Proceedings of the 2007 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY 20-22 June 2007

Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models

Nils K. Svendsen, Stephen D. Wolthusen

Abstract—**Critical infrastructures such as the electric grid, oil and gas pipelines, telecommunications, and financial services are characterized by direct and transitive interdependencies which, owing to their complexity and the scale at which these occur, are not readily visible. Moreover, vulnerabilities in elements of the infrastructure can lead to cascading and cyclical failures only after some delay or as a result of feedback cycles in the infrastructure. In this paper we therefore describe several statistical and algorithmic approaches for the analysis of infrastructure interdependencies which can take into account not only abstract interdependencies but also selected properties of infrastructure types such as buffering of resources. Based on a multigraph model we analyze the interactions of random failures and targeted attacks and use graph statistics to identify critical components in infrastructure topologies, thereby providing a mechanism for the development of more robust infrastructures and more effective allocation of defensive capabilities for existing critical infrastructure.**

I. Introduction

The failure of critical infrastructures (CI) can result in severe economic disruptions and can also result in loss of life or the failure of services which impede public health and well-being. These services, including energy, financial services, health care, public services, and transportation sectors, must therefore be maintained at adequate levels [1], [2]. While localized failures can and do occur, critical infrastructure protection (CIP) is primarily concerned with the analysis and prevention of large-scale disruptions such as the November 2006 failure of the electric power grid throughout much of continental Europe and earlier failures in this infrastructure such as the August 2003 power outages in the northeastern U.S. and Canada [3], [4], [5]. A particular property of CI is their interdependency; the failure of infrastructure components may lead to cascading effects either within the same type of infrastructure (e.g. the power grid) or extending to other infrastructure types. Moreover, cascading failures may also be cyclical in nature and hence include feedback cycles in which an initial failure in one type of infrastructure will, through several cascading intermediate effects, result in more extensive failures in the same infrastructure type. While the identification of such interdependencies for potential remediation or at least closer surveillance is challenging in its own right given the large scales that need to be considered (e.g. national telecommunications networks and power grids), the fact that detrimental effects can arise after considerable delays and propagation of transitive failures, makes it desirable to develop models which can identify such dependencies at the planning stage or at least for more targeted direction of remediation efforts. While such transitive and cyclical effects in response to individual component failures (regardless of the cause, e.g. material defects, human errors, sabotage, or acts of terrorism) have been studied before [6], [7], the interactions between such isolated failures and component failures as predicted by defect and reliability models is of particular interest since such stochastic failures can introduce further instabilities and feedback cycles into the systems considered here. This also applies in case of multiple exceptional events (e.g. as caused by a natural disaster or coordinated terrorist attack) as the additional perturbation will affect the ability to stabilize and recover overall functionality of the infrastructure network. We therefore extend the infrastructure models described in earlier research by a stochastic component failure model and then investigate the interactions between the different infrastructure failure types. The information gained from this simulation can then be used in the configuration and interconnection of infrastructure elements and types or, in case of legacy infrastructure, be used to at least identify areas exhibiting exceptional vulnerability or those whose failure is predicted to have disproportionate cascading effects. Beyond scenario-based simulations, however, we also describe statistical approaches for the identification of critical strongly connected components in interdependency graphs, which can once again be used for prioritization of resources in protecting such components to ensure that the overall infrastructure service cluster provided by the component is not jeopardized. The remainder of the paper is structured as follows: Following a brief review of infrastructure interdependency models described in earlier research by the authors, section II proceeds to introduce a model element for random component failure, which permits the investigation of interactions between random failures and targeted attacks as well as of metastability effects caused by such random failures. Section III then elaborates this model in a

N. K. Svendsen: Gjøvik University College, Norway.
S. D. Wolthusen: Gjøvik University College, Norway and Royal Holloway, University of London, UK.

series of scenarios which are simulated over topologies representative of the infrastructure types and their interconnections. These simulation results and their implications are then reviewed in section IV, while section V provides a brief review of related work. Section VI then concludes with a discussion of the results as well as of ongoing further research on extending both the model and the analytical mechanisms applied to the model.

II. Infrastructure Models

This section summarizes the essential parts of the model previously introduced by the authors [6], [7], and introduced the notion of random failures in the model.

A. Basic graph model and terminology

Interactions among infrastructure components and infrastructure users are modeled in the form of directed multigraphs, which can be further augmented by response functions defining interactions between components. In the model, vertices $\mathcal{V} = \{v_1, \ldots, v_k\}$ are interpreted as producers and consumers of m different types of services. Transfer of services takes place along edges between the nodes. Each edge can transport or transfer one dependency type d_j chosen from the set $\mathcal{D} = \{d_1, \ldots, d_m\}$. In the general case it is assumed that all nodes v_a have a buffer of volume V_a^j (indicating a scalar resource; this may represent both physical and logical resources and, moreover, may be subject to further constraints such as integral values) for all dependency types d_j. Each node also has a capacity limit $N_{\mathrm{Max}}(v_a, d_j)$ in terms of the amount of resource d_j that can be stored in the node. The dependency types can be grouped into three classes:

1. *Ephemeral:* Where $V_a^j = 0$ for all nodes v_a, and it follows that $N_{\mathrm{Max}}(v_a, d_j) = 0$.
2. *Storeable and incompressible:* Where $N_{\mathrm{Max}}(v_a, d_j) = \rho V_a$, ρ is the density of the resource.
3. *Storeable and compressible:* Where $N_{\mathrm{Max}}(v_a, d_j) = P_{\mathrm{Max}}(v_a, d_j) V_a$, $P_{\mathrm{Max}}(v_a, d_j)$ is the maximum pressure supported in the storage of resource d_j in the node v_a.

Further refinements such as multiple storage stages (e.g. requiring staging of resources from long-term storage to operational status) and logistical aspects are not covered at the abstraction level of the model described here. Pairwise dependencies between nodes are represented with directed edges, where the head node is dependent on the tail node. The edges of a given infrastructure are defined by a subset $\mathcal{E}$ of $\boldsymbol{\mathcal{E}} = \{e_1^1, e_2^1, \ldots, e_{n_1}^1, e_1^2, , \ldots, e_{n_m}^m\}$, where $n_1, \ldots, n_m$ respectively are the numbers of dependencies of type $d_1, \ldots, d_m$, and e_i^j is the edge number i of dependency type j in the network. A dependency between two nodes v_a and v_b is uniquely determined by $e_i^j(v_a, v_b)$.

In addition to the type, two predicates $C_{\mathrm{Max}}(e_i^j(v_a, v_b)) \in \mathbb{N}_0$ and $C_{\mathrm{Min}}(e_i^j(v_a, v_b)) \in \mathbb{N}_0$ are defined for each edge. These values respectively represent the maximum capacity of the edge $e_i^j(v_a, v_b)$ and the lower threshold for flow through the edge. Hence, two $k \times m$ matrices, where k is the number of vertices and m is the number of dependency types, C_{Max} and C_{Min} are sufficient to summarize this information. Let $r_a^j(t)$ be the amount of a resource of dependency type j produced in node v_a at time t. $D(t)$ is defined to be a $k \times m$ matrix over $\mathbb{Z}$ describing the amount of resources of dependency type j available at the node v_a at time t. It follows that the initial state of D is given by

$$D_{aj}(0) = r_a^j(0). \tag{1}$$

For every edge in $\mathcal{E}$ a response function $R_i^j(v_a, v_b)$:

$$D_{aj} \times V_a^j \times N_a^j \times N_{\mathrm{Max}}(v_a, j) \times C_{\mathrm{Max}} \times C_{\mathrm{Min}} \to \mathbb{N}_0 \tag{2}$$

that determines the i-th flow of type j between the nodes v_a and v_b is defined. The function $R_i^j(v_a, v_b)$ w.l.o.g. is defined as a linear function, and may contain some prioritizing scheme over i and v_b. By constraining the response function to a linear function and discrete values for both time steps and resources, linear programming approaches can be employed for optimization of the relevant parameters; interior point methods for this type of problem such as [8], [9] can achieve computational complexity on the order of $O(n^{3.5})$, making the analysis of large graphs feasible.

Given the responses at time t, the amount of resource j available in any node v_a at time $t+1$ is given by

$$D_{aj}(t+1) = r_a^j(t) + N_a^j(t) + \sum_{i,s \mid e_i^j(v_s, v_a) \in \mathcal{E}} R_i^j(v_s, v_a, t). \tag{3}$$

A node v_a is said to be functional at time t if it receives or generates the resources needed to satisfy its internal needs, that is $D_{aj}(t) > 0$ for all dependency types j which are such that $e_i^j(v_b, v_a) \in \mathcal{E}$, where $b \in \{1, \ldots, a-1, a+1, \ldots k\}$. If this is the case for only some of the dependency types the node is said to be partially functional, and finally of no requirement are satisfied the node is said to be dysfunctional. For further argumentation on the motivation for and the granularity of the model we refer to [7].

B. Non-storeable resources (Electric Grid Network)

In networks with edges representing a non-storable resource d_j, outbound edges are immediately impacted by inbound edges. Using the model described in section II-A, we have that $V_a^j = N_{\mathrm{Max}}(v_a, d_j) = 0$. The response function is thus a function $R_i^j(v_a, v_b)$:

$$D_{aj} \times V_a^j \times C_{\mathrm{Max}} \times C_{\mathrm{Min}} \to \mathbb{N}_0, \tag{4}$$

and the given the available resources and constraints in a node v_a at time t the available resources at time $t+1$ are given by

$$D_{aj}(t+1) = r_a^j(t) + \sum_{i,s \mid e_i^j(v_s, v_a) \in \mathcal{E}} R_i^j(v_s, v_a, t). \tag{5}$$

The function $R_i^j(v_a, v_b)$ depends on the mechanism governing flows and conservation laws in the different networks. In the power distribution network the generated power originates from a small number of power plants or generators. A transport network, which may interconnect several power plants, delivers the power to a large number of transformers, which serve the low voltage distribution network, potentially though several intermediate sub-distribution networks. As a consequence the resulting graph is a directed network where multiple edges of different orientation between two nodes are rare occurrences. Based on the discussion in [6] the following simplified procedure is hence used to generate the power distribution network topology:

1. *Growth*: At every time step a new node is added to the network. This node defines the head of an edge connecting it to an already existing node.
2. *Preferential attachment*: The tail of the edge is selected among the existing nodes with probability proportional to the degree of the node.
3. *Redundant connection*: After the final time step a sparse random graph is placed on the top of the network.

As the network grows large, the influence of the sparse random graph will be small, and the probability of a node having k edges will follow a power law distribution with exponent $\gamma = 3$ [10]. Finally the response function for each edge is defined. In the case of quantitative analysis of service delivery this function should be an implementation of Kirchhoff's first rule, ensuring that all the flow into a node together with the flow generated by a node equals the output and the consumption of the node for the given resource type. In order to explore the presented model, however, such a detailed approach is not necessary, as the model instance under discussion focuses primarily on the functionality of the node. The principal issue in this case is that the electricity is consumed as it propagates through the networks and cannot e.g. be stored in subgraph cycles. Thus the response function as described here only illustrates an abstract resource which is being consumed as it flows through the network. Introducing a threshold function

$$T(x, c) = \delta(x - c)x, \tag{6}$$

where

$$\delta(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0. \end{cases} \tag{7}$$

the implemented response function is of the form

$$R_i(v_a, v_b, t)) = T(\frac{1}{2}D_a(t), C_{\mathrm{Min}}(e_i(v_a, v_b))), \tag{8}$$

where D_a is the current available in the node a at time t. Equation 8 indicates that two units of input current to the node are required to produce one unit of output current along an outgoing edge. As there is only one dependency in the network, the dependency type is not specified. Moreover, for the purposes of this example we also assume that there exists only one power dependency between two nodes and no prioritization scheme is defined over the outgoing edges. A node in the power distribution network is defined to be functional if it is has incoming current or generates current internally. The given response function can provide information on whether a node is functional or not, but does not provide any physical representation of the level of functionality of a given node in the network, which provides a sufficient level of details for the purposes of the present study.

C. Storeable resources (Gas or Oil Pipeline)

In numerous infrastructures the service delivery resource can be stored and accumulated in the nodes over time. In networks with edges representing service delivery of a storeable resource d_j, outbound edges are not immediately impacted by inbound edges. The amount of resource buffered in the node may increase in periods with an excess of input, and may decrease during periods while the amount of incoming resources are low or completely cut off. This ensures the operation of the node over a certain time in case of no input but may also be the source of fluctuations in the system. Assuming that a node represents some facility capable of receiving, storing, and distributing a resource, the response function and the amount of resource d_j available in any node are given by equation 3 (for an overviews of pipeline components and operating regimes see e.g. [11]); further discussion of the model is found in [7], where we divided a pipeline into three main parts:

1. *The gathering system:* Consists of low pressure, low diameter pipelines that transports one or several fluids from the wellhead to the processing plant
2. *The transportation system:* Moves fluid in large quantities over long distances with few or no major supplies or off-takes between the end points of the pipeline
3. *The distribution system:* Delivers fluid to the consumers, has a large number of off-takes, and can be significantly branched

In our model the pipeline is divided into pipeline segments. A pipeline segment is defined to be the piece of pipeline between two branchings. A branching can be a supply or an off-take, and is represented with an edge in our model. For simplicity, our sample networks are constructed without loss of generality such that compressors, metering stations, and valves only are present in branchings. Additional storages are also represented as pipe segments. We choose to model the gathering system as a number of in-branchings [12]. The root nodes represent the networks transportation system. Meters, valves and compressor stations can be inserted as several nodes in line with the root node. The distribution network is, from the root nodes, viewed as out-branchings [12]. In reality these spanning

oriented trees are interconnected for redundancy purposes.

Every pipe segment P_a is represented as a node v_a. In accordance with the general model presented in section II-A, each node has a buffer of volume V_a, and a pressure limitation $P_{\text{Max}}(v, a)$. The relation between pressure and volume for gasses is given by the ideal gas law $PV = nRT$, where n is the number of moles, R is the universal gas constant, and T is the temperature [13]. As an approximation we assume that the temperature remains constant in the pipeline, and normalizing the relations such that $RT = 1$, we get the relationship

$$PV = N, \tag{9}$$

where N is the amount of some arbitrary unit of gas.

The difference in pressure between different segments is the force driving fluid from one node to another, and is therefore the input to our response function in the model. The velocity of the flow, or response, depends on several parameters, among others the length of the pipe segment, the diameter of the pipe, and the friction between the pipe and the fluid. This means that the velocity of the fluid will reach an upper bound, and may enter a regime of turbulence which again can cause a drop in velocity. Given the pressure P_a and P_b of two connected nodes v_a and v_b, we name the pressure difference ΔP_{ab}. The response function $R_i(\Delta P_{ab}, t)$ shall define the flow, in terms of amount of particles from v_a to v_b at time t. This is obviously not a linear relationship. Roughly it can be described as low for small ΔP_{ab}, then growing proportionally with ΔP_{ab} until the growth decays and the velocity tend to some threshold. This is approximately expressed by the logistic equation [14]. Bounded growth as a function of a variable x is of the form

$$\frac{A}{1 + e^{(B-Cx)}},$$

where A is the upper bound, B defines the translation of the curve along the x axis, and C maximal derivative of the curve. To represent that the ΔP_{ab}, e.g. due to friction, must be larger than some threshold to flow through a pipe a threshold is introduced. We can now define the response function as

$$R_i(\Delta P_{ab}, t) = \begin{cases} 0 & \text{if } \Delta P_{ab}(t) \leq \frac{C_{\max}}{10}, \\ \frac{C_{\max}}{1+e^{f(t)}} & \text{if } \Delta P_{ab}(t) \geq \frac{C_{\max}}{10}, \end{cases} \tag{10}$$

where $f(t) = (2.5 - 10\Delta P_{ab}(t))/C_{\max}$, $\Delta P_{ab}(t)$ is the pressure difference at time t, and $C_{\max}$ is the capacity of the pipe. The values of B and C are chosen arbitrarily in oder to get a suitable growth shape on the curve. The order of the considered edges influences the result. Fluid is consumed in the intersection, thus the potential pressure difference diminished. To approximate continuous behavior the sequence of the edges is altered from time step to time step. Therefore, on average, the behavior of the intersection is correct. By ordering the edges in a list a static prioritizing scheme can be set, if delivery to certain parts of the network is considered critical. Based on the response function defined in equation 10 the amount of fluid available in a pipe segment is given by

$$D_a(t+1) = r_a(t) + N_a(t) + \sum_{i,s \mid e_i(v_s,v_a) \in \mathcal{E}} R_i(v_s, v_a, t). \tag{11}$$

By altering the computation of R_i and D_a we can observe the flow through the network over time. One must also be aware of the pressure limitation of the pipeline components. Infinite pressure cannot be tolerated, thus in the case that $r_a(t)$ gives a positive contribution it must be possible to diminish or eliminate it. The same also holds true for incoming pressure that valves can be closed and is implemented in this model. The goal of a pipeline is to deliver fluid to customers who, in this model, are represented as leaf nodes in the distribution network, or as off-takes from intermediate nodes in the distribution network. We chose to measure the functionality of the network in terms of the fraction of the leaf nodes receiving sufficient quantities of fluid to cover their needs. permitting comparison of the the performance of different network configurations. Additional constraints can be added, such as prioritized fluid flow to specific nodes in order to maintain functionality of the particular node.

D. Graph element reliability (Telephony Transport Layer)

Often we are not only interested in the performance characteristics of system components or how the system reacts under attacks, but also interested in the reliability of the system, i.e. the systems ability to provide uninterrupted service. There are many introductions to reliability theory, our approach is based on Helvik [15]. The reliability of a system can be characterized by the systems reliability function, its failure rate and by the mean time to first failure. An infrastructure where there has traditionally been focuses on sound engineering and quality of service is the telecommunication layer. Thus expanding the telephony transport layer model to contain element reliability is a natural extension of the models we have presented previously [6], [7]. In the original model we used the hierarchical network model of the telecommunication transport layer as described e.g. in [16], as it is representative of much of the currently deployed telecommunication infrastructure. The telecommunication transport layer is modeled as a number of disconnected trees which are connected to a fully connected transportation network through their root nodes.

The model extension becomes visible in the response function. As the functionality of a node previously only depended on its power supply, reliability constraint is now introduced for the edges of the telephony layer. Several types of failures may occur in an edge. We focus on three types of failures: Failures that reduced the capacity of an edge, on/off failures, and total failure of the edge. For ev-

ery edge the state is reflected as a function of time. We introduce a capacity function $c_i(v_a, v_b, t)$ for every edge in the transport layer. The range of $c_i(v_a, v_b, t)$ goes from 0 to $C_{i,max}(v_a, v_b)$, the maximal capacity of the edge. The response function then becomes

$$R_i(v_a, v_b, t) = c_i(v_a, v_b, t)\delta(D_a(t) - C_{\mathrm{Min}}(e_i(v_a, v_b))), \quad (12)$$

where D_a is the current available in the node a at time t and δ is as defined in equation 7. It follows from the definition of equation 2 that a directed edge between the nodes v_a and v_b is defined if there is power available in node v_a and the capacity of the edge is different from 0. Again, no redundant links are defined between two nodes and no prioritization scheme is defined over the edges. The functionality of the node is then given by the sum of outgoing capacities divided by the sum of the maximal outgoing capacities.

In addition, each connection in the telephony transport layer is bidirectional, as one way voice communications are typically of limited interest. The functionality of a node thus depends on if the node itself and the node it is connected to has an effective power supply. Only in this case can the switch deliver the two way service it is meant to.

E. Types of failure and interesting time durations

There are two principal types of failures, persistent failure where manual intervention is required for rectification: physical faults, irreversible interactions or operational faults or environmental faults, and non persistent failure which is a transient failure, reversible interactions or operational faults and design faults, not caused by physical change of the system and can be rectified by removing the error from the system (automatically or manually). Our model includes three types of edge failure: The edge may lose some or all of its capacity or it can fluctuate in a on/off mode. Applying statistical analysis on historic data a set of characteristics times of system components can be derived. In order not to make the presented model too complex we choose, again, a simplified approach. The main purpose of the model is to capture some of the essential properties of large, complex systems. There are two characteristic times of particular interest from a critical infrastructure protection viewpoint, the mean time between failure (MTBF) and the mean down time (MDT). The down time is defined to be the time from the system ceases to deliver a specified set of services and until service provision is restored. MTBF gives an estimate on when the next failure will occur in the system. We assume that all edges are independent and identically distributed. This is a fair assumption as we do not consider cascading failures in this case, on failures due to faults and errors inside the nodes. Further we assume that every edge $e_i^j(v_a, v_b)$ has a failure rate $\lambda_i^j(v_a, v_b)$, this rate can be equal for all the edges. We then define the failure process of each edge to be a Poisson process with rate $\lambda_i^j(v_a, v_b)$.

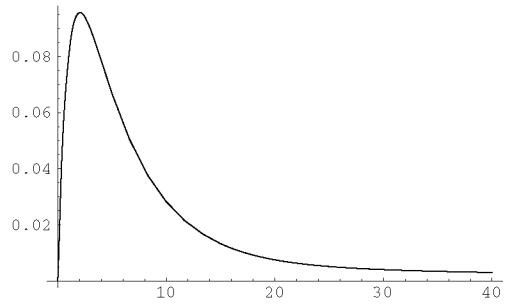


Fig. 1. The probability density function $f_m(t)$ of the repair process with parameters $\mu_a = 1/5$, $\mu_w = 1/50$, $\mu_q = 1/1$, and $p = 0.7$.

The edge remains in the failure state until it has been repaired. The repair can either be automatic or manual. Helvik [15] presents a model of the manual repair process dividing the repair process into an administrative delay (modeled by a negative exponential distribution with parameter μ_a), a quick repair time (modeled by a negative exponential distribution with parameter μ_q occurring with probability p), and a repair time including a logistic delay (modeled by a negative exponential distribution with parameter μ_w). The mean down time becomes [15]

$$MDT = \mu_a^{-1} + p\mu_q^{-1} + (1-p)\mu_w^{-1}.$$

The probability density function

$$\begin{aligned} f_m(t) &= \frac{e^{-\mu_a t}((\mu_a(p-1)+\mu_q)\mu_w - p\mu_a\mu_q)}{(\mu_a-\mu_q)(1-\mu_w/\mu_a)} \\ &- \frac{\mu_w e^{-\mu_w t}(p-1)(\mu_a-\mu_q) + p\mu_q e^{-\mu_q t}(\mu_w-\mu_a)}{(\mu_a-\mu_q)(1-\mu_w/\mu_a)} \end{aligned}$$

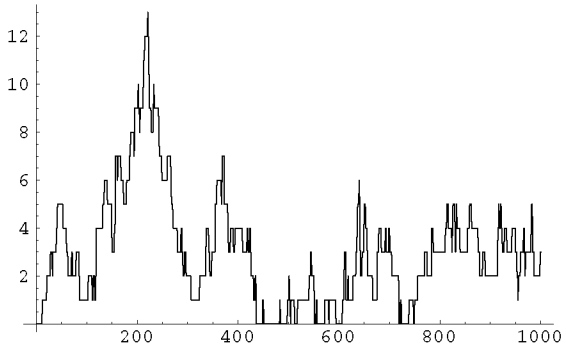
is obtained by convolutions of the processes as in [15]. Note that the logistic delay may give rise to a long and heavy tail in the density function, as indicated by the plot in figure 1 (parameters taken from [15]).

III. Simulations

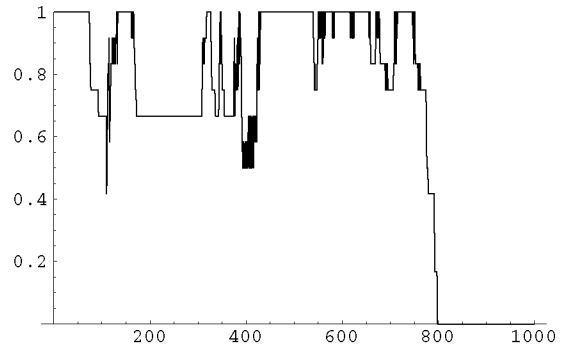
In this section we will assume that the failure rates of the telephony transport layer dominates the failure proscess. Given that a failure might be a ADSL line going down, or having heavily reduced capacity, this is a fiar assumption. Given the failure intensity $\lambda_i^j(v_a, v_b)$ of a given edge, the time to next failure of edge can be drawn from the Poisson distribution using standard statistical methods [17]. We generate independent uniform $(0, 1)$ random variables $U_1, U_2, \ldots$ stopping at

$$N + 1 = min\left\{n : \times_{i=1}^{n} U_i < e^{-\lambda}\right\},$$

the random variable N then has the desired Poisson distribution. Simulating the down time is done by drawing

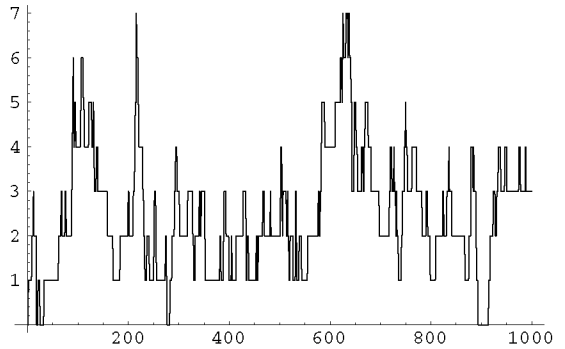


(a)Number of failures as a function of time.

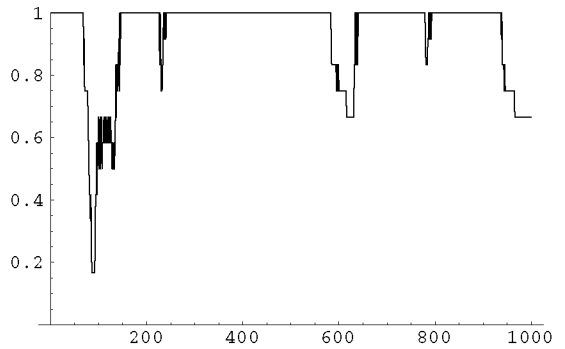


(b)The level of functionality of the pipeline as a function of time.

Fig. 2. The level of functionality in the gas distribution network as a function of time as random errors occurs. The failure rate in the Poisson process is $\lambda = 400$ and the parameters for the parameters of the repair process are $\mu_a = 1/3$, $\mu_w = 1/9$, $\mu_q = 1/1$, and $p = 0.7$.



(a)Number of failures in the telecommunication network as a function of time.



(b)The level of functionality of the pipeline as a function of time.

Fig. 3. The level of functionality in the gas distribution network as a function of time as random errors occurs. In this case $\mu_w = 1/6$, while all other parameters are unchanged compared to the scenario in figure 3.

random values from the probability density function of the repair process. This is done using the rejection method described among others in [17]. Given a density function $g(x)$ from which we can simulate random values Y. Let c be a constant such that

$$\frac{f(y)}{g(y)} \leq c, \qquad \forall\, y.$$

The rejection method then provides the following technique for simulating a random variable having density f:
1. Simulate Y with density g and random variable U.
2. If $U \leq f(Y)/(cg(Y))$, set $X = Y$, else return to 1.
In our simulation we have assumed a cutoff at 10 times the mean duration of the repair proses and used the uniform distribution as g. The simulations are carried out over three interconnected infrastructures, the power distribution network (30 nodes), and telephony transport layer (21 nodes) and pipeline (22 nodes).

Figure 2 shows a sample run of the model with parameters as described in the figure text. In this case we see how the functionality of the gas distribution network drops to zero at a point when critical infrastructure components fails. This scenario is the same as studied in depth in [7]. From this we know with the given scenario the failure of the gas distribution network leads to a total failure of the telecommunication network and a very limited functionality of the power distribution network.

IV. Analysis

This section discusses the effect of component failure in one network on the functionality of the components in the other networks. The section also includes a brief discussion of how the functionality of the network can be improved/deteriorated. We also give an example of how basic graph theoretic analysis of the underlying atypical graph can indicate how the robustness of the interconnected networks can be improved.

A. The effect of component failure over time

When administrating a network there are essentially three well known parameters that can be adjusted in order to improve the reliability of the network. These are:
1. *Infrastructure:* Increase the component lifetime or reliability in order to reduce the mean time between failure

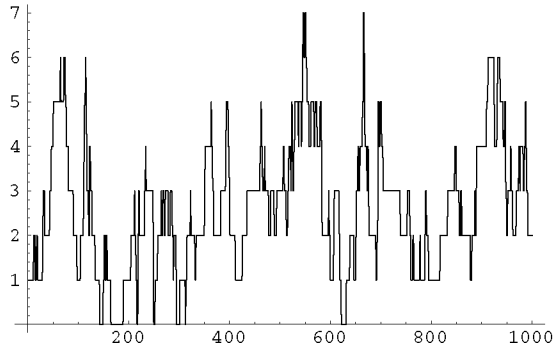
2. *Service/Maintenance:* Shorten the repair times on some or all the nodes. Alternatively one can increase the number of components in stock to reduce the expected number of repairs leading to logistic delay, or improve the logistics in order to bring down the logistic delay.
3. *Topology:* Add redundant incoming edges to nodes that seems to be critical for the functionality of the network.
Knowing that the main contribution of the thick tail of the probability density function in figure 1 is the expected repair time including logistic failure, it is tempting to see what happens if we bring this time down with a factor 2/3 for all nodes in the network. The result of this simulation is shown in figure 3. We see that in this case the number of simultaneous failures oscillates around 2, and that the peaks are smaller than in the case presented in figure 2(b). Comparing with the results from [7] this is a pretty good result, as our analysis then showed that due to the interdependencies of the network one persistent failure in the power distribution grid could lead to a total failure of the interconnected networks. Apparently the infrastructure is less sensitive to failures in the telecommunication network.

B. Detection of critical components and possible counter measures

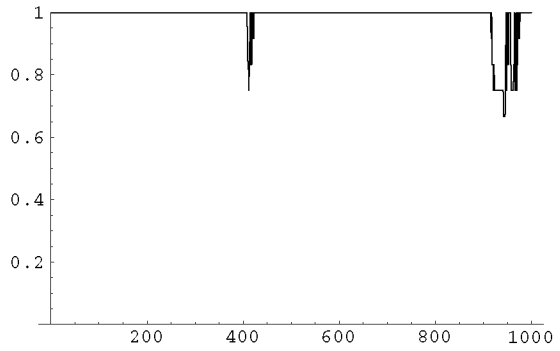
The previous section showed that applying some general measures to all nodes in the network leads to an improvement to the overall robustness. This is not a surprising result, but not very attractive, as the cost to implement this measure on all nodes is likely to be high. We would like to apply algorithms that can be applied on the network in order to identify critical interconnections.

An obvious method is to compare the log files of the simulations over several long time runs to identify weak or vulnerable connections and configurations. This is a similar approach as going through accidents in order to identify what went wrong. As errors may appear simultaneously several runs are necessary in order to identify the critical connections from those that just happened to be down.

A computationally more effective approach is to apply classical algorithms to the the underlying atypical graph and see of some of the statistical properties of this can identify appropriate measures. On our sample network we apply the following approach:
1. Consider the atypical graph
2. Identify the cut points, or the smallest cut sets, of the graph [12]
3. For the pipeline nodes being cut points, or belonging to a cut set, located in the transportation network or the upper part of the distribution network of the gas pipeline add a redundant link from the telephony network.
Applying this strategy to our sample networks we add two redundant edges from the telephony transport network to the pipeline. The effect of the addition of these redundancies is shown in figure 4, showing a considerabely impovement of the network robustness.



(a)Number of failures in the telecommunication network as a function of time.



(b)The level of functionality of the pipeline as a function of time.

Fig. 4. The level of functionality in the gas distribution network as a function of time as random errors occurs. All parameters are the same as in the scenario in figure 2, but two redundant edges added interconnecting the telephony transport layer and the pipeline.

C. Instability induced by the combination of random failure and targeted attacks

Modeling targeted attacks towards a network is known to be a difficult task. General questions to consider regarding an attacker is the attackers resources, knowledge, and motivation. In case of critical infrastructure some attacker models are: script kid, hacker, terrorist, foreign nation, and foreign nation at war. We do not intend to model these attackers. The goal of our approach has been to find a method to maximize the resilience of the network to simultaneous failures, and to maintain the functionality of certain regions or specific nodes of the network for as long as possible. The simulations and analysis presented above has given us a tool to analyze the network based on these criterion. For now, attacks are in cooperated in the model by assuming that the failure rate is higher and the mean time to repair is longer than the properties of the network components indicate, thus leaving a buffer for attacks. Obviously some of the methods used to improve the resilience of the network can also be used to maximize the damage in case of an attack.

V. Related Work

Models and simulations of critical infrastructures have been pursued at an abstract level in research by Barton and Stamber [18], the high-level simulation by North [19], and the subsequent attempt to translate mechanisms for the modeling of complex adaptive systems by Thomas *et al.* [20] as well as approaches using system dynamics such as that proposed by Pasqualini and Witkowski [21]. Control systems approaches, e.g. the model proposed by Sullivan *et al.* [22] can provide significant levels of detail but are constrained in their size and accuracy; the latter issue is at least in part addressed by the inclusion of hybrid control mechanisms as proposed by James and Mabry [23]. Similar approaches have also been described by Amin [24] and Rinaldi [25]; these models vary considerably in their level of detail and range from simple binary dependency analyses to networks of models in which sub-aspects may be modeled by continuous physical submodels.

VI. Conclusion

In this paper we have presented an abstract model of critical infrastructures which aims to capture essential properties of different infrastructure types while retaining an overall computational complexity which makes it amenable for large-scale analyses. This necessarily is less accurate than domain-specific models, but it does allow for the modeling of interactions and interdependencies which such domain models cannot capture. We have also presented several selected analytical and statistical approaches using the example of different disruption and attack techniques, demonstrating the suitability of the model particularly for improving robustness of the infrastructure in an effective manner. Future work will include applications of statistical physics to the characteristics of the model as well as extensions of the sub-models for different infrastructure types.

References

[1] R. T. Marsh, ed., *Critical Infrastructures: Protecting America's Infrastructures*. Washington D.C., USA: United States Government Printing Office, 1997. Report of the President s Commission on Critical Infrastructure Protection.

[2] J. Brömmelhörster, S. Fabry, and N. Wirtz, eds., *Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen*. Bonn, Germany: Bundesamt für Sicherheit in der Informationstechnik, 2004.

[3] E.ON Netz GmbH, "Bericht über den Stand der Untersuchungen zu Hergang und Ursachen der Störung des kontinentaleuropäischen Stromnetzes am Samstag, 4. November 2006 nach 22:10 Uhr," tech. rep., E.ON Netz GmbH, Bayreuth, Germany, Nov. 2006.

[4] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, "Bericht über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006," tech. rep., German Federal Regulatory Agency for Electricity, Gas, Telecommunications, Postal and Railway Systems, Berlin, Germany, Feb. 2007.

[5] D. Hilt, "Technical Analysis of the August 14, 2003, Blackout," tech. rep., North American Electric Reliability Council, Princeton, NJ, USA, July 2004.

[6] N. K. Svendsen and S. D. Wolthusen, "Multigraph Dependency Models for Heterogeneous Critical Infrastructures," in *First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, (Hanover, NH, USA), IFIP, Springer-Verlag, Mar. 2007. In press.

[7] N. K. Svendsen and S. D. Wolthusen, "Connectivity models of interdependency in mixed-type critical infrastructure networks," *Information Security Technical Report*, vol. 12, 2007. In press.

[8] N. Karmarkar, "A New Polynomial Time Algorithm for Linear Programming," *Combinatorica*, vol. 4, no. 4, pp. 373–395, 1984.

[9] A. Schrijver, *Combinatorial Optimization*. Berlin, Germany: Springer-Verlag, 2003. Three volumes.

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

[11] H. Aalto, *Real-Time Receding Horizon Optimisation of Gas Pipeline Networks*. PhD thesis, Department of Automation and Systems Technology, Helsinki University of Technology, Espoo, Finland, May 2005.

[12] J. Bang-Jensen and G. Gutin, *Digraphs: theory, algorithms and applications*. Springer-Verlag, first ed., 2006.

[13] S. S. Zumdal, *Chemical Principles*. Hughton Mifflin Company, third ed., 1998.

[14] C. H. Edwards Jr. and D. E. Penny, *Differential Equations and Bounrdary Value Problems, Computing and Modeling*. Prentice Hall International, first ed., 1995.

[15] B. E. Helvik, "Dependable computing systems and communication networks: Design and evaluation." Draft Lecture Notes, Department of Telematics, NTNU, January 2001.

[16] R. L. Freeman, *Fundamentals of telecommunications*. Wiley Series in Telecommunications and Signal Processing, John Wiley & Sons , Inc., first ed., 1999.

[17] S. M. Ross, *Introduction to Probability Models*. Academic Press Ltd, sixth ed., 1997.

[18] D. C. Barton and K. L. Stamber, "An Agent-Based Microsimulation of Critical Infrastructure Systems," tech. rep., Sandia National Laboratories, Infrastructure Surety Department, Albuquerque, NM, USA, 2000.

[19] M. J. North, "Agent-Based Modeling of Complex Infrastructures," in *Proceedings of the Simulation of Social Agents: Architectures and Institutions Workshop*, (Chicago, IL, USA), pp. 239–250, Oct. 2000.

[20] W. H. Thomas, M. J. North, C. M. Macal, and J. P. Peerenboom, "From Physics to Finances: Complex Adaptive Systems Representation of Infrastructure Interdependencies," tech. rep., Naval Surface Warfare Center Technical Digest, Dahlgren, VA, USA, 2003.

[21] D. Pasqualini and M. Witkowski, "System Dynamics Approach for Critical Infrastructure and Decision Support," in *Proceedings of the Fall Meeting 2005 of the American Geophysical Union*, (San Francisco, CA, USA), American Geophysical Union, Dec. 2005.

[22] K. Sullivan, J. C. Knight, X. Du, and S. Geist, "Information Survivability Control Systems," in *Proceedings of the 21st International Conference on Software Engineering*, (Los Angeles, CA, USA), pp. 184–192, IEEE Computer Society Press, May 1999.

[23] J. James and F. Mabry, "Building Trustworthy Systems: Guided State Estimation as a Feasible Approach for Interpretation, Decision and Action Based on Sensor Data," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, (Big Island, HI, USA), IEEE Computer Society Press, Jan. 2004.

[24] M. Amin, "Toward Self-Healing Infrastructure Systems," *IEEE Computer*, vol. 33, pp. 44–53, Aug. 2000.

[25] S. M. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, (Big Island, HI, USA), IEEE Computer Society Press, Jan. 2004.