Complex networks and social network analysis in information fusion

Pontus Svenson
Data and Information Fusion
Swedish Defence Research Agency
SE 164 90 Stockholm Sweden
ponsve@foi.se

Abstract - ***Complex networks has recently emerged as an independent area of study. It has connections to random graph theory from mathematics as well as to social network analysis and recent work by physicists interested in understanding the behaviour of large, interacting networks. Network models are important for information fusion in two manners. First, the command and control networks of distributed information fusion systems must be designed in such a way that they are both robust against failures and attacks and so that information spreads quickly in them. Second, network models and social network analysis is an important tool to use when analyzing the opponents facing us in international operations. In this paper, we describe the basics of complex network models and point out how they can be used for both these purposes. By simulating several different network architectures, it will be possible to choose the best.***

Keywords: complex networks, social network analysis, distributed fusion, information fusion, complex adaptive systems.

1 Introduction

In order to provide good decision support systems for ths tasks that face the Swedish Defence forces today and tomorrow, it will be necessary to integrate knowledge of *complex networks* in the information fusion systems.

Information fusion [1] deals with filtering the information avalanche from sensors that commanders will face in the future network-based defence. The network will consist of large numbers of sensor platform and processing nodes. In order to ensure that the command and control networks are robust against enemy attacks and component failures, it is necessary to design them so that they can withstand both enemy attacks and component failure. Additionally, they must be designed so that information, orders, and service-requests are spread as fast as possible.

Future command and control systems will also need to be designed to facilitate the use of distributed fusion. There will be several local fusion nodes that gather and fuse data collected at different places in the network of platforms. This means that in addition to the robustness and communication requirements mentioned above, the specific fusion algorithms chosen might also impose constraints on the network used.

It is important to distinguish between the physical and the logical communication networks. The physical network consists of the actual hardware that transmits information and will not be discussed here. The logical communication network uses the physical to transmit information between sender and recipient.

Knowledge of network models and methods for analyzing them is also needed in order to be able to model the enemies that we are facing. In the international operations that the Swedish defence forces are performing today and in the future Nordic Battle Group, we face new kinds of enemies and perform different kinds of tasks. Instead of a technically advanced, hierarchically organized enemy, our opponents will be gangs, clans, guerillas, and other kinds of loosely organized groups. In order to analyze the behaviour of such groups, it is necessary to use methods from social network analysis [2, 3]. By modelling the groups and individuals we are facing in a network, we can determine many important properties of the opponents.

Here, we present various models of networks and discuss how they could be used for both modelling loosely organised enemies and for improving the communication networks in a distributed information fusion system.

For more information on complex network, we refer to [4, 5, 6, 7]

This paper is outlined in the following way. Section 2 gives a brief overview of various types of network models. Section 4 lists some of the most important social network measures and discusses how they could be used to improve situational awareness, while section 5 presents suggestions for how to achieve increased synchronization in command and control systems. The paper concludes in section 6.

2 Network models

2.1 Simple networks

In order to properly describe a general network or graph, two things are needed. First, we need a list

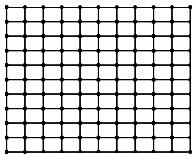


Figure 1: A square lattice.

of the *nodes* of the graph. The nodes can be named and have various properties associated to them, but for describing the graph it is enough that they can be enumerated from 0 to $N-1$. Second, we must know which nodes are connected to which. This is most easily thought of as a list of *edges* (i,j) that are connected. Each edge can have various properties associated to it (*e.g.*, a weight w_{ij}). Most often, the graph is described using the *neighbour matrix* or *contact matrix* A_{ij}, whose entries are are non-zero if and only if nodes i and j are linked. It is sometimes convenient to consider the graph as a function $\phi(i)$ that gives a list of the neighbours of node i.

Edges can be either directed (meaning, for example, that an edge (i,j) can only transmit information from i to j) or undirected. A graph is connected if there is a chain of edges connecting any pair of nodes in it. A natural generalisation of graphs is to replace the edges by triples i,j,k or even n-tuples. Such structures are called hypergraphs. An important application of hypergraphs is to model sets of individuals that only interact in a group, never individually, for example, a group of rioters that meet at a certain place.

The simplest kinds of networks are regular, like the one shown in figures 1.

%leavevmode

All regular lattices have some features in common. By looking at the graphs in figure 1 it is for instance apparent that these graphs are clustered, in the sense that if we remove one node, its neighbours will still have a short path between them. Another interesting characteristic of regular lattices is that the average distance between nodes is quite large. For a lattice with N sites in D dimensions[1], it grows as $N^{1/D}$.

A natural extension of the regular lattice is to consider other graphs where all nodes are equivalent (i.e., have the same neighbourhood). The simplest example of such a graph is the complete graph with N nodes, K_N. This consists of N nodes where each node is connected to each of the other (so the graph has $\left(\begin{array}{c} N \\ 2 \end{array}\right)$ edges).

2.2 Classical random graphs

Traditionally, two different models of random graph processes have been used [8]. In the first model, $\mathcal{G}(N,p)$, each possible edge (i,j) is considered and included in the graph with a probability p. The other model, $\mathcal{G}(N,M)$, instead selects without replacement M of the $\left(\begin{array}{c} N \\ 2 \end{array}\right)$ possible edges. Note that these models are *not* completely equivalent. For the latter model, the graph is guaranteed to have exactly M edges, while the number of edges is a stochastic variable for the former. In the thermodynamic limit of $N, M \to \infty$, choosing

$$M = p\left(\begin{array}{c} N \\ 2 \end{array}\right)$$

gives graphs that should share all relevant properties. An important quantity characterizing different random graphs is their *connectivity* or *average degree* γ, which measures the average number of neighbours that the nodes have. For random graphs with N nodes and M edges, this is given by $\gamma = 2\frac{M}{N} = p(N-1)$ for the two ensembles.

Graph theory is a fascinating mathematical subject with many deep results; see for instance [8, 9]. One of the most interesting results is that there is a phase transition as the connectivity γ of a random graph grows. For small γ, the random graph consists of many isolated trees[2] of nodes. At $\gamma = 1$ this suddenly changes and a giant component emerges. The size of the giant component scales linearly with the number of nodes, N. This percolating transition is somewhat surprising — note that the graph can not be connected until it has a connectivity of at least $2(N-1)/N$. Another important result is that the average path-length between two nodes scales as $\log N$ for large N.

The random graph model, however, is not sufficient to describe many naturally occurring networks.

2.3 Small world graphs

There are many different kinds of networks in Nature. Perhaps the first that comes to mind is the social network of a society. Here each node represents a person, while there is an edge between two persons if they know each other. What does this graph look like? It is very unlikely that it would be a regular lattice — our acquaintances are not ordered in such a simple way. The social network however shares an important feature with regular lattices: they are clustered. Clustering means that there is a high probability that two neighbours of a given node also are direct neighbours themselves. An alternative way to think about it is to consider the average path length between two neighbours of a node i. Since both nodes are neighbours of i, this is obviously smaller than 2. If node i is now removed from the graph, we have to find a new shortest path between the nodes. If this new path length is still small, the graph is clustered. All regular lattices are obviously clustered, and social networks are clustered too: if person A knows persons B and C, there is a high probability that B and C will also know each other.

Real social networks are clustered in several ways: everybody's acquaintances can be divided into several distinct clusters, *i.e.*, the people one knows from work all know each other, while the overlap between this

[1] The simplest example to think of is $\mathcal{Z}_l^D$, where nodes are placed at integer coordinates and edges link nodes that whose coordinates differ by ± 1 in exactly one dimension. Choose $l = N^{1/D}$ to get N nodes.

[2] A tree is a connected graph without loops.

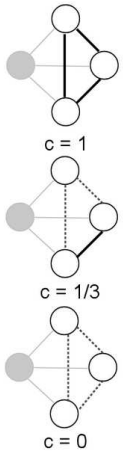


Figure 2: Examples of clustering coefficients. We wish to calculate the clustering coefficient of the grey node on the left, which has three neigbours (indicated by grey lines). The dark lines show the edges in the neighbourhood of the grey node that actually appear in the graph, while the dotted lines show all three possible such edges.

group and one's neighbours often is zero. This can be modelled by allowing the network to have edges of different kinds, or by superimposing several different networks on top of each other.

Mathematically, we can measure the degree of clustering in a graph by the *clustering coefficient*, C, defined as the average over all nodes of the local clustering coefficient C_i. For a given node i, consider its immediate neighbourhood, *i.e.*, the set of nodes to which it is linked. The *local clustering coefficient* is now given by the fraction of all possible edges between nodes in the neighbourhood that actually appear in the graph. Figure 2 shows an example that should make the definition clear.

Another important feature of social networks is the so called small world effect: When two strangers meet, it sometimes happens that the two people turn out to have mutual acquaintances.

The idea behind small world networks was first introduced by Milgram [10] in 1967. Milgram's experiment consisted of studying the path of letters addressed to a stockbroker in Pittsburgh. The letters were given to people in rural Nebraska with the rule that the current holder of the letter must hand it over to somebody with whom they were on a first-name basis. The average number of links in the chain of people between Nebraska and Pittsburgh was six, hence the term "Six degrees of separation". The number is of course not exact (a severe shortcoming of the experiment was that only one third of the letters were actually delivered!), but the phenomenon that people are linked via a small number of nodes has been verified by later, more careful experiments (e.g, [11]).

The small world effect has later been popularised by occurring in media, such as the movie "Six Degrees of Separation". There are also various amusing games using the same concept, such as the web site `http://www.cs.virginia.edu/oracle/` where a user can find the distance between an arbitrary actor and Kevin Bacon. Actors here represent the nodes of the graph, and two actors are linked if they have participated in the same movie. It should be noted that the actors represented in the database are American and European ones. The network of actors in Indian movies, for instance, probably has few connections to this.

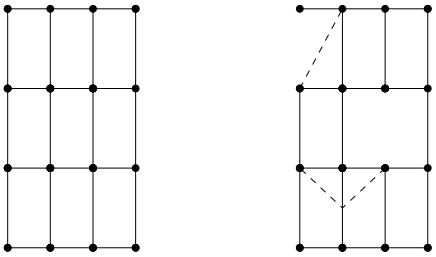


Figure 3: This figure shows the construction of a small world starting from a $2D$ square lattice (left). In the right figure, two edges have been rewired and are shown as dashed lines.

Another example are the Erdös numbers. Named after the famous mathematician Paul Erdös [12], these are defined recursively: Erdös has Erdös number 0; a person has Erdös number $n+1$ if they have co-authored a paper with somebody who has Erdös number n (there are at least 507 persons with Erdös number 1; see the web site `http://www.oakland.edu/~grossman/erdoshp.html`).

Regular lattices do get shorter and shorter distances between nodes as the dimensionality increases (the diameter scales as $N^{1/d}$ for a d-dimensional lattice with N nodes, so it decreases if we increase d and keep N constant), but this is still too large to explain the small world effect. Instead, new graph models are needed.

A small world graph is intermediate between a regular lattice and a random graph — it has both clustering (like a regular lattice) and short maximum distances (like the random graph). It is constructed by considering in turn all the bonds (i, j) of a start graph (most often a regular lattice) and with some probability p replacing them with (i, k), where k is a new, randomly chosen, node. So by changing the rewiring probability p we can interpolate between the regular lattice and a random graph. An example of a small world obtained by rewiring the square lattice is shown in figure 3. Note that the small world for $p = 1$ differs slightly from a random graph, since all nodes are guaranteed to have a local connectivity of at least $\gamma/2$ where γ is the connectivity of the regular lattice. The distribution of connectivities is more broad for the small world with $p = 1$ than for the corresponding random graph.

The advance of the Internet and other communications networks has highlighted the need to be able to not only describe but also design networks that communicate efficiently. Efficiently here has two distinct meanings — the obvious one that a message from A to B should be transmitted along the shortest possi-

ble path, and also an equally important one that the network should be fail-safe. If a node suddenly disappears, it should be possible to quickly find alternate paths between the rest of the nodes that don't involve the dead node. A very clear definition of small world behaviour in terms of *efficiency* has been given by Latora and Marchiori [13]. They measure the local efficiency as the time needed to communicate in the network, assuming unit velocity of signal propagation. The efficiency between two nodes is thus

$$\epsilon_{ij} = \frac{1}{d_{ij}} \tag{1}$$

where d_{ij} is the shortest distance between nodes i and j and $d_{ij} = \infty$ if there is no path between the nodes. The global efficiency is the average of this over all pairs of nodes in the graph. A high global efficiency corresponds to a small diameter of the graph. The local efficiency for a node i is calculated as an average of ϵ_{ik} over all neighbours k of i, and the total local efficiency of the graph is then the average of this over all nodes. The local efficiency is a measure of the fault tolerance of the network.

In addition to efficiency and clustering, there are a large number of measures that can be used to characterize a graph's properties. Many of these measures come from sociology, and have been used to determine, *e.g.*, the influence and power of individuals in different social networks. Others come from computer science, or have been suggested by physicists.

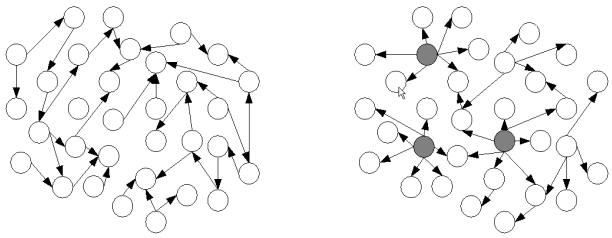
A small world graph still has the same poissonian distribution of node-connectivities as random graphs. A different class of networks are the so-called scale free graphs, which instead have a power-law distribution.

3 Scale free and growing graphs

A network is called scale free if there is no characteristic length scale in it. In contrast to lattices, whose characteristic length scale is the lattice spacing, a scale free graph divides its edges unequally among its nodes: the degree distribution follows a power-law. This means that there are a few nodes (called hubs) that have very many edges, whereas most of the nodes have very few. An important characteristic of scale free networks is that while they are robust against accidental failures, they are very vulnerable to deliberate attacks against hubs.

A deterministic model for generating scale free graphs has been introduced by Barabási and Ravasz [14]; this model generates the graph by iteratively replacing nodes with small graphs, in a manner similar to the construction of self-similar fractals.

There are many models of growing networks. In these models, one starts with a single node at time $t = 0$. In each new time-step a new node is added to the graph and a new edge is created that connects this node to one of the older ones with a probability that depends on the connectivity of that node. If this probability is simply proportional to the node's connectivity (k), the model is reduced to the scale-free graph



(a) Random network (b) Scale-free network

Figure 4: This figure shows the difference between a random network and a scale free network. Note the presence of hubs (nodes with many neighbours) in the right network.

model of Barabasi and Albert [15]; see also [16]. It has been shown that the case where the probability is proportional to the connectivity is the *only* case which also leads to a power-law for the distribution of connecitivities in the entire graph [17]. If the probability is proportional to k^γ for any $\gamma \neq 1$, we get stretched exponential (if $\gamma < 1$) distributions or graphs where the majority of the edges share a common central node (for $\gamma > 1$).

The best example of a growing network is the Internet — each node that is added could be interpreted either as a new computer that is connected to it or a new web-site that is created. The edges created between this node and the older ones are then the hyperlinks that the addition of a new site entails. It turns out, however, that a more complicated model is needed to model the Internet, see below.

So-called acquaintance networks, such as the Erdös graph, have been studied, among others, by Newman [18]. Such network have the characteristic that a small number of nodes have many edges. These nodes cannot be ignored when studying communication on such networks.

The crucial point of Newman's new model is that the probability distribution of the number of neighbours, that the neighbours of a specified node has, is not independent of that node. In social networks, a node with very few neighbours is likely to be linked to other nodes that also have few neighbours; while a node with many neighbours have similar nodes among its neighbours.Clustering is important for this calculation. If we know both the degree distribution[3] and the clustering coefficient of a network, it is possible to calculate the number of neighbours at distance two from a given node. This is important to know when conducting research on social networks.

For example, we might be interested in how a network of terrorists grows in a country.

A very interesting approach to the problem of analysing growing networks has recently been introduced by Kleinberg and co-authors [19]. Perhaps the most prominent example of a growing network today is the Internet. The paper examines data representing routers on the Internet for a tvo year period, and

[3] *i.e.*, the probability that a node has a certain number of neighbours

finds that the link-density of the network increases with time, *i.e.*, that the number of edges $e(t)$ is related to the number of nodes $n(t)$ by a power-law

$$e(t) \propto n(t)^a, \tag{2}$$

with $a = 1.18$.

Having such a relation between $e(t)$ and $n(t)$ means that the connectivity $\gamma = \frac{e}{n}$ is time-dependent, in sharp contrast to most models of graphs and networks. The authors find a similar relation (but with different a's) also for three different kinds of citation networks. In addition to the super-linear scaling of edges with nodes, they also find that the average distance (also, somewhat non-standard, referred to as the effective diameter) between nodes *decreases* as a function of time. Recall that the average distance for a random graph grows as the logarithm of the number of nodes. While the two observations at first glance seem to be related, the authors note that it is possible to construct graphs that satisfy one of them but not the other. For large graphs, it is not practical to compute the diameter exactly. Instead, various approximate algorithms can be used. Since the shrinking diameter propery is very surprising, the authors check that their result is robust by using several different such approximations to calculate the diameter. They also check for errors due to the presence of a giant component; the shrinking diameter is present also if the calculation is restricted to just the giant component.

The paper presents several simple models that exhibit the densification property, and also give one model, the *Forest Fire model* that possessess both it and also displays shrinking effective diameters.

The Forest Fire starts from a graph with just one node and then adds one additional node at each time-step. At time t, let G_t be the current graph and v the added node. A node $w \in G_t$ is now selected randomly, and an edge $v \rightarrow w$ is formed. Most graph models would now continue by selecting another w and possibly adding an edge to it. In contrast, the Forest Fire model selects a random number of the nodes in G_t that were linked to w, and adds edges from v to these nodes. This process is then repeated recursively for each of those nodes. (The process terminates if it reaches a node that has already been encountered. It is also possible to distinguish between out- and in-links when selecting the neighbours of w; see the paper [19] for details.) Intuitively, the graph is generated in a similar way as friendships are formed: a newcomer finds one friend and with a certain probability becomes friends also with the friend's friends, and so on. The name Forest Fire comes from a certain similarity to lattice cellular automata models used for studying Forest Fires. A natural extension of the model is to select several starting points w at each time-step.

4 Using social network analysis methods for achieving situational awareness

Social network analysis [2, 3] was introduced by sociologists as a means of analyzing communications and relations in groups. It is a quite mature area of research, which has produced a large set of different measures to be used when analyzing a network. Here we can only discuss some of the various measures that can be used. A more extensive list can be found in [20].

In order to achieve situational awareness, it is necessary to have a clear picture of who the opponents are. Level 2 information fusion is sometimes said to deal with determining the relations between the objects that are output by the level 1 fusion system. In conventional war, the relations between the observed entities are given by a doctrine that the enemy follows. For example, the background knowledge that an armoured company consists of four platoons, each platoon having 3 tanks in it, allows us to automatically aggregate sensor observations into situation pictures of platoons and companies [21]. In operations other than war, the old methods that relied on doctrinal information can no longer be used. One approach for reducing the amount of information presented to the user in these kinds of environments is to classify groups of objects based on what capabilities or resources they have [22]. In some situations, however, it might be useful also to classify the observed entities based only on their relations to other entities. This could be the case, for example, if we in a peace-enforcing operation are facing several different opponents whose alliances between them shift from day to day. Such classification could be performed by analyzing the social networks of the opponents. Commanders and analysts could also be helped by including support for "what if" exploratory analysis in the system. For example, an analysts could use social network analysis methods to determine the possible paths of communication between two currenly opposed groups. These paths could then be put under surveillance, so that we would get some warning if the two groups are negotiating.

The simplest measures that can be applied to a network simply measure the number of connections that each node has. Another approach is to determine the minimum distance to other nodes in the network, i.e., determining how central the node is in the network. For some networks (such as the scale free networks), this can give a reasonably good measure of the importance of a node. However, for many social networks it gives quite misleading results.

A class of more advanced measures instead look at the flow in the network. In some networks, all links are associated with a maximum capacity that can be transported along it. This is the case, for example, for communications networks — the bandwidth imposes limits on the amount of data that can be sent along a link. For other networks, the flow algorithms assume that the capacity of each link is equal to 1.

The simplest flow-oriented measure simply determines the shortest paths between all nodes in the network. A node's importance is then given by the number of such shortest paths that pass it. This measure is called the betweenness centrality measure.

Betweenness centrality, however, can also give misleading results. By focusing on only the shortest path, beteenness misses many cases where there are several short paths between nodes. An improved measure is the max flow centrality measure, which determines all the possibly paths between all the nodes in the network. Each node is then ranked according to the total amount of flow that passes through it.

(The measures that measure flow can of course also be used for determining the value of different edges in the network.)

Yet another way characterizing a social network is to look at the community structure in it. A community is loosely defined as a part of the network whose nodes have more connections within themselves than to nodes that are outside it. It is related to the concept of a clique, a maximally connected subgraph, but differs since it does not require full connectivity. (It must be mentioned that the exact definition of a community is of course application-dependent.) Recently, several fast algorithms for determining the community structure of a network has been published [23, 24, 25, 26]. Such algorithms could be used when analyzing, for example, the media network in a country in order to determine which newspapers are independent of each other.

By using such community finding algorithms, it is possible to do classification of groups of rioters in real time. By observing individuals in the crowd and determining which communities they belong to according to data in known data bases, the situation pictures can be augmented with information on the believed allegiances of the participants in the riots.

In addition to being useful when facing loosely organized opponents in international operations, the approach presented here can also be used for counterterrorism analysis or by police that are investigating gangs of criminals.

A necessary future extension of standard social network analysis is to include support for analysing networks that contain uncertain links. The uncertainty in the links could arise from problems with getting accurate data on the communication patterns of the opponent which we are trying to analyse. We believe that *random sets* will prove useful for this. When analysing dark networks, it will most likely be impossible to get accurate representations of the social networks. Simulation will be an important tool in such cases. By simulating all possible network structures that are consistent with the known properties of the opponent, it will be possible to provide the user with better situational awareness.

5 Synchronization

How we achieve synchronization of intent among own units and coalition partners is an important and difficult question whose answer depends more on the organization and methodology used than on technical innovations and systems. Nevertheless, it is interesting to study how various technological system could help facilitate such synchronization. For example, how should the communication networks be constructed to improve the speed by which commander's intent and situation pictures are spread?

One way of answering this question is by studying simple models of fusion and command nodes on various networks. By using a simple model that can be simulated (or possibly even solved exactly) on different kinds of networks and study the differences in behaviour that arise, we can determine at least qualitatively what the differences between the networks are.

In order to use the results from such experiments for designing the military networks, it is of course necessary that the model is sufficiently similar to real fusion system.

One possible model that could be used for such experiments is the so-called *voter model* version of the Ising model. The voter model consists of a number of agents that vote either "yes" or "no". How they chose to vote depends on how their neighbours vote. In the most simple version of the model, each agent selects one of its neighbours randomly and adjusts its vote to be the same. There are also versions with more interesting interactions.

6 Discussion

Most suggestions for network-based defence system rely on a service-based architecture. In such systems, it is necessary to match the commander or analyst that is requesting a service with the platform or fusion node that can provide it. In order to do this as efficiently as possible, it is necessary to design the logical communication networks so that this type of communication is facilitated. Different network topologies can have significantly different impact on the ease with which information is found in a network.

As stated in the introduction, it is important to know how to model networks for several different reasons [27]. We must be able to analyze the enemy's social and organizational structures as well as their communication networks. We must also be able to model the interaction network that will emerge when our commanders and operators communicate with each other. Not all of this communication will emanate from the hierarchical structure of the task-force: if two people know each other, they will most likely communicate (by phone, email, or instant messaging) even if they are not supposed to. Instead of banning such communication, the network-based defence system needs to exploit it and use it in order to achieve synchronization and fast information spreading. In order to do this as well as possible, it is necessary to model and

simulate the emerging networks.

References

[1] D. L. Hall and J. Llinas, editors. *Handbook of Multisensor Data Fusion*. CRC Press, Boca Raton, FL, USA, 2001.

[2] John P Scott. *Social Network Analysis: A Handbook*. SAGE Publications, 2nd edition, 2000.

[3] S. Wasserman and K. Faust. *Social Network Analysis: Methods and Applications*. Cambridge University Press, 1994.

[4] S. N. Dorogovtsev and J. F. F. Mendes. *Evolution of Networks: From Biological Nets to the Internet and WWW*. Oxford University Press, 2003.

[5] Romualdo Pastor-Satorras and Alessandro Vespignani. *Evolution and Structure of the Internet : A Statistical Physics Approach*. Cambridge University Press, 2004.

[6] Eli Ben-Naim, Hans Frauenfelder, and Zoltan Toroczkai, editors. *Complex Networks*, volume 650 of *Lecture Notes in Physics*. Springer, 2004.

[7] Romualdo Pastor-Satorras, Miguel Rubi, and Albert Diaz-Guilera, editors. *Statistical Mechanics of Complex Networks*, volume 625 of *Lecture Notes in Physics*. Springer, 2003.

[8] Béla Bollobás. *Random Graphs*. Academic Press, New York, 1985.

[9] Béla Bollobás. *Graph Theory: An Introductory Course*. Springer-Verlag, New York, 1979.

[10] S. Milgram. The small world problem. *Psychology Today*, 2:60, 1967.

[11] C. Korte and S. Milgram. Acquaintance linking between white and negro populations: Application of the small world problem. *J. Personality and Social Psychology*, 15:101, 1970.

[12] P. Hoffman. *The Man Who Loved Only Numbers*. Hyperion, New York, 1998.

[13] Vito Latora and Massimo Marchiori. Efficient Behaviour of Small-World Networks. *Phys. Rev. Lett.*, 87:198701, 2001.

[14] A-L. Barabási and E. Ravasz. Deterministic Scale-Free Networks. eprint cond-mat/0107419.

[15] A. L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286:509, 1999.

[16] R. Albert and A-L. Barabási. Statistical Mechanics of Complex Networks. eprint cond-mat/0106096.

[17] P. L. Krapivsky, S. Redner, and F. Leyvraz. Connectivity of Growing Random Networks. *Phys. Rev. Lett.*, 85(21):4629, 2000.

[18] Mark E. J. Newman. Ego-centered networks and the ripple effect. eprint cond-mat/0111070.

[19] J. Leskovec, J. Kleinberg, and C. Faloutsos. Graphs over time: Densification laws, shrinking diameters and possible explanations. In *Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, page 177, 2005.

[20] L. da F. Costa, F. A. Rodrigues, G. Travieso, and P. R. Villas Boas. Characterization of complex networks: A survey of measurements. eprint cond-mat/0505185 (http://www.arxiv.org/abs/cond-mat/0505185), 2005.

[21] Simon Ahlberg, Pontus Hörling, Karsten Jöred, Göran Neider, Christian Mårtenson, Johan Schubert, Hedvig Sidenbladh, Pontus Svenson, Per Svensson, Katarina Undén, and Johan Walter. The ifd03 information fusion demonstrator. In *Proc 7th International Conference on Information Fusion*, 2004.

[22] Pontus Svenson. Capabilities-based force aggregation using random sets. In *Proc 8th International Conference on Information Fusion*, 2005.

[23] M E J Newman and M Girvan. Finding and evaluating community structure in networks. *Physical Review E*, 69:026113, 2004.

[24] M E J Newman. Fast algorithm for detecting community structure in networks. *Physical Review E*, 69:066133, 2004.

[25] Aaron Clauset. Finding local community structure in networks. *Physical Review W*, 72(026132), 2005.

[26] Aaron Clauset, M. E. J. Newman, and Cristopher Moore. Finding community structure in very large networks. *Physical Review E*, 70:066111, 2004.

[27] FMV. Teknisk prognos 2005. FMV dokument 57900/2005.