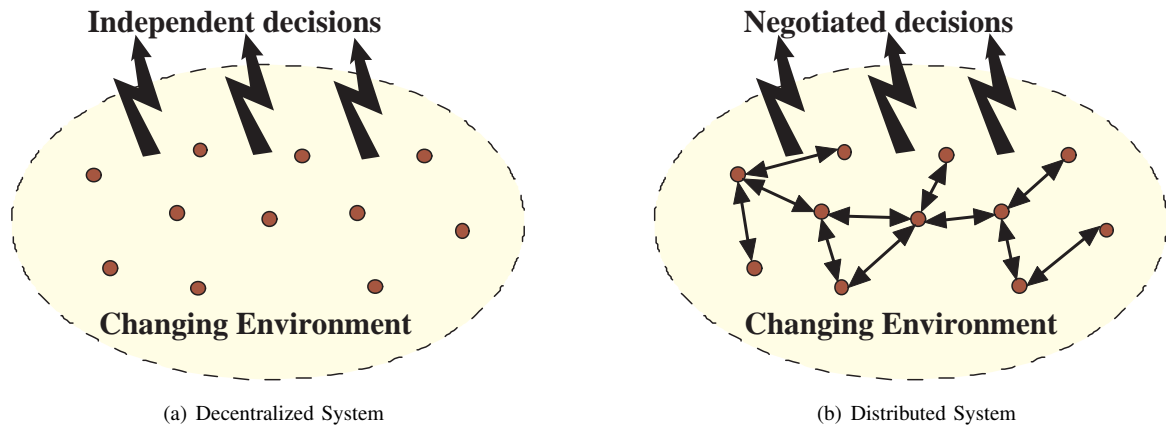(a) Decentralized System   (b) Distributed System

Fig. 2. Decentralized vs. Distributed Systems.

- **Robustness:** Robustness refers most commonly to the structural and other properties of a system that allow it to withstand or tolerate stress, perturbations or variations in its internal structure or external environment without malfunctioning but the same time without adapting, i.e. without in any way durably changing either its structure or its dynamics. In other words, it is the ability of a networked system to sustain a giant component. Recent work on network theory has started to address the question of the robustness of complex networks to failure and directed attack. They suggested that the network connectivity, and hence its functionability, is robust against random failure of nodes [4], [5], [6] and to some extent is even robust against intentional attacks [7]. Moreover, researches [8] showed that for many physical networks, the removal of nodes can have a much more devastating consequence when the intrinsic dynamics of flows of physical quantities in the network is taken into account.

- **Resilience:** As defined by [9], resilience refers to *"the capacity of a system to absorb and utilize or even benefit from perturbations and changes that attain it, and so to persist without a qualitative change in the systems structure."* Such a system may, however, take new external conditions into account by absorbing them into its mode of functioning. The difference (if any) between resilience and robustness thus seems to lie in the extent to which (non-structural) changes in the dynamics may be introduced into a system under the impact of changes in external circumstances. When networked systems break down or are subject to attack, problems can cascade throughout infrastructure, capable of disabling the network almost entirely. Under these circumstances, resilience can be seen as the ability of systems to respond in ways that rectify themselves or rapidly contain the consequences of the accident or deliberate disruption. Recently, there has been much interest in the resilience of real-world networks to failure of nodes or to intentional attacks [4], [5], [6].

- **Non-linearities:** Complex adaptive systems are governed by non-linear equations. Therefore, the output of such a system is not proportional to input. This deduction is driven by the observation that we cannot predict how a system will work by understanding the behavior of the constituent elements separately, and combining them additively. Furthermore, a salient property of most dynamical processes in complex systems is their almost unavoidable nonlinearity. Part of the recent interest in the study of dynamics on complex networks comes from the understanding that techniques and expertise developed in the study of nonlinear dynamics and chaos can be useful in the study of such nonlinear systems.

To sum up, complex adaptive systems are all around us. Most things we take for granted are complex adaptive systems, and the elements in every system exist and behave in total ignorance of the concept but that does not impede their contribution to the system. Complex Adaptive Systems are a model for thinking about the world around us not a model for predicting what will happen.

IV. NETWORK MODELING PARADIGMS

Recent advances in the characterization of complex systems have given rise to the revival of network modeling, resulting in the introduction and study of three main classes of modeling paradigms.

A. Random Networks

For more than 40 years, science treated complex networks as being completely random. This paradigm has its roots in the work of Alfred Renyi and Paul Erdos who addressed for the first time in history one of the most fundamental questions pertaining to our understanding of our interconnected universe: How do networks form? Their solution laid the foundation of the theory of random networks which came to dominate our idea on network modeling.
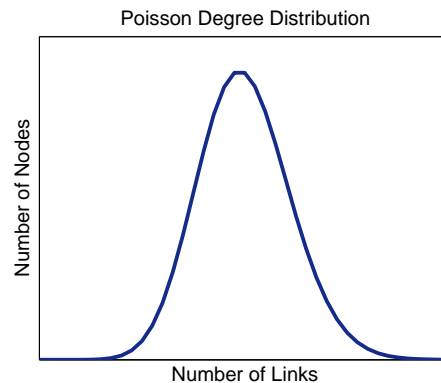

Fig. 3.   Poisson degree distribution.

Earlier study of network structure has been focused on random networks, of which nodes have equal probability of connecting with each other. Random networks, which are variants of the Erdos-Renyi model [10], [11], are still widely used in many fields and serve as a benchmark for many modeling and empirical studies. This paradigm of network modeling can be characterized by (a) a low average path length, (b) a small clustering coefficient, and (c) a degree distribution following a Poisson distribution with a bell shape as depicted in Fig. 3. The latter characteristic reveals that although not all nodes in this kind of network would be connected to the same degree, most would have a number of connections hovering around a small, average value.

Random networks are robust to coordinated attacks (that is, to the selection and removal of a few nodes that play a crucial role in maintaining the network's connectivity) but on the other hand are intolerant to accidental failure due to the fact that they are not highly interconnected. Specifically, the connectedness of a randomly distributed network decays steadily as nodes fail, slowly breaking into smaller, separate domains that are unable to communicate.

B. Small-world Networks

Motivated by the inefficiency of both random networks and regular lattices to provide an adequate framework within which to study real-world complex networks, a new class of models collectively called small-world models was introduced by Watts and Strongatz in 1998 [12]. Small world models interpolate between the highly clustered regular lattices and random graphs (as shown in Fig. 4). In particular, these models are based on the 'six degrees of separation' model in that they have a high degree of local clustering or cliqueness (like a regular lattice network) and a relatively short average minimum path (like a completely random network).

p = 0 ———————————————→ Increasing Randomness ————————————→ p = 1

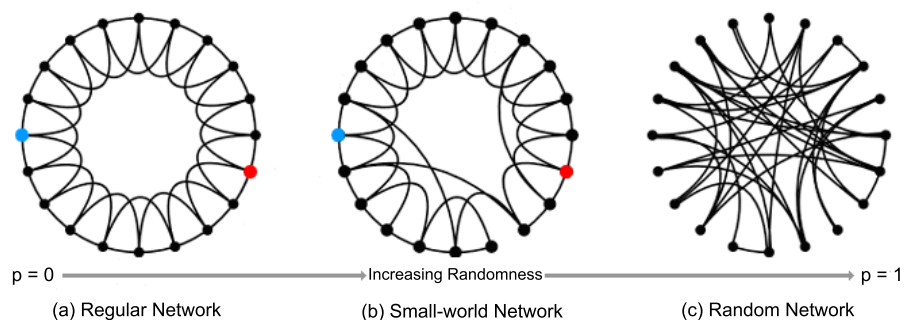(a) Regular Network   (b) Small-world Network   (c) Random Network

Fig. 4.   A small world network is between a regular lattice network and a random network. After [12].

In a pioneering article [12], Watts and Strongatz studied a simple model starting from an ordered finite-dimensional ring lattice with N nodes connected to their first K neighbors (having $N >> K$) as shown in Fig. 4a and replacing the original links by random ones with some probability $0 \leq p \leq 1$. By varying p, Watts and Strongatz could closely monitor the transition between order ($p = 0$ and Fig. 4a) and randomness ($p = 1$ and Fig. 4c). They found that this model paradigm is able to

transform a 'sparse' network (i.e. a regular lattice with $N >> K$) into a small-world with relatively short paths between any two nodes by setting p between zero and 1 ($0 < p < 1$ and Fig. 4b). Moreover, the new model was found to be much more highly clustered than a random graph.

According to Watts and Strogatz [12], *"models of dynamical systems with small-world coupling display enhanced signal propagation speed, computational power, and synchronizability."* These findings have profound implications for many real systems. In a telecommunication network for example, 'small-world connectivity' might improve the ease with which ideas diffuse through the system. In a transportation network, 'small-world topology' could improve the flow of people or goods through the network.

Taking all these into consideration, the obvious inference is that the Watts and Strogatz model addresses the connectivity issue of a network but on the other hand it does not say anything on how nodes would use shortcuts to reach remote nodes. Similarly, there are some important issues that are not addressed by the small-world model as, for example, the affect of mobility on the small-world networks as well as the robustness, efficiency and scalability of those networks.

To sum up, small-worlds networks are characterized by (a) a high clustering coefficient like regular lattices, and (b) a short characteristic path length as well as a degree distribution typical of random networks. It is believed that many real world networks including social networks (e.g. film actors), the electrical power grid, and the neural network of the nematode worm C.elegans (studied in [12]), exhibit small-world phenomenon, but the real challenge is how to impose it on an engineered dynamic system as, for instance Mobile Ad-hoc Networks (MANETs) or Wireless Sensor Networks (WSNs).

C. Scale-free Networks

In the late 1990s, attempts were made to explore and explain the structure of the World Wide Web. Researchers tried to apply the concept of small worlds to explain the functionality of the web, but this didn't quite work, although the web was considered a small-world rather than a random network. The reason was that in the small-world model of Watts and Strogatz, each node has only a few connections compared to the total number of nodes in the system as can be seen in Fig. 5.

(a) Small-world network   (b) Scale-free network   (c) Random network
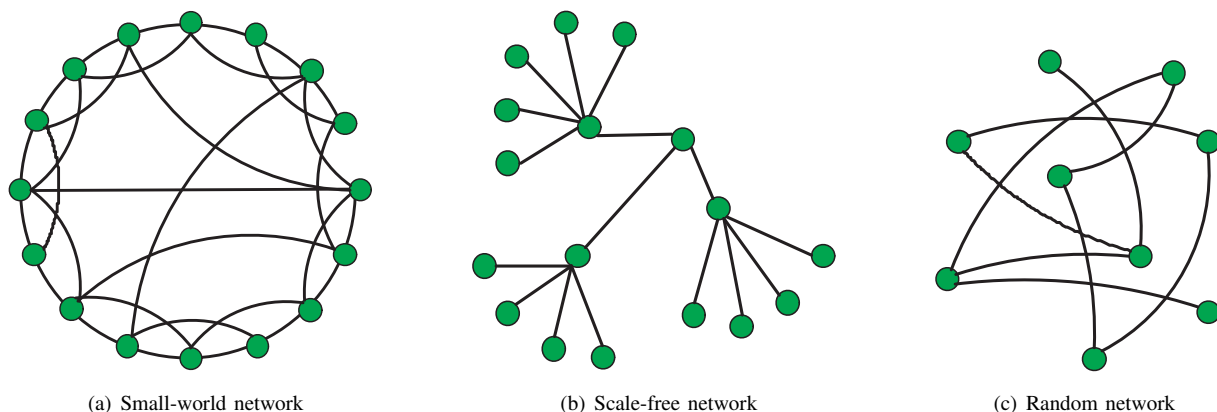
Fig. 5. Network modeling paradigms.

Recent research efforts led to one of the most interesting developments in the understanding of complex networks; the discovery that for most large networks the degree distribution significantly deviates from a Poisson distribution. In particular, for a large number of real networks, including the World Wide Web (WWW) [13], the Internet [14], the mail network [15], [16], etc., the degree of distribution was found to follow a power-law tail, $p(k) \sim k^{-\gamma}$ as illustrated in Fig. 6, which defines the probability of a node having k edges. These network topologies that exhibit power-law distributions in the connectivity of network nodes were originally introduced by Barabasi and Albert [17]) as generic, yet universal network models called scale-free models, aiming to offer a universal theory of network evolution by focusing on the network dynamics.

In contrary to the model of small-world networks which introduces isolated clusters of highly interconnected nodes, scale-free networks consist of highly connected hubs that hold together the network. It seems like that these two network theory approaches run counter, but these two properties are compatible, as stated in [18], which also demonstrates that *"a network can be both highly clustered and scale-free when small, tightly interlinked clusters of nodes are connected into larger, less cohesive groups. This type of hierarchy appears to exist in a number of systems, from the World Wide Web (in which clusters are groupings of web pages devoted to the same topic) to a cell (in which clusters are teams of molecules responsible for a specific function)"*.

The network models discussed thus far (random and small-world networks) are formed by a fixed number of nodes N that are randomly connected or rewired. Additionally, they assume that new edges are placed randomly, something which more specifically means that the probability that two nodes are connected (or their link is rewired) does not depend on the node's degree. These two assumptions do not apply in most real world networks as, for example, the Internet and the World Wide
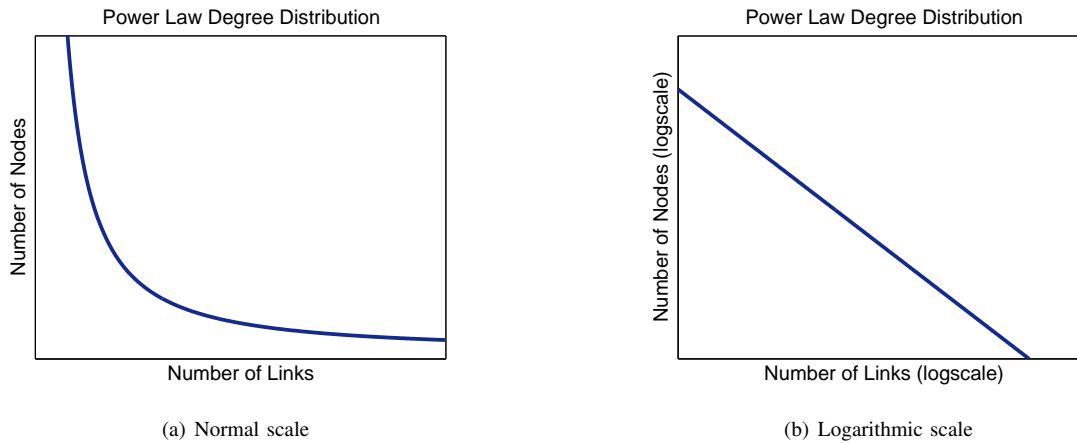
(a) Normal scale

(b) Logarithmic scale

Fig. 6. Power-law tail.

TABLE I

SCALE-FREE NETWORKS ARE EVERYWHERE. AFTER [18].

Network	Types	Nodes	Links
Cellular Metabolism	Biology	Molecules involved in burning food for energy	Participation in the same biochemical reaction
Protein regulatory	Biology	Proteins that help to regulate a cell's activities	Interactions among proteins
Sexual relationships	People	People	Sexual contact
Hollywood	People	Actors	Appearance in the same movie
Research collaborations	People	Scientists	Co-authorship of papers
Internet infrastructure	Technology	Routers	Optical and other physical connections
World Wide Web	Knowledge	Web pages	URLs

Web. Towards this direction, a variety of approaches for generating ensembles of graphs having scale-free characteristics have been proposed including the preferential attachment (Barabasi-Albert model [17]), power-law random graph [19], the linearized chord diagram (LCD) model [20], etc.

1) Barabasi-Albert (BA) model: The first and perhaps the most studied of the models in this vein, is the Barabasi-Albert model [17]. This model is based on two key features, namely growth and preferential attachment which are shown in Fig. 7. The term growth refers to the continuous addition of new vertices and edges to the network, as for example, the WWW grows exponentially by adding new web pages. In addition, according to the preferential attachment mechanism, new nodes added into a network have higher probability of connecting to the existing nodes with high connectivity, i.e., a 'rich-gets-richer' phenomenon. For example a newly created web page will more likely include links to well known, popular documents with high connectivity.

The topology of Barabasi-Albert networks grows by the continuous addition of new nodes starting from a small number of nodes which increases throughout the lifetime of the network. The connection or rewiring of the nodes takes into account the preferential attachment mechanism, such that the likelihood of connecting to a node depends on the node's degree, i.e. the likelihood is proportional to the number of links that the existing node already has. Therefore, heavily linked nodes (called hubs) tend to quickly accumulate even more links, while nodes with only a few links are unlikely to be chosen as the destination for a new link. It is as if the new nodes have a 'preference' to attach themselves to the already heavily linked nodes. This is apparent in Fig. 5, which reveals that the nodes of a scale-free network aren't randomly or evenly connected but the degree distribution (number of links per node) follows a power law.

As implied by the Barabasi-Albert model, scale-free networks consist of a relatively small number of highly connected nodes, hubs of connectivity and a large number of low degree nodes which are accumulated around hubs. Scale-free networks are characterized by (a) a low average path length, (b) varying clustering coefficient - but much larger than in random networks - depending on other topology details (it decreases as the node degree increases), and (c) a power-law degree distribution. Based on their inhomogeneous topology, scale-free networks can be amazingly robust against random failures. In particular, since failures occur at random and the vast majority of nodes are those with small degree, the likelihood that a hub be affected is almost negligible. Even if such event occurs, the network will not lose its connectedness, which is guaranteed by the remaining hubs. Simulations on scale-free networks [18] reveal that even if as many as 80 percent of randomly selected routers within the Internet fail, the remaining ones still form a compact cluster in which there will still be a path between any two nodes. On the other hand, the presence of hubs makes the scale-free networks more vulnerable to targeted attacks. To this extend, if we choose a few major hubs and take them out of the network (targeted attack), it simply falls apart and is turned into a set of rather isolated graphs. Therefore, there is an imperative need to protect the Achilles' heel of scale-free networks against
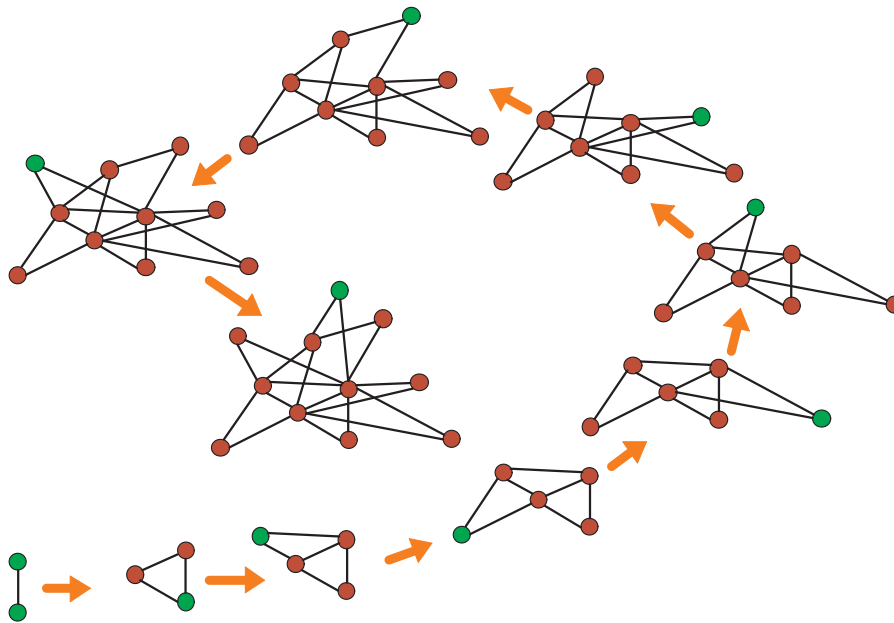
Fig. 7. Birth of a scale-free network based on Barabasi-Albert model. After [18].

malicious targeted attacks in order to maximize the network lifetime. This of course should be based on further analysis, for example, on determining how many hubs are essential for the liveness of a given network.

Despite the fact that the Barabasi-Albert model has been extensively studied, most of the related work appears to be of a heuristic or experimental rather than mathematical nature. Several heuristic and experimental studies on the Barabasi-Albert model can be found in the extensive surveys [3] and [26]. In contrast, so far there has been rather little rigorous mathematical work; what there is sometimes confirms and sometimes contradicts the heuristic results. See [19], [24], [25], [22] and [23] for some examples, or the survey [21].

2) Other Models: Aiello et. al [19] proposed a random graph model which is a special case of sparse random graphs with given degree sequences which satisfy a power-law. This model involves only a small number of parameters, called logsize and log-log growth rate. These parameters capture some universal characteristics of massive graphs. The study of these parameters reveals what other network properties can be derived from its scale-free nature.

Moreover, a precisely defined model, the linearized chord diagram or LCD model, was introduced in [20], motivated by the vague description of Barabasi-Albert, and incorporating its key features as well as other useful mathematical properties. The LCD model considers two basic characteristics of a precise version of the Barabasi-Albert model from the mathematical point of view, namely robustness to random damage, and vulnerability to malicious attack.

Further elaboration of scale-free models which arise from attempts to explain the power law, starting from basic assumptions about the growth of the graph is given in the survey [21].

V. REAL COMMUNICATION NETWORKS AS COMPLEX SYSTEMS

The study of most complex networks has been initiated by the desire to understand various real networks, such as communication networks. Over the last decade, remarkable progress has been made in the field of complex systems, providing theoretical foundations and conceptual framework including emergent phenomena, self-organizing infrastructures, cooperative behavior, adaptability, robustness, resilience, evolution, decentralization and so on. Theoretical understanding has evolved from simple models into structured models that view systems as wholes. In these models, the heterogeneities and details of the system under study are becoming increasingly included.

As traditionally conceived, science and engineering lack the conceptual framework to understand systems, manage and control them intelligently or create them intentionally from scratch. The remarkable progress of science over the centuries has largely built up a science of the simple which nowadays underlines the need for a science of the complex, for a view of systems as wholes.

Inspired by the recent advances in complex theory, we should take a deeper look at the communication network anatomy. It is beyond any doubt that network anatomy is important to be characterized, because the structural and evolutionary properties of networks are considered to affect their function. This study should be embraced by the interplay between the dynamics and the structure of complex networks. In fact, in the last few years it became clear that in spite of the inherent differences, most of real communication networks, as, for example, the Internet [14], the World Wide Web (WWW) [13], and the mail

network [15], [16], are characterized by similar topological properties as the complex networks structures. Further analysis of real communication network paradigms in the context of complex systems will be presented in Section VI.

Complex networks can be characterized by large scale topologies, decentralized/distributed resource management, extreme heterogeneity of the constituent elements, relatively small characteristic path lengths, high clustering coefficients, power-law degree distributions, modularity etc., which are all properties highly correlated to real communication networks too. Attempts to explain such similarities may be fueled by the study of universal structural properties in real communication networks as well as by the theoretical understanding of evolutionary laws governing the emergence of these properties.

A. Complex Network Attributes

In general, communication networks are characterized by a chain of possible complex attributes that can be viewed from the perspective of complex (adaptive) networks. These attributes are illustrated below:
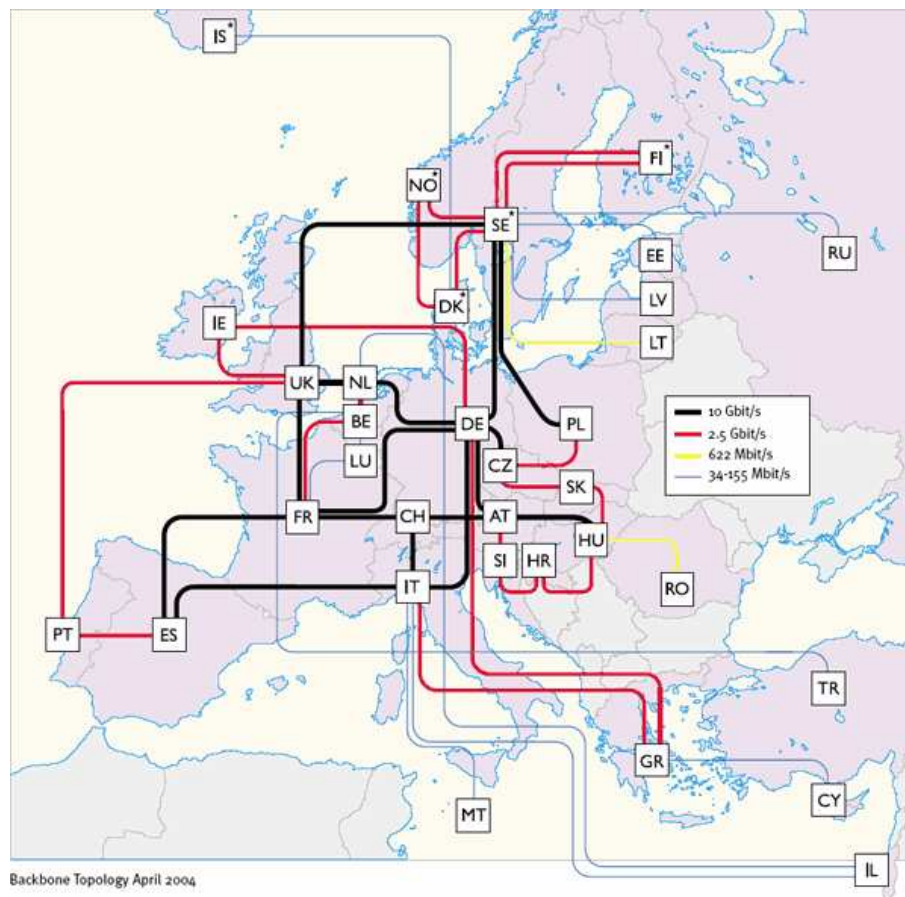

Fig. 8. Gigabit European Academic Network (GEANT) backbone topology.

- **Structural complexity:** The overwhelming majority of communication networks have complex topology like the intricate tangle shown in Fig. 8. As far as the structural properties are concerned, there was an increasing voiced need to pay attention to the evolutionary mechanisms that have shaped the topology of a network, and to the design of new models based on random networks [10], [11], small-world networks [12], and scale-free networks [13], [17], which retain the most significant properties observed empirically. This research was motivated by the expectancy that the characterization and the modeling of the structure of a network would lead to a better knowledge of its dynamical and functional behavior. Furthermore, the structural complexity of a network can be influenced from both node and connection diversity. Multiple complications can be observed due to the fact that a network can consist of different kinds of nodes which can be interconnected through links having different weights and directions, resulting in a high level of heterogeneity.

  Consequently, the wiring diagram of a network is considered to affect its functional robustness and resilience to external perturbations, such as random failures, or targeted attacks. At the same time, the network topology plays a crucial role in determining the emergence of collective dynamical behavior, such as synchronization, or in governing the main features of relevant processes that take place in complex networks, as, for example, the spreading of information.

  Apparently, it remains a challenge to answer some fundamental questions as, for example, 'How does one characterize the wiring diagram of such networks?', or 'Are there any unifying principles underlying their topology?'.

- **Network evolution:** The wiring diagram of a communication network is subject to dynamic changes over time. This is a basic characteristic of dynamically changing environments like, for example, the WWW, where links are created and lost over time. From this point of view, the evolution of a communication network can be parallelized with the evolution of a complex (adaptive) network which is considered to be very sensitive to initial conditions or to small perturbations, leading to multiple pathways by which the system can evolve.
- **Dynamical complexity:** The network and each node within it could be non linear dynamical systems which their state may vary over time as a result of the evolution. The understanding of the evolutionary laws governing the emergence of the structural properties should be based on the study of dynamical processes of complex networks. In this context, network problems in traditional areas such as robust flow and congestion control, fault and attack tolerance, error resilience, decentralized/distributed operation, which are just in the forefront of the current research on network dynamics, are intended to be addressed based on concepts arising from the dynamical processes of complex networks.

  To this end, from the perspective of non linear dynamics, we would like to understand how an enormous network of interacting dynamical systems (e.g., sensor nodes, computer devices, routers, etc.) will behave collectively, given their individual non linear dynamics and coupling architecture.

All the aforementioned attributes of networked systems remain open challenges which can be possibly addressed by complex systems. Powerful new ideas and techniques can be found by studying the similarities between real communication networks and other complex systems. In this respect, complex systems science can be seen to bridge the gaps between the natural, social and formal sciences, and especially between engineering and the sciences.

B. Complex Network Design Principles

Our increasing ability to address the aforementioned challenges will be based on some basic features of complex systems which have been already studied to some extend, such as (a) self-organization and adaptability, (b) robustness and resilience, and (c) decentralized/distributed operation. These features are analyzed below and may be seen as the main design principles of contemporary networked systems as depicted in Fig. 9. The study of these features - from complex systems perspective - is based on a combination of the growing mass of empirical data which has recently become accessible, and the large increase in computational power which can support and underpin significant advances in the theoretical understanding of complex systems.
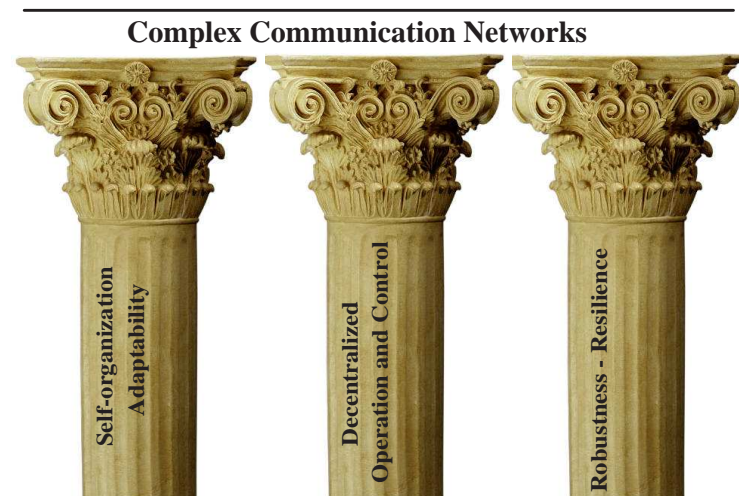

Fig. 9.   Design Principles of Contemporary Networked Systems.

1) Self-Organization and Adaptability: Self-organization refers to the evolution of a system into an organized form in the absence of external pressures. Self-organization leads a system from a large region of state space to a persistent smaller one, under the control of the system itself. This smaller region of state space is called an attractor.

There are three major principles of self-organization mechanisms: feedback loops, local state evaluation, and interaction between individuals. One major component in understanding the interaction of components producing a complex pattern are positive and negative feedback loops as shown in Fig. 10. As explained in Section III, positive feedback acts as an amplifier for a given effect (or perturbation), leading to an explosive growth. This feedback, will drive the system even further away from its own original setpoint, thus amplifying the original perturbation signal, and eventually become explosive. In negative feedback loop the system responds in an opposite direction to the perturbation. It is a process of feeding back to the input a part of a system's output, so as to reverse the direction of change of the output. This tends to keep the output from changing, so it is stabilizing and attempts to maintain constant conditions. This often results in equilibrium such that the system will return to its

original setpoint. In fact, negative feedback is used to efficiently control the system behavior in order to prevent over-reactions and mis-regulations. The second ingredient is the local state. This means that all subsystems are acquiring and action upon information that are stored locally. Any global control or dependency is prevented in order to enable fully autonomous behavior embedded into a global context. Information transfer between individuals is necessary to update the local state. There are two ways to conduct such interactions: direct interaction or communication between related subsystems and indirect information exchange by interacting with the environment (also known as stigmercy [53]).
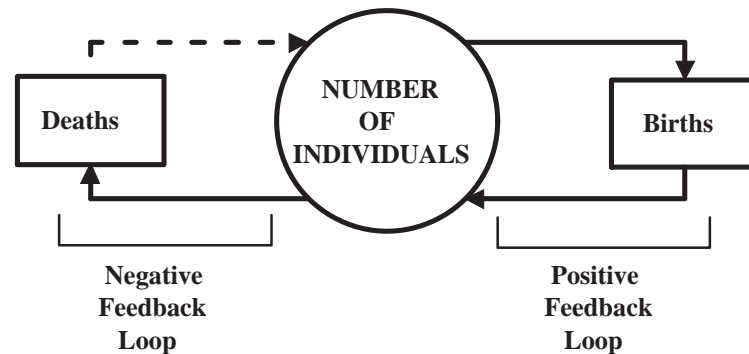

Fig. 10.   System control using positive and negative feedback loops. After [46].

Because of its decentralized character, self-organization tends to be robust, resisting perturbations. A self-organizing system is typically driven by non-linear dynamics, because of circular or feedback relations between the constituent components (Fig. 1). Non-linear systems have in general several stable states, and this number tends to increase as an increasing input of energy pushes the system farther from its equilibrium.

Adaptability allows for the modification of a system's behavior in order to adapt to requirements posed by exogenous factors (e.g. users of a network) or environmental changes. Therefore, adaptation may be driven by users to provide them flexibility and ensure that their exact requirements will be fulfilled. Furthermore, to adapt to a changing environment, a system needs a variety of stable states that is large enough to react to all perturbations but not so large as to make its evolution uncontrollably chaotic. The most adequate states are selected according to their fitness, either directly by the environment, or by subsystems that have adapted to the environment at an earlier stage.

Formally, the basic mechanism underlying self-organization is the (often noise-driven) variation which explores different regions in the systems state space until it enters an attractor. This precludes further variation outside the attractor, and thus restricts the freedom of the systems components to behave independently. This is equivalent to the increase of coherence, or decrease of statistical entropy, that defines self-organization.

The study of such complex methodologies promises to enable more scalable self-organizing communication network infrastructures. Especially in the area of complex communication networks that are subject to dynamic topology changes (e.g., ad hoc and sensor networks), such solutions are considered of prime importance in order to enable them to simplify development and deployment. Self-organization and adaptability promise to drive the implementation of novel autonomously evolving mechanisms, capable of coping with global tasks (emergent behavior).

In the last few years, there was an increasing need to develop robust and efficient techniques which would be able to address various issues as, for example, congestion/overload control, data dissemination, quality of service (QoS) provision, power consumption, etc., in the forthcoming pervasive networking world. Given the often large number of perturbations that influence the structure of a networked system, it became obvious that the implementation of the aforementioned techniques should be done on the basis of self-organization and adaptability. Towards this direction, the goal is to teach each node belonging to the network to self-organize for performing the requested tasks like event detection, periodic/continuous measurements and tracking taking into consideration energy and QoS constraints, i.e. showing an emergent global behavior.

Motivated by recent studies on complex nature and biological systems, researchers think about to adopt and apply the underlying principles to engineering and computer science, especially for self-organization. The combination of nature and self-organizing technical systems was first introduced by Eigen [43]. In a recent study, Gerherson [44] provides a discussion on when and how to best model a system as self-organizing, and argues that self-organizing systems, rather than a type of systems, are a perspective for studying, understanding, designing, controlling, and building systems. The study of nature and biologically-inspired systems relies primarily on the artificial immune system [45], swarm intelligence [46], evolutionary (genetic) algorithms [47], and cell and molecular biology based approaches [48]. First attempts are in progress to study the behavior of swarms of insects, typically ants and bees, and to adapt the discoveries to build more efficient sensor networks [50], [52]. Furthermore, a special form of biologically-inspired computing with organic properties, namely organic computing [51] is attempting to build high-scalable architectures, which are self-organizing, self-maintaining, and self-healing.

2) Robustness and Resilience: The robustness and resilience of critical infrastructures (i.e. real communication networks) in particular, and complex networks in general, are issues of great importance. Complex communication networks seem to display a high degree of robustness and resilience even though key components regularly malfunction and local failures rarely lead to loss of the global information-carrying ability of the network. This property of complex networks is often attributed to their design (i.e. the redundant wiring of their underlying network structure) and evolution. However, even though they remain unaffected by random component failures, they seem vulnerable to targeted attacks on its key components. Nevertheless, it remains an open challenge to identify whether the network topology - beyond redundancy - is able to play a substantial role in the robustness and error/attack tolerance of such complex systems.

Recent work on network theory has started to address primarily the topological aspects of robustness and resilience in complex networks with respect to failure and directed attack caused by edge and/or node removal.

Initial efforts towards this direction were made by [10] and [36] addressing the reliability of a network with respect to edge removal based on random graph theory. The network model used in these early investigations was a randomly connected graph H_N consisting of N nodes. By removing a p fraction of edges, the researchers were seeking to evaluate the probability that the resulting subgraph is connected and extract any dependencies among connectedness and the removal probability p. Results carried out by [36] revealed that a broad class of H_N graphs displays a threshold-oriented behavior. In particular, a threshold probability $p_c(N)$ exists, such that for $p < p_c(N)$ the subgraph remains connected, but for $p > p_c(N)$ the subgraph is considered fragmented.

Needless to say that the removal of a single edge is not considered as harmful as the removal of a node. In the latter case, the effects on the robustness of an arbitrary graph are even more devastating, since the removal of a node results to malfunctioning of all the edges attached on it as well. The effects of node removal have been recently studied with respect to random graphs and scale-free networks addressing their robustness against accidental node failures and intentional attacks.

Because of its immediate practical consequences to Internet and distributed systems, the problem of characterizing the robustness and error tolerance of complex networks has received growing attention, especially after the seminal papers by Albert and Barabasi [4], who addressed node removal in scale-free models of Internet, and Callaway et al. [6] investigation on exponential networks under attack. Other related works include Holme et al. [37] comprehensive comparative investigation of the resilience of several types of networks considering different schemes for attacking nodes and edges, and Cohen et al.'s analysis of Internet breakdown [5]. Works targeting specific types of network include, but are not limited to, Newman's investigation of e-mail networks [38], Jeong at al. study of metabolic systems [39], and Dunne's analysis of food webs [40]. More recently, the concept of L-expansions of a complex network was suggested [41] which, by enhancing the network connectivity, was believed to present good potential for increasing the resilience of existing networks. Moreover, Motter and Lai [8] showed that for many physical networks, the removal of nodes can have a much more devastating consequence when the intrinsic dynamics of flows of physical quantities in the network is taken into account.

These studies suggested that the network connectivity, and hence its functionality, is robust against random failure of nodes, and to some extent is even robust against intentional attacks. Results revealed that real networks (e.g., Internet) are naturally evolved to be quite resistant to random failure of nodes, but the presence of a few nodes with exceptionally large load, which is known to be ubiquitous in natural and man-made networks, has a disturbing side effect: the attack on a single important node one of those with high load may trigger a cascade of overload failures capable of disabling the network almost entirely. Such an event has dramatic consequences on the network performance, because the functionality of a network relies on the ability of the nodes to communicate efficiently with each other.

More specifically, Albert and Barabasi [4] studied error and attack tolerance in exponential (random) and scale-free networks. They demonstrated that complex communication networks which incorporate a scale-free behavior, such as the Internet and the WWW, display a surprising degree of robustness, even though some significant constituent components are regularly subject to malfunction and local failures rarely lead to the loss of global information-carrying ability of the network. In order to address the error tolerant characteristic of exponential and scale-free networks, they studied the changes in their diameter (the average length of the shortest paths between any two nodes in the network), when a small fraction f of nodes was randomly or intentionally removed. Measurements revealed that in case of random node removal in exponential networks, the diameter increases monotonically with f, despite their redundant wiring. This behavior is rooted in the homogeneity of such networks: since all nodes have approximately equal number of edges attached on them, they all contribute equally to the network's diameter, thus the removal of each node causes the same amount of damage. On the other hand, scale-free networks display a totally different behavior. It was illustrated that scale-free networks including the Internet and the WWW, display an unexpected degree of error tolerance against random failures due to their inhomogeneous (power-law) connectivity distribution. Such networks display an unexpected degree of robustness, such that their ability to communicate to high failure rates remains unaffected even by unrealistically high failure rates. However, these networks are extremely vulnerable to directed attacks since their diameter increases rapidly, doubling its original value if 5% of the nodes are intentionally removed. On the contrary, measuring the diameter of an exponential network, they found that owing to their homogeneity, there is no substantial difference whether the nodes are removed randomly or in decreasing order of connectivity.

3) Decentralized Operation and Control: Complex networked systems consist of similar components which directly interact with their nearest neighbors. Even when these components interact with their neighbors in a simple and predictable fashion,

the resulting system often displays complex behavior when viewed as a whole.

Decentralized operation and control are considered to be inextricable ingredients of complex networks since they provide resistance against perturbations (robustness and resilience). In fact, decentralization is the process of dispersing decision-making closer to the point of service or action. This feature of complex communication networks allows flexibility that facilitates self-organization. Such flexibility is facilitated by lack of dependency on central decision-making. However, it has to be done in a manner that allows some control. This control may arise through the self-organization itself, or through the interaction between components that is enabled by self-organization.

Apparently, formal control theory cannot be efficiently applied in complex networks since most optimal control techniques suffer from severe limitations as they cannot handle systems of very high dimension and with a large number of inputs and outputs. It is also infeasible to control these networks with centralized schemes (the typical outcome of most optimal control design techniques) as these require high levels of connectivity, impose a substantial computational burden, and are typically more sensitive to failures, attacks, and modeling errors than decentralized schemes.

The decentralization of decisions is often recommended in the design of complex networks, and the decomposition and coordination of decisions are a great challenge. The mechanisms behind this network of decentralized design decisions create difficult management and coordination issues. Standard techniques to modeling and solving decentralized design problems typically fail to understand the underlying dynamics of the decentralized processes and therefore result in sub-optimal solutions. From this angle, it remains crucial to understand the mechanisms and dynamics behind a decentralized set of decisions within a complex design process. Towards this direction, the structure as well as the evolution of the network should be exploited for the development of successful optimal control techniques.

C. Modeling Pattern Formation in Complex Networks

Complex systems consist of multiple elements which are arbitrarily interconnected and interact with each other as well as with their environment in unpredictable and unplanned ways. From this mass of interactions patterns emerge as a result of negative and positive non-linear feedback mechanisms acting at different spatiotemporal scales. Even though the interactions may be simple, the behavior of the whole system can be complex. Similarly, a network consists of nodes which are interconnected through arbitrary links and interact with each other in unpredictable and unplanned ways, using rules imposed by various protocols. From this point of view, complex systems seem to provide a theoretical framework for the study of the robustness and stability in real communication networks under perturbations, based on self-organized and decentralized operation. The way the patterns are formed and evolve within a complex environment can be investigated and the inherent complex mechanisms that provoke this behavior will provide the basis on which robust network approaches will be developed.
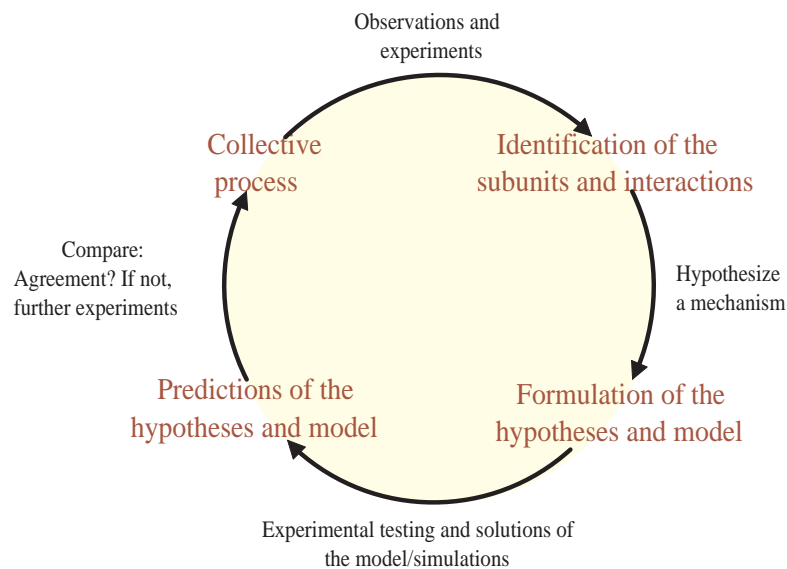

Fig. 11.   Cycle of study for pattern formations.

The study and the modeling of pattern formations in real communication networks should involve some basic steps as shown in Fig. 11. Initially, the identification of subunits and interactions involved in a collective process can be carried out through observations and experiments in the complex system's environment. Then, a hypothesis formation (simulation and/or modeling) should be developed and its correctness based on its capability to cope with system's perturbations should be carefully tested. In other words, by changing the rules or parameters of the system in a controlled manner, it should be determined whether the outcome matches that was predicted by the hypothesis (simulation/model).

VI. Real Network Paradigms

In this section we investigate the two most prevalent real communication networks, namely, the Internet and the World-Wide Web (WWW) that have been extensively studied in literature. We focus primarily on the validity and the effectiveness of the proposed models to capture the dynamics of the interaction among the constituent components of each network.

A. The Internet

The Internet network has become the largest and most complex artificially deployed system. It possesses similar structural properties to the ones characterizing many other complex systems: plethora of often heterogeneous subsystems (sources and routers) performing complex functions, interconnected by heterogeneous links (wired, wireless, satellite links) often incorporating complex dynamics themselves. There are several factors contributing to the immense complexity of the system: the large-scale and size as a result of its exponential growth; the fragmented nature of the underlying infrastructure; the semi-hierarchical organization; the extreme heterogeneity as a result of the diverse network technologies and communication protocols and services which are accommodated; the distributed management of the available resources; the complex structures which arise in the implementation of the various functionalities of the layered protocols, etc.
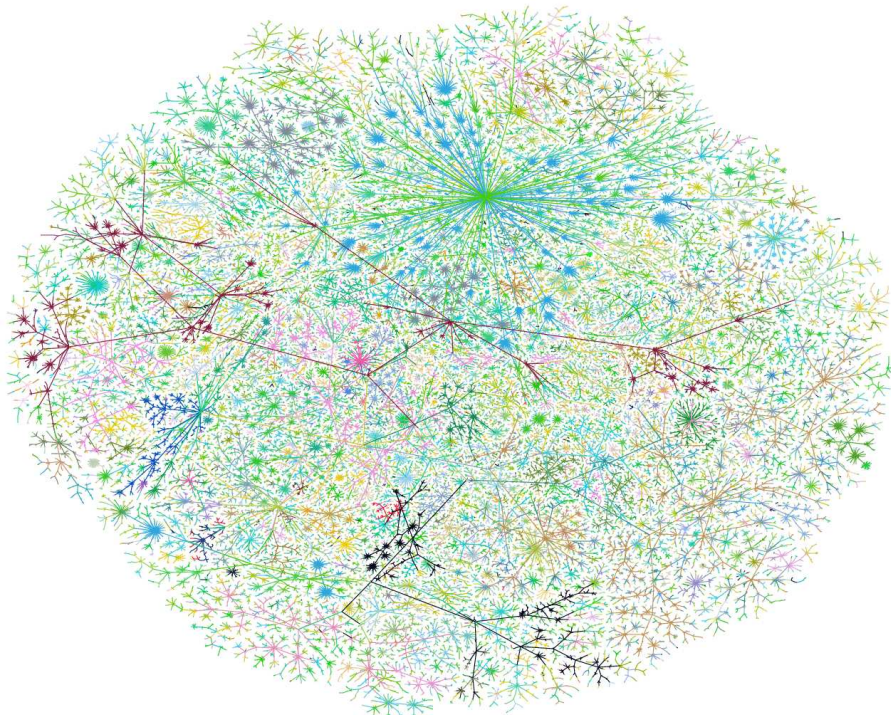

Fig. 12. Full Internet map of 29 June 1999. After [34].

Many of the complex network functions which drive the current Internet, have been developed using engineering intuition, heuristics and ad-hoc nonlinear techniques, with the objective of making the system resilient to failures and robust to changing environments. The problem with this approach is that very little is known why these methods work and very little explanation can be given when they fail. Given the lack of a coherent and unified theory of complex systems, these methods do not have analytically proven performance properties and can thus prove to be ineffective as the system evolves over time. When such vulnerabilities do show up, designers usually resort to even more complex network functions to solve the problem, thus contributing to a spiral of increasing complexity. These observations highlight the necessity to develop a new theoretical framework to help explain the complex and unpredictable behaviors of the Internet and offer alternative network protocols which are provably effective and robust. Such a framework can serve as a starting point to develop a unified theory for complex systems, useful in explaining how the interaction between the individual components of such systems allows the emergence of a global behavior that would not be anticipated from the behavior of components in isolation.

In the remainder of this section we take a glimpse into the evolution of the Internet [55], and we examine recent studies raising doubts whether the BA model is verified by the empirical data, focusing on the robust, yet fragile (RYF) nature of the Internet [32].

1) The Evolution of the Internet: Over the last few years, several studies have touched on the static nature of the Internet topology [14], [57], [58] and [59]. Contrarily, a recent study [55] focuses on the evolution of the Internet topology based on real data. In this study, Siganos at al. [55] studied the network evolution at three different levels: the node level, the network level and the path level, trying to explain the macroscopic properties of the network through the study of microscopic phenomena.

In one of the most popular studies on the Internet topology, Faloutsos et al. [14] introduced the use of power-laws based on static measurements. Power-laws seem to describe several topological properties such as the degree distribution, and their exponents can characterize concisely the topology. Siganos and et al. [55] discovered that the exponent of the power-law degree distribution remained practically constant over a three-year period. Also, their results showed that the Internet exhibits the 'rich-get-richer' behavior, involving the preferential attachment of new nodes in a non-linear way, in contrast to that imposed by the BA model [17]. In addition, it was revealed that the generation of the internal edges is preferential but deviates from linearity.

Furthermore, measurements demonstrated that even though the network grows at an exponential pace (both the number of nodes and the number of edges grow exponentially), the characteristic path lengths remain the same. This 'small-world' phenomenon can be justified by the observation that more than 99% of nodes are within 6 hops. However, the inflation of the routing paths compared to the topological distances at the autonomous system level seems to increase over time.

2) On the validity of the BA model: The most popular mechanism for the growth of the Internet is a theoretical approach proposed by Barabasi and Albert, widely known as the BA model, which is based on the preferential attachment of new nodes to high degree existing nodes. The majority of the results carried out by the Albert and Barabasi study [4] on the scale-free nature of the Internet and the World Wide Web were based on the BA model. The results pointed out that these scale-free networks display high resilience to random loss of links, but on the other hand, they are very susceptible to deliberate attack. According to the researchers, this behavior is attributed to the existence of a limited number of hubs that are highly connected, forming the system's backbone as shown in Fig. 13(a).
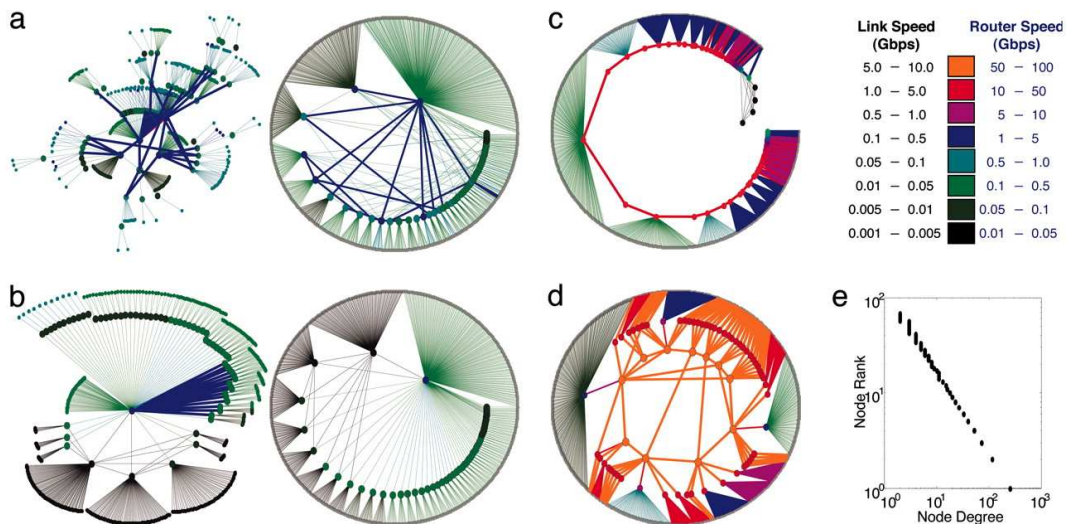

Fig. 13. Diversity among graphs having the same degree sequence D. (a) RNDnet: a network consistent with construction by PA. The two networks represent the same graph, but the figure on the right is redrawn to emphasize the role that high-degree hubs play in overall network connectivity. (b) SFnet: a graph having the most preferential connectivity, again drawn both as an incremental growth type of network and in a form that emphasizes the importance of high-degree nodes. (c) BADNet: a poorly designed network with overall connectivity constructed from a chain of vertices. (d) HOTnet: a graph constructed to be a simplified version of the Abilene network (the backbone for the Internet2 academic network). (e) Power-law degree sequence D for networks shown in ad. Only di ¿ 1 is shown. After [32].

In a recent study by Doyle et al. [32], some doubts were raised with respect to the validity of the BA model for modeling the today's Internet. Doyle at al. claimed that the results carried out in [4] regarding the 'hub-like' core structure of the Internet (often called its 'Achilles' heel'), were based on a quite general scale-free model which does not take into account any details of the today's Internet such as technology, economics or engineering.

Doyle and his research team investigated how the scale-free BA model compares with the real Internet [32], and suggested a more coherent perspective of the Internet as, for example, its robust yet fragile nature, which is possible in a way that is fully consistent with Internet technology, economics, and engineering. They dig deeper in to the real structure of the Internet and tried to falsify the popular belief that the structure of the Internet follows a scale-free distribution which then results in being sensitive to target attacks at the hubs. Indeed, the number of connections follow a scale-free distribution, but there are various ways to derive such a distribution. All networks illustrated in Fig. 13 have the identical scaling-degree sequence D shown in Fig. 13e. Fig. 13a shows a scale-free graph created using the preferential attachment mechanism according to the BA model. It is beyond any doubt that the 'hub-like' (highest-degree) nodes are essential for graph connectivity, and this feature can be

seen even more clearly for the more idealized scale-free network (SFnet) shown in Fig. 13b. Therefore, the scale-free claims would certainly hold if the Internet looked at all like Figs. 13a and b.

Doyle et al. argued that the components of the Internet with the most connections are not the crucial hubs of the Internet. As demonstrated in [32], the Internet looks nothing like the graphs depicted in Figs. 13a and b. On the other hand, the Internet seems much closer to Fig. 13d, which has the same degree sequence D but is otherwise completely different, with high-degree vertices at the periphery of the network, where their removal would have only local effects. Thus, although scaling-degree sequences imply the presence of high-degree vertices, they do not imply that such nodes form necessarily 'crucial hubs' in the scale-free sense.

Carlson and Doyle [33] proposed a conceptual framework for capturing the highly organized, optimized, and robust yet fragile structure of complex highly evolved systems called Highly Optimized Tolerance (HOT). HOT is motivated primarily by systems from biology and engineering and emphasizes, (i) highly structured, non-generic, self-dissimilar internal configurations, and (ii) robust yet fragile external behavior. The paper by Doyle et al. [32] presents toy networks reflecting the HOT approach to modeling the router-level Internet and compare it with the corresponding scale-free network (SFnet) models. This toy network called HOTnet, depicted in Fig. 13d, captures the kind of essential domain-specific tradeoffs that occur in engineering.

A HOT model of the Internet's router-level topology requires two general elements: constraints and functional objectives. First, the technological (bandwidth) and economic (costs) constraints on components such as routers and links and their interconnection restrict what topologies are feasible or possible. Second, network backbones, and router-level connectivity more generally, are subsystems in the larger, decentralized and layered Internet infrastructure. The consequence is that such subsystems can only be understood fully in terms of the functions that they provide to the higher layers of the protocol stack and the rest of the network. The main purpose for building physical network infrastructures at the lower layers of the protocol stack is to carry effectively the expected or projected overall traffic demand generated at the higher layers, which in turn is ultimately driven by users at the application layer. Such technological explanations are understandably avoided in physics but are essential for engineering networks, and this gap is responsible for much of the difference between the two approaches (HOTnet vs. SFnet) described in [32].

In contrast with scale-free and related methods, in which power laws have been a central focus of their 'emergent complexity' view, HOT seems to exploit power laws in completely different ways, having its focus on the 'organized complexity'. The resulting model seems to capture the true router-level structure of the Internet as it generates statistics more in line with the real Internet (e.g., supported by engineering data).
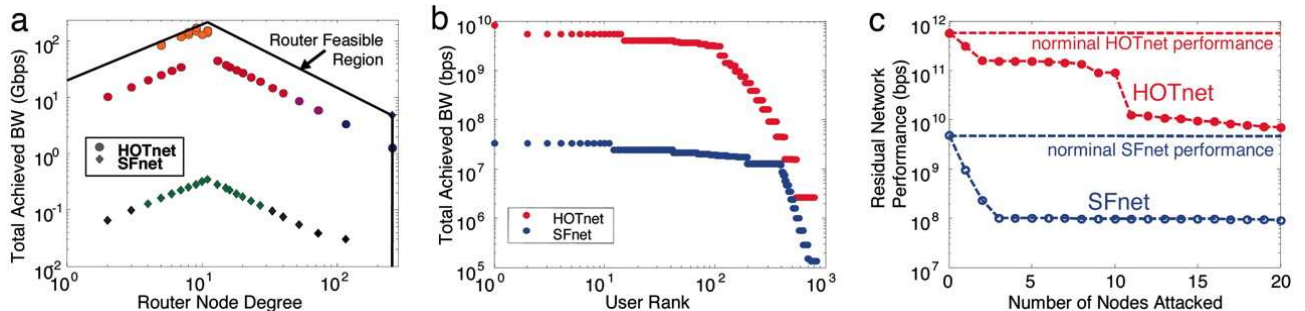

Fig. 14. HOTnet vs. SFnet. (a) Achieved router utilization: HOTnet is close to the 'efficient frontier', and SFnet operates significantly below this frontier, with the highly connected hub core router (the diamond in the right upper corner of the feasible region) representing a glaring bottleneck. (b) Achieved distribution of end-user bandwidths: HOTnet delivers a wide range of realistically different bandwidths to end users, whereas SFnet delivers uniformly low bandwidth to all users. (c) The Achilles' heel of the Internet: robustness of HOTnet vs. SFnet is measured as residual performance after successive deletion of worst-case nodes (deleting the worst 20 vertices corresponds to removing ≈ 20% of the routers). After [32].

Comparative studies involving the two network models, namely, HOTnet and SFnet revealed that SFnet demonstrates poorer performance in terms of the utilization of individual routers within the network. This is shown in Fig. 14a which illustrates the overall feasible configuration region encapsulating the conservation between router degree and router throughput. The inefficiency of the SFnet emerges due to the fact that the high-degree hubs become saturated and create severe bottlenecks, leaving the rest of the network with low overall utilization. In contrast, the connectivity in HOTnet is such that the core routers are highly used and therefore enable greater overall network throughput.

An additional view into the performance and utilization of these two networks is based on the distribution of bandwidth that is actually delivered to the end users under maximum-flow conditions, as shown in Fig. 14b. The distribution of achieved end-user bandwidth for HOTnet is highly variable but is considerably higher than the corresponding bandwidth received by users in SFnet, who get uniformly low bandwidth. Another issue (not quantified in [32]) is that no matter where the high-degree SF hubs were located physically, the link costs to connect them would be prohibitively high. In contrast, the design aspects incorporated into HOTnet seem to ensure that the deployed routers are used efficiently and the network is able to satisfy end-user bandwidth demands that are highly variable with relatively few long-range links. Therefore, HOTnet model seems

to outperform SFnet as it seems to incorporate a combination of high throughput, high router utilization, low link costs, and realistic end-user bandwidth.

In addition, Fig. 14c demonstrates that the SFnet graph is fragile to the deletion of worst-case vertices (here, worse case means highest degree) but resilient to failures/deletions of other vertices. In contrast, HOTnet is not only robust to worst-case deletions (here, worst cases are low connectivity core vertices) but also shows high tolerance to deleting other vertices. As shown in Fig. 13d, high-degree routers are located at the edges of a HOTnet graph. Thus, loss of edge routers disconnects only low-bandwidth users and has no other effect on overall connectivity. SFnet has such a poor nominal performance which is worst than HOTnet after the latter has sustained substantial damage. From this point of view, the Achilles' heel claim for SF networks does not seem to hold simply on the basis of having a scaling-degree sequence D. If we consider that the actual Internet is more like HOTnet than SFnet, it also has a great deal of additional robustness. In the case the real Internet consists of multiple redundant HOTnet-type backbones that are moderately loaded, the ability to reroute traffic will ensure that end users typically experience no discernible degradation in performance when core routers fail. In particular, the real Internet would never experience the type of separation of the network into disjoint components as claimed by the Achilles' heel hub argument unless massive losses occurred.

The study of Doyle et al. [32] manifests a different approach about the network robustness: the fact that protocols and feedback regulation and not simple redundancy enable this extraordinary robustness. The layered architecture of the Internet with its build-in feedback control enables its robust performance even in the presence of frequent disruptions and enormous heterogeneity. Although the lower layers of the protocol stack (physical, link and network layers in terms of fiber-optic cables and routers) have hard technological and economic constraints, each higher layer define its own, often unique connectivity resulting to increasingly virtual and unconstrained corresponding network topologies. All the components consisting the Internet have to obey the protocols, but due to the extensive feedback regulation, the overall system can tolerate otherwise enormous variability within these constraints and still deliver robust functionality to applications, which are also the least constrained components. The system, by design, is robust to components that 'fail off' by removal from the network, whether caused by focused attacks or other failures due to the fact that the complete absence of a component is allowed.

On the other hand, this strong robustness of the Internet coexists with an equally extreme fragility to components 'failing on', particularly by malicious exploitation or hijacking of the very mechanisms that confer its robustness properties at higher levels in the protocol stack. Worms, viruses, spam, and denial-of-service attacks remain familiar examples. This robust yet fragile tradeoff is a critical aspect of the Internet, and much research is devoted to enhancing these protocols in the face of new challenges. Thus, understanding Internet robustness requires a perspective that incorporates protocols, layering, and feedback regulation, and this view suggests that the most essential robust yet fragile features of the Internet actually come from aspects that are only indirectly related to graph connectivity. The robust yet fragile features of the Internet are the result of its highly evolved nature, and the key objective of the HOTnet approach has been to incorporate some of the most essential features in a simple model that can be used to highlight the potential dangers of ignoring such aspects entirely (as in the SFnet approach). Table II shows that SFnet and HOTnet are opposite in essentially every meaningful sense, and the real Internet network is much more like HOTnet.

TABLE II
SFNET VS. HOTNET AND THE REAL INTERNET. AFTER [32].

Feature	SFnet	HOTnet	Real Internet
High-degree vertices	Core	Periphery	Periphery
Degree distributions	Power law	Power law	Highly variable
Generated by	Random	Design	Design
Core vertices	High degree	Low degree	Low degree
Throughput	Low	High	High
Attack tolerance	Fragile	Robust	Robust
Fragility	High-degree/hubs	Low-degree/core	Hijack network

B. The World Wide Web (WWW)

The World Wide Web (WWW) is a complex communication system that operates on top of the Internet, which despite its increasing role in communication, it remains uncontrolled. From the perspective of networks, the WWW forms a huge directed graph consisting of hypertext documents (nodes) and hyperlinks (edges).

Until the late 1990s the World Wide Web was also considered as a random (exponential) network. However, this assumption was falsified by recent studies which spotted that the characteristics of the random network didn't apply to the behavior of the WWW. Instead, it was revealed that the WWW behaves as a graph following the power law degree distribution. Some researchers tried to explain such such scale-free link distributions as a result of network growth processes. The models and results carried out by a research team around Barabasi and Albert [13], [4], [17], [28], are based on the preferential addition of links to high degree nodes. On the other hand, Huberman and Adamic [60], [61] argue on the absence of correlation between

age and the number of hyperlinks which opposes the preferential attachment concept. Furthermore, a Bornholdt and Ebel study [62] provides a new approach in modeling $p(k)$ for incoming hyperlinks based on a model originally designed by Simon [63] in 1955 to explain power-law distributions in other systems. Some of the results carried out by the aforementioned studies are illustrated in the next few paragraphs.

Recent research efforts by Albert et al. [13] and [4] as well as Barabasi et al. [17] and [28] capture the scale-free behavior of the World Wide Web which arises by the observation that the probabilities $p(k)$ for k inbound or outbound links (i.e., links to or from a hypertext document, respectively) on the WWW significantly deviates from that of a randomly linked network. More specifically, studies [13] and [28] showed that the probabilities $p_{out}(k)$ and $p_{in}(k)$ that a hypertext document (web page) has k outgoing and incoming links follow a power law degree distribution over several orders of magnitude, that is, $p(k) \sim k^{-\gamma}$, with $\gamma_{in} = 2.1$ and $\gamma_{out} = 2.45$. These measurements were based on raw data obtained from the complete map of the nd.edu (University of Notre Dame) web site in 1999 which contained $\approx 3.25 \times 10^5$ documents and $\approx 1.47 \times 10^6$ hyperlinks. These observations are depicted in the following figure.
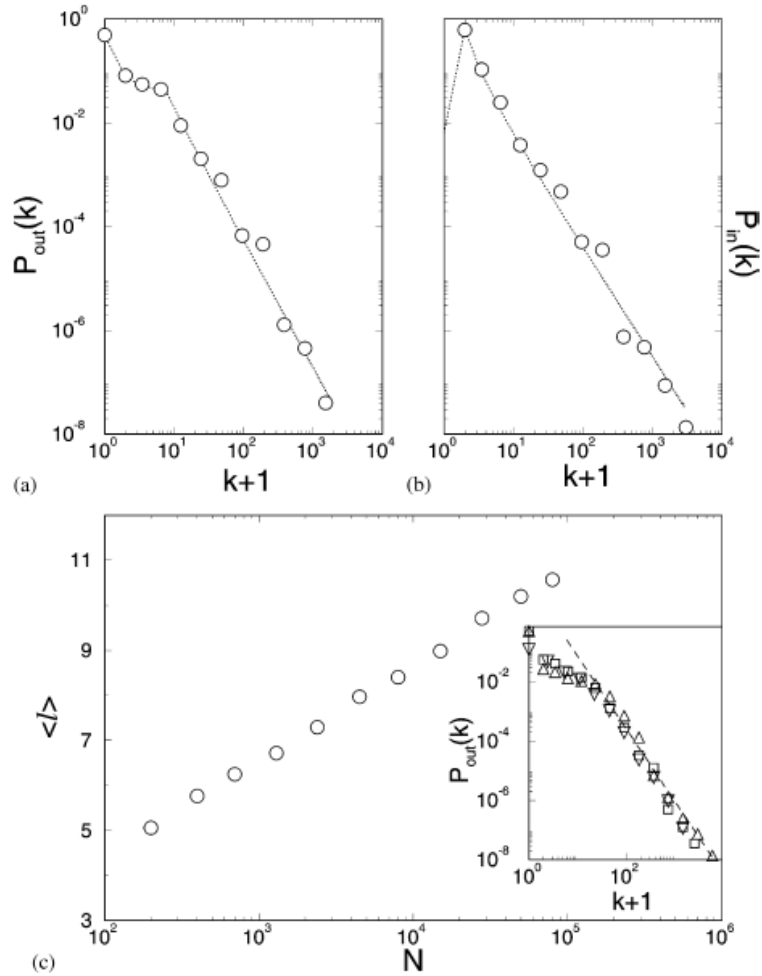

Fig. 15. The distribution of (a) outgoing hyperlinks (URLs found on an HTML document) and (b) incoming hyperlinks (URLs pointing to a certain HTML document). The dotted lines in (a) and (b) represent the analytical fits used as input distributions in constructing the topological model of the WWW, the tail of the distributions following $p(k) \sim k^{-\gamma}$, with $\gamma_{out} = 2.45$ and $\gamma_{in} = 2.1$. (c) Average of the shortest path between two documents as a function of the system size, as predicted by the BA model. To show that the power-law tail of $p(k)$ is a universal feature of the WWW, in the inset we show $p_{out}(k)$ obtained by starting from whitehouse.gov (squares), yahoo.com (upward triangles) and snu.ac.kr (downward triangles). The slope of the dashed line is $\gamma_{out} = 2.45$, as obtained from nd.edu in (a). After [28].

However, the observed values do not seem to agree with the predicted data. As already mentioned, the scale-free Barabasi-Albert (BA) model [17] involves a preferential attachment mechanism that constructs a network of non-directed links. This model predicts the WWW scaling exponent γ to be approximately equal to 2.9 while the measured values were significantly different ($\gamma_{out} = 2.45$ and $\gamma_{in} = 2.1$). On the other hand, the average measured shortest path l between two hypertext documents in the domain nd.edu was found to be 11.2. This value agrees well with the prediction $\langle l_{3 \times 10^5} \rangle = 11.6$ obtained from the BA model.

Huberman and Adamic ([60], [61]) studied a crawl of 2.6×10^5 sites, each one representing a different domain name and they found that the distribution of hyperlinks followed the power law as shown in Fig. 16(a). However, the researchers argue

against the 'rich get richer' phenomenon emerging from the preferential attachment mechanism of the BA model according to which older hypertext documents acquire more hyperlinks than newer ones and they increase their connectivity as the network grows. Whereas the BA model predicts that older documents have more time to acquire hyperlinks at a faster rate than newer documents, Huberman and Adamic's results carried out by querying the InterNIC database imply that there is no correlation between the age of a document and its number of hyperlinks as depicted in Fig. 16(b). Based on these findings, they proposed a new model according to which the number of new hyperlinks pointing to a document at each time step is a random fraction of the number of hyperlinks already pointing to it. Additionally, new documents, each with a different growth rate, appear at an exponential rate. This model yields scatter plots similar to Fig. 16(b), and can produce any power-law exponent $\gamma > 1$.
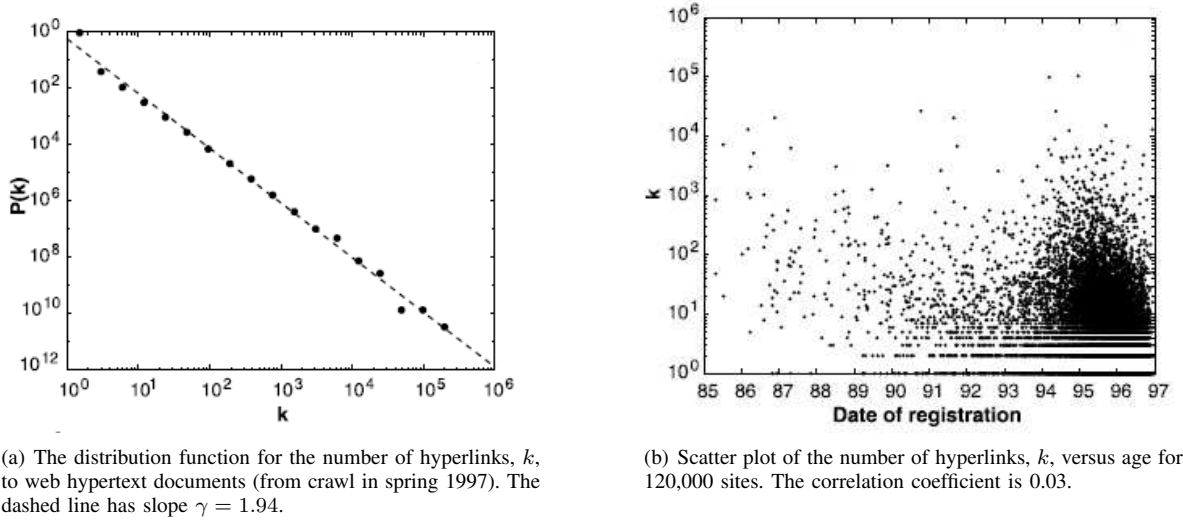

(a) The distribution function for the number of hyperlinks, k, to web hypertext documents (from crawl in spring 1997). The dashed line has slope $\gamma = 1.94$.

(b) Scatter plot of the number of hyperlinks, k, versus age for 120,000 sites. The correlation coefficient is 0.03.

Fig. 16.   After [61]

The two aforementioned models fail to predict a scaling exponent γ that agrees with the observed value. They either calculate a large exponent ($\gamma = 2.9$) with steep characteristics ([13], [28]), or provide a wide range of values $\gamma > 1$ ([61], [60]). Motivated by a simple and elegant model for scaling phenomena proposed by Simon in 1955 [63], Bornholdt and Ebel [62] created a model to capture the dynamics of the incoming hyperlinks. The proposed model sketches a simple stochastic process for adding new nodes and incoming links and is able to finely predict the scaling exponent $\gamma_{in} = 2.1$ in accordance with the observed values.

The Simon's model was originally proposed to explain the scaling behavior observed in distributions of word frequencies in texts or city population figures. It models the dynamics of a system of elements with associated counters which are incremented at a rate depending on their current values as new elements are constantly added. Bornholdt and Ebel adapted the Simon's model to the WWW network creating a new model which considers only incoming hyperlinks. In particular, they re-write its basic steps in the context of a growing network, defining class $[k]$ to be the set containing all nodes with identical connectivity k in terms of incoming hyperlinks. The cardinality of such a class $[k]$, i.e., the number of all nodes with connectivity k are denoted by $f(k)$. For the growth process, the following steps are iterated:

1) **Step 1:** With probability α add a new node and attach a link to it from a node chosen in an arbitrary way (ignore the source node of the directed link).
2) **Step 2:** Else add one link from an arbitrary node (again ignore the source node of the directed link) to a node j of class $[k]$ chosen with probability:

$$P_{[k]} = \frac{k \times f(k)}{\sum_i i \times f(i)} \qquad (2)$$

As stated in Step 1, α is the probability that a new node (document) is added. In the context of the WWW, the total number of web hypertext documents and web hyperlinks increases with time. Thus, using the AltaVista data sets from May and October, 1999 [7], Bornholdt and Ebel estimated the probability for adding a new web page (document) from the ratio of the observed increase in document creation rate and hyperlink creating rate to:

$$\alpha \approx \frac{68 \times 10^6}{732 \times 10^6} \approx 0.1 \qquad (3)$$

Although the generalization of Simon's model to the WWW network accurately predicts the power law exponent of $p(k)$ for incoming hyperlinks, this model has its faults. For example, it does not specify the origin of directed links, so its usefulness as a model for topological parameters other than $p(k)$ (e.g., average path length between pairs of nodes) is severely limited.

Viewed in this way, Barabasi and Albert's model is more robust, since it constructs a network in which each link has two well-defined ends, allowing the model to predict network quantities other than $p(k)$. However, we believe that the World Wide Web's structure is more complex than that assumed by all the models we have presented in this section, thus more intensive research efforts are expected towards this direction.

VII. CONCLUSIONS

All in all, in this technical report we give a detailed description of the basic concepts and properties exhibited in complex adaptive systems and discuss the most important network modeling paradigms emerged over the last few years. Furthermore, we study real communication networks from the perspective of complex systems. Attempts to decipher and explain the similarities between these two approaches may be fueled by the study of universal structural properties in real communication networks as well by as the theoretical understanding of evolutionary laws governing the emergence of these properties. In this report we take a holistic view of the design principles emerged from complex systems found in nature that can be applied to real communication networks such as the Internet and the World-Wide Web in order to cope with their complex attributes. Similarly, we refer to the increasing voiced need to model the pattern formations appeared in real communication networks in the context of similar complex patterns, since the pattern formations found in complex systems exhibit adequate degrees of robustness, resilience and self-organization. Finally we investigate the two more prevalent real communication networks that have been extensively studied in literature focusing on the validity and the effectiveness of the proposed models to capture the dynamics of the interaction among the constituent components of each network.

Recent research efforts by Erdos and Renyi, Watts and Strogatz, Barabasi and Albert, etc., have forced the idea that networks form randomly into a direction of organization and hidden order. The characteristics of random networks, small-world networks and scale-free networks can be observed in many levels of different disciplines. It is an imperative need to develop a new theoretical framework to help explain the complex and unpredictable behaviors of communication networks and design alternative network protocols which are provably effective and robust. Such a framework can serve as a starting point to develop a unified theory for complex systems, useful in explaining how the interaction between the individual components of such systems allows the emergence of a global behavior that would not be anticipated from the behavior of components in isolation.

Nothing in traditional science and engineering has prepared us to manage such systems, and our intuition offers little or no guidance: we need new ideas, new metaphors and new methods. Powerful new ideas and techniques can be found by studying the similarities between several complex systems found in nature. In this respect, complex systems science can be seen to bridge the gaps between the natural, social and formal sciences, and especially between engineering and the sciences. The natural sciences offer the scientific method to study the rules or laws of natural origin that govern the universe, based on 'natural' objects and phenomena - bacteria, ant/termite colonies, flocks of birds, oceans, atoms, etc. By comparison, engineering studies bridges, microchips, chemical processors and communication networks, phenomena resulting from human intervention in the natural world. From the point view of science, the complex behavior of a system is perceived as an emerging phenomenon to be understood, while engineering perceives an engineering problem to be tackled. The aim of complex systems science is to answer fundamental questions that cut across the boundaries between these complementary views of complexity, and to offer practical tools for solving concrete problems.

REFERENCES

[1] C. F. Kurtz and D. J. Snowden, "The new dynamics of strategy: Sense-making in a complex and complicated world," IBM Systems Journal, Vol. 42, No. 3, 2003.
[2] M. E. J. Newman, "The structure and function of complex networks," SIAM Review, Vol. 45, No. 2, 2003, pp. 167-256.
[3] R. Albert and A.-L. Barabasi, "Statistical mechanics of complex networks," Reviews of Modern Physics, Vol. 74, January 2002.
[4] R. Albert, H. Jeong and A.-L. Barabasi, "Error and attack tolerance of complex networks," Nature, 406, 2000, pp. 378-382.
[5] R. Cohen, K. Erez, D. B. Avraham and S. Havlin, "Breakdown of the Internet under Intentional Attack," Phys. Rev. Let. 86, April 2001, pp. 3682-3685.
[6] D. S. Callaway, M. E. J. Newman, S. H. Strogatz and D. J. Watts, "Network Robustness and Fragility: Percolation on Random Networks," Phys. Rev. Let. 85, December 2000, pp. 5468-5471.
[7] A. Z. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, J. L. Wiener, "Graph structure in the Web," Computer Networks, Vol. 33, June 2000, pp. 309-320.
[8] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," Phys. Rev. E. 66, December 2002.
[9] C. S. Holling, "Resilience and stability of ecological systems," Annual Review of Ecology and Systematics, Vol. 4, 1973, pp. 1-23.
[10] B. Bollobas, "Random Graphs," Academic Press, London, 1985.
[11] P. Erdos, and A. Renyi, "On Random Graphs I," Publ. Math. Debrecen, 6, 1959, pp. 290-297.
[12] D. J. Watts, and S. H. Strogatz, "Collective Dynamics of 'Small-World' Networks" Nature, Vol. 393, No. 4, pp. 440-442, 1998.
[13] R. Albert, H. Jeong and A.-L. Barabasi, "Diameter of the world wide web," Nature, 401, London, 1999, pp. 130-131.
[14] M. Faloutsos, P. Faloutsos and C. Faloutsos, "On power-law relationships of the Internet topology," Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication, 1999, pp. 251-262.
[15] Y. Tsai, C.-C.Lin, and P. -N.Hsiao, "Heavy tail Distribution in Email Network," Proceedings of the 2002 SoftCom, 2002, pp. 167-170.
[16] H. Ebel, L.-I. Mielsh, and S. Bornholdt, "Scale-free topology of e-mail networks," Physical Review E 66, 2002.
[17] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," Science 286, 1999, pp. 509-512.
[18] A.-L. Barabasi and E. Bonabeau, "Scale-Free Networks," Scientific American, May 2003, p.50, www.sciam.com.
[19] W. Aiello, F. Chung, and L. Lu, "A Random Graph Model for Power Law Graphs," Experiment. Math. Vol. 10, 2001, pp. 5366.
[20] B. Bollobas and O. Riordan. "The Diameter of a Scale-Free Random Graph," To appear in Combinatorica. Preprint available from World Wide Web (http://www.dpmms.cam.ac.uk/ omr10/).

[21] B. Bollobas and O. Riordan, "Mathematical Results on Scale-Free Random Graphs," In Handbook of Graphs and Networks, edited by Stefan Bornholdt and Heinz Georg Schuster, Weinheim: Wiley-VCH, 2002, pp. 134.

[22] C. Cooper and A. Frieze, "On a General Model of Web Graphs," In Proceedings of ESA, Lecture Notes in Computer Science 2161, Heidelberg: Springer-Verlag, 2001, pp. 500511.

[23] C. Cooper and A. Frieze, "Crawling on Web Graphs," STOC, 2002.

[24] B. Bollobas, O. Riordan, J. Spencer and G. Tusnady, "The Degree Sequence of a Scale-Free Random Graph Process," Random Structures and Algorithms Vol. 18, 2001, pp. 279290.

[25] P. G. Buckley and D. Osthus, "Popularity Based Random Graph Models Leading to a Scale-Free Degree Sequence," Preprint available from World Wide Web (http://www.informatik.hu-berlin.de/ osthus/).

[26] S. N. Dorogovtsev and J. F. F. Mendes, "Evolution of Networks," Adv. Phys. Vol. 51, 2002.

[27] D. J. Watts, "Small worlds: The Dynamics of Networks between Order and Randomness," Princeton Univ. Press, Princeton, NJ, 1999.

[28] A.-L. Barabasi, R. Albert, and H. Jeong, "Scale-free characteristics of random networks: the topology of the world-wide web," Physica A 281, 2000, pp. 69-77.

[29] New England Complex System Institute (NECSI) Webpage, http://necsi.org/.

[30] J. Goldstein, "Emergence as a Construct: History and Issues", Emergence: Complexity and Organization Vol. 1, 1999, pp. 49-72.

[31] E. Jen, "Stable or Robust? What's the difference?", Santa Fe Institute, http://discuss.santafe.edu/robustness/stories/StoryReader24, 2001.

[32] J. C. Doyle, D. L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, "The "robust yet fragile" nature of the Internet", Proceedings of the National Academy of Sciences of the United States of America, Vol. 102, No. 41, October 2005, pp. 14497-14502.

[33] J. M. Carlson, and J. C. Doyle, "Complexity and robustness," Proceedings of the National Academy of Science, Vol. 99, Suppl. 1, 2002, pp. 2538-2545.

[34] Internet Mapping Project: Map Gallery, Website: http://www.cheswick.com/ches/map/gallery/index.html, as appeared in Fubruary 2007.

[35] K. Claffy, T. E. Monk and D. McRobb, "Internet Tomography," Nature Web Matters, January 1999.

[36] G. Margulis, "Probabilistic characteristics of graphs with large connectivity," Prob. Peredachi Inform. Vol. 10, 1974, pp. 101-108.

[37] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Vertex overload breakdown in evolving networks," Phys. Rev. E. 65, Issue 6, 2002.

[38] M. E. J. Newman, S. Forrest, and J. Balthrop, "Why social networks are different from other types of networks," Phys. Rev. E. 66, Issue 3, 2003.

[39] H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, and A. L. Barabasi, "The large-scale organization of metabolic networks," Nature, London 407, 2000.

[40] J. A. Dunne, R. J. Williams, and N. D. Martinez, "Food-web structure and network theory: The role of connectance and size," Proceedings of the National Academy of Sciences of the U.S.A., Vol. 99, No. 20, 2002.

[41] L. da F. Costa, "Expanded Complex Networks and their Percolations," Phys. Rev. E. 70, 2004.

[42] The Complexity and Artificial Life Research Concept for Self-Organizing Systems, Website: http://www.calresco.org/, as appeared in March 2007.

[43] M. Eigen, "The Hypercycle: A Principle of Natural Self Organization," Springer Verlag, 1979.

[44] C. Gerhenson and F. Heylighen, "When Can we Call a System Self-organizing?" Proceedings of 7th European Conference on Advances in Artificial Life (ECAL 2003), Dortmund, Germany, September 2003, pp. 606-614.

[45] Y. Ishida, "The immune system as a prototype of autonomous decentralized systems: an overview," Proceedings of 3rd International Symposium on Autonomous Decentralized Systems (ISADS 97), Berlin, Germany, April 1997.

[46] E. Bonabeau, M. Dorigo, and G. Theraulaz, "Swarm Intelligence: From Natural to Artificial Systems," Oxford University Press, 1999.

[47] S. K. Das, N. Banerjee, and A. Roy, "Solving Otimization Problems in Wireless Networks using Genetic Algorithms," in Handbook of Bio-inspired Algorithms, 2004.

[48] F. Dressler and B. Krger, "Cell biology as a key to computer networking," German Conference on Bioinformatics 2004 (GCB'04), Bielefeld, Germany, Abstract and Poster, October 2004.

[49] B. Krger and F. Dressler, "Molecular Processes as a Basis for Autonomous Networking," IPSI BgD Transactions on Advances Research: Issues in Computer Science and Engineering, Vol. 1, January 2005, pp. 43-50.

[50] B. A. Kadrovach and G. B. Lamont, "A Practicle Swarm Model for Swarm-based Networked Sensor Systems," Proceedings of 2002 ACM Symposium on Applied Computing, Madrid, Spain, 2002, pp. 918-924.

[51] C. Mller-Schloer, C. von der Malsburg, and R. P. Wrtz, "Organic Computing," Informatik Spektrum, Vol. 27, August 2004, pp. 332-336.

[52] R. Muraleedharan and L. A. Osadiciw, "Sensor Communication Network Using Swarm Intelligence," Proceedings of 2nd IEEE Upstate New York Workshop on Sensor Networks, Syracuse, NY, USA, October 2003.

[53] G. Di Caro and M. Dorgio, "AntNet: Distributed Stigmergetic Control for Communication Networks," Journal of Artificial Intelligence Research, Vol. 9, 1998, pp. 317-365.

[54] L. Li, D. Alderson, J. C. Doyle, and W. Willinger, "Towards a Theory of Scale-Free Graphs: Definition, Properties and Implications," Internet Mathematics. In Press. (2006)

[55] G. Siganos, M. Faloutsos, and C. Faloutsos, "The Evolution of the Internet: Topology and Routing," Technical Report UCR-CS-2002-05065, May 2002.

[56] Q. Chen, H. Chang, R. Govindan, S. Jamin, S. J. Shenker, and W. Willinger, "The Origin of Power-Laws in Internet Topologies Revisited," Proceeddings of 21st Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2002, Vol. 2, pp. 608-617.

[57] B. Cheswick, and H. Burch, "Internet mapping project," Wired Magazine, December 1998. See http://cm.belllabs. com/cm/cs/who/ches/map/index.html.

[58] R. Govindan, and H. Tangmunarunkit, "Heuristics for internet map discovery," Proceedings of IEEE INFOCOM, Tel Aviv, Israel, March 2000.

[59] J.-J. Pansiot, and D Grad, "On routes and multicast trees in the Internet," ACM Computer Communication Review, Vol. 28, No. 1, January 1998, pp. 41-50.

[60] B. A. Huberman, and L. A. Adamic, "Growth dynamics of the World-Wide Web," Nature, 401, London, 1999, pp. 131.

[61] L. A. Adamic, and B. A. Huberman, "Power-Law Distribution of the World Wide Web," Science, Vol. 287, No. 5461, March, 2000, pp. 2115a.

[62] S. Bornholdt, and H. Ebel, "World Wide Web scaling exponent from Simons 1955 model," Physical Review E, Vol. 64, 2001.

[63] H. A. Simon,"ON A CLASS OF SKEW DISTRIBUTION FUNCTIONS," Biometrika, Vol. 42, 1955, pp. 425-440.