Stochastic Dependencies Between Critical Infrastructures

Sandra König
Austrian Institute of Technology GmbH
Digital Safety & Security Department
Wien, Austria
Email: sandra.koenig@ait.ac.at

Stefan Rass
Universität Klagenfurt
Institute of Applied Informatics, System Security Group
Klagenfurt, Austria
Email: stefan.rass@aau.at

***Abstract*—Critical infrastructures (CIs) are characterized by their high importance for the welfare of a society and failure of such an infrastructure has a significant impact on our everyday life. However, a problem in one critical infrastructure also affects other infrastructures, e.g., if electricity is only partly available this also affects hospitals. The effects of even a partial failure of a provider on a critical infrastructures are hard to predict unless strict assumptions are made. The damage depends, among other things, on the availability of substitutes, but also on external influences such as weather, temporary demand or load peaks, etc., which is why we propose a stochastic model where the state of an infrastructure is a random variable. Each infrastructure changes its state depending on what the other CIs do, based on a probabilistic change transition regime. This allows to model complex interdependencies, whose underlying dynamics may be stochastic or deterministic yet partly unknown. The model of the entire CI thus consists of several Markov chains, which retains simplicity for implementation in a software such as R, and flexibility to capture various forms of mutual influence between CIs. We illustrate this by giving a small example. The main contribution of this work is a model that partly unifies three different models of risk propagation (Bayesian networks, percolation and system dynamics) under a single simulation/percolation framework.**

***Index Terms*—critical infrastructure; stochastic dependencies; Markov chain; risk propagation**

I. Introduction

Critical infrastructures (CIs) are typically supply networks satisfying the basic needs of society, such as power, water, food, health care, transportation, etc. Besides this high dependency of the society on CIs, there are also mutual dependencies among these CIs, such as hospitals depend on electricity, water, food supply and working transportation lines. A main characteristic of a CI is that a failure with a CI does not only affect the CI itself, but has a huge impact on the dependent CIs, as well as on society. This has manifested in the last years as, for example, the disruption of electric power in California in 2001 [1] affected several other critical infrastructures, the major power outage in Italy [2], which lasted for about 12 hours, resulted in a financial damage of over 1 billion euros or the most recent hacking of the Ukrainian power grid caused a power outage of several hours [3]. In general, such dependencies between CIs can be either *continuous*, as it is the case of electricity where a stable supply is required, or *instantaneous*, for example, if the CI's support is just required in an emergency situation (e.g., police, fire brigade, or similar). In this work, we consider structures that mutually and *continuously* depend on input from several providers, such as water or electricity (see [4][5], for a more detailed discussion). The case of an instantaneous dependency will be revisited briefly later on.

Reduced or even missing supply from a critical provider may cause significant problems for an infrastructure. The actual damage depends on the degree of failure of the provider, but is also influenced by many other factors such as availability of substitutes (see [6] for work related to water supply). Since the consequences of a reduced support are not always exactly predictable, we introduce a stochastic model that describes how a critical infrastructure depends on other infrastructures whose input is needed for smooth operation. This abstract model can be applied to any type of infrastructure, as long as the dependencies from other infrastructures are known and can be classified qualitatively in terms of "how severe" a provider's outage is on a finite scale (say, from 1 to 5. See [7] for a discussion of this requirement in light of compliance, auditing and monitoring). The model thus speaks about different "degrees of failure", where the particular meaning of such a "degree" is up to the specific characteristics of the CI (e.g., status 3 may mean different things or problems for a water provider than for a hospital). In particular, not every failure yields to a complete blackout of the infrastructure of interest. On the other hand, the model is not too complex by considering only dependencies between two infrastructures at a time and by grouping infrastructures into different classes with different characteristics.

Paper Outline

The remainder of this article is organized as follows: after a recap of the current research situation in Section II, Section III introduces our model for dependencies between critical infrastructures. Section IV describes how such a model may be used to simulate how the states of a critical infrastructures change and Section V shows a small example. Finally, we provide concluding remarks in Section VI.

II. Related Work

Several models have been developed for dependencies among critical infrastructures. In [8], a framework for addressing infrastructure interdependencies is presented that describes five different classes of critical infrastructure interdependencies (including also dependencies of information and communication technologies). Recent models consider random

 ISBN: 978-1-61208-582-1

failure and stochastic dependencies. For example, a multi-graph model is used to analyze random failures and their effects on critical infrastructures in [9]. Other models look explicitly at interdependencies of higher order to identify and assess the effect of failures not only for direct "consumers" but also for subsequent infrastructures in the dependency chain [10][11]. Such cascading effects have been investigated in [12] by means of an Input-output Inoperability Model (IIM) that is based on financial data. Further, Hierarchical Holographic Modeling (HHM) [13] has been used to describe the diverse nature of CI networks and analyze failures therein. More complex models are based on Bayesian networks [14] as, for example, the Hierarchical Coordinated Bayes Model (HCBM) [15] or other approaches (cf. [16] and references therein). Our work is also related to various approaches by simulation and co-simulation [17][18][19][20][21]. Typically, these are applicable when the analyst is much more informed about the infrastructure in question, since the simulation depicts the internal dynamics (even up to the level of concrete network packets to be exchanged). Our perspective is much more high-level and assumes the absence of these details up to only categorical valuations of interdependencies (cf. [4][22][23][24] for more comprehensive overviews).

III. Random Dependencies of a Critical Infrastructure

Dependencies between CIs are conveniently described by a simple directed graph. The nodes represent the CIs and a directed edge from CI 1 to CI 2 indicates that CI 2 depends on input from CI 1. Such a visualization helps to get an overview of dependencies in a larger area (e.g., in a geographical region or an entire country) but it is not suitable to get a deeper understanding of how these dependencies influence the functionality of the CIs. For this sake, the model needs to describe both the critical infrastructures as well as the dependencies between them in more detail. At the same time, it is infeasible to describe every possible impact of every dependency since such a model grows exponentially (in the number of parameters). As a trade-off, we propose the following solution on middle ground.

A CI is described as a node that can be in one of k different *states* representing its functionality where state 1 represents the situation where everything works smoothly, ranging up to state k that means total failure, with intermediate states corresponding to different levels of restricted service provisioning. Each CI continuously depends on input from different *providers* that may not always work correctly themselves. Even a partial failure of one provider may change the CIs state. For example, if there is not enough electricity most infrastructures are affected in some way and may no longer work properly. This situation is captured by describing each CI as a 'big' node with two types of internal nodes: k *status nodes* indicate the state of the CI itself while $n_i \cdot k$ *input nodes* represent all possible states of the n_i input nodes (provider).

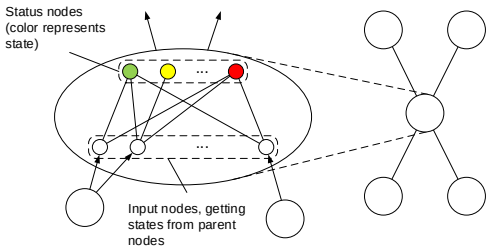

Fig. 1. Model of the inner structure of a critical infrastructure

This idea can be visualized, as shown in Figure 1, by representing each of the k states of the CI by a node with a color representing the degree of damage (cf. the top set of nodes in Figure 1). Each of the n_i provider may again be in one of the same k states and we represent all these different configurations by $n_i \cdot k$ nodes below the status nodes. Note that this modeling allows a node to be in several states simultaneously. The state communicated to the next node is, according to the maximum principle, the most severe among the given states (i.e., a system is only as secure as its weakest element). In practice, a node may indeed encounter multiple problems of different severity at the same time; nonetheless, the degree of trouble in which a CI is, is surely determined by the most severe of its current issues. Moreover, the model straightforwardly generalizes to several states in different respects, say, if a number $d > 1$ of distinct security goals are in question. For instance, a node could maintain a status regarding confidentiality, and another status regarding availability. In this context, imagine an electricity provider who has experienced a data leakage where customer data has been stolen. This is a confidentiality breach, but the power supply is still up and running, so there is no availability issue. In that case, we can make the internal graph d-partite, with d output layers, each corresponding to its own security goal. The status reported to subsequent nodes is then the worst status per security goal (and not the overall worst case status over all nodes, since this would not make sense for obvious reasons; just reconsidering the availability vs. confidentiality example from before).

As consequences of (partial) failure of a provider are not always predictable and depend on many factors that cannot be controlled (in particular they depend on other suppliers themselves), we apply a stochastic model to describe the influence an CI has on another. More explicitly, this means that the current state of one provider yields a specific state of the critical infrastructure only with a certain probability. In other words, any edges in Figure 1 transmits a problem with a specific probability. We assume that every node in the lower row (representing one state of one provider) has the potential to change the state of the CI. Technically speaking, we describe changes between the states of the CIs as a Markov chain, that is, every state of a provider influences the state of the infrastructure it provides input for. This includes the situation where the state does not change as well as the situation that

 ISBN: 978-1-61208-582-1

the condition gets better since one of the providers recovered. A more detailed analysis of such situations is postponed to future work.

A. The Model

Let us take a look on a critical infrastructure v that provides input to another infrastructure u. The state of u changes depending on the states of its provider v but these changes are by no means predictable. Thus, we describe the state by a random variable S that is multinomial distributed, which we denote by MN($\vec{p}$), i.e., the j-th component p_j of $\vec{p}$ gives the probability that S takes on the value j. These likelihoods depend on the current state i of the input node, i.e., if u works properly it is not likely that the dependent node v faces serious problems. Thus, we describe these transitions by a stochastic matrix. However, the transition probability is also influenced by the type of connection between the two nodes. For that purpose, we classify all edges and define a transition probability matrix for each of the defined classes that represents its characteristics. Thus, if a node v is in state i and the connection to u is of class c, the state of u follows a multinomial distribution NM($\vec{p}_{i,c}$) with a probability vector $\vec{p}_{i,c}$. In the graphical model of Figure 1, the possible transitions and likelihoods are reflected in the bipartite graph, and the transition matrix is the *biadjacency* matrix of that bipartite graph.

B. Relation to Other Models

The model used here can be seen as a generalization of the stochastic error spreading model in [25] in the sense that the (real-valued) transition probabilities between different components are replaced by transition matrices that describe the influence for each level of failure. More precisely, we can replace the transition probability p_i for an edge of type i by a stochastic matrix $\vec{P}_i$ that describes the transition probabilities for each degree of failure for both the dependent and the depending node. As described in [26], these probabilities can be estimated by expert opinions (e.g., by taking the median of all scores assigned by experts) or other stochastic models, such as described in [27].

Moreover, some simple forms of Bayesian networks also appear as special cases of this model: let in be a node over which a parent reports its status, and let $v_1, \ldots, v_k$ be the status nodes of the CI. The weight that the model assigns to the edge $in \to v_i$ is the conditional probability $\Pr(v_i|in)$. This is just what a Bayesian network [28] would describe/require in the same modeling. The difference to general Bayesian networks lies in the difficulty to express joint distributions in this form, since an output state is conditionally dependent on several input nodes, but not jointly conditionally so.

Finally, by making the edge weights for the model binary, we can model deterministic dependencies to some extent: for example, if the outage of a parent node causes the outage of the given CI, then the respective internal edges in the bipartite inner model graph get assigned the weight 1. This will cause the simulated chain to go to the worst status node for sure when its parent has an outage. Again, not all kinds of dynamics can be expressed like this, for the same reasons as with the general Bayesian networks.

The limitations imposed here save us from the exponential complexity that Bayesian networks induce for their specification (as we would require a conditional probability on all subsets of parent nodes; and there are exponentially many of them). For deterministic dynamics, there are endless possibilities to describe what can happen using rules; a sufficiently flexible way of representing such dynamics is, indeed, offered by Bayesian networks, but this comes with the same complexity issues as mentioned before. In light of this, the limitations are a trade-off between model flexibility and computational feasibility of its specification.

IV. Simulation of Stochastic Dependencies

The stochastic dependency model between critical infrastructures can straightforwardly be implemented in a software such as `R`. This simulation starts with an incident happening at some node, which subsequently (and indirectly) triggers descendant CIs to change their status according to the likelihoods in their inner bipartite graphs. The simulation thus reveals how far an incident will propagate (within the runtime of the simulation), and can thus be used to estimate the effect a problem in one component has on a specific critical infrastructure or generally on other components. Additionally, it allows an empirical estimation of the number of components that are in a critical state (i.e., reach the highest status k).

More explicitly, we model the network of infrastructures as a graph with n vertices $v \in V$ that represent the infrastructures and edges $e \in E$ representing the connections between them. A usual difficulty in specifying such probabilistic models is the issue of where to get the conditional probabilities from. To mitigate this practical obstacle, we let the weighting be discrete and according to edge classes, meaning that each edge (representing an inner or mutual dependency) is assigned to one class c out of the set $\{1, 2, \ldots, C\}$ of candidate classes, in which each class represents a different levels of importance of a CI for its successor CI (provider-consumer dependency). Each edge $v \to u$ is then associated with a representative number for its class c that acts the probability used for the simulation. This allows the model parameterization to be done upfront and independent of the concrete CI, and eases matters of model parameterization in absence of empirical data to estimate conditional probabilities. Depending on this class c the state i of v influences the state of u through a multinomial distribution MN($p_{i,c}$). That is, the j-th component of the vector $p_{i,c}$ gives the probability that u will be in state j in this situation. In pseudo-code, an algorithm that simulates T timesteps looks as shown in Figure 2.

The result of this simulation is a network of connected critical infrastructures where each CI is in a specific state. For visualization, we can use color codes, ranging from green to indicate a working state to red, alerting about a critical

 ISBN: 978-1-61208-582-1

```
1: t ← 0
2: while t < T
3:   for each node v, set N(v) = {u ∈ V : (v,u) ∈ E}
4:     for each neighboring node u ∈ N(v)
5:       let c be the class of v → u,
6:       let i be the current state of node v,
7:       draw the status of u from MN(p_{i,c})
8:       t ← t + 1.
9:     endfor
10:  endfor
11:endwhile
```

Fig. 2. Simulation Algorithm

condition. Numerically, the results of the simulation can be summarized as a table that lists how many components are on average in any of the possible states.

V. An Illustrative Example

Let a subnetwork of a CI consist of a hospital that depends on a water provider, an electricity provider as well as transportation infrastructures (roads). The dependencies between the different components in the network are classified as either "minor", "normal" or "critical" depending on how important the service provisioning is for the CI. In this small example, we classified input from the electricity provider as "normal" (as we assume existence of an emergency power system), input from a water provider as "critical" (substitution by bottled water is usually just possible for a limited period of time) and the transport connection as "minor", since even if roads are temporarily congested or blocked, aerial transportation remains possible for critical patients.

Arbitrary transition matrices were chosen depending on the class of the connection. Here, we consider 5 possible states for each node, where 1 represents the situation where everything works smoothly, while 5 stands for serious problems including total failure. In a practical application, these values need to be estimated by experts familiar with the infrastructure's operation (possibly aided by other simulation methods accounting for the internal system dynamics). For the specification of a dependency on the chosen scale from 1 to 5, we specify a matrix $T_{minor/normal/critical} = (t_{ij})_{i,j=1}^{5}$, in which the ij-th entry corresponds to the conditional likelihood $t_{ij} := \Pr(\text{CI gets into state } j \mid \text{provider is in state } i)$. For the example, let

$$T_{minor} = \begin{pmatrix} 0.6 & 0.2 & 0.2 & 0.0 & 0.0 \\ 0.5 & 0.2 & 0.2 & 0.1 & 0.0 \\ 0.4 & 0.2 & 0.2 & 0.2 & 0.0 \\ 0.3 & 0.2 & 0.2 & 0.2 & 0.1 \\ 0.3 & 0.2 & 0.2 & 0.2 & 0.1 \end{pmatrix},$$

$$T_{normal} = \begin{pmatrix} 0.4 & 0.2 & 0.2 & 0.2 & 0.0 \\ 0.4 & 0.2 & 0.1 & 0.3 & 0.0 \\ 0.3 & 0.2 & 0.2 & 0.2 & 0.1 \\ 0.2 & 0.2 & 0.2 & 0.3 & 0.1 \\ 0.2 & 0.2 & 0.1 & 0.3 & 0.2 \end{pmatrix}$$

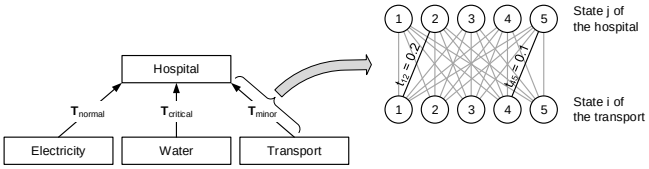

Fig. 3. Example Instance

and

$$T_{critical} = \begin{pmatrix} 0.3 & 0.2 & 0.2 & 0.2 & 0.1 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.0 & 0.2 & 0.2 & 0.3 & 0.3 \\ 0.0 & 0.1 & 0.2 & 0.3 & 0.4 \\ 0.0 & 0.0 & 0.0 & 0.2 & 0.8. \end{pmatrix}.$$

Figure 3 (left side) displays the dependencies graphically, with arrows annotated according to the criticality of the dependency. The right part of Figure 3 shows how the inner model of Figure 1 corresponds to a dependency, and is instantiated according to the matrices above. For example, if a provider classified as "minor" is in state 4 (i.e., it has rather serious problems) this will yield to a state 5 of the critical infrastructure that depends on it with a likelihood of 0.1.

Initially, we assume that all components operate smoothly and are in state 1 except for the water provider that is in state 2 facing some (temporary) problems. This scenario yielded to a critical state for the hospital in 16 out of 100 cases. Note that in this example, this critical state can only be caused by the state of the water provider since a CI of normal or even minor importance will never cause a critical level while bing in state 1 (i.e., both entries in the transition matrices are zero).

In Table I we show the average number of nodes (CIs) that are in each of the 5 possible states. This information is especially useful in larger networks to get an overview on the impact of a problem in one critical infrastructure on the entire network of CIs.

TABLE I. AVERAGE NUMBER OF AFFECTED NODES DUE TO INCREASED LEVEL OF CRITICALITY

Criticality	1	2	3	4	5
Nodes	2.05	1.15	0.31	0.33	0.16

VI. Conclusion and Future Work

In this work, we introduced a model for dependencies between critical infrastructures that assumes random effects of failures. In particular, the extent to which a problem in one infrastructure influences another one depends on how serious the problem is (represented by the state of this infrastructure) and by the nature of the connection between them (described by the connection's classification). The effect on another infrastructure is again described through several states that indicate the severity. However, the effect itself is random due to the impossibility of precise prediction. While this model captures many important aspects of such dependencies it is still quite simple and can straightforwardly be implemented. We

 ISBN: 978-1-61208-582-1

have sketched the implementation in pseudo code and applied the simulation to a small example.

Extensions to the model along future work are possible in various ways. In the form presented, the model assumes an independent influence of all providers to a specific CI. Dependencies with an inner interplay of two providers cannot be described in the given model. For example, two providers being mutually substitutes for one another, a dependency of a CI on the total input of several providers (irrespectively of the individual supplies). Taking these into account seems to involve more complex stochastic dependency models (e.g., copulas [29]) to describe distributions conditional on several variables. At the same time, this also brings the model complexity closer to exponential in the number of the CIs, with Bayesian networks being located at the end of the spectrum along this generalization. A "middle ground model" is thus an interesting goal to strive for, starting from our work presented here.

ACKNOWLEDGMENT

This work was done in the context of the project "Cross Sectoral Risk Management for Object Protection of Critical Infrastructures (CERBERUS)", supported by the Austrian Research Promotion Agency under grant no. 854766.

REFERENCES

[1] S. Fletcher, "Electric power interruptions curtail California oil and gas production," *Oil Gas Journal*, 2001.

[2] M. Schmidthaler and J. Reichl, "Economic Valuation of Electricity Supply Security: Ad-hoc Cost Assessment Tool for Power Outages," *ELECTRA*, no. 276, pp. 10–15, 2014.

[3] J. Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," 2016, URL: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/ [accessed: 2017-07-26].

[4] R. Setola, V. Rosato, E. Kyriakides, and E. Rome, Eds., *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach*, ser. Studies in Systems, Decision and Control. Cham and s.l.: Springer International Publishing, 2016, vol. 90.

[5] R. Klein, E. Rome, C. Beyel, R. Linnemann, W. Reinhardt, and A. Usov, "Information modelling and simulation in large interdependent critical infrastructures in irriis," in *Critical Information Infrastructure Security: Third International Workshop, CRITIS 2008, Rome, Italy, October13-15, 2008. Revised Papers*, R. Setola and S. Geretshuber, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 36–47.

[6] E. Luiijf, M. Ali, and A. Zielstra, "Assessing and improving scada security in the dutch drinking water sector," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 3-4, pp. 124–134, 2011.

[7] A. Abou El Kalam and Y. Deswarte, "Critical infrastructures security modeling, enforcement and runtime checking," in *Critical Information Infrastructure Security: Third International Workshop, CRITIS 2008, Rome, Italy, October13-15, 2008. Revised Papers*, R. Setola and S. Geretshuber, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 95–108.

[8] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, pp. 11–25, 2001.

[9] N. K. Svendsen and S. D. Wolthusen, "Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models," in *2007 IEEE SMC Information Assurance and Security Workshop*, June 2007, pp. 247–254.

[10] M. Theoharidou, P. Kotzanikolaou, and D. Gritzalis, "Risk assessment methodology for interdependent critical infrastructures," *International Journal of Risk Assessment and Management*, vol. 15, no. 2-3, pp. 128–148, 2011, [accessed: 2017-08-15]. [Online]. Available: http://www.inderscienceonline.com/doi/abs/10.1504/IJRAM.2011.042113

[11] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Assessing n-order dependencies between critical infrastructures," *International Journal of Critical Infrastructures*, vol. 9, no. 1-2, pp. 93–110, 2013, URL: http://www.inderscienceonline.com/doi/abs/10.1504/IJCIS.2013.051606 [accessed: 2017-08-01].

[12] R. Setola, S. De Porcellinis, and M. Sforna, "Critical Infrastructure Dependency Assessment Using the Input-Output Inoperability Model," *International Journal of Critical Infrastructure Protection (IJCIP)*, vol. 2, pp. 170–178, 2009.

[13] Y. Y. Haimes, "Hierarchical Holographic Modeling," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 11, no. 9, pp. 606–617, 1981.

[14] M. I. Jordan, Ed., *Learning in graphical models*. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1999.

[15] Y. Haimes, J. Santos, K. Crowther, M. Henry, C. Lian, and Z. Yan, "Risk Analysis in Interdependent Infrastructures," in *Critical Infrastructure Protection*, ser. IFIP International Federation for Information Processing. Springer, Boston, MA, 2007, pp. 297–310.

[16] T. Schaberreiter, S. Varrette, P. Bouvry, J. Röning, and D. Khadraoui, *Dependency Analysis for Critical Infrastructure Security Modelling: A Case Study within the Grid'5000 Project*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 269–287.

[17] R. Caire, J. Sanchez, and N. Hadjsaid, "Vulnerability analysis of coupled heterogeneous critical infrastructures: A Co-simulation approach with a testbed validation," in *IEEE PES ISGT Europe 2013*. IEEE, 2013, pp. 1–5.

[18] R. Jaromin, B. Mullins, J. Butts, and J. Lopez, "Design and Implementation of Industrial Control System Emulators," in *Critical Infrastructure Protection VII*, ser. IFIP Advances in Information and Communication Technology, J. Butts and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, vol. 417, pp. 35–46.

[19] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications," in *ISGT 2011*. IEEE, 2011, pp. 1–6.

[20] M. Faschang, F. Kupzog, R. Mosshammer, and A. Einfalt, "Rapid control prototyping platform for networked smart grid systems," in *Proceedings IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society*. Vienna, Austria: IEEE, 2013, pp. 8172–8176.

[21] M. Findrik, P. Smith, J. H. Kazmi, M. Faschang, and F. Kupzog, "Towards secure and resilient networked power distribution grids: Process and tool adoption," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*. Sidney, Australia: IEEE Publishing, 2016, pp. 435 – 440.

[22] J. Butts, *Critical Infrastructure Protection VII: 7th IFIP WG 11. 10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers*, ser. IFIP Advances in Information and Communication Technology. Berlin/Heidelberg: Springer Berlin Heidelberg, 2013, vol. v.417, URL: http://ebookcentral.proquest.com/lib/gbv/detail.action?docID=3091963 [accessed: 2017-07-31].

[23] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. IEEE, 2004, pp. 1–8.

[24] E. Wiseman, "Critical Infrastructure Protection and Resilience Literature Survey: Modeling and Simulation," URL: http://www.dtic.mil/get-tr-doc/pdf?AD=AD1003598 [accessed: 2017-07-31].

[25] S. König, S. Schauer, and S. Rass, *A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks*. Cham: Springer, 2016, pp. 67–81.

[26] S. König, S. Rass, S. Schauer, and A. Beck, "Risk Propagation Analysis and Visualization using Percolation Theory," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no. 1, pp. 694–701, 2016.

[27] L. Carin, G. Cybenko, and J. Hughes, "Cybersecurity Strategies: The QuERIES Methodology," *Computer*, vol. 41, no. 8, pp. 20–26, 2008.

[28] T. Koski and J. M. Noble, *Bayesian Networks*, ser. Wiley Series in Probability and Statistics. Wiley, 2009.

[29] R. B. Nelsen, *An Introduction To Copulas*, ser. Lecture Notes in Statistics 139. Springer, 1999.

 ISBN: 978-1-61208-582-1