Chapter 16

METRICS FOR QUANTIFYING INTERDEPENDENCIES

Emiliano Casalicchio and Emanuele Galli

Abstract The quantification of interdependencies is a major challenge when attempting to analyze the behavior of critical infrastructures. This paper presents a taxonomy of interdependency quantification metrics based on their information content, decision support and risk analysis capabilities, and computational costs. The paper also discusses a systematic approach for computing metrics and performance indices that measure the effectiveness of strategies designed to enhance critical infrastructure protection and resilience. A case study is used to illustrate the computation of the metrics and performance indices, and their application to the analysis of critical infrastructure interdependencies.

Keywords: Interdependencies, metrics, federated simulation

1. Introduction

A critical infrastructure is a physical system that, if disrupted, can seriously affect the national security, economy and social welfare of a nation. Examples of critical infrastructures include telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government and emergency services [1]. Clearly, modern society cannot function if large portions of the critical infrastructure are disrupted or destroyed.

In order to understand the behavior of critical infrastructures, it is necessary to accurately model and quantify their interdependencies [14]. Researchers have proposed several qualitative and quantitative techniques for analyzing interdependencies. Qualitative approaches rely on mathematical formalisms such as Leontief-based models [10], Markov chains [2], Petri nets [8], hierarchical holographic modeling (HHM) [7, 9] and graph theory [15, 16]. Quantitative approaches typically engage discrete simulation or agent-based modeling and simulation (ABMS) [3–6, 14].

While considerable research has focused on interdependency modeling and analysis, very few efforts have examined the issue of quantifying interdependencies. Zimmerman [17] has proposed explicit metrics for quantifying interdependencies. One metric measures the "direction" of infrastructure failures as the ratio between the number of times one type of infrastructure causes damage to another type of infrastructure and the number of times other types of infrastructures cause damage to the first type of infrastructure. Zimmerman and Restrepo [18] have specified a metric that measures the duration of cascading effects; they use this metric to quantify the effects of U.S. power grid outages on other infrastructures.

This paper presents a taxonomy that classifies interdependency metrics on the basis of their information content, decision support and risk analysis capabilities, and computational costs. In addition, it describes systematic approaches for computing metrics using system or model observations, and for calculating performance indices that measure the effectiveness of strategies designed to enhance critical infrastructure protection and resilience.

In general, interdependency metrics may be classified as those that measure the macro characteristics of interdependencies and their impact on system behavior and those quantify the strengths or weaknesses of infrastructures and infrastructure components. Metrics in the first category support decision making at the organizational or strategic level while those in the second category support decision making at the engineering or practical level.

We also use statistical measures, namely the percentile value, cumulative distribution function (CDF) and complementary cumulative distribution function (CCDF). The percentile value and CDF of an observed state variable are used to quantify the degree of satisfaction or goodness of choice. The CCDF of a set of observed outcomes is used to perform survivability analyses.

We employ a case study to illustrate the computation of metrics and performance indices, and their use in analyzing critical infrastructure interdependencies. Two scenarios are examined, outage propagation in infrastructures and victim rescue after a terrorist attack.

2. Metrics and Performance Indices

We classify metrics for quantifying critical infrastructure interdependencies in terms of decision support capabilities, information content and computational cost. In particular, we identify three categories of metrics: (i) shape metrics that quantify macro or "shape" characteristics of interdependencies such as direction [17] and duration [18] (Figure 1(a)); (ii) core metrics that measure the causes and effects of outages for specific infrastructure components (Figures 1(b) and (c)) and the effectiveness of strategies/mechanisms for improving critical infrastructures protection and resilience; and (iii) sector-specific metrics that measure the states of infrastructures at the global and component levels.

Figure 2 shows how core, shape and sector-specific metrics are positioned in the three dimensional space of decision support capabilities, information

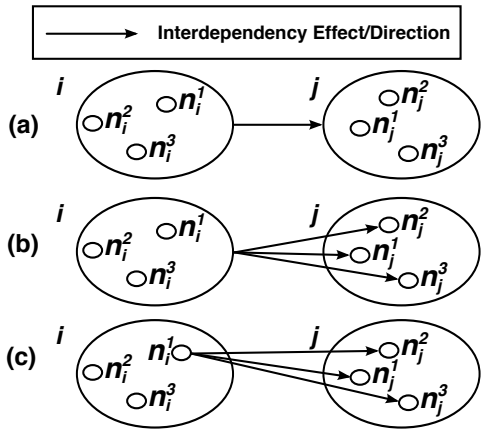

Figure 1. (a) Shape metrics; (b, c) Core metrics.

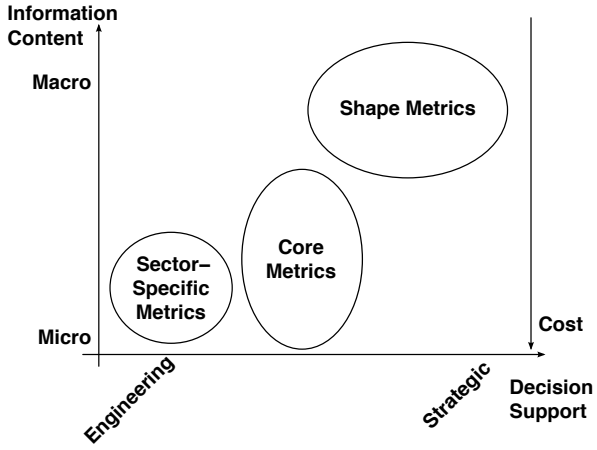

Figure 2. Taxonomy of metrics for quantifying interdependencies.

content and cost. The decision support dimension ranges from the engineering level (low) to the strategic level (high). The information content dimension ranges from the micro level (low) to the macro level (high). The cost dimension ranges from low to high. The first two dimensions are qualitative in nature while cost dimension values depend on the implementation and case study.

2.1 Shape Metrics

Consider the direct metric, relative duration ($R_{i,j}$), which measures the cascading effect of an outage [18]. $R_{i,j} = \frac{T_j}{T_i}$ is defined as the ratio of the duration T_j of an outage in infrastructure j due to an outage in infrastructure i and the duration T_i of the outage in infrastructure i. The computation of a shape

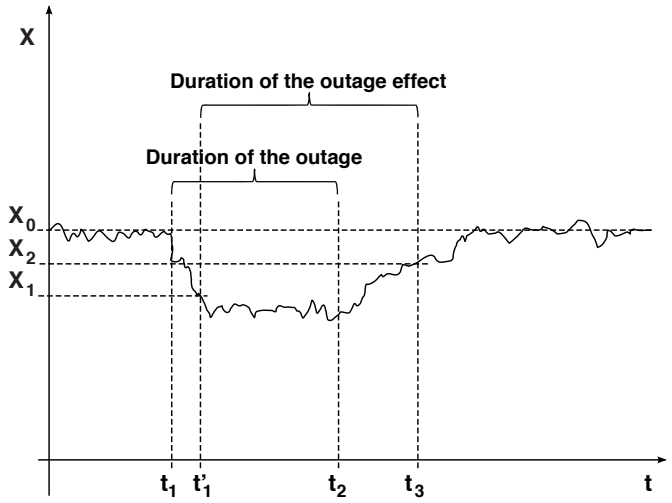

Figure 3. Relationship between sector-specific and direct metrics.

metric involves measuring $R_{i,j}$ and quantifying the impact on infrastructure j. The solution is to use sector-specific metrics. $R_{i,j}$ is a function $f(\cdot)$ of the time t and the set of sector-specific metrics M_j used to measure the performance levels or capabilities of infrastructure j. In other words, $R_{i,j} = f(t, m_j^1, m_j^2, ..., m_j^p)$ where $m_j^k \in M_j$.

Consider the example presented in Figure 3. Suppose that at time t_1 there is a power grid outage (infrastructure i), and at time $t'_1 \geq t_1$, a decrease is observed in X, the overall throughput of the communication network (infrastructure j): $X(t) = X_0$ if $t \leq t_1$ and $X(t) \leq X_1$ if $t \geq t'_1$. X_1 is the critical threshold for network performance, i.e., when $X < X_1$ the network loses the ability to provide services. If the power grid outage is fixed at time t_2 and, after time t_3, the throughput is observed to return to X_0, $X(t) \geq X_2$ at time t_3 and $X(t) \rightarrow X_0$ for $t \geq t_3$, we assert that, at time t_3, the cascading effect of the power grid outage has ended. We assume that, when $X(t) \geq X_2$, the communication network can provide services (obviously, $X_1 \leq X_2 \leq X_0$). $R_{i,j}$ is a function $f(t, X)$ of the time and throughput: $R_{g,n} = \frac{t_3 - t'_1}{t_2 - t_1}$ where t'_1 is such that $X(t) \leq X_1$ for $t \geq t'_1$ and t_3 is such that $X(t) \geq X_2$ for $t \geq t_3$.

As observed by Zimmerman and Restrepo [18], if $R_{i,j} < 1$, the infrastructure j can react on its own to the outage (e.g., reconfigure its services). Otherwise, if $R_{i,j} > 1$, the infrastructure j is heavily dependent on the outage and it needs some time to restore its services after the outage ends.

An example of an aggregate measure of a shape metric is the total relative duration $R_{i,I}$ of an outage in infrastructure i on a set of infrastructures I. Suppose that the power grid outage impacts the communication network and transportation system, and that the communication network outage impacts credit card transactions. The cascading effect ends when all the infrastructures

are restored to their normal operating conditions. Then, the total relative duration of an outage in infrastructure i is given by $R_{i,I} = \max_{j \in I, j \neq i} \{R_{i,j}\}$ where $R_{i,j}$ is a function of sector-specific performance indices of infrastructure j.

2.2 Core Metrics

The direct metric $R_{i,j}$ quantifies a macro characteristic of the interdependencies between infrastructures i and j, but it does not give any information about the infrastructure nodes involved in or affected by the outage propagation. Nor does it provide the impact of the failure of a specific infrastructure or infrastructure component. Core metrics quantify the effects of interdependencies at the level of infrastructure nodes or, more deeply, at the level of node components. Thus, core metrics provide insight into the causes and effects of outages.

Two core metrics can be obtained by refining the shape metric $R_{i,j}$ in order to identify the weakest node in infrastructure j or the most important node in infrastructure i. To identify the weakest node in infrastructure j with respect to an outage in infrastructure i, we define $R_{i,n_j^k} = f(t, M_j^k)$ where n_j^k is the k^{th} node of infrastructure j and M_j^k is the set of metrics used to measure the performance or capabilities of n_j^k. The weakest node is then obtained by evaluating the expression $n_j^l = max_{k \in N_j} \left\{ R_{i,n_j^k} \right\}$ where N_j is the set of nodes comprising infrastructure j.

Similarly, to identify the most important node in infrastructure i that affects infrastructure j, we define $R_{n_i^h,n_j^k} = f(t, M_j^k)$ where n_i^h is the h^{th} node of infrastructure i. The most important node in infrastructure i is determined by evaluating the expression $n_i^l = max_{h \in N_i} \left\{ R_{n_i^h,n_j^k} \right\}$ for each $k \in N_j$.

In general, if a sector-specific metric $m_j^k \in M_j^k$ is used, the weakest node in infrastructure j with respect to an outage in infrastructure i is obtained by evaluating the expression $n_j^l = max_{k \in N_j} \left\{ \Delta m_j^k \right\}$ where Δm_j^k is the variation of the sector-specific metric considered. Similarly, the most important node in infrastructure i that affects the behavior of infrastructure j is obtained by evaluating the expression $n_i^l = max_{h \in N_i} \left\{ \Delta m_j^k \right\} \; \forall k \in N_j$. Obviously, depending on the metric considered, the maximization problem can be turned into a minimization problem.

In addition to measuring the loss of performance or capability of an infrastructure, core metrics can be used to measure the effectiveness of strategies for protecting critical infrastructures or enhancing their resilience. For example, core metrics can quantify the effects produced by changing a rescue plan, the consequences of network re-engineering or the effects of a new service reconfiguration strategy. Also, core metrics can be used to specify the probability that a certain percentage of a population will be rescued after an incident, the percentage of fatalities in a population or the duration of rescue operations. These concepts cannot be quantified using direct metrics. Other examples that can

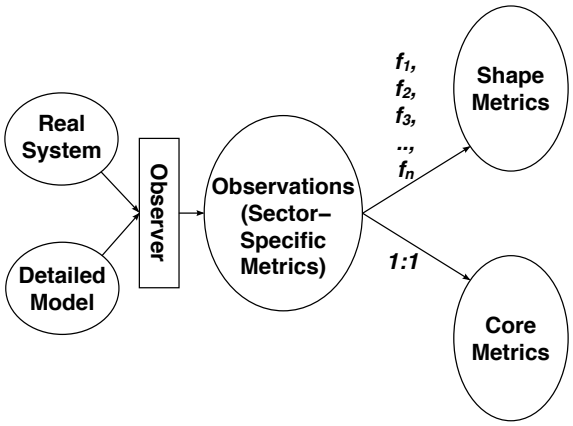

Figure 4. Computing shape and core metrics from sector-specific metrics.

be quantified by core metrics are the number of damaged infrastructure nodes, the time taken to recover node functionality, the time taken to reconfigure a system or network, and more.

2.3 Computing Shape and Core Metrics

As discussed above, sector-specific metrics are used to compute shape and core metrics. Figure 4 illustrates the relationships between sector-specific metrics, core metrics and shape metrics and the processes for computing shape and core metrics. Parameters that can be used directly as core metrics (i.e., without any transformation) are determined by analyzing a real system or a detailed model of the system (or both). To compute shape metrics, is necessary to identify the relevant sector-specific metrics and the appropriate transformation functions $(f_1, ..., f_n)$ as described in Section 2.1.

2.4 Metric Characteristics

Table 1 summarizes the characteristics of shape metrics, core metrics and sector-specific metrics. In particular, it compares the three types of metrics based on their information content, decision support capabilities and computational cost.

2.5 Statistical Performance Indices

A statistical metric can be used to express the degree of satisfaction with respect to the X^{th} percentile of a performance index. The X^{th} percentile of a dataset is defined as the value that is larger than $X\%$ of the data. The X^{th} percentile of a random variable is obtained by inverting its cumulative distribution function (CDF), which is defined as $F_X(x) = P\{x \leq X\}$. For

Table 1. Summary of interdependency metric characteristics.

Metrics	**Information Content**	**Decision Support**	**Cost**
Shape metrics	Macro level	Support decisions at the organizational and strategic levels	*Low/Medium* Detailed model is not mandatory
Core metrics	Micro level	Support decisions at the engineering and practical levels; Quantify the causes and effects of outages	*Medium/High* Detailed model is mandatory (typically a simulation model)
Sector-specific metrics	Engineering level		
	Input for computing shape and core metrics		

example, the 95^{th} percentile of X is $\tau = F_X^{-1}(0.95)$. Thus, the percentile of interest is easily obtained by plotting the CDF.

For performance indices such as crisis resolution time, rescue time and number of failed nodes it makes sense to measure the degree of satisfaction of a new (counter)measure. On the other hand, for the number of repaired nodes, it is more appropriate to compute X such that $P\{x > X\} = Y$. The value of X is computed using the complementary cumulative distribution function (CCDF). The CCDF, which is commonly used in survivability analysis, is defined as $F_c(x) = 1 - F_X(x) = Pr\{x > X\}$. Upon inverting F_c, we obtain $X = F_c^{-1}(Y)$.

3. Case Study

A report by the U.S. Homeland Security Advisory Council [11] emphasizes that techniques and tools for analyzing critical infrastructure interdependencies and their consequences "are of value only if applied within the context of a clear objective – a desired outcome that is measurable." We use a case study to demonstrate our methodology and, in particular, the application of interdependency metrics.

The case study, which is derived from [4, 5], considers three critical infrastructures: the communication network used for data transmission and voice calls, the power grid and the transportation network of urban roads. Other infrastructures involved in the case study are hospitals and health care centers and the Information System for Civic Emergency Management (IS4CEM), which coordinates recovery in the event of terrorist attacks, catastrophes and infrastructure outages. IS4CEM also provides information about health care center availability, transportation network availability and event evolution.

Two scenarios are examined, outage propagation and victim rescue after a terrorist attack. The outage propagation scenario only considers the main

infrastructures (power grid, transportation network and communication network). The scenario demonstrates how shape metrics can quantify the effect of a power grid outage on the behavior of a communication network.

On the other hand, the victim rescue scenario illustrates how core metrics can be used to study the evolution of a crisis in the presence of various types of power grid outages. The scenario assumes several persons have been injured after a terrorist attack. The communication network is used by the injured victims, citizens, authorities, rescue crews and hospitals. Hospitals and rescue crews use the IS4CEM to coordinate rescue operations. The transportation network is used by rescue crews to reach the injured and take them to hospitals; the network is also used by injured victims who drive themselves to hospitals for first aid. The power grid supplies the communication network, IS4CEM, hospitals, rescue crew stations and the transportation network (traffic lights).

4. Interdependency Analysis

Our simulation experiments using Federated ABMS [5] were designed to demonstrate the ability of core metrics to quantify interdependencies and to verify that the statistical measures used as performance indices are appropriate. Three power grid outage situations were considered for the outage propagation and victim rescue scenarios: no outage, one outage and two outages. The nodes experiencing outages were selected randomly. In the outage propagation scenario, we assume that the time to fix the outage is constant. In the victim rescue scenario, we assume that the outage is permanent for the duration of the simulation.

The scenarios involved three hospitals, ten power grid nodes and ten routers and access points. The victim rescue scenario involved ten rescue team members and 50 injured victims. A total of 50 simulations were conducted for each case for each of the two scenarios; each simulation used a different seed for random number generation.

4.1 Outage Propagation Scenario

We assume that at time $t = 100$ ticks, one or two randomly selected power grid nodes fail. We also assume that no auxiliary power systems are available; therefore, when a power grid node fails, one or more network nodes (routers or access points) go out of service until they receive power. The time taken to repair a power grid node outage is set at 300 ticks.

Figure 5 compares the overall throughput of the communication network $X = \sum_{i \in \mathcal{N}} X_i$ where $\mathcal{N}$ is the set of nodes in the network and X_i is the throughput of node i. As expected, X decreases if one or more routers fail. We assume that the critical threshold for network performance is 8,000 Mbps.

Figure 6 presents the overall throughput at the start ($t = 100$) of a power grid outage (left-hand side) and at the end ($t = 400$) of the outage (right-hand side). As shown in Figure 6 (left), when there is one outage, X degrades at $t = 100$; after three ticks X falls below 8,000 Mbps and stabilizes to around 7,000

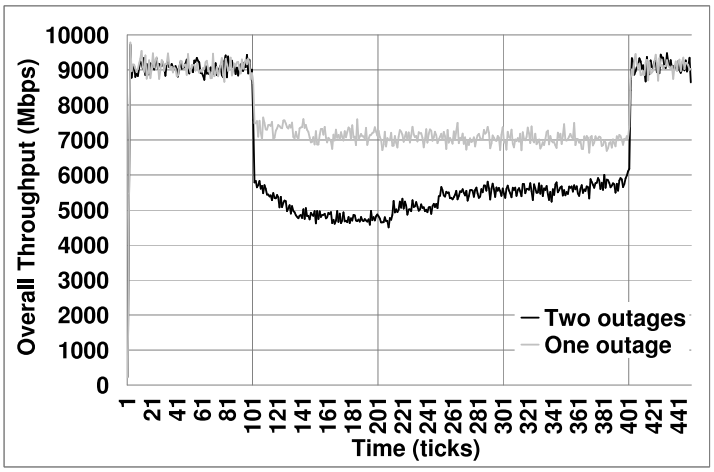

Figure 5. Overall throughput of the communication network.

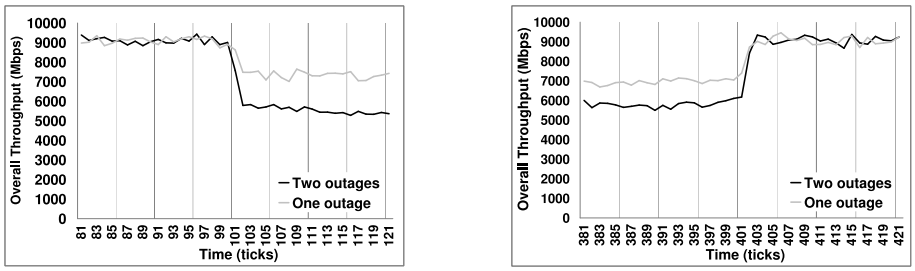

Figure 6. Overall throughput during a power grid outage.

Mbps after 100 additional ticks. When the outage ends at $t = 400$, four ticks pass before normal operating conditions are re-established (Figure 6, right), corresponding to $R_{g,n} \approx 1$. Normal operating conditions are rapidly restored due to the robustness of the routing algorithm and also because delays due to nodes being rebooted or damaged during the abnormal shutdown are not taken into account.

In the case of two outages, a significant degradation in the overall throughput is observed. After three ticks, the overall throughput falls below 6,000 Mbps (Figure 6, left) and after 30 additional ticks, it is below 5,000 Mbps. However, at $t = 214$, the reconfiguration features of the routing algorithm take effect, and at $t = 250$, the overall throughput stabilizes to around 5,500 Mbps (Figure 6, right). Also in this case, $R_{g,n} \approx 1$ and normal operating conditions are re-established a few ticks after the power outages end (Figure 6, right).

The time plot of the sector-specific metric is useful for analysis. When the critical threshold for the throughput is 8,000 Mbps, $R_{g,n} \approx 1$, and the duration of the communication network outage is about the same as that in the power

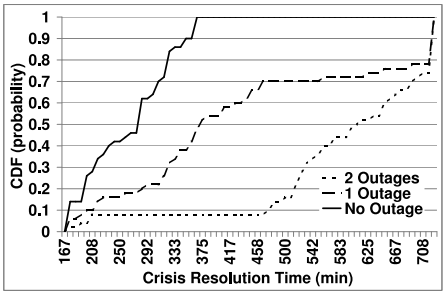

Figure 7. Crisis resolution time CDF.

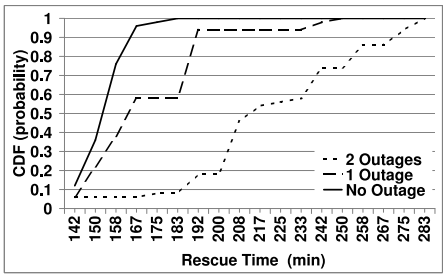

Figure 8. Rescue time CDF.

grid. However, if the critical threshold is reduced to 5,300 Mbps, $R_{g,n} = 0$ in the case of one outage and $R_{g,n} \approx 0.35$ for two outages (Figure 5).

4.2 Victim Rescue Scenario

We assume that at time $t = 0$, 50 people are injured in a terrorist attack ($N_w = 50$). We compare the results for the three cases (no outage, one outage and two outages) using the 90^{th} percentile value, CDF and CCDF.

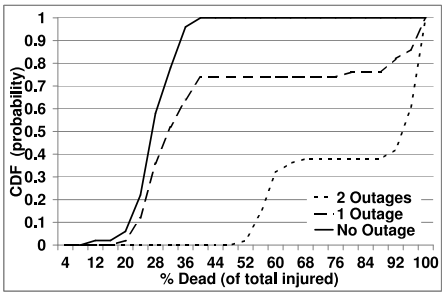

Figure 9. Percentage of dead CDF.

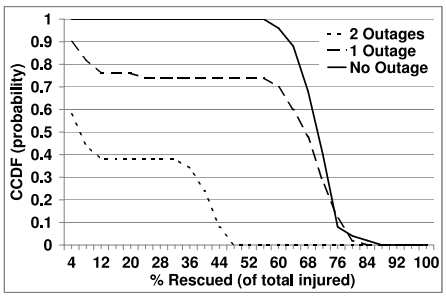

Figure 10. Percentage of rescued CCDF.

Figures 7, 8 and 9 show the CDFs of the crisis resolution time (T_c), rescue time (T_r) and percentage of dead ($W_d\%$), respectively. The CDF plots give an excellent indication of system behavior and how the outages increase T_c, T_r and W_d. The CCDF is used to analyze the number of injured victims who are rescued (Figure 10). The CCDF gives the probability that more than $W\%$ of the injured are rescued, i.e., $P\{W_r > W\}$. The value of W such that $P\{W_r > W\} = p$ is obtained by inverting the CCDF.

Table 2 presents the 90^{th} percentile values for T_c, T_r and W_d. Using the CDF and the concept of percentile is easy to compute the probability p_d that $W\%$ of the injured will die and the probabilities p_r and p_c that T_r and T_c, respectively, are less than T seconds, i.e., $p_d = F_d(W)$, $p_r = F_r(T)$ and $p_c = F_c(T)$ where F_d, F_r and F_c are the CDFs of W_d, T_r and T_c, respectively.

Table 2. T_c, T_r and W_d (90^{th} percentile values).

	Outages		
Metric	**Zero**	**One**	**Two**
T_r (sec)	165.83	187.96	269.44
T_c (sec)	350	725	725
W_d (%)	34.66	99	100

Table 3. $W\%$ values such that $P\{W_r > W\} = p$.

	Outages		
$\boldsymbol{P\{W_r > W\}}$	**Zero**	**One**	**Two**
0.90	64%	6%	0%
0.75	66%	22%	0%
0.50	72%	68%	6%

Table 3 shows the $W\%$ values (i.e., more than $W\%$ of the injured are rescued) for various values of $p = P\{W_r > W\}$. These are obtained by fixing a value for p and extracting the corresponding value of W from the CCDF.

5. Conclusions

The interdependency quantification metrics presented in this paper are useful for analyzing and simulating the behavior of critical infrastructures. Shape metrics, with their macro-level information content, support decision makers at the organizational and strategic levels. These metrics can be computed based on engineering-level observation or using high-level system observations that engage simulation or analytic models. In contrast, core metrics measure the causes and effects of outages for specific infrastructure components and the effectiveness of strategies for improving critical infrastructures protection and resilience. They require more computational overhead than shape metrics, but they give decision makers useful information about outages and direct or indirect quantification of interdependencies. Sector-specific metrics measure the states of infrastructures at the global and component levels, and provide input for computing shape and core metrics. Statistical measures, such as the percentile, CDF and CCDF, are also useful for analysis. The case study, involving simulations of outage propagation and victim rescue scenarios, demonstrate the value of the metrics and statistical measures for analyzing critical infrastructure interdependencies.

References

[1] I. Abele-Wigert and M. Dunn, *International CIIP Handbook, Volume 1*, Center for Security Studies, Swiss Federal Institute of Technology, Zurich, Switzerland, 2006.

[2] S. Asavathiratham, B. Lesieutre and G. Verghese, The influence model, *IEEE Control Systems*, vol. 21(6), pp. 52–64, 2001.

[3] E. Bonabeau, Agent-based modeling: Methods and techniques for simulating human systems, *Proceedings of the National Academy of Sciences*, vol. 99(3), pp. 7280–7287, 2002.

[4] V. Cardellini, E. Casalicchio and E. Galli, Agent-based modeling of interdependencies in critical infrastructures through UML, *Proceedings of the Agent-Directed Simulation Symposium of the Spring Simulation Multiconference*, pp. 119–126, 2007.

[5] E. Casalicchio, E. Galli and S. Tucci, Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures, *Proceedings of the Eleventh International Symposium on Distributed Simulation and Real-Time Applications*, pp. 182–189, 2007.

[6] D. Dudenhoeffer, M. Permann and M. Manic, CIMS: A framework for infrastructure interdependency modeling and analysis, *Proceedings of the Winter Simulation Conference*, pp. 478–485, 2006.

[7] B. Ezell, J. Farr and T. Wiese, Infrastructure risk analysis model, *Journal of Infrastructure Systems*, vol. 6(3), pp. 114–117, 2000.

[8] O. Gursesli and A. Desrochers, Modeling infrastructure interdependencies using Petri nets, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, pp. 1506–1512, 2003.

[9] Y. Haimes, *Risk Modeling, Assessment and Management*, Wiley-Interscience, Hoboken, New Jersey, 2004.

[10] Y. Haimes and P. Jiang, Leontief-based model of risk in complex interconnected infrastructures, *Journal of Infrastructure Systems*, vol. 7(1), pp. 1–12, 2001.

[11] Homeland Security Advisory Council, Report of the Critical Infrastructure Task Force, Department of Homeland Security, Washington, DC (www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf), 2006.

[12] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman and D. Coury, EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components, *IEEE Transactions on Power Systems*, vol. 21(2), pp. 548–558, 2006.

[13] M. North, N. Collier and J. Vos, Experiences creating three implementations of the Repast agent modeling toolkit, *ACM Transactions on Modeling and Computer Simulation*, vol. 16(1), pp. 1–25, 2006.

[14] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[15] N. Svendsen and S. Wolthusen, Connectivity models of interdependency in mixed-type critical infrastructure networks, *Information Security Technical Report*, vol. 12(1), pp. 44–55, 2007.

[16] 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, 2007.

[17] R. Zimmerman, Decision-making and the vulnerability of interdependent critical infrastructures, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 5, pp. 4059–4063, 2004.

[18] R. Zimmerman and C. Restrepo, The next step: Quantifying infrastructure interdependencies to improve security, *International Journal of Critical Infrastructures*, vol. 2(2/3), pp. 215–230, 2006.