Multigraph Critical Infrastructure Model

Bernhard Schneidhofer, Stephen Wolthusen

To cite this version:

Bernhard Schneidhofer, Stephen Wolthusen. Multigraph Critical Infrastructure Model. 10th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2016, Arlington, VA, United States. pp.149-167, 10.1007/978-3-319-48737-3_9. hal-01614863

Chapter 9

MULTIGRAPH CRITICAL INFRASTRUCTURE MODEL

Bernhard Schneidhofer and Stephen Wolthusen

Abstract Interdependencies between critical infrastructures have been studied widely, but largely at the abstract and structural levels with an emphasis on large infrastructure networks and frequently their stochastic properties. However, an in-depth understanding of infrastructure interdependencies and the likely impact of degradation of selected elements are important for an adversary intent on maximizing attack efficiency. This chapter describes a simple multigraph model for several classes of interdependent critical infrastructure elements and an attack tree model with attribute domains extended by acyclic phase-type distributions to capture temporal dependencies. The efficacy of this modeling approach is demonstrated via a case study involving regional interdependent infrastructures that include the electric power, water and telecommunications sectors in a bounded region. The case study uses extensive simulations to demonstrate that an adversary with access only to publicly-available information and the ability to analyze a multigraph model can cause severe harm.

Keywords: Infrastructure dependency analysis, multigraph model, attack modeling

1. Introduction

Considerable research has been devoted to understand dependencies and interdependencies between critical infrastructures, including approaches that leverage graph models and graph metrics and algorithms to determine the criticality of infrastructure elements [6]. Such dependencies may extend to multiple levels and result in cascading effects [15] that, in turn, can form the basis of risk assessment and mitigation mechanisms [17].

It is frequently of interest to understand how infrastructure sectors and elements in the sectors interact in a heterogeneous infrastructure network rather than considering infrastructure elements as a single, homogeneous structure.

This has been studied previously with particular emphasis on the interconnections between the electric power and information infrastructures [5, 19].

However, many vulnerability effects resulting from disruptions are not immediately visible from a mere study of the connectivity between components; instead, they require the explicit consideration of dependency links [7]. It is important to note that it is not only different infrastructure sector networks that exhibit such properties, but that the effects also arise from other aspects such as proximity [1] and clustering of embedded sub-networks [4]. At the same time, most research on susceptibility to attacks has concentrated on homogeneous networks [10], with some work explicitly considering attacks on individual sub-networks [12] and their join structures [21].

A natural question that arises from this research is whether the models may be employed to identify attack vectors or, conversely, targets that require particular attention because their loss could have disproportionate effects. In an attempt to answer this question, this research enhances earlier work on multigraph models [19] by a constructive mechanism for attack vector identification. Specifically, attack trees with attribute domains proposed by Kordy et al. [14] are extended by acyclic phase-type distributions proposed by Arnold et al. [2] to capture temporal dependencies [2]. A key contribution of this chapter is the use of an extended case study that engages open-source intelligence for a bounded region comprising the electric power, water supply and telecommunications sectors to validate the proposed modeling approach. The approach provides a lower bound on an adversary's ability to identify vulnerable structures and dependencies. The results demonstrate that even with modest effort it is possible to construct attack scenarios that have significant impacts.

2. Modeling Framework

It is relatively straightforward to divide an infrastructure (sector) network into structural and functional aspects. For example, a water supply system can be expressed as a topology of pumping stations and interconnecting pipes as well as annotations (capacities and gradients), while the functional aspect can be represented as network flows. Both aspects can be subjected to disturbances such as stochastic failures, constraints and deliberate attacks.

Based on the work of Svendsen and Wolthusen [19, 20], a heterogeneous infrastructure network is formally defined as a graph $\mathcal{N}$ whose vertex set $V(\mathcal{N}) = \{v_1, \dots, v_k\}$ comprises components (nodes) capable of producing, storing or consuming services of fungible resources that flow through the network. Each pairwise dependency between nodes is represented as an arc whose head node is dependent on the tail node. Appropriate differentiation between types of services is achieved by introducing dependency types.

A dependency type is a type of interaction between two vertices. This can either be the delivery of a service or a fungible resource. The set of dependency types $\{d_1, \dots, d_m\}$ is denoted by $\mathcal{D}$. The i^{th} arc carrying dependency type d_j between two vertices v_a and v_b is uniquely defined as $(v_a, v_b)_i^j$. The corresponding arc set is:

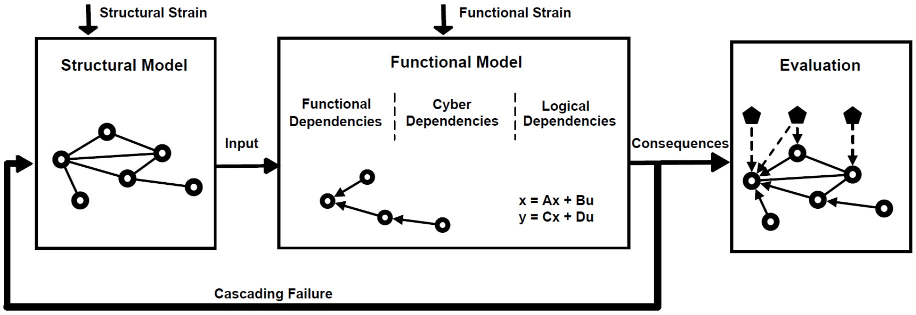

Figure 1. Modeling a single infrastructure (adapted from [11]).

$$\mathcal{A} = \{(v_1, v_2)^1_1, \ldots, (v_{k-1}, v_k)^m_{e_{(k-1,k,d)}}\}$$

where $e_{(k-1,k,d)}$ is the number of arcs from $v_{k-1,k}$ to v_k of type d_m.

2.1 Individual Infrastructure Graphs

An infrastructure network can also be partitioned as proposed by Johansson and Hassel [11] with an additional static hierarchical layer inserted to facilitate evaluation as illustrated in Figure 1.

To derive the functional model, the structural model is evaluated to identify the physical, cyber and logical dependencies as well as the dependency types. External strain to the model can be applied in two ways: (i) structural strain; and (ii) functional strain. Structural strain, such as the complete failure of a substation in an electric power network, corresponds to the removal of a component in the graph. Functional strain can be represented by changing the system constraints and evaluating the changes in generation, supply and demand.

2.2 Interdependent Infrastructures

To obtain an interdependence model, various structural models of the critical infrastructure sectors are merged into a single structural model via the multigraph representation with suitable join structures. This requires the evaluation of each individual infrastructure with respect to all others in order to identify and add structural dependencies between them when necessary.

3. Modeling Approach

A bounded region in Austria was chosen to validate the model and, especially, attack mechanism discovery. The pertinent data sets came from a geographical information system set up as part of the INSPIRE Project as required by European Council Directive 2007/2/EC [8] as well as maps and cartographical

Table 1. Openly-available information about the electric power sector.

	Information Areas								
Categories	**Substations**	**Grid Groups**	**Power Supply Lines**	**Power Line Specifications**	**Transformers**	**Busbars**	**Power Generation**	**Power Consumption**	**Geographical Location**
380 kV	✓	✓	✓				N/A.	P	✓
220 kV	✓		✓	✓			N/A	P	✓
110 kV	✓	✓	✓			P	N/A		✓
Power Stations	N/A	✓	✓	✓	✓	✓	✓	✓	✓
Load Nodes	N/A	✓	✓				N/A		✓

information provided by the Austrian Federal Office for Metrology and Surveying and the System Study Model provided by the European Network of Transmission System Operators for Electricity (ENTSO-E) [16].

3.1 Electric Power Sector Model

Geographical information system data of the target area and additional map overlay layers for electric grids were the basis for the electric power sector model. Over the course of two weeks in March 2015, a dedicated field survey was conducted in the target area to verify and supplement the model data. Table 1 provides an overview of the acquired data. Note that ✓denotes available, P partially available and N/A not applicable.

The structural model of the electricity sector comprises 543 nodes and 603 edges with five voltage levels ranging from 20 kV to 380 kV. The nodes represent substations, power stations and power line junctions, and the edges represent power lines (overhead and underground). The total nominal power generation capacity of all the power stations in the model is 1,012.33 MW.

The graph of the functional model comprises directed edges that represent chains of up to seven wind turbines connected in series to a single busbar. Figure 2 shows the mixed graph of the functional and structural models. The graph of the functional model is traversed in a breadth-first manner starting at substations and terminating at each reachable wind turbine to calculate simulation values (e.g., available nominal generation capacity values). Each wind turbine is a closed-loop control system that is dependent on an embedded microcomputer. The cyber dependencies are modeled as 427 additional directed dependency edges from the electric power sector model to the telecommunications and SCADA sector models.

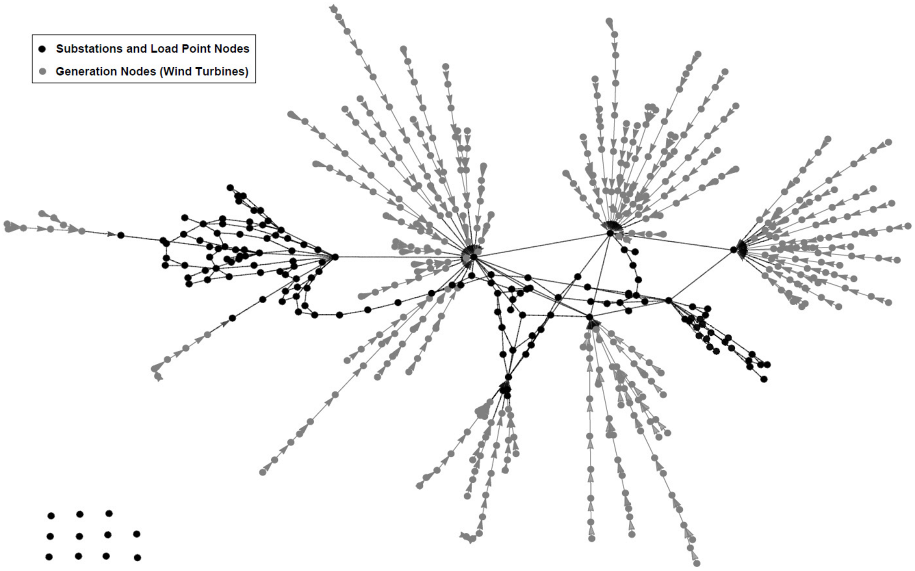
● Substations and Load Point Nodes
● Generation Nodes (Wind Turbines)

Figure 2. Combined structural and functional models for the electric power sector.

Table 2. Openly-available information about the water sector in the target area.

	Information Areas							
Facilities	**Generation Capacity**	**Throughput Capacity**	**Storage Capacity**	**Flow Direction**	**Technical Specifications**	**Power Grid Connection**	**Water Consumption**	**Geographical Location**
Wells	✓	✓	✓	✓	P	✓	N/A	✓
Purification	✓	✓	✓	✓	P	✓	N/A	✓
Pressure Booster Stations	✓	✓	✓	✓	P	✓	N/A	✓
Reservoirs	✓	✓	✓	✓	P	✓	N/A	✓
Pipes	N/A	✓	N/A	✓	✓	N/A	N/A	✓
Load Nodes	N/A	N/A	N/A	N/A	P	P	✓	✓

3.2 Water Sector Model

Information pertaining to the water sector model was obtained from the regional water distribution system operator and from self-supplying municipalities. Table 2 provides an overview of the acquired information. Note that ✓denotes available, P partially available and N/A not applicable.

The structural model of the water sector is based on cartographic data of the water system and pipe network supplied by the water distribution system operator. In total, the water network is represented in terms of 178 nodes and 194 edges. The nodes correspond to wells, purification plants, pressure booster stations, reservoirs and pipe junctions. Edges represent different kinds of water pipes. The graph representation of the functional model was derived from the logical operation and water flow directions of the system in its nominal operating mode. The supplementary functional model of the water distribution system is expressed as a capacity model that considers in-feed node capacity and load node demand. The consequences arising from system strain were estimated using breadth-first searches. Note that wells, purification plants and pressure booster stations need electricity to function. The electric power grid has 49 20 kV power junctions that supply the water nodes and create physical dependencies between the electric power and water sectors.

3.3 Telecommunications Sector Model

Data for the telecommunications sector was sourced from network backbone planning documentation in the target area and supplemented by planning documents from wind turbine operators and the electric power telecommunications network operator; this data was referenced to a geographical information system. The structural model comprises 434 vertices and 466 edges. The vertices represent network backbone nodes, wind turbine closed-loop control systems, SCADA command centers and substation network nodes; and the edges represent various types of telecommunications cables. The functional model of the telecommunications sector is not expressed in terms of dependency edges, but functionally as executable code. Each wind turbine intelligent electronic device is considered to be functional if there is a communications path between the device and its operator's SCADA center or substation. Five dedicated SCADA centers belonging to the involved wind farm operators and thirteen substation telecommunications centers were identified from the gathered information.

4. System Analysis

The model described above was used to conduct a vulnerability analysis. This, in turn, was used to construct attack scenarios based on the reference scenario presented in Section 5. In order to be able to triage attack scenarios, it was necessary to obtain additional information about the operating parameters because the basic model retains only relatively coarse information that does not allow the effective ranking of candidate attacks. The analysis presented below was performed using a mixed discrete event simulation approach.

4.1 Global Vulnerability Analysis

A global vulnerability analysis was conducted to obtain an overview of the vulnerabilities present in the modeled systems, the associated consequences

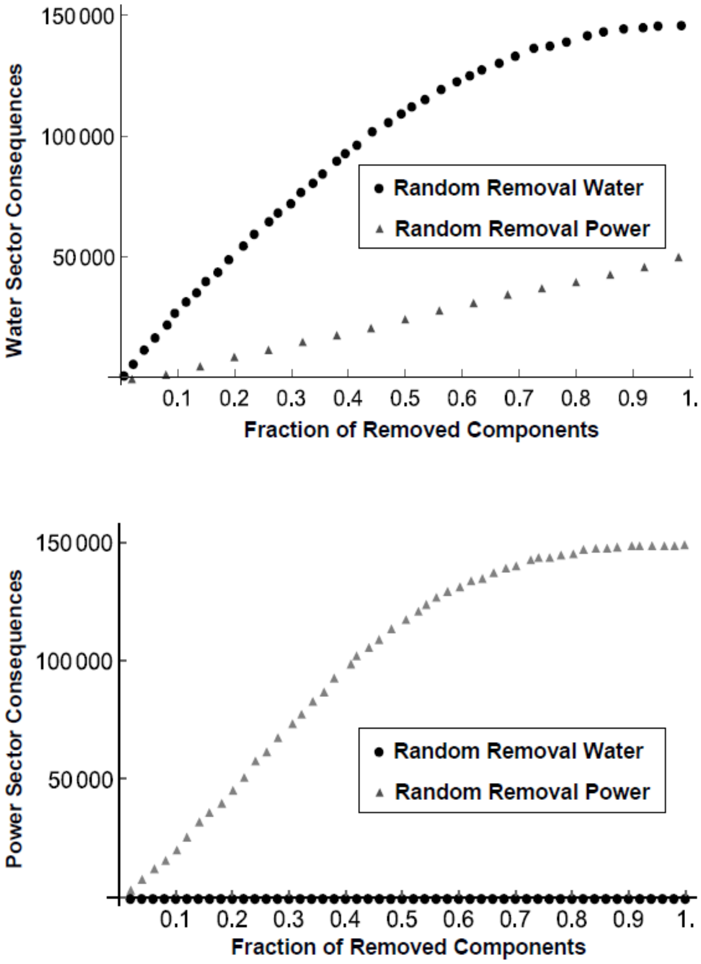

Figure 3. Estimated consequences following random vertex removal.

of failure scenarios and the (inter)dependency characteristics in the combined model. The model was exposed to random vertex removal to obtain indicators of the strained infrastructure modes in the functional model. The consequence measures observed were the consumers without power or water supply and the gap between the nominal and available power generation capacities.

Electric Power and Water Supply Interaction. Figure 3 shows the strain in the form of random vertex removal applied to the electric power sector and water sector models (mean values computed after 100 iterations). From a vulnerability point of view, it can be argued that the electricity system is more robust to strains than the water system. In Figure 3 (top), it can be seen that

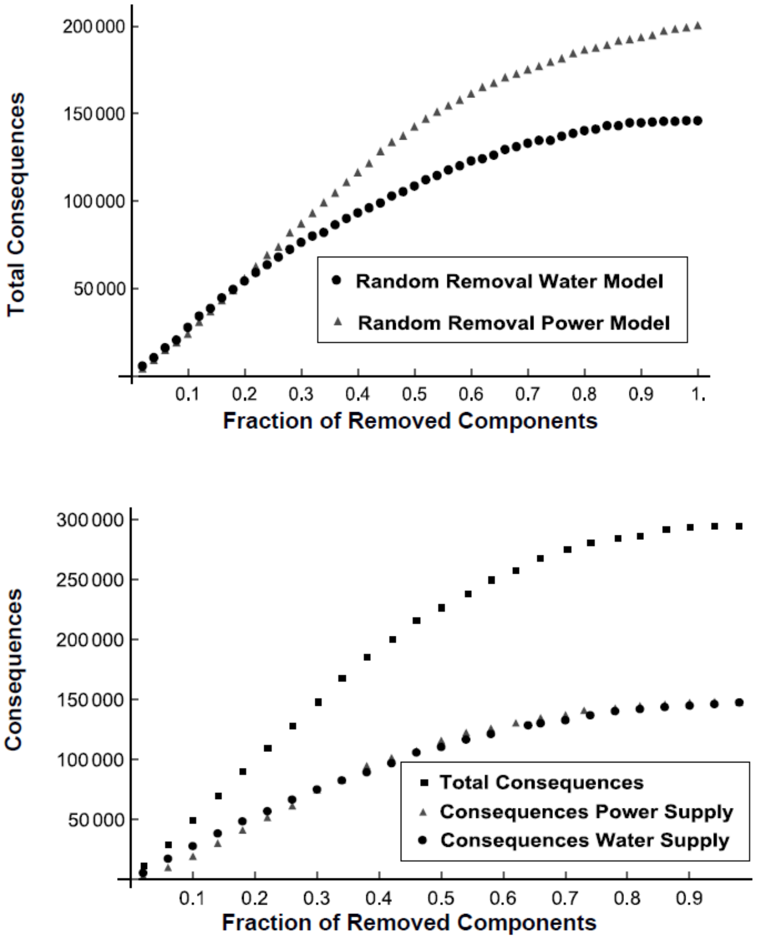

Figure 4. Total consequences following random vertex removal.

random vertex removal in the electricity model also has a significant impact on the water supply. When 20% of the vertices in the electricity model are removed, about 6% of the consumers also lose their water supply. On the other hand, Figure 3 (bottom) shows that there is no dependency of the electricity system on the water sector.

Figure 4 shifts the perspective to the global system (mean values computed after 100 iterations). Figure 4 (top) shows the total consequences – consumers who lose electricity and/or water supply when the model is exposed to strain in either sector. The total consequences are roughly equal up to the random removal of 22% of the nodes in either sector. After this threshold, random node removal in the power sector has higher overall consequences. Figure 4 (bottom) shows the results of an analysis in which nodes are randomly removed from

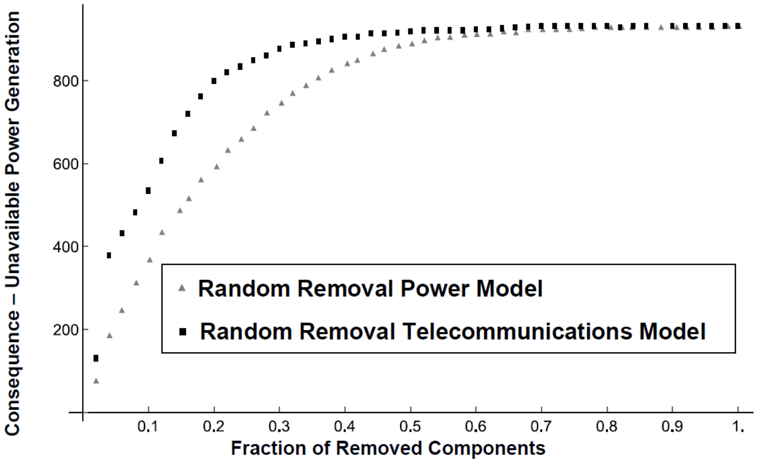

Figure 5. Power generation consequences (electricity and telecommunications).

both model components. The results show that, until 35% of the infrastructure nodes are removed, there are slightly higher consequences to the water sector than the electric power sector; beyond this threshold, the situation reverses.

Power Generation. Figure 5 shows the consequences in terms of the total nominal power output lost due to the wind turbines affected by the random removal of nodes in the electric power and telecommunications sectors. Interestingly, random removal of 10% of the nodes in the electricity model results in a lost nominal power output of about 300 MW, whereas the same 10% removal in the telecommunications model results in nearly 600 MW of lost nominal power output. In an attack scenario that is only concerned with this single consequence measure, targeting the telecommunications sector would be approximately twice as effective as targeting the electricity sector.

4.2 Critical Node Analysis

An attacker would be interested in identifying the weakest elements or largest consequence measures, including those resulting from cascading effects, in order to choose effective attack scenarios. Critical node analysis can offer valuable insights into attack selection. Note that, in this work, the search is restricted to dual simultaneous node failures instead of employing a more complex heuristic that would require 700,000 iterations.

Water and Power Supply. Table 3 lists the top five combinations for simultaneous failures in the electric power (P) and water (W) sectors. Also, it provides information about the strained nodes and consequences. The dual failure scenarios are dominated by the failure of Substation 2721, which supplies

Table 3. Top five subsets of critical components for simultaneous failures (P + W).

Rank	System {Component}	Strained Nodes Total (P + W)	Consequences P + W	Total Consequences
1	P {2721}, P {2742}	4 (2+2)	18512 + 7269	25781
2	P {2721}, P {2738}	4 (2+2)	17623 + 6293	23916
3	P {2721}, W {3735}	16 (1+15)	14787 + 8964	23751
4	P {2721}, P {2744}	2 (2+0)	23610 + 0	23610
5	P {2721}, P {2835}	3 (2+1)	14787 + 8759	23546

electricity to a number of nearby cities and enables a number of further scenarios with greater consequences. Around 75% of all computed dual failure scenarios have consequences in a single sector and roughly 12% of all scenarios have no consequences to electricity or water supply.

Table 4. Top five subsets of critical components for simultaneous failures (T + P).

Rank	System {Component}	Strained Nodes Total (T + P)	Consequences Power Generation
1	P {2770}, P {2849}	7 (5+2)	795.35 MW
2	P {2770}, T {4369}	5 (3+2)	795.35 MW
3	P {2770}, P {2715}	86 (2+84)	694.35 MW
4	P {2770}, T {4333}	85 (2+83)	694.35 MW
5	P {2770}, P {2719}	126 (3+123)	647.70 MW

Power Generation. Table 4 lists the top five combinations for simultaneous failures in the telecommunications (T) and electric power (P) sectors that result in severe consequences to the power generation grid group. The top five list is dominated by the top ranking single critical component, Electricity Node 2770, which supplies the SCADA center that manages the largest number of wind turbines. This readily identifies a measure for enhancing resilience.

5. Wind Turbine Attack Scenario

Based on the exploration in Section 4, the possibilities of interrupting power generation in the target area by attacking wind turbine telecommunications facilities and their control system networks are discussed. The attack goal for the wind turbine SCADA scenario is defined as follows:

- **Power Grid Frequency Impact:** The attack goal is set at 75 MW of power generation capacity to become unavailable within 30 seconds. This value corresponds to the primary control mechanism in the Austrian power grid [18]. A sudden loss of this magnitude would have a significant impact on the grid operation frequency [9].

5.1 Targeting a Wind Turbine System

The standard security approach in modern industrial networks is physical separation (i.e., air gap security), which is not a viable concept in this scenario. The real situation involves various electricity and telecommunications connections that bridge the gap in order to provide the required information, control and management functionality [13]. For the scenario at hand, the following three main attack paths for gaining access to the control networks are identified:

- **VPN and Remote-Dial-In:** Several wind turbine systems operate with backup telecommunications access via vulnerable virtual private network solutions over ISDN and leased lines.
- **Maintenance and Control Panels:** In some instances, the standard set-up for a wind turbine facility is altered with external control boards. The display cases are easily accessible at the ground level and make it simple to obtain physical access.
- **Webcams and Video Surveillance:** Several wind turbines in the target area are equipped with network cameras on top of their towers and entrance-area video surveillance cameras. In a limited number of cases, the cameras are connected to the control network and the camera administration web interfaces are directly available on the Internet via public IP addresses.

After access to the control network of a wind turbine system has been obtained, a variety of attacks ranging from man-in-the-middle to denial-of-service are possible. Figure 6 shows a standard network setup for a wind farm. The individual implementation details differ from model to model, but the overall design is similar.

5.2 Targeting Multiple Wind Turbines

Targeting a single wind turbine is inadequate to realize the scenario goal of causing a generation loss of 75 MW in a short timeframe. The following vulnerabilities could be leveraged to target multiple wind turbines at the same time:

- **Wind Farm Control PLC/RTU:** An attack on a wind farm control unit would enable the attacker to control a portion of the wind turbine control system. In the scenario at hand, this would result in a power loss of 18 to 30 MW for a single wind farm.
- **SCADA Center:** If access to the control network can be gained, it is feasible to target systems at a higher level from the supervisory network portion. This would influence a much larger number of wind turbines.

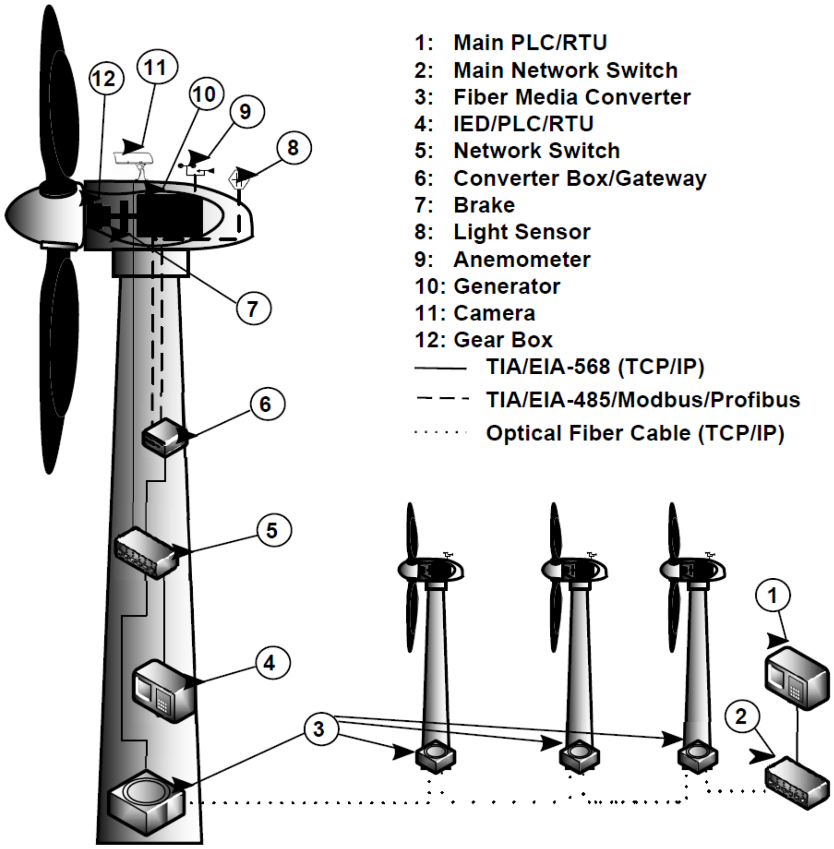

Figure 6. Wind turbine control system network (illustration by Arne Nordmann).

- **Safety Policies:** A legal requirement has a profound impact on the operating requirements for wind turbines. Specifically, to protect against ice shedding, it is inadequate to shut down a single affected wind turbine because the adjacent turbines may also suffer from icing. As a result, forced emergency shutdown commands must be sent to all the turbines in the vicinity. Re-starting each affected turbine requires manual intervention by a technician.

5.3 Attack Modeling

Detailed attack trees for the scenario were constructed to further explore the possible attacks on the control network. In particular, two different types of attack trees were employed: (i) attack-defense trees with attribute domains [3, 14]; and (ii) acyclic phase-type distributions [2].

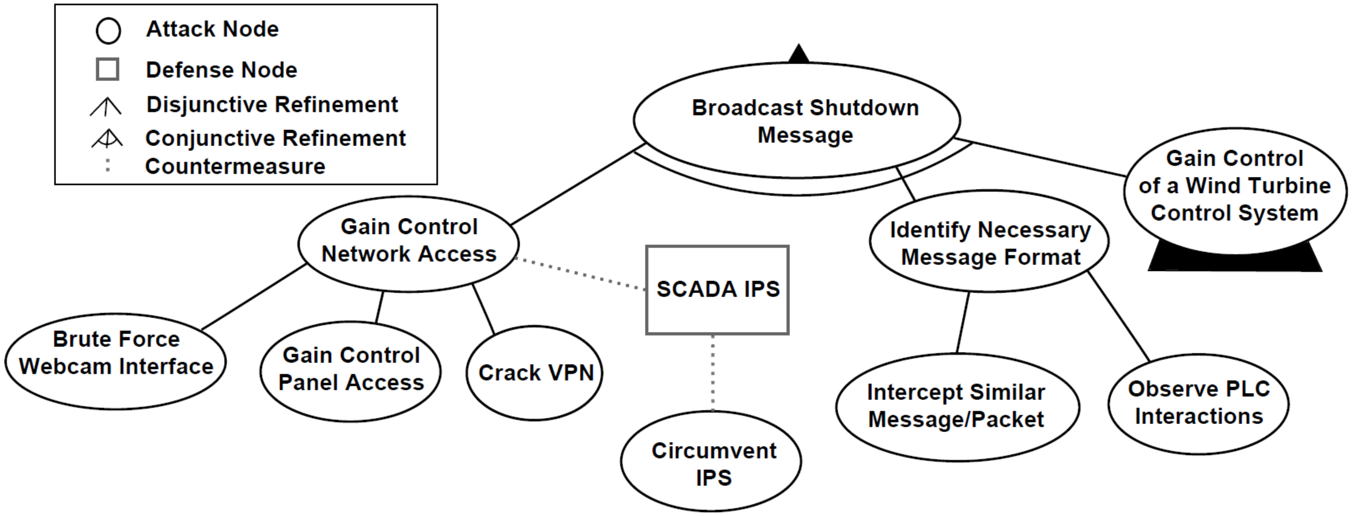
Attack Node
Defense Node
Disjunctive Refinement
Conjunctive Refinement
Countermeasure
Broadcast Shutdown Message
Gain Control of a Wind Turbine Control System
Gain Control Network Access
SCADA IPS
Identify Necessary Message Format
Brute Force Webcam Interface
Gain Control Panel Access
Crack VPN
Circumvent IPS
Intercept Similar Message/Packet
Observe PLC Interactions

Figure 7. Partial attack-defense tree for the wind turbine scenario.

Table 5. Wind turbine sensitivity analysis.

Basic Attack Step	After 20 hours	After 30 hours	After 40 hours
Brute force webcam	+1.08%	+0.65%	+0.23%
Gain control panel access	+9.30%	+4.72%	+1.55%
Crack VPN access	+3.45%	+1.97%	+0.68%
Conduct offline reconnaissance	+0.01%	+0.01%	+0.00%
Sniff Ethernet/IP traffic	+0.34%	+0.16%	+0.05%
Sweep DNP3 requests	+0.08%	+0.04%	+0.01%
Capture EtherCAT frames	+0.34%	+0.16%	+0.05%
Enumerate SCADA services	+5.20%	+2.48%	+0.79%
Sniff credentials	+4.88%	+2.67%	+0.90%
Forge authenticated messages	+7.99%	+4.11%	+1.35%
Bribe operator	+1.42%	+0.83%	+0.29%
Intercept similar message	+1.76%	+1.46%	+0.70%
Construct attack from traffic and documentation	+23.39%	+13.60%	+4.81%

Figure 7 shows a portion of the attack-defense tree for the scenario. The attribute domains correspond to the minimal execution time and difficulty for the attacker. Assuming the sequential execution of attack steps, an attacker would need 41.5 hours for a successful attack or 21 hours assuming parallel execution. Some of the evaluated scenario variants only require intermediate technical skills.

For further evaluation, the basic attack-defense tree was translated to the acyclic phase-type distribution formalism as shown in Figure 8. The main differences are the addition of sequential logic gates that model time dependencies and the absence of defense steps. Each basic attack step execution time is fitted to an exponential distribution. After the attack tree construction is complete, it can be converted into an acyclic phase-type distribution.

As an illustration of the possible cases that can be explored, Figure 9 presents the difference in attack probabilities and the time needed for a successful attack caused by adjusting the attack model for two of the calculated scenario variants. Specifically, Figure 9 (top) shows the successful attack probabilities of the standard scenario compared with a scenario variant without control panel vulnerabilities. Figure 9 (bottom) shows the successful attack probabilities of the standard scenario compared with a scenario variant with strong network message authentication in place. This approach also facilitates the evaluation of countermeasures and defense steps.

A sensitivity analysis was conducted to determine the basic attack steps that have the greatest impact on the overall scenario. Table 5 presents the results. After an initial calculation of the attack tree, for each basic attack step, another calculation was performed with twice the estimated execution

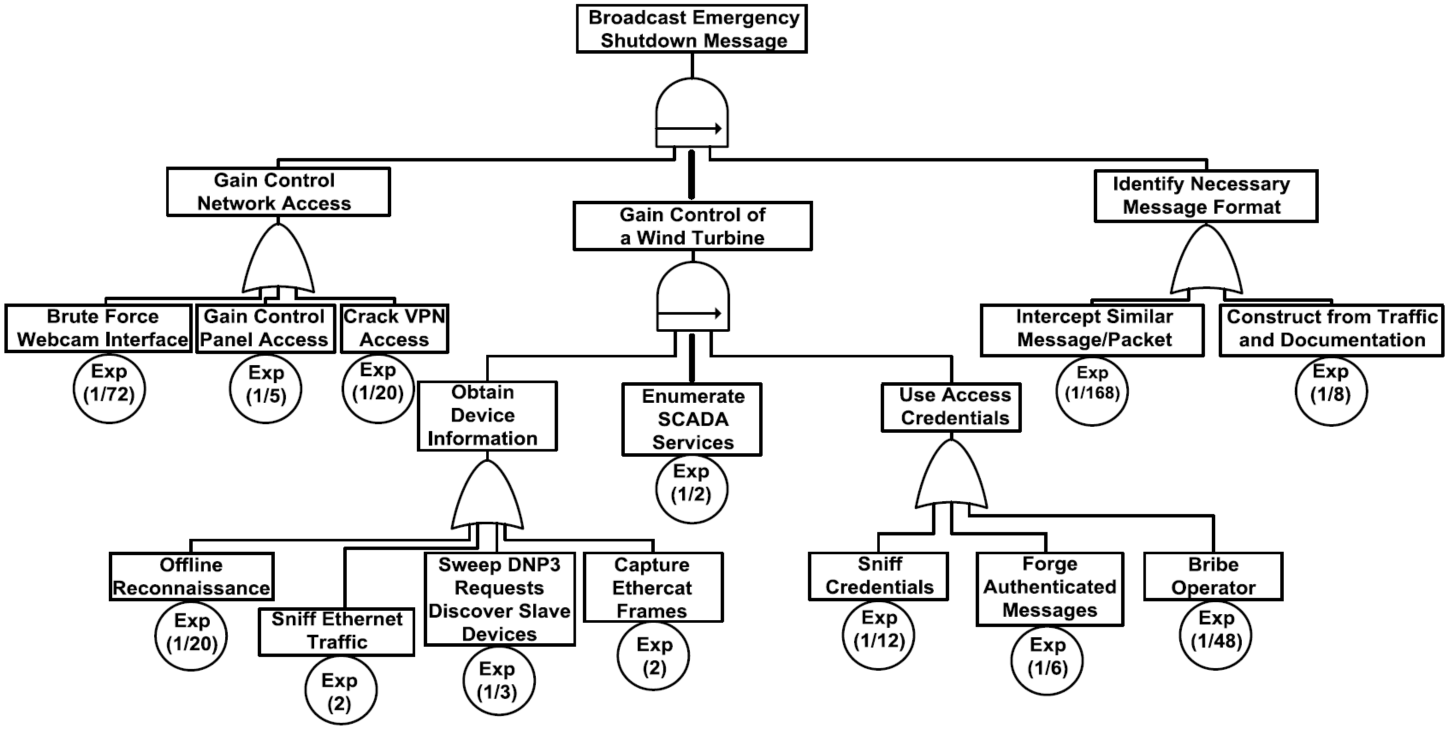
Broadcast Emergency Shutdown Message
Gain Control Network Access
Gain Control of a Wind Turbine
Identify Necessary Message Format
Brute Force Webcam Interface
Exp (1/72)
Gain Control Panel Access
Exp (1/5)
Crack VPN Access
Exp (1/20)
Obtain Device Information
Enumerate SCADA Services
Exp (1/2)
Use Access Credentials
Intercept Similar Message/Packet
Exp (1/168)
Construct from Traffic and Documentation
Exp (1/8)
Offline Reconnaissance
Exp (1/20)
Sniff Ethernet Traffic
Exp (2)
Sweep DNP3 Requests Discover Slave Devices
Exp (1/3)
Capture Ethercat Frames
Exp (2)
Sniff Credentials
Exp (1/12)
Forge Authenticated Messages
Exp (1/6)
Bribe Operator
Exp (1/48)

Figure 8. Partial attack tree for the wind turbine scenario (time-dependent).

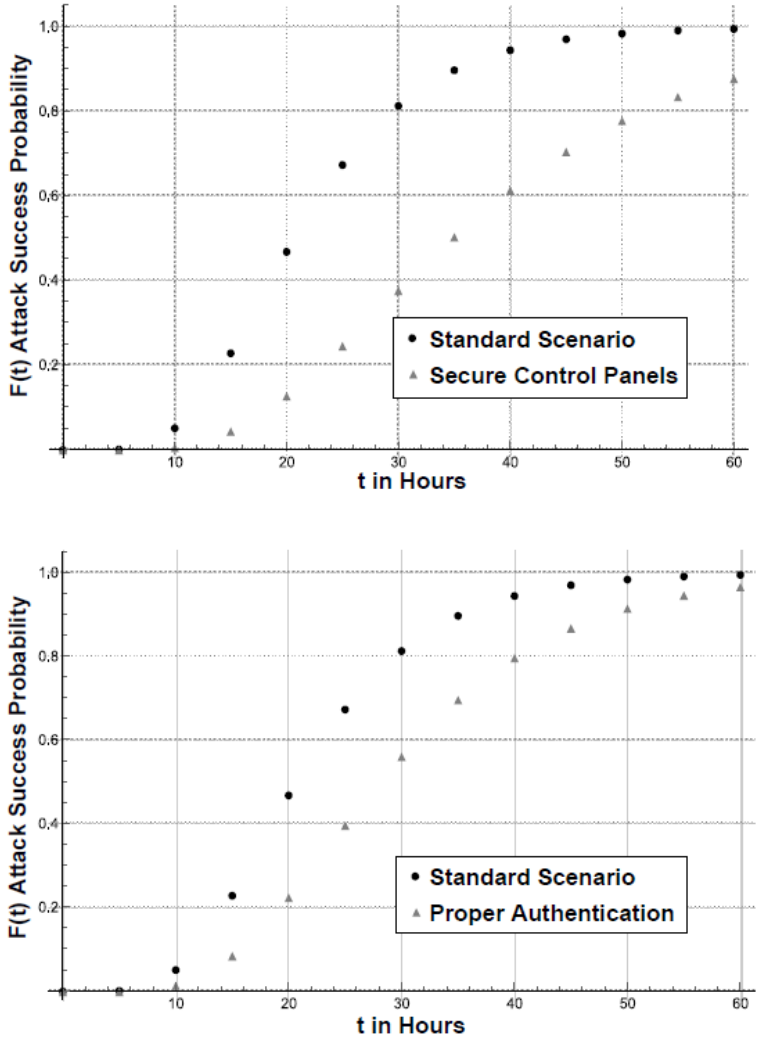

Figure 9. Comparisons of the probabilities of successful attacks.

time and the results are compared against the standard scenario. It is clear that the attack steps with the greatest impact are discovering the composition of the shutdown message, sending forged authenticated messages to the control network and accessing the control network via the control panel.

6. Conclusions

The multigraph model presented in this chapter is specifically designed for modeling critical infrastructure interdependencies and conducting analyses of diverse attack scenarios. The approach leverages an attack tree model with attribute domains extended by acyclic phase-type distributions to capture temporal dependencies. The efficacy of the modeling approach is demonstrated via a case study involving regional interdependent infrastructures that include the electric power, water and telecommunications sectors. The case study, which incorporates global vulnerability and critical node analyses and simulations of degradation and attack candidates, enables the largely automatic triage of attack scenarios. A key contribution is the use of open-source intelligence to validate the proposed modeling approach; the results provide a lower bound on an adversary's ability to identify vulnerable structures and dependencies. All the steps in the case study, including the development and analysis of the model and attack scenarios are solely based on information available to the general public. This strongly suggests that an attacker with modest resources would be able to achieve large-scale effects.

Future work will develop effective search heuristics to permit the exploration of longer attack chains (length greater than two). This restriction is currently imposed by a bounded, but exhaustive, search as well as buffering effects. While the proposed work may not be directly applicable to the infrastructure sectors considered in this chapter, buffering and explicit flows allow the inclusion of temporal dynamics for other types of infrastructures.

References

[1] R. Abdalla and K. Niall, Location-Based Critical Infrastructure Interdependency (LBCII), Technical Report, DRDC Toronto TR 2009-130, Defence R&D Canada, Toronto, Canada (`cradpdf.drdc-rddc.gc.ca/PDFS/unc100/p533788_A1b.pdf`), 2010.

[2] F. Arnold, H. Hermanns, R. Pulungan and M. Stoelinga, Time-dependent analysis of attacks, in *Principles of Security and Trust*, M. Abadi and S. Kremer (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 285–305, 2014.

[3] A. Bagnato, B. Kordy, P. Meland and P. Schweitzer, Attribute decoration of attack-defense trees, *International Journal of Secure Software Engineering*, vol. 3(2), pp. 1–35, 2012.

[4] A. Bashan, Y. Berezin, S. Buldyrev and S. Havlin, The extreme vulnerability of interdependent spatially embedded networks, *Nature Physics*, vol. 9(10), pp. 667–672, 2013.

[5] M. Beccuti, G. Franceschinis, M. Kaaniche and K. Kanoun, Multilevel dependability modeling of interdependencies between the electricity and information infrastructures, in *Critical Information Infrastructure Security*, R. Setola and S. Geretshuber (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 48–59, 2009.

[6] F. Cadini, E. Zio and C. Petrescu, Using centrality measures to rank the importance of the components of a complex network infrastructure, in *Critical Information Infrastructure Security*, R. Setola and S. Geretshuber (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 155–167, 2009.

[7] G. Dong, R. Du, L. Tian and R. Liu, Robustness of network of networks with interdependent and interconnected links, *Physica A: Statistical Mechanics and its Applications*, vol. 424, pp. 11–18, 2015.

[8] European Council, Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 Establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), Brussels, Belgium, 2007.

[9] L. Grigsby, *The Electric Power Engineering Handbook*, CRC Press, Boca Raton, Florida, 2012.

[10] S. Iyer, T. Killingback, B. Sundaram and Z. Wang, Attack robustness and centrality of computer networks, *PLOS ONE*, vol. 8(4), 2013.

[11] J. Johansson and H. Hassel, Vulnerability analyses of interdependent technical infrastructures, in *Risk and Interdependencies in Critical Infrastructures*, P. Hokstad, I. Utne and J. Vatn (Eds.), Springer-Verlag, London, United Kingdom, pp. 67–94, 2012.

[12] A. Kelic, D. Warren and L. Philips, Cyber and Physical Infrastructure Interdependencies, Sandia Report SAND2008-6192, Sandia National Laboratories, Albuquerque, New Mexico, 2008.

[13] E. Knapp, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems*, Syngress, Waltham, Massachusetts, 2011.

[14] B. Kordy, S. Mauw, S. Radomirovic and P. Schweitzer, Foundations of attack- defense trees, in *Formal Aspects of Security and Trust*, P. Degano, S. Etalle and J. Guttman (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 80–95, 2011.

[15] P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, Assessing n-order dependencies between critical infrastructures, *International Journal of Critical Infrastructures*, vol. 9(1-2), pp. 93–110, 2013.

[16] A. Semerow, S. Hohn, M. Luther, W. Sattinger, H. Abildgaard, A. Diaz Garcia and G. Giannuzzi, Dynamic study model for the interconnected power system of Continental Europe in different simulation tools, *Proceedings of the IEEE PowerTech Conference*, 2015.

[17] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou and D. Gritzalis, Risk mitigation strategies for critical infrastructures based on graph centrality analysis, *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 34–44, 2015.

[18] A. Steyrer, Threat of Austrian Energy Supply through Smart Metering and Smart Grid (Bedrohung der Osterreichischen Energieversorgung durch Smart Metering und Smart Grid), M.S. Thesis, Vienna University of Technology, Vienna, Austria, 2013.

[19] N. Svendsen and S. Wolthusen, Multigraph dependency models for heterogeneous infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 337–350, 2008.

[20] N. Svendsen and S. Wolthusen, Modeling approaches, in *Critical Infrastructure Protection*, J. Lopez, R. Setola and S. Wolthusen (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 68–97, 2012.

[21] G. Weldehawaryat and S. Wolthusen, Modeling interdependencies over incomplete join structures of power law networks, *Proceedings of the Eleventh International Conference on the Design of Reliable Communication Networks*, pp. 173–178, 2015.