Statistically robust design for the all-electric ship from a network theoretic perspective

Statistically Robust Design for the All-Electric Ship from a Network Theoretic Perspective

Josh A. Taylor and Franz S. Hover
Department of Mechanical Engineering
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139
Email: jatl@mit.edu, hover@mit.edu

***Abstract*— Recent progress in understanding the robustness properties of large-scale networks leads one to consider how such results can inform design of the all-electric ship. Network robustness seems to be correlated with certain statistical properties, which may give rise to a natural design procedure wherein the statistics of the network become the main design goals. This would represent a departure from the current design paradigm. We have performed systematic cascading failure simulations based on a notional cruiser topology, in comparison with equal-cost random and scale-free networks. Although preliminary, our results show that some advantage can be obtained through the alternative designs.**

I. Introduction

Deterministic design of large-scale, dynamic systems poses increasingly intractable questions about the complex interactions of components and subsystems. Simulations with or without hardware in the loop are the usual method for uncovering weaknesses in both steady state operation and in response to unexpected component failures, but in very large systems such simulations are prohibitively expensive, inaccurate, or simply impossible. The all-electric ship as a micro-grid is a very good example: the number of distinct power node points numbers at least in the hundreds, and when the power system description is augmented by local controllers and electronics, as well as hierarchical control structures and agents, the number of participant nodes runs well into the thousands. Current tools for simulation, which help to support "design through analysis," cannot begin to assess the dynamic behavior of all possible interconnections in the power distribution system (PDS).

The general properties of very large networks were addressed in a series of seminal publications in the late 1990's. More recent work has turned now to the questions of *a priori* design for robustness, and effective reconfiguration. In fact, we have a growing understanding of what statistical properties in large-scale networks will lead to robust design, both within and without the context of an active reconfiguration. Our main argument here is that such an approach in the AES can have major benefits, one of which is that a network could, in principle, be designed to statistically have no failure mode. This is a network that has no weak points, short of massive damage at many locations, and a network that is robust even against deliberate localized attack on the most critical elements.

We provide a short introduction to some of the recent results for statistical design in the next section. Then we discuss a specific simulation carried out to assess, for the first time, the robustness of a grid based on a notionl cruiser high-level topology. We compare this with scale-free and random networks with the same nominal load distribution, capacity, and number of links, as well as compatible damage conditions.

II. Background

A short review of recent results in standard network models convinces that this is indeed a possible route to robust design. We distinguish three basic strategies. First, certain global properties of large networks inherently lead to robustness without reconfiguration. Second, specific nominal arrangements can be devised that are robust against several failures, again without reconfiguration. Third, we can consider active reconfiguration to maintain network functionality; reconfiguration in large-scale systems generally homogenizes the remaining links, and this is not the same objective taken in current PDS optimization schemes.

A common measure of network functionality is mean shortest path, i.e. the mean number of edges between all node pairs. A network's robustness can be measured in terms of mean shortest path as well, by measuring its increase as a function of malignant changes to the network. A first broad result is that scale-free networks, such as the Internet and terrestrial power grids, show strong robustness against attacks on or failures in random links [3]. It is well-known also, however, that such networks are not robust against deliberate attacks, which are generally taken occur on the most heavily loaded elements. A fully random Erdos-Reyni network which does not have the scale-free property is markedly better in this latter case; this has been confirmed in particular using accurate models of the internet and of power grids [6]. The distinction between these two types of networks has to do with the probability distribution of node interconnections: in a scale-free network, this distribution is a power law, whereas in a random network, the distribution is Poisson.

In specific configuration design, a fundamental question is how to lay out the nominal topology so that robustness is achieved with minimal cost, e.g., minimal overcapacity. If the overcapacity factor is taken as a constant across the network, scale-free networks are not robust to deliberate attack, and

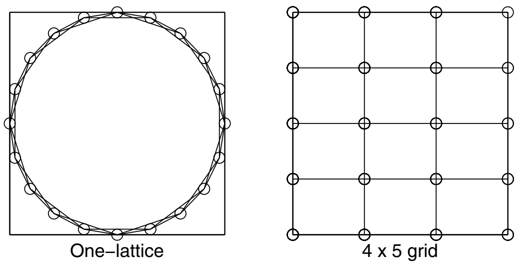

Fig. 2. Arrangements of cruiser copies. Left: Connection of twenty notional cruiser modules in a ring with connections to the two closest neighbors on each side. Right: Tiling of twenty cruiser modules in a 4x5 lattice, with connections between adjacent modules.

neither are random networks [10]. Providing overcapacity only on the most heavily loaded nodes, surprisingly, can both improve robustness and also create a mechanism for minimizing cost [14]. Along these lines, Wang and Chen [15] give a specific recipe for choosing link capacities so as to avoid cascading failures; a scheme that identifies those paths which avoid heavily loaded edges and nodes has also been developed [12]. The role of fluctuating loads is a relatively new line of inquiry [8].

Reconfiguration of large networks after failures appears to be most effective when the objective is to homogenize the network. In a packet communication setting, Motter [9] advocates the additional, selective removal of those components whose presence creates an inordinate amount of traffic, due to their interconnection. A potential difficulty in reconfiguration on large scales is the time scale required for such computation.

These approaches should be considered as tools that might inform the design of the AES. Nominal configuration design in particular seems to be particularly appealing because it defines specific system connections and weights, and because it does not involve the computations associated with real-time reconfiguration. We provide an analysis on a network representative of the integrated power systems being considered for the electric ship.

III. SIMULATIONS

A. Procedure

We simulate a cascading failure scenario for four networks: a scale-free network, an Erdos-Renyi random network, and two networks based on the notional cruiser line diagram in Fig. 1.

The notional cruiser-based networks are abstractions of a typical electric ship power grid. For each, the network depicted in Fig. 1 was replicated twenty times. In one, the copies were arranged in a ring and connected to their two nearest neighbors on either side (forming a one-lattice), and in the other each copy was connected to its neighbors in a four by five grid. Fig. 2 illustrates these two arrangements. The first is representative of a geographically constrained arrangement on a vessel, with a full tie-back from bow to stern, whereas the second is a straight two-dimensional tiling.

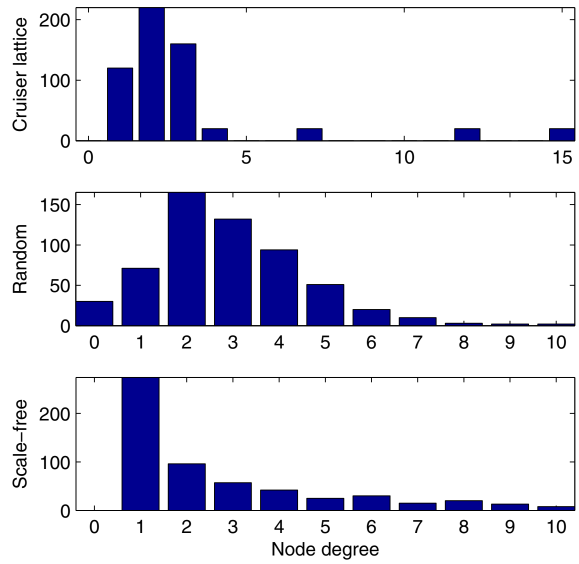

Fig. 3. Histograms of node degree for cruiser networks and realizations of scale-free and random networks. The random network has a binomial distribution; the scale-free network follows a power law, $p(d) = d^{-\gamma}$

All MTG (main turbine generator) and ATG (auxiliary turbine generator) nodes were treated as 36 MW and 4 MW power sources respectively, and the propulsion nodes as 36.5 MW loads. Each PCM was assigned a 0.5 MW load, and all line capacities were set to 40 MW. Although the PCM loads are quite small compared with the propulsion loads, rerouting of power through any line could power a propulsion motor and this is why we have maintained the 40 MW line capacity throughout. Connections between cruiser copies were made by cross-linking their PDM3P and PDM3S nodes (see figure).

In the Erdos-Renyi random network, links were formed between pairs of nodes with a fixed probability, independent of other links. A value of $p = 0.0027$ was used to ensure each run's random network had in the mean the same number of links as the cruiser-based network. The scale-free network was constructed according to the method of [11]. The basic procedure is to sample the number of links κ coming out of each node from a power law distribution $p \sim \kappa^{-\gamma}$, and then randomly connect the half-links to those of other nodes. To make the scale-free network comparable to the cruiser model, κ was restricted to $\{1, ..., 10\}$, and $\gamma = 1.4$ was used. These parameters lead to a network with approximately the same number of links as the cruiser-based networks.

The loads and sources used by both the scale-free and random networks were identical to those used in the cruiser-based networks. Fig. 3 shows histograms of the degree distributions for the cruiser-based, scale-free and random networks. The scale free network follows a power law distribution, while the random network, the degree distribution of which follows a binomial distribution, resembles a Poisson distribution [7].

We recompute the load-flow problem after every link or

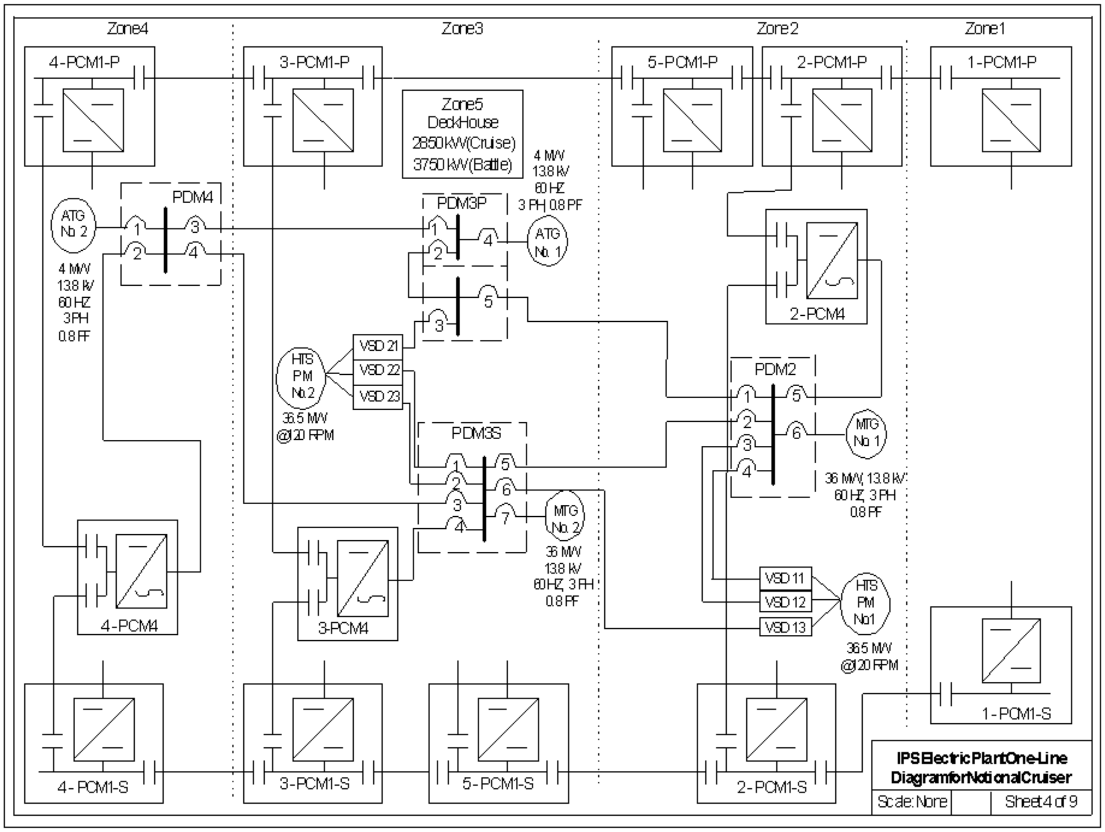

Fig. 1. Notional cruiser line diagram from [1]

node failure [6]. The cascading failure scenario was as follows:

1) Compute the network flow solution for the nominal network.
2) Remove a set of nodes from the graph, as well as all links connected to them. These nodes can be specified, randomly chosen, or sampled from a distribution proportional to the degree of each nodes, such that high degree nodes have a higher chance of being removed.
3) Recompute the load flow solution for the new graph.
4) Remove nodes connected to dead nodes with probability $p = x_{ij}/c_{ij}$, where i is a dead node, j is its neighbor, x_{ij} is the power flow from i to j, and c_{ij} is the capacity of the link.
5) Repeat steps (3) and (4) until there are no new node removals.

The network flow solution is obtained via linear programming [13], and is a simplified DC load flow for a power system, in which there are N_S power sources S and N_L loads L. The optimization is written

$$\max \textstyle\sum_{i=1}^{N_l} L_i$$

$$\begin{array}{c} 0 \leq L_i \leq L_i^* \quad \forall\ i \\ 0 \leq S_i \leq S_i^* \quad \forall\ i \\ |x_{ij}| \leq c_{ij} \quad \forall \text{ links } \{i,j\} \\ \sum_j x_{ij} + S_i = L_i \quad \forall\ i \end{array} \tag{1}$$

To avoid defining source and load sets, we adopt the conventions that $S_i^* = 0$ at non-source nodes and $L_i^* = 0$ at non-load nodes, and that $x_{ij} = -x_{ji}$.

For each network, the same loads and sources were used, as well an identical constraint $c_{ij} = c = 40$ MW for all links. The optimization is similar to that in [4], but with power instead of current. More detailed model physics can included in the optimization, e.g. [5]; however, for our purposes a simplified approach is sufficient.

Two scenarios were considered: near-worst-case failures and a geographic attack. In the former, the initial set of removed nodes was randomly chosen such that nodes with higher degree d (the number of links) were chosen with proportionally higher probability than those with lower degree, such that the probability that node i was initially removed satisfied the proportionality $P(\text{node } i \text{ was initially removed}) \sim d_i$. Our model includes about six hundred nodes, of which thirty are eliminated in each of these attacks. In the geographic attack on the cruiser networks, two modules were randomly selected, and then half the nodes in each chosen modules and half the nodes in a neighboring module were removed. This corresponds with sixty nodes being destroyed, or about ten percent of the total network.

One thousand Monte Carlo simulations of each scenario were conducted. For each run new scale-free and random

TABLE I

MEAN RATIO OF LOAD SERVED BEFORE AND AFTER A NEAR WORST-CASE ATTACK

Network	Cruiser lattice	Cruiser grid	Scale-free	Random
L_C/L_N	0.87	0.87	0.83	0.91

TABLE II

MEAN RATIO OF LOAD SERVED BEFORE AND AFTER A GEOGRAPHIC ATTACK.

Network	Cruiser lattice	Cruiser grid	Scale-free	Random
L_C/L_N	0.87	0.87	0.78	0.86

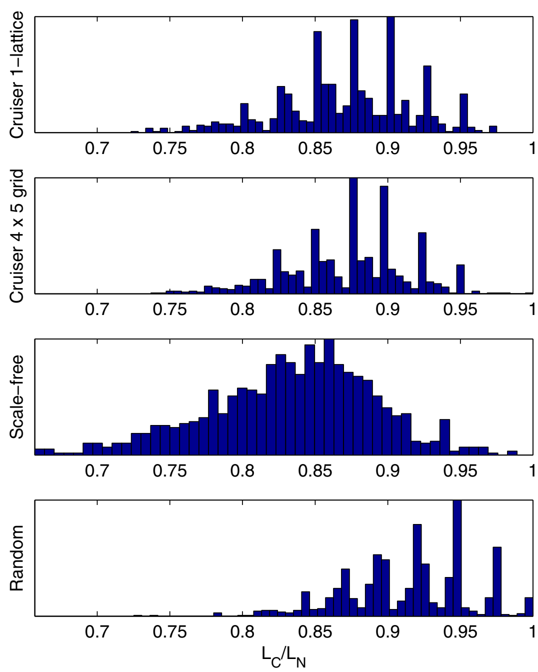

Fig. 4. Histograms of the ratio of load served after a near-worst-case attack L_C and nominal load served L_N for each network. $L_C/L_N = 1$ means all the loads are served.

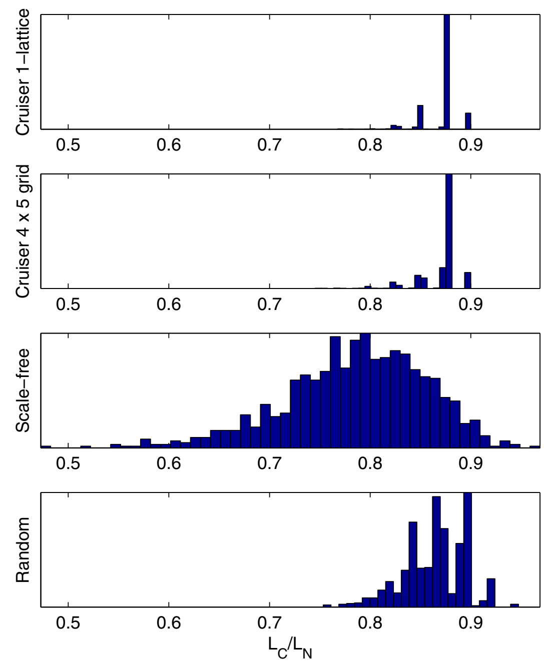

Fig. 5. Histograms of the ratio of load served after a geographic attack L_C and nominal load served L_N for each network.

networks were constructed. As a metric for robustness, we observe the ratio of load served after the cascade to the nominal load served, L_C/L_N. This quantity represents the functionality of the ship, i.e. how much of it is operating at its nominal condition.

B. Results

Tables I and II respectively give the mean over all trials for the near-worst-case attack and geographic failure scenarios, and Fig. 4 and 5 histograms of L_C/L_N for each network.

The cruiser-based networks exhibit similar robustness for the worst-case attacks, significantly better than that of the scale-free network, but slightly worse than the purely random network. It is well known that random networks are more robust to attacks targeting high-degree nodes than scale-free networks [2], and this explains why the scale-free network performs poorly. A grid with highly connected hub nodes will be less robust to substantial damage, whereas by distributing component dependencies throughout the ship there is a higher probability that functionality can be maintained through damage.

In a geographic node removal situation once again the scale-free network performs poorly. In the mean, the random network is slightly less robust than the cruiser-based networks. One can see in Fig. 5 that although there are more cases with higher remaining functionality after the cascade, the tail is longer, admitting more situations with very substantial damage propagation.

C. Design Strategy and Future Work

Based on our findings, a clear and well-known guideline is to avoid centralized architectures with very highly connected nodes. More broadly, however, the statistical network perspective can be useful in designing for robustness in a more directed way. Consider for example the following optimization:

$$\begin{gathered} \max_{p_d} L_C/L_N \quad \text{subject to} \\ \sum_{i=1}^{N} p_{d_i} = 1, \;\; p_{d_i} \geq 0 \end{gathered} \tag{2}$$

p_{d_i} is the probability of a node in the network having degree d_i. Here the ratio of load served after an attack to the nominal load served is being optimized over the degree distribution of the network, i.e. the probability that a node will have a given number of links. Note that (2) contains (1) as well as all other aspects of the failure scenario - the statistics of the network itself are being optimized for a particular scenario. Although this does not fully define a network, the degree distribution is strongly connected to its robustness characteristics.

It would be computationally intractable to optimize the deterministic layout of a large integrated power system. However, by knowing the near-optimal degree distribution for a particular scenario, the statistical robustness of designs can be assessed merely by looking at their degree distribution, and hence used to guide design decisions, e.g. how much redundancy should be incorporated.

IV. Conclusion

Our present model of the cruiser/AES architecture is simplistic, but with reasonable upward scaling and load distributions we have shown that there can be significant variations in robustness against failures, depending on the interconnections. In particular, a random network appears to have a consistent advantage in terms of load served after a cascade that is caused by a near-worst-case failure or attack. The findings are preliminary, but serve to motivate further work in this area. Several focus areas stand out. Needless to say, a randomly connected network may not be possible on the actual vessel for practical reasons, such as wireway spaces. Hence, the basic drivers for conventional layouts have to be articulated and reconciled with the network point of view. Secondly, as noted in the Introduction, the AES is a large-scale system *in multiple domains*; this fact increases the size of the network under consideration, and requires different node and link models. We believe the potential for statistical design over multiple domains is a rich area, but virtually unexplored to date.

Acknowledgment

Work is supported by the Office of Naval Research Grant N00014-02-1-0623, monitored by Dr. T. Ericsen.

References

[1] Notional cruiser one line diagram. In *Electric Ship Research and Development Consortium*, July 2007.

[2] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi. Error and attack tolerance of complex networks. *Nature*, 406:378, 2000.

[3] Maximino Aldana and Philippe Cluzel. A natural class of robust networks. *Proceedings of the National Academy of Science*, 100(15):8710–8714, 2003.

[4] K.L. Butler, N.D.R. Sarma, and V.R. Prasad. A new method of network reconfiguration for service restoration in shipboard power systems. *Transmission and Distribution Conference, 1999 IEEE*, 2:658–662 vol.2, Apr 1999.

[5] K.L. Butler, N.D.R. Sarma, and V. Ragendra Prasad. Network reconfiguration for service restoration in shipboard power distribution systems. *Power Systems, IEEE Transactions on*, 16(4):653–661, Nov 2001.

[6] Paolo Crucitti, Vito Latora, and Massimo Marchiori. Model for cascading failures in complex networks. *Physical Review E*, 69(045104(R)), 2004.

[7] M. O. Jackson. *Social and economic networks*. Princeton University Press, 2008.

[8] Dong-Hee Kim and Adilson E. Motter. Fluctuation-driven capacity distribution in complex networks. *New Journal of Physics*, 10(053022), 2008.

[9] Adilson E. Motter. Cascade control and defense in complex networks. *Phys. Rev. Lett.*, 93(9):098701, Aug 2004.

[10] Adilson E. Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. *Physical Review E*, 66(065102(R)), 2002.

[11] Adilson E. Motter, Takashi Nishikawa, and Ying-Cheng Lai. Range-based attack on links in scale-free networks: Are long-range links responsible for the small-world phenomenon? *Phys. Rev. E*, 66(6):065103, Dec 2002.

[12] Mirko Schafer, Jan Scholz, and Martin Greiner. Proactive robustness control of heterogeneously loaded networks. *Physical Review Letters*, 96(108701), 2006.

[13] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, June 1998.

[14] B. Wang and B. J. Kim. A high-robustness and low-cost model for cascading failures. *EPL*, 78(48001), 2007.

[15] Wen-Xu Wang and Guanrong Chen. Universal robustness characteristic of weighted networks against cascading failure. *Physical Review E*, 77(026101), 2008.