RESILIENCE QUANTIFICATION FOR PROBABILISTIC DESIGN OF CYBER-PHYSICAL SYSTEM NETWORKS

Yan Wang
School of Mechanical Engineering
Georgia Institute of Technology
Atlanta, GA 30332, USA
Email: yan.wang@me.gatech.edu
Tel: +1-404-894-4714

ABSTRACT

Cyber-physical systems (CPS) are the physical systems of which individual components have functional identities in both physical and cyber spaces. Given the vastly diversified CPS components in dynamically evolving networks, designing an open and resilient architecture with flexibility and adaptability thus is important. To enable a resilience engineering approach for systems design, quantitative measures of resilience have been proposed by researchers. Yet, domain dependent system performance metrics are required to quantify resilience. In this paper, generic system performance metrics for CPS are proposed, which are entropy, conditional entropy, and mutual information associated with the probabilities of successful prediction and communication. A new probabilistic design framework for CPS network architecture is also proposed for resilience engineering, where several information fusion rules can be applied for data processing at the nodes. Sensitivities of metrics with respect to the probabilistic measurements are studied. Fine-grained discrete-event simulation models of communication networks are used to demonstrate the applicability of the proposed metrics.

1. INTRODUCTION

Cyber-physical systems (CPS) [1] are the physical systems of which individual components have new capabilities of data collection, information processing, network communication, and even control mechanism, and have functional identities in both physical and cyber spaces. Internet of Things (IoT) is an example application of CPS. IoT refers to uniquely identifiable physical objects that form an Internet-like structure in cyber space [2]. The original idea of IoT was to extend the capability of radio-frequency identification (RFID) chips with Internet connectivity. Later, the concept was generalized to any physical objects with data collection, processing, and communication capabilities. We can imagine that in the future any object we interact with in our daily lives would probably have the functions of data collection and exchange, be it thermostat, pen, car seat, or traffic light. The objects in the physical environment also form a virtual space of information gathering and sharing. This information can affect every decision we make daily, such as which jacket to wear, which medicine to take, which commute route to follow, etc. These physical objects are realizations of CPS, and IoT is formed by the networked CPS objects or components.

There are some new challenges in designing CPS components. The complexity of CPS components has increased from traditional products. Designing each product requires the consideration of hardware, software, as well as network connectivity, which is beyond the existing mechatronics systems, where hardware and software are simultaneously designed but with much lower complexity. CPS components are meant to be Internet-ready. Each component is an open system that can be re-configured and re-adapted into the evolution of the Internet itself. Therefore, the concept of open system design with robust and diverse connectivity becomes important. In addition, the functions of networked CPS are collected efforts from individual components. The confederated systems formed by individuals do not have centralized control and monitoring units. Ad hoc networks are formed by vastly different and heterogeneous components. The reliabilities as well as working conditions of the individual components can be highly

diverse. It would also be common that CPS networks experience disruptions because of harsh working environment or security breach. Good adaptability and resilience are important in designing the architecture of such networked systems. Yet, different from traditional communication networks, CPS networks do not just transfer information. Each node of the networks also generates new information through its sensing units. CPS networks are also different from traditional sensor networks, where the main task of sensors is collecting information whereas the logical reasoning for decision making is still done at centralized computers. In CPS networks, the level of computational intelligence and reasoning capability of the nodes are much higher and a major portion of decisions are done locally at individual nodes.

In this work, resilience of CPS network architecture is studied. The term resilience had been loosely used and semantically overloaded, until recently researchers started looking into more quantitative and rigorous definitions [33-41]. Generally speaking, resilience refers to the capability of a system that can regain its function or performance after temporary degradation or breakdown. Different definitions of how to measure resilience have been developed. All available quantitative definitions of resilience rely on some metrics of system function or performance. Nevertheless, how to quantify functionality or performance of systems such as communication and transportation networks still remains at a very abstract level in these studies. The performance metrics can be domain dependent. There is a need of developing quantitative performance metrics for systems of CPS. Based on the performance metrics, resilience of CPS networks then can be measured and compared. In this paper, formal metrics to quantify the functionality and performance of CPS networks are proposed, which are based on entropy and mutual information associated with the prediction and communication capabilities of networks. The performance metrics are defined based on a generic probabilistic model of CPS networks and demonstrated with detailed network

simulations. The design and optimization of CPS network architecture based on the performance metrics for resilience is also demonstrated.

In the remainder of this paper, an overview of resilience research is provided in Section 2, which includes the quantitative studies of resilience and the applications in engineering and networks. It is seen that resilience is a common and interdisciplinary subject for complex system study across many domains. Yet, the effort of quantitative analysis for resilience engineering and system design is still very limited. A probabilistic model of CPS networks is described in Section 3, where the performance metric to quantify resilience is proposed. In Section 4, the metrics are applied in system design and sensitivity studies. In Section 5, the proposed metrics are demonstrated and the applicability is verified from detailed network simulations.

2. BACKGROUND

2.1 The Multidisciplinary Concept of Resilience

The history of systematic resilience study can be retrieved back to early 1960s by ecologists, who were interested in ecosystem stability. The ecosystem may be stabilized at more than one stable equilibrium. In contrast, resilience studied in engineering focuses on the system behavior near one stable equilibrium and studies the rate at which a system approaches the steady state following a perturbation. The studies are about how to improve the ability to resist the change and how to reduce the time of recovery.

The resilience perspective emerged in ecology more than four decades ago through the study of interacting population of predator and prey in an ecosystem [3,4,5,6]. Resilience is regarded as the capacity to absorb shocks and maintain dynamic stability in the constant transient states. The accepted definition of resilience in ecology is the capacity to persist within one or several stability domains. Resilience determines the persistence of relationships within an ecosystem and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist

[6]. The measure of resilience is the size of stability domains, or the amount of disturbance a system can take before its controls shift to another set of variables and relationships that dominate another stability region [7]. The concept of slow and fast variables at multiple time scales is observed in ecosystems. Because of the dynamics nature of the ecosystem, the terms "regimes" and "attractors" were proposed to replace "stable states" and "equilibria" [8]. The resilience of ecosystems emphasizes not only persistent and robustness upon disturbance, but also adaptive capacity to regenerate and renew in terms of recombination and self-reorganization. Ecosystem resilience has also been proposed to be a major index of environmental sustainability during economic growth. Economic activities are sustainable only if the life-support ecosystems on which they depend are resilient [9].

The resilience of regional economics is generally considered as the capability of returning to a pre-shock state, as defined and measured by employment, output, and other variables, after disturbances or adverse events such as economic crisis, recessions, and natural disasters [10,11]. Several notions of regional resilience have been proposed. For example, Foster [12] defined regional resilience as the ability of a region to anticipate, prepare for, respond to, and recover from a disturbance. Hill et al. [13] defined it as the ability of a region to recover successfully from shocks to its economy that either throw it off its growth path or have the potential to throw it off its growth path. Yet, there is no standard and precise definition and measurement. Unlike physical or ecological systems, a regional economy may never be in an equilibrium state. It can grow continuously. Therefore, regional economics resilience emphasizes on returning to the pre-shock path or state, regardless whether it was in equilibrium or not. The four dimensions of regional resilience are: *resistance* (the vulnerability or sensitivity of a regional economy to disturbances and disruptions), *recovery* (the speed and extent to return to the pre-shock state), *re-orientation* (the adaptation and re-alignment of regional economy and its impact to the region's output, jobs, and incomes), and *renewal* (the resumption of the growth path) [11].

The term resilience has been used in materials science for decades. A material with good resilience is similar to a spring. It reacts on compression, tension, or shearing forces elastically and rebounds to its original shape. The term appeared in the literature of textile material [14,15,16] and rubber [17,18,19] as early as in 1930s. The resilience of a material is generally regarded as the energy dissipation property of storing and releasing energy elastically, and can be characterized as the ratio of energy given up in recovery from deformation to the energy applied to produce the deformation, which is measured through the energy loss during repeated load and unload cycles [19].

With the continuing downscaling of CMOS technologies and reduction of power voltage, sporadic timing errors, device degradation, and external environment radiation may cause so-called single-event transient errors in computer chips and microelectronic systems. Designers of such computing systems use resilience to describe the systems' fault tolerance [20,21,22,23]. The main approaches to enhance error resilience include error checking for recovery, co-design of hardware and software, and application-aware hardware implementation. Hardware resilience can be achieved by applying machine learning algorithms to process data collected from fault-affected hardware and perform classification for inference and decision making [24, 25]. Statistical error compensation [26] can be applied to maximize the probability of correct prediction given hardware errors.

The reliability and resilience of cyberinfrastructure and cybersecurity have been the research focus for decades [27,28]. Resilience of computer network is regarded as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation [29]. The considered factors for computer network resilience include fault tolerance due to accidents, failure, and human errors; disruption tolerance due to external environment such as weather, power outage, weak connectivity, and malicious attacks; and traffic tolerance because of legitimate flash crowd or denied

of service attacks. Fault tolerance typically relies on redundancy if the failures of components are independent, whereas survivability depends on diversity for correlated failures.

To improve the reliability and safety of socio-technical systems with a proactive and systems engineering approach, resilience engineering is a term people coined to promote the concept of enabling the capability of anticipating and adapting to the potential accidents and system failures [30]. It is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions. The emphasized capabilities are anticipation, learning, monitoring, and responding. It is concerned with exploiting insights on failures in complex systems, organizational contributors to risk, and human performance drivers in order to develop proactive engineering practices. In resilience engineering, failure is seen as the inability to perform adaptations to cope with the dynamic conditions in real world, rather than as breakdown or malfunction [31]. The scope of systems includes both physical and humans, as human error is one of the major sources of system failures. Domain experts' over-confidence could also impede the proper development of anticipation of unexpected severe situations [32]. The important issues of resilience engineering include the dynamics and stability of complex systems.

2.2 Quantification of Resilience

Most of the existing studies in resilience focus on the conceptual and qualitative level of system analysis. Although various definitions of resilience have been proposed [33,34], there are limited quantification methods to measure the resilience of systems for analysis and comparison. These methods calculate resilience based on the curve of recovery. The curve of recovery shows the dynamic process that the function or performance of a system degrades during a shock and recovers afterwards. The typical concepts are illustrated in Figure 1, by which Francis and Bekera [34] used to define resilience factors. In the figure, F_o is the original stable system performance level, F_d is the performance level immediately

post-disruption, F_r^* is the performance level after an initial post-disruption equilibrium state has been achieved, F_r is the performance at a new stable level after recovery efforts have been exhausted, t_δ is the slack time before recovery ensues, t_r is the time to final recovery. Other researchers used the curves with minor variations, for instance, without explicit consideration of the initial post-disruption equilibrium state F_r^*, or the new stable state F_r being the same as the original stable state F_o. Definitions of resilience from the perspective of reliability are also available. For example, Youn et al. [35,36] defined resilience as the sum of system reliability and probability of restoration, which can be estimated from the information of probabilities that a system is at different states. Hu and Mahadevan [37] defined resilience with the considerations of probability of failure, probabilities of failure and recovery times, and performance.

Several resilience metrics based on the recovery curve have been proposed. Francis and Bekera [34] proposed a resilience measurement based on the ratios between the new stable states and the original state as

$$\rho = S_p \frac{F_r}{F_o} \frac{F_d}{F_o} \tag{1}$$

where S_p is the speed recovery factor calculated from recovery times to new equilibrium. In this metric of resilience, F_d/F_o captures the absorptive capacity of the system, and F_r/F_o expresses the adaptive capability. Therefore, the more functionality retained relative to the original capacity, the higher the resilience is.

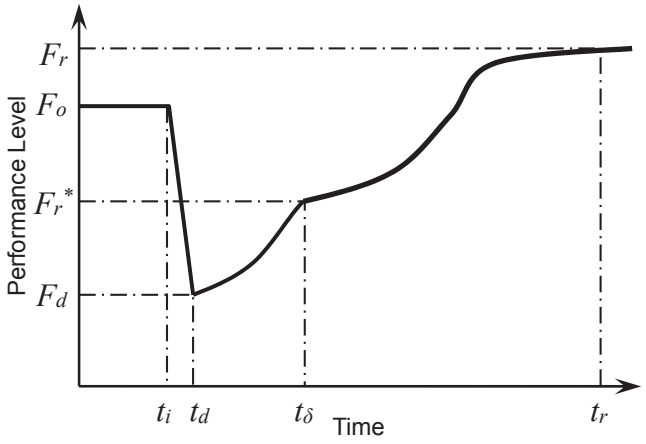


Figure 1: System performance curve used by Francis and Bekera [34].

Bruneau and Reinhorn [38,39] quantified resilience by

$$R_1 = \frac{1}{t_r - t_i} \int_{t_i}^{t_r} Q(t)dt \tag{2}$$

where $Q(t)$ is a dimensionless functionality function that has the value between 0 and 1, t_i is the time when the adverse event occurs that causes the loss of functionality, and t_r is the time of full recovery. That is, resilience is the area under the curve of performance divided by the time of duration, which is the average functionality. Among four factors of resilience that authors proposed, rapidity, robustness, resourcefulness, and redundancy, the first two are quantified. Rapidity is the slope of the functionality curve during recovery as $dQ(t)/dt$, whereas robustness is quantified as $1-L$ where L is a random variable that represents the loss of functionality due to the adverse event.

Ouyang et al. [40] proposed a resilience metric based on the expected area under the performance curve as

$$R_2 = \frac{\int_{t_i}^{t_r} F(t)dt}{\int_{t_i}^{t_r} F^*(t)dt} \tag{3}$$

where F is the performance curve as a stochastic variable, and F^* is the target performance curve. The resistant, absorptive, and restorative capabilities are considered all together in the integral form.

To provide more granularity for different failure and recovery modes, Ayuub [41] proposed the metric

$$R_3 = \frac{T_d\left[\frac{\int_{t_i}^{t_d} F(t)dt}{\int_{t_i}^{t_d} F^*(t)dt}\right] + T_r\left[\frac{\int_{t_d}^{t_r} F(t)dt}{\int_{t_d}^{t_r} F^*(t)dt}\right]}{T_d + T_r} \quad (4)$$

where $T_d = t_d - t_i$ and $T_r = t_r - t_d$ are the disruption and recovery time periods respectively. This metric provides the additional measures of failure and recovery speeds.

Notice that the above resilience definitions are based upon some performance measure F or Q. This measure can be domain specific. The performance metrics proposed in this paper provide a formal way to quantify the performance of CPS networks so that the resilience can be assessed according to most of the above quantities.

2.3 Resilience of Networks

The most relevant domain to CPS network resilience is the resilience of telecommunication networks such as Internet, wireless networks, and vehicular networks [29,42]. Resilience can be qualitatively measured in a state space formed by service parameters and operational state. The quantitative approaches measure system resilience by message delivery failure probabilities due to packet loss [43], payload error [44], or delay [45] during transmission. For topological analysis, the communication failures are quantified based on the connectivity in the Erdös-Rényi random graph [46]. Simulation models [47] have also been developed. The performance and resilience of networks are measured by packet delivery ratio [47], route diversity [48], node valence and connectivity [49,50], or quality of service [51,52].

The resilience of supply chain, logistics, and transportation networks has also been studied in the recent decade [53,54,55,56]. Most of the studies remain conceptual. In addition to the concepts of response and recovery, supply chain management also emphasizes proactive approach for readiness before and growth after disruption. Only limited efforts are given to quantitative analysis, particularly on resource allocation optimization under uncertainty, such as with differentiation between disruption and regular supply variability [57], facility location design [58,59], post-disaster recovery [60], multi-sourcing [61],

and inventory control [62,63,64]. For networks design, node valence and topological distances are used to quantify accessibility, robustness, flexibility, and responsiveness of networks [65].

Different from the above efforts which focus only on the capability of information exchange or material supply in networks, both communication and reasoning capabilities of CPS networks are considered in this study. A probabilistic model is proposed to quantify the capabilities of CPS networks, which is described in the following section.

3. PROBABILISTIC MODEL OF CPS NETWORK ARCHITECTURE

The architecture of CPS networks is modeled as a graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$, in which $\mathcal{V} = \{v_i\}$ is a set of N nodes represent IoT-compatible products, and $\mathcal{E} = \{(v_i, v_j)\}$ is a set of edges that indicate the information flow from node v_i to node v_j. An adjacency matrix $\boldsymbol{A} \in \mathbb{I}^{N\times N}$ is used to model the topology and its elements defined as

$$A_{ij} = \begin{cases} 1, & (v_i, v_j) \in \mathcal{E} \\ 0, & otherwise \end{cases}$$

In the probabilistic model, the correlations among nodes are represented with the correlation probability matrix $\mathbf{C} \in [0,1]^{N\times N}$ and its elements are conditional probabilities $C_{ij} = P(x_j|x_i)$ with random state variables x's associated with the nodes. Therefore the edges in the probabilistic graph model are directed.

3.1 Probabilistic Model

In CPS networks, each node has its own sensing, computation, and reasoning capabilities. The *prediction probability* that node v_i detects the true state of world θ is

$$P(x_i = \theta) = p_i \tag{5}$$

where x_i is the state variable of the i^{th} node. The information dependency between nodes is modeled with *P-reliance probability*

$$P(x_j = \theta | x_i = \theta) = p_{ij} \tag{6}$$

which is the probability that node v_j predicts the true state of world given that node v_i predicts correctly. Similarly, we also have *Q-reliance probability*

$$P(x_j = \theta | x_i \neq \theta) = q_{ij} \tag{7}$$

The *entropy* corresponding to the prediction probability of the i^{th} node is

$$H(x_i) = -p_i \log p_i - (1 - p_i) \log(1 - p_i) \tag{8}$$

and the ones to reliance probabilities are

$$H(x_{ij}) = -p_{ij} \log p_{ij} - (1 - p_{ij}) \log(1 - p_{ij})$$

$$H(x_{ij}^C) = -q_{ij} \log q_{ij} - (1 - q_{ij}) \log(1 - q_{ij}) \tag{9}$$

Additionally, the *conditional entropies* that quantify the information inter-dependency between state variables x_i's are defined as

$$H(x_j|x_i) = -\sum_{x_i} \sum_{x_j} P(x_j|x_i) P(x_i) \log P(x_j|x_i)$$

$$= -p_{ij} p_i \log p_{ij} - (1 - p_{ij}) p_i \log(1 - p_{ij}) - q_{ij}(1 - p_i) \log q_{ij} - (1 - q_{ij})(1 - p_i) \log(1 - q_{ij}) \tag{10}$$

The *mutual information* between state variables x_i and x_j is defined as

$$M(x_i, x_j) = H(x_j) - H(x_j|x_i) = H(x_i) - H(x_i|x_j) \tag{11}$$

which measures the extent that knowing one variable influences the knowledge about the other. It is zero if the two variables are independent. Mutual information thus can give an estimate of how much information exchange occurs among nodes in CPS networks. In a normal situation, the system is functioning at a stable level of information exchange. When the system is disrupted with connections broken down, the amount of information exchange will reduce. Therefore, mutual information is proposed here to measure the performance of CPS networks, described in the next section.

3.2 Performance Metrics of CPS Networks

A metric that measures the performance of a system should have the following properties [66]. First, the metric should be deterministic and monotone so that one-to-one correspondence between systems and measures can be established. Mutual information of two random variables x and y is non-negative. It is zero when the two variables are totally uncorrelated. It reaches maximum when the two are the same variable. That is, $0 \leq M(x, y) \leq M(x, x)$. In addition, mutual information is a symmetric metric and $M(x, y) = M(y, x)$.

Second, the metric should be dimensionality independent so that the performances of systems can be compared regardless their sizes. Calculating the average value of pairwise mutual information is necessary so that the measure is independent of the number of nodes. In addition, mutual information of random variables with discrete probability distributions also depends on the number of possible values for the random state variables, i.e. the size of state space or the probability mass functions associated with the state variables. A dimensionless measure for probabilistic design should incorporate the degrees of freedom for the system and the sizes of the state space.

Third, the metric should be sensitive to the change of systems when used for resilience measurement. The function and reliability of a system are sensitively dependent on those of subsystems and components. The metric should also be sensitive enough to reflect the changes at the component level.

Based on the above requirements, the proposed performance metric for a CPS network with *N* nodes and *D*-nary state variables is

$$F = \frac{1}{DN^2} \sum_{i=1}^{N} \sum_{j=1}^{N} M\left(x_i, x_j\right) \tag{12}$$

which is the average pairwise mutual information of the system. In the current setting of probabilistic design, *D*=2 (i.e. $x_i = \theta$ or $x_i \neq \theta$).

To demonstrate and evaluate the applicability of the proposed entropy and mutual information based performance metric to resilience measurement, a simulation study is conducted. In this study, the prediction and reliance probabilities for a network are first randomly generated. Then samples of the random state variables are generated based on the prediction and reliance probabilities. Within each iteration, for each state variable x_i, its value as either true or false prediction is sampled based on prediction probability p_i in Eq.(5). The prediction of x_j is then updated to a sample that is drawn based on reliance probability either p_{ij} in Eq.(6) or q_{ij} in Eq.(7), depending on the value of x_i. The update of prediction is based on the following best-case rule of information fusion

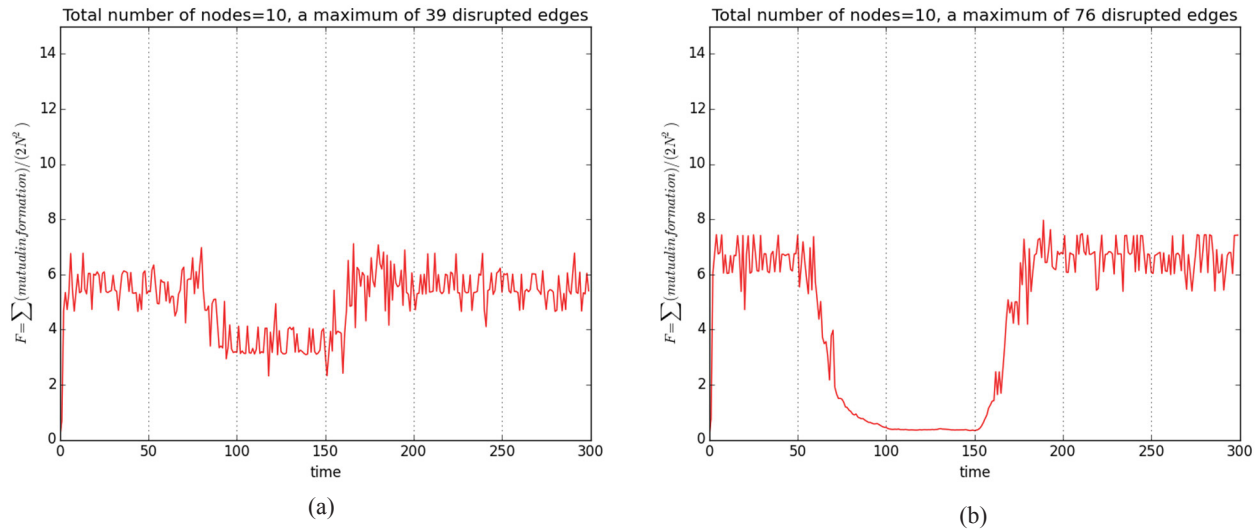
$$P\big(x_j = \theta\big) = 1 - \prod_{i=1}^{N}\big(1 - P(x_j = \theta | x_i)\big) \tag{13}$$

where any correct prediction as a result of the information cue from any connected node leads to a success. The sampling iterations continue until enough numbers of samples for all nodes are drawn for one time step. The prediction probabilities for all nodes are then updated based on the frequencies of correct predictions from the samples. The mutual information for each pair is calculated and the system performance in Eq.(12) is estimated. With the updated prediction probabilities, the system moves on to the next time step, and the same sampling and update procedures continue until the predetermined time limit is reached.

During the simulation, the system disruption and recovery occur at certain time steps, which are modeled with the changes of reliance probabilities. When the disruption occurs, the reliance probabilities (both p_{ij} and q_{ij}) of some randomly selected pairs are set to be zeros. At the recovery stage, these disconnected pairs are reconnected with the previous reliance probabilities recovered.

Figure 2 shows the performance measures from the simulation of a system with 10 nodes. For each iteration, 500 samples are drawn. The disruption starts at time step 50 and ends at time step 100, during which a number of connections are randomly selected as disrupted edges at each time step. By the time

step of 100, the total number of disrupted connections is 39 for the case in Figure 2(a) and is 76 for the case in Figure 2(b). The recovery period starts from time step 150 and ends at time step 200. The system is fully recovered by time step 250 and reaches the new equilibrium. It is seen that the proposed performance metric can sensitively detect disruptions from its trend. The volatility is mostly due to the relatively small number of nodes and sample sizes.

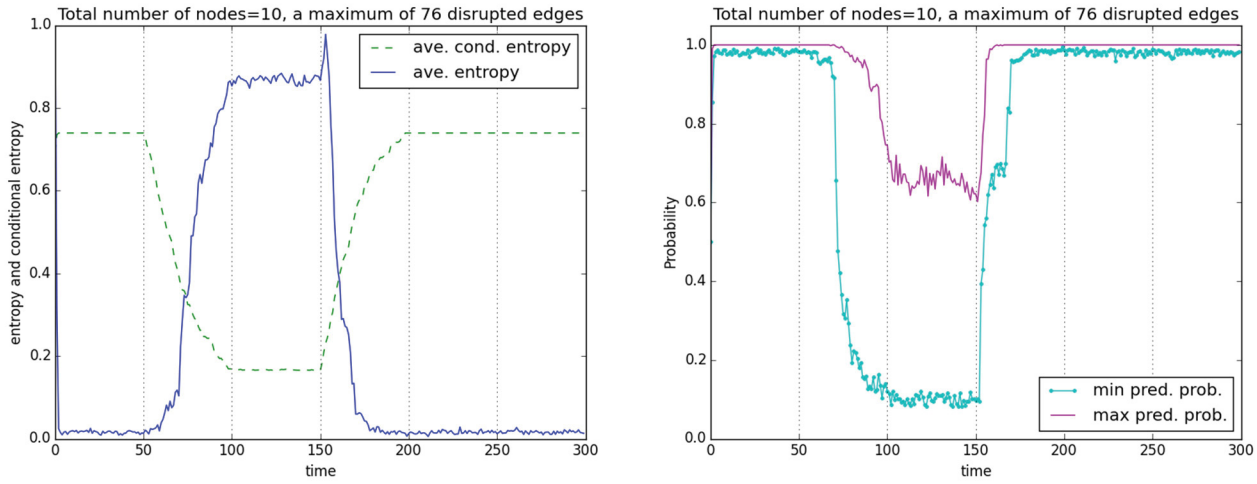


(a) (b)

Figure 2: Performance measure in Eq. (12) for a simulated CPS network with 10 nodes. (a) The maximum number of disconnected edges is 39. (b) The maximum number of disconnected edges is 76.

The dynamics of entropies and probabilities in the system in Figure 2(b) is shown in Figure 3. The average values of conditional entropies calculated from Eq.(10), and the average values of entropies calculated from the prediction probabilities in Eq.(8) are shown in Figure 3(a). During the disruption, the conditional entropies decrease, while the entropies associated with the prediction probabilities increase. The entropies have small values during the normal working period, because the prediction probabilities are relatively high. This is illustrated in Figure 3(b) where the maximum and minimum values of prediction probabilities among the 10 nodes are compared. The highest prediction probability is one. During the disruption, the differences between the prediction probabilities significantly increase. In other words, disruption affect the prediction capabilities of some nodes, and their prediction probability drop.

This in turn affects other nodes. It is seen the highest value of prediction probability among the nodes becomes less than one.

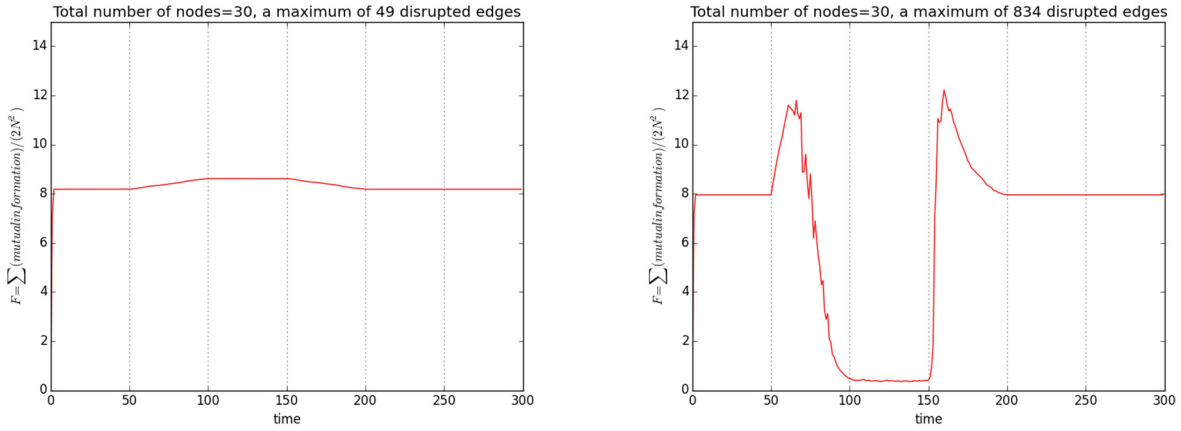


(a) (b)

Figure 3: The entropies and prediction probabilities of the simulated system in Figure 2(b) where the maximum number disconnected edges is 76. (a) The average conditional entropy calculated from Eq. (10) and the average entropy calculated from prediction probability in Eq.(8). (b) The minimum and maximum values of prediction probabilities among 10 nodes.

The number of nodes affects the overall performance and reliability of the system. Figure 4 shows the simulation results when the number of nodes increases to 30 and the total number of connections is 870. It is seen in Figure 4(a) that the system performs fairly robustly when the maximum number of disrupted connections is 49. The mutual information increases slightly instead of decrease during the disruption. This is because mutual information includes two components, entropy and conditional entropy, according to Eq.(11). During the disruption period, the conditional entropies associated with those disrupted edges reduce to zeros, whereas the prediction probabilities thus entropies of the relevant nodes are not affected. As a result, the mutual information increases. This phenomenon is also observed in Figure 4(b) where the maximum number of disrupted connections is 828. Shortly after the disruption starts at time step 50, the

average mutual information increases. Again, this is due to the reduction of conditional entropies while entropies associated with prediction probabilities remain unchanged, which is verified by plotting the average entropies and conditional entropies in Figure 5(a) and the maximum and minimum prediction probabilities in Figure 5(b). As the number of disconnected edges keeps increasing, prediction probabilities are affected. Mutual information starts decreasing until the maximum number of 828 disconnections is reached at time step 100. The system is stabilized in the next 50 time steps until recovery starts. During recovery, mutual information returns to the level prior to disruption reversely. After time step 200, the system is fully recovered.



(a) (b)

Figure 4: Performance measure of a simulated CPS network with 30 nodes. (a) The maximum number of disconnected edges is 49. (b) The maximum number of disconnected edges is 834.

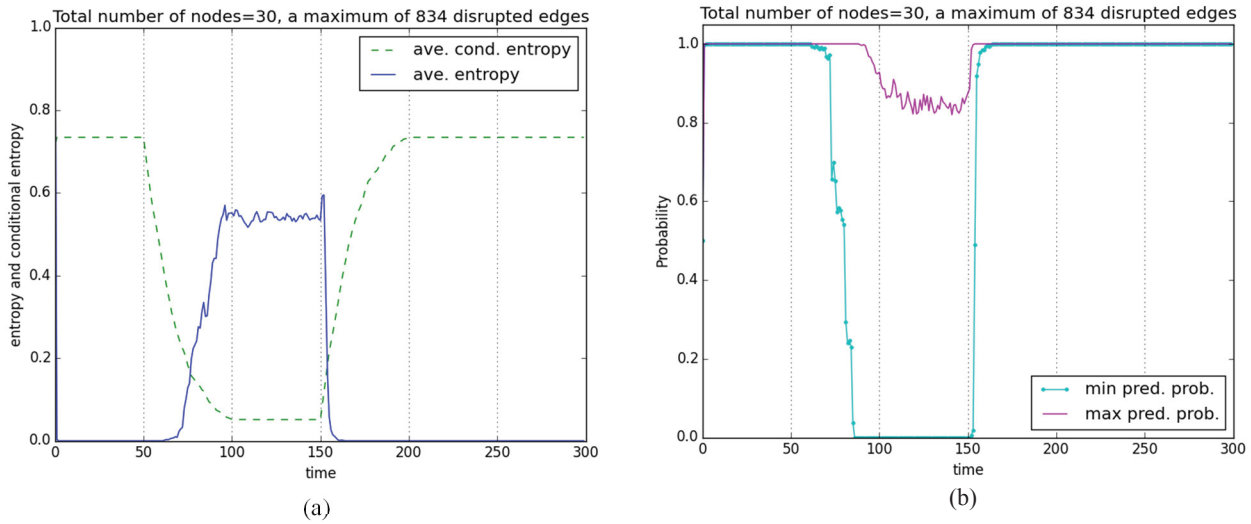


Figure 5: The entropies and prediction probabilities of the simulated system in Figure 4(b) where the maximum number disconnected edges is 834. (a) The average conditional entropy and the average entropy. (b) The minimum and maximum values of prediction probabilities among 30 nodes.

Notice that the average entropies are zeros at the normal working condition for the large network of 30 nodes in Figure 5(a). This is because the prediction probabilities of all nodes are ones before disruption, shown in Figure 5(b). The network is fully connected at the beginning because all pair-wise reliance probabilities are randomly generated. The predictions by all nodes are accurate. The predictions become not reliable after the number of disconnected edges reaches certain level after disruption has started. Some of the prediction probabilities reduce. As a result, the average entropy increases. The prediction capabilities of the nodes quickly recover after some of the connections resume. Intuitively the system should become more resilient to disruption when the number of nodes increases. It is confirmed by the simulation results. The examples show that the mutual entropy based performance measure is sensitive to the system topological change. It provides detailed information about the changes of prediction and reliance probabilities. The entropy and mutual information based metrics allow us to quantify the resilience of CPS networks or IoT systems described with the probabilistic model. These performance

metrics can be applied in further studies of system resilience and probabilistic design of the system architecture.

4. PROBABILISTIC DESIGN OF CPS NETWORK ARCHITECTURE

With the performance metric quantitatively defined, system design and optimization can be performed. The overall goal of the system architecture design for CPS networks is to find the optimum network topology such that the system performance is maximized.

It is seen that the reliability of prediction is related to the number of nodes in the system and connections that are available during disruption. Larger systems with more nodes and more connections tend to be more robust and give correct predictions than smaller systems. Therefore the design decision variables need to include the number of nodes, the respective prediction probabilities, and pair-wise reliance probabilities. Note that the topology of networks in the proposed probabilistic model is quantified by. reliance probabilities instead of binary connectivity. In addition, the performance of prediction is also related to the information fusion rules, based on which the prediction probabilities are updated. Design decisions also include the selection of the rules.

In this section, several information fusion rules for reasoning at the CPS component level are described. The sensitivities of system performance with respect to the prediction and reliance probabilities are also analyzed. Sensitivity analysis of design variables provides some insight of search domains in design optimization.

4.1 Information Fusion Rules at CPS Component Level

The prediction probabilities are also sensitively dependent on the rules of information fusion during prediction update. When receiving different cues from topologically correlated neighbors, a node needs to update its prediction probability to reflect the true state of the world. Several rules can be devised in addition to the best-case rule in Eq.(13). They are listed as follows.

- Best-case (optimistic)

$$P(x_j) = 1 - \prod_{i=1}^{M}\left(1 - P(x_j|x_i)\right) \tag{14}$$

If any of the *M* correlated nodes provides a positive cue, the prediction of the node is positive. Some variations of the rule include when the cases of negatively correlated nodes are also considered, as

$$P(x_j) = 1 - \prod_{i=1}^{M}\left(1 - P(x_j|x_i)\right)\left(1 - P(x_j|x_i^C)\right) \tag{15}$$

as well as when the node's own observation is excluded, as

$$P(x_j) = 1 - \prod_{i=1, i\neq j}^{M}\left(1 - P(x_j|x_i)\right) \tag{16}$$

- Worst-case (pessimistic)

$$P(x_j) = \prod_{i=1}^{M} P(x_j|x_i) \tag{17}$$

The prediction of the node is positive only if all of the *M* correlated nodes provide positive cues. Similarly, there could be some variations of the rule, such as

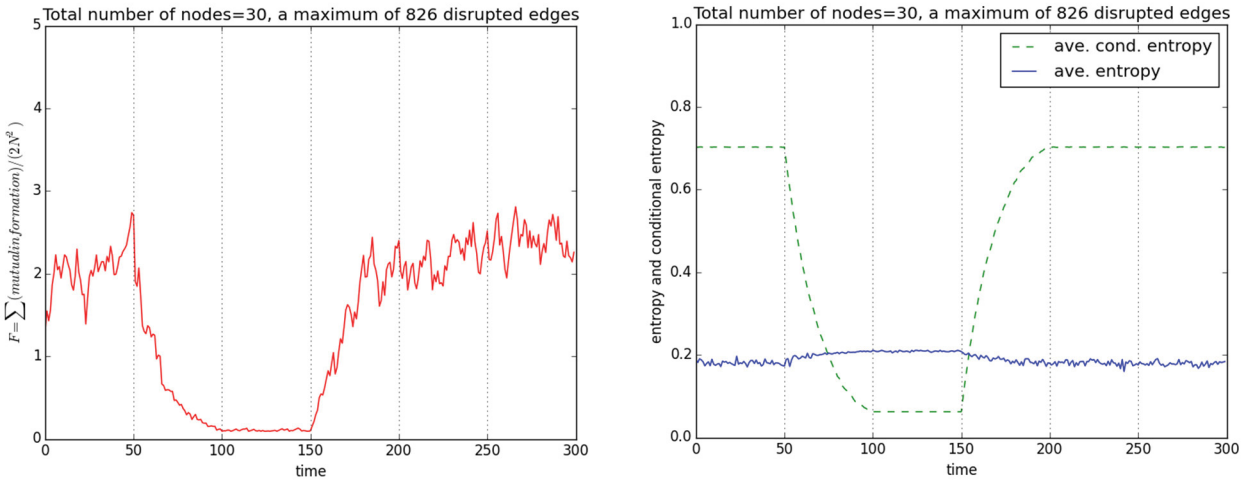
$$P(x_j) = \prod_{i=1, i\neq j}^{M} P(x_j|x_i) \tag{18}$$

- Bayesian

$$P'(x_j) \propto P(x_j)\left(P(x_j)\right)^r \left(1 - P(x_j)\right)^{M-r} \tag{19}$$

The prediction of the node is updated to P' from prior prediction P and the cues that the *M* correlated nodes provide, among which *r* of them provide a positive cue.

Figure 6 shows the simulation results based on the Bayesian fusion rule, where the update of prediction probabilities is gradual and much slower than the update based on the other two rules. Some other rules can be defined for information fusion, such as product-sum, weighted average, evidence-based, etc. Those empirical rules are less restrictive than the above three conventional ones.



(a) (b)

Figure 6: Simulation results based on the Bayesian fusion rule for a system of 30 nodes with a maximum of 826 disrupted connections. (a) Average mutual information performance measure. (b) Average conditional entropy and entropy.

4.2 Sensitivities of Performance Metrics with Respect to Probabilities

The closed-form local sensitivities of conditional entropies with respect to prediction and reliance probabilities can be obtained as

$$\frac{\partial H(x_j|x_i)}{\partial p_{ij}} = p_i \log \frac{1-p_{ij}}{p_{ij}} \tag{20}$$

$$\frac{\partial H(x_j|x_i)}{\partial q_{ij}} = (1-p_i) \log \frac{1-q_{ij}}{q_{ij}} \tag{21}$$

$$\frac{\partial H(x_j|x_i)}{\partial p_i} = p_{ij} \log \frac{1-p_{ij}}{p_{ij}} + q_{ij} \log \frac{q_{ij}}{1-q_{ij}} + \log \frac{1-q_{ij}}{1-p_{ij}} \tag{22}$$

It is seen in Eqs.(20) and (21) that the first derivatives of conditional entropy with respect to reliance probabilities are monotonically positive when $p_{ij} < 0.5$ and $q_{ij} < 0.5$. That is, for small reliance probabilities, increasing their values would increase the conditional entropies. On the other side, the derivatives become negative when $p_{ij} > 0.5$ and $q_{ij} > 0.5$, and the trend is the opposite.

The first derivatives of conditional entropies with respect to prediction probabilities are not monotonic, as seen in Eq.(22). They are functions of reliance probabilities, which have (0.5,0.5) as a saddle point, as

shown in Figure 7. When $q_{ij} < 0.5$ and $q_{ij} < p_{ij} < 1 - q_{ij}$, or $q_{ij} > 0.5$ and $1 - q_{ij} < p_{ij} < q_{ij}$, the sensitivities are in the positive domain.

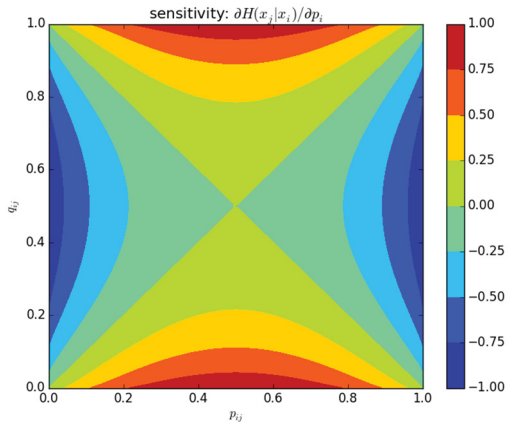
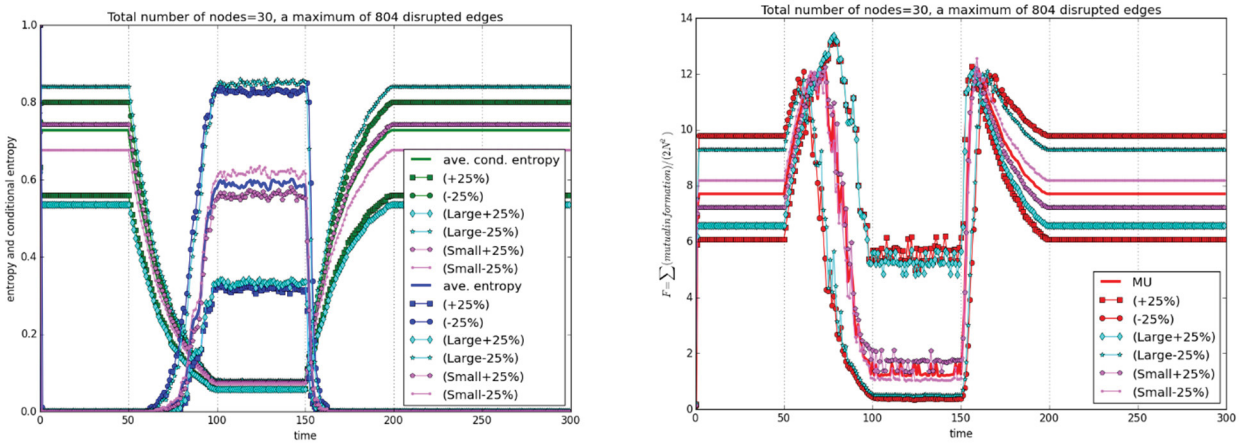


Figure 7: Sensitivity of conditional entropy with respect to prediction probability

Understanding the local sensitivity of conditional entropies is useful for local adjustment of probabilities especially when the system's prediction probabilities are not sensitive to the changes of reliance probabilities. Either increasing the large reliance probabilities that are greater than 0.5 or decreasing the small ones that are less than 0.5 for those uninterrupted nodes will reduce the conditional entropies. Figure 7 also suggests that it is better to focus the adjustment of reliance probabilities in either the upper right quarter of the domain where both P- and Q-reliance probabilities are larger than 0.5, or the lower left quarter where both P- and Q-reliance probabilities are less than 0.5. Because the individual effect of adjusting probabilities in other two quarters could be similar. But with the combination, the overall trend can be compromised and dampened.



(a) (b)

Figure 8: Sensitivity analysis based on the best-case fusion rule by increasing all reliance probabilities by 25% (+25%), reducing all by 25% (−25%), increasing only those large probabilities that are greater than 0.5 by 25% (Large+25%), reducing only these large probabilities (Large−25%), increasing only those small probabilities that are less than 0.5 by 25% (Small+25%), and reducing only those small probabilities (Small−25%). (a) Average conditional entropies and entropies. (b) Average mutual information.

The sensitivity analysis is verified by the simulation results shown in Figure 8. The sensitivity analysis is done by varying the levels of reliance probabilities. Six different situations are tested, including increasing and reducing all reliance probabilities by 25%, increasing and reducing only those large probabilities that are greater than 0.5 by 25%, and increasing and reducing only those small probabilities that are less than 0.5 by 25%. In case a probability value after such perturbation exceeds 1, it is set to be the value of 1 as the upper bound. It is seen in Figure 8(a) that increasing the reliance probabilities will reduce the average conditional entropy, whereas reducing them will increase the conditional entropy. Increasing or reducing only the large reliance probabilities will have the same effect on the conditional entropy. That is, adjusting only the large reliance probabilities is sensitive enough to obtain desirable system performance. The trend of adjusting small reliance probabilities is the opposite. Increasing only the small reliance probabilities will increase conditional entropy. However, in this case, the end effect of adjusting small probabilities is not as significant as adjusting large ones. The end effect of adjusting probabilities on average entropy is the same. Both conditional entropies and entropies are more sensitive

to the large reliance probabilities than to the small ones. Similarly, in Figure 8(b), changing large reliance probabilities gives the similar results of changing all of the probabilities on the mutual information.

Therefore, improving those relatively reliable connections or sources of information with large reliance probabilities is more effective to optimize the system performance than simultaneously considering all connections in a system. In other words, the attention of resilience engineering for these networks needs to be focused more on the relatively good and trustable communication channels instead of the weakest links, as we usually do for reliability consideration.

The sensitivity of the system is also dependent on the information fusion rules. When the Bayesian rule is applied, the system is not sensitive to the changes of reliance probabilities any more. As shown in Figure 9, the variation of the average mutual information as a result of different reliance probabilities is small.

According to the quantitative definitions of resilience in Section 2.2, the systems with the Bayesian rule are more robust, however less resilient, than the ones with the best-case rule. Notice that robustness, instead of resilience, is directly related to sensitivity. A system is less resilient if its performance is more likely to deteriorate under small disruption. The less resilient system can also be robust at the same time if it is not sensitive to the change or adjustment of system parameters and its performance always deteriorate quickly. In the above sensitivity studies, common random numbers are used in the comparison among different systems. This is to reduce the variance introduced in the simulation.

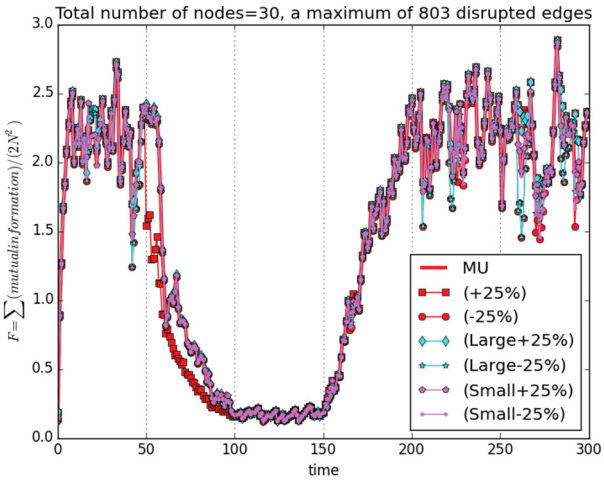


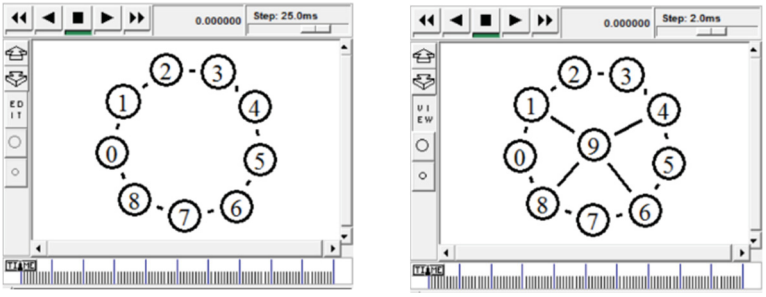
Figure 9: Sensitivity of a simulated system based on the Bayesian rule

5. DEMONSTRATION WITH DISCRETE-EVENT SIMULATIONS

To demonstrate how the proposed performance metrics can be applied to actual CPS networks and how effective the metrics can be used in measuring network performance, discrete-event simulation models for computer networks are used here to illustrate. The fine-grained simulation models, which are built with ns-2 [67], are as detailed as the physical networks with the models of data packets and different Internet protocols such as TCP and UDP. Data are generated and transmitted from one node to another.

In the first example, a ring network with 9 nodes is modeled, as shown in Figure 10(a). TCP is used as the communication protocol. Application data flows with FTP sources are modeled from nodes #0 to #5, #2 to #6, #4 to #8, #7 to #3, #5 to #1, and #8 to #3. All connections have a packet loss rate of 0.01. The model is run to simulate the traffic for 10 seconds of time. At clock time 3.0 second, a network disruption occurs, where either one, two, or three edges are disconnected. The connections are resumed at clock time 5.0 second. The numbers of packets that are sent and received for each data flow path are summarized in Table 1. Each column in the table corresponds a flow path. Four scenarios (no disruption, one-edge, two-edge, and three-edge disconnections during disruption) are simulated. In this model, sensing and prediction capabilities of CPS are not simulated. Only communication is modeled. It is

assumed that only positive prediction information is transferred between nodes. Therefore the prediction probability associated with each source node is estimated as the ratio between the number of packets sent and a reference number, assuming that sending more implies a higher capability of prediction. The common reference number can be set as the theoretical upper limit by which the maximum number of packets can be sent by a source under any circumstance for the time period under consideration. The upper limit used in this example as the reference is 5000. The P-reliance probability for each path is estimated as the ratio between the number of packets received by sink and the one sent by source. The ratio can be less than one because of packet loss and traffic jam. Assuming Q-reliance probabilities are zeros, entropy, conditional entropy, and mutual information are calculated from the prediction and P-reliance probabilities. The average entropy, conditional entropy, and mutual information for all paths are also listed in the last column of Table 1.



(a) (b)

Figure 10: Two ring models simulated in ns-2 for demonstration

Table 1. The simulation results and performance metrics of a ring network with four different scenarios

	#0 to #5	#2 to #6	#4 to #8	#7 to #3	#5 to #1	#8 to #3	Average
a. No disruption							
Packets sent by source	2079	1264	1191	1177	1226	734	
Packets received by sink	2055	1247	1191	1160	1211	727	
Prediction probability	0.4158	0.2528	0.2382	0.2354	0.2452	0.1468	
P-reliance probability	0.9885	0.9866	1.0	0.9856	0.9878	0.9905	
Entropy	0.9794	0.8157	0.7920	0.7873	0.8036	0.6018	0.7966
Conditional Entropy	0.0378	0.0260	0.0	0.0257	0.0234	0.0114	0.0207
Mutual Information	0.9417	0.7897	0.7920	0.7617	0.7802	0.5904	0.7759
b. Disruption (edge 6-7)							
Packets sent by source	1490	1436	466	484	1034	569	
Packets received by sink	1481	1419	466	476	1027	567	
Prediction probability	0.2980	0.2872	0.0932	0.0968	0.2068	0.1138	
P-reliance probability	0.9940	0.9882	1.0	0.9835	0.9932	0.9965	
Entropy	0.8788	0.8651	0.4471	0.4588	0.7353	0.5113	0.6494
Conditional Entropy	0.0159	0.0266	0.0	0.0118	0.0121	0.0038	0.0117
Mutual Information	0.8629	0.8384	0.4471	0.4470	0.7232	0.5074	0.6377
c. Disruption (edges 6-7, 2-3)							
Packets sent by source	1471	586	721	909	225	205	
Packets received by sink	1435	579	715	897	218	195	
Prediction probability	0.2942	0.1172	0.1442	0.1818	0.045	0.041	
P-reliance probability	0.9925	0.9881	0.9917	0.9868	0.9689	0.9512	
Entropy	0.8741	0.5213	0.5951	0.6840	0.2648	0.2469	0.5310
Conditional Entropy	0.0187	0.0110	0.0100	0.0184	0.0090	0.0115	0.0131
Mutual Information	0.8554	0.5103	0.5851	0.6656	0.2558	0.2353	0.5179
d. Disruption (edges 6-7, 2-3, 0-8)							
Packets sent by source	1045	966	285	484	230	343	
Packets received by sink	1037	964	280	476	222	336	
Prediction probability	0.2090	0.1932	0.0570	0.0968	0.0460	0.0686	
P-reliance probability	0.9923	0.9979	0.9825	0.9835	0.9652	0.9796	
Entropy	0.7396	0.7081	0.3154	0.4588	0.2692	0.3607	0.4753
Conditional Entropy	0.0135	0.0041	0.0073	0.0118	0.0100	0.0099	0.0094
Mutual Information	0.7260	0.7040	0.3082	0.4470	0.2592	0.3508	0.4659

It is seen from this example that the proposed metrics of entropy, conditional entropy, and mutual information are sensitively dependent upon the change of network traffic pattern. From scenarios of no disruption to three-edge disruption, the performance of network is reduced gradually. The average values of entropy, conditional entropy, and mutual information also change monotonically.

As the further comparison, the ring network in Figure 10(a) is modified to Figure 10(b), where a new node and four edges are inserted. The same four scenarios are simulated in the second ring network, and the statistics of packets are collected in the same way. The calculated metrics are average entropy (0.8869, 0.7524, 0.7524, 0.7524), conditional entropy (0.0150, 0.0194, 0.0194, 0.0194), and mutual information

(0.8719, 0.7331, 0.7331, 0.7331) respectively for four scenarios. The metrics between the two examples are compared in Figure 11. The metrics indicate that Model 2 is more resilient than Model 1, which is easy to verify from the topology since Model 2 includes more edges and is less susceptible to disruptions.

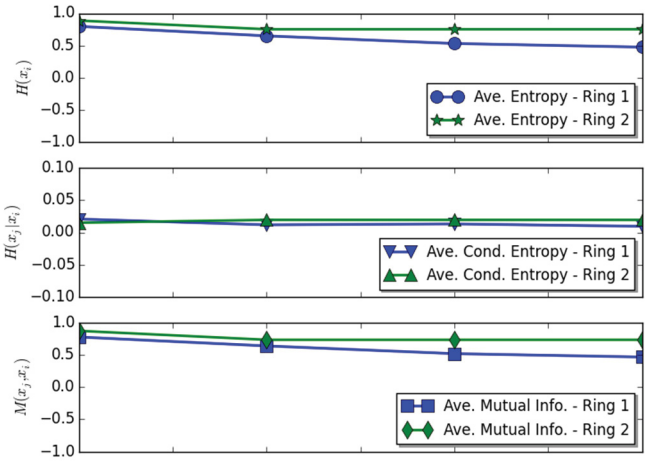


Figure 11: Comparison of metrics for the two simulated ring models

6. DISCUSSIONS

The simulation studies in this research demonstrated that entropy and mutual information can be applied as the metrics for functionality and performance measures for CPS systems in order to assess resilience. The proposed probabilistic design framework requires prediction and reliance probabilities as the inputs. These quantities may be derived from historical data or solicitation. Obtaining reliable and consistent estimations of probabilities is a challenging research issue itself. The studies here mostly focus on communication. More comprehensive investigations are needed for sensing, reasoning, and prediction capabilities.

At individual node level, several information fusion rules such as best-case, worst-case, and Bayesian can be defined so that the prediction probability associated with a node is updated based on the received information from neighboring nodes during reasoning. It is seen that the system resilience and robustness

are sensitively dependent on the fusion rules. During the system design process, information aggregation rules also need to be optimized based on the expected dynamics of performance.

The proposed metrics perform reasonably well with the simple reasoning scheme based on the information fusion rules. As future extensions, the proposed performance metrics need to be further tested with some other information fusion rules. Choosing appropriate rules is expected to be an important task in designing CPS networks and systems.

The sensitivity studies also show that the system performance is influenced more by the tightly coupled nodes, where reliance probabilities are high, than those loosely coupled ones. The optimization of systems is more effective if efforts are focused on these connections with high reliance probabilities, if the available resource is limited for improvement. Design optimization methods also need to be further explored based on the preliminary result of sensitivity analysis. The system design and optimization based on the performance and resilience metrics mostly requires a multi-objective optimization approach, since these metrics provide multi-facet assessment. If system dynamics needs to be considered, dynamic programming approaches can also be taken.

Although the proposed metrics and probabilistic measure are in the context of CPS networks, the methodology can potentially be extended for other networked systems where strong interdependency exists among individual components. Information, energy, and material flows can all be modeled similarly. For instance, in supply chain or transportation networks, prediction probability can correspond to the probability that goods or supplies satisfy the demand at a node, probability distribution of demand, or the distribution of inventory levels at a node, whereas reliance probabilities characterize the correlations between demands at different nodes (percentage of supply from one node goes to another), percentage of transport capacities being employed, or probability that transportation is not interrupted. Different node

types (source, sink, warehouse, hub, retailer, etc.) and edge types (shortest path, minimum cut, etc.) can be differentiated with different types of prediction and reliance probabilities.

7. CONCLUSION

In this paper, generic CPS network performance metrics are proposed based on entropy, conditional entropy, and mutual information to allow for quantitative resilience engineering of such networks. In CPS networks, each node corresponds to a CPS component. The processes of communication during information exchange between nodes and reasoning at individual nodes are characterized with reliance and prediction probabilities respectively in a probabilistic design framework. The resilience of the system then can be quantified with the proposed performance metrics of entropy and mutual information. Simulation studies show that these metrics are reasonable and consistent quantities to measure how communication and reasoning capabilities are affected during network disruption. The metrics are shown to be sensitive to the changes of network topology.

APPENDIX

In information theory, Shannon entropy is typically used to measure the amount of uncertainty or how much information a set of possible values, each of which has a corresponding probability, would contain. For a discrete random variable X, which may have a finite set of possible values $\mathcal{X}$, Shannon entropy is defined as

$$H(X) = -\sum_{x\in\mathcal{X}} p(X = x) log p(X = x) \tag{23}$$

For continuous variable, integral operator is used instead of summation in Eq.(23).

Conditional entropy, defined as

$$H(X|Y) = \sum_{y\in y} p(Y=y)H(X|Y=y)$$

$$= -\sum_{x\in X}\sum_{y\in y} p(X=x,Y=y)log(X=x|Y=y) \quad (24)$$

quantifies how much additional information random variable X can provide if the value of random variable Y is known.

Mutual information, defined as

$$M(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

$$= \sum_{x\in X}\sum_{y\in y} p(X=x,Y=y)log\left(\frac{p(X=x,Y=y)}{p(X=x)p(Y=y)}\right) \quad (25)$$

measures the mutual dependency between random variables X and Y.

ACKNOWLEDGEMENTS

This work is supported in part by U.S. National Science Foundation under grant number CMMI-1663227.

REFERENCES

[1] Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In *Proceedings of the ACM 47th Design Automation Conference* (pp. 731-736).

[2] K. Ashton, "That 'Internet of Things' Thing," *RFiD Journal*, vol.22, pp.97-114, 2009.

[3] Holling, C. S. (1961). Principles of insect predation. *Annual Review of Entomology*, *6*(1), 163-182.

[4] Rosenzweig, M. L., & MacArthur, R. H. (1963). Graphical representation and stability conditions of predator-prey interactions. *American Naturalist*, *97*(895), 209-223.

[5] Lewontin, R.C. (1969). The meaning of stability. In: Diversity and Stability of Ecological Systems. Brookhaven Symposia in Biology No 22. Brookhaven, New York.

[6] Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, *4*,1-23.

[7] Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. *Global Environmental Change*, *16*(3), 253-267.

[8] Scheffer, M., & Carpenter, S. R. (2003). Catastrophic regime shifts in ecosystems: linking theory to observation. *Trends in ecology & evolution*, *18*(12), 648-656.
[9] Arrow, K., Bolin, B., Costanza, R., Dasgupta, P., Folke, C., Holling, C. S., Jansson, B.-O., Levin, S., Mäler, K.-G., Perrings, C., & Pimentel, D. (1995). Economic growth, carrying capacity, and the environment. *Science*, *268*, 520-521.
[10] Christopherson, S., Michie, J., & Tyler, P. (2010). Regional resilience: theoretical and empirical perspectives. *Cambridge Journal of Regions, Economy and Society*, *3*(1), 3-10.
[11] Martin, R. (2012). Regional economic resilience, hysteresis and recessionary shocks. *Journal of Economic Geography*, *12*(1), 1-32.
[12] Foster, K. A. (2007). A Case Study Approach to Understanding Regional Resilience. Institute of Urban and Regional Development, University of California, Berkeley, Report No. 2007-08.
[13] Hill, E., Wial, H., & Wolman, H. (2008). Exploring regional economic resilience. Institute of Urban and Regional Development, University of California, Berkeley, Report No. 2008-04.
[14] Schiefer, H. F. (1933). The Compressometer An Instrument for Evaluating the Thickness, Compressibility and Compressional Resilience of Textiles and Similar Materials. *Textile Research Journal*, *3*(10), 505-513.
[15] Mark, H. (1946). Some remarks about resilience of textile materials. *Textile Research Journal*, *16*(8), 361-368.
[16] Hoffman, R. M. (1948). A Generalized Concept of Resilience. *Textile Research Journal*, *18*(3), 141-148.
[17] Fielding, J. H. (1937). Impact resilience in testing channel black. *Rubber Chemistry and Technology*, *10*(4), 807-819.
[18] Turner, L. B., Haworth, J. P., Smith, W. C., & Zapp, R. L. (1943). Carbon Black in Butyl Rubber. *Industrial & Engineering Chemistry*, *35*(9), 958-963.
[19] Dillon, J. H., Prettyman, I. B., & Hall, G. L. (1944). Hysteretic and Elastic Properties of Rubberlike Materials Under Dynamic Shear Stresses. *Journal of Applied Physics*, *15*(4), 309-323.
[20] Liu, J. W., Shih, W. K., Lin, K. J., Bettati, R., & Chung, J. Y. (1994). Imprecise computations. *Proceedings of the IEEE*, *82*(1), 83-94.
[21] Hegde, R., & Shanbhag, N. R. (1999). Energy-efficient signal processing via algorithmic noise-tolerance. In *Proceedings of the 1999 international symposium on Low power electronics and design, August 16-17, 1999, San Diego, CA, USA*, pp. 30-35.
[22] Cho, H., Leem, L., & Mitra, S. (2012). ERSA: Error Resilient System Architecture for Probabilistic Applications. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *31*(4), 546-558.
[23] Chippa, V. K., Mohapatra, D., Raghunathan, A., Roy, K., & Chakradhar, S. T. (2010). Scalable effort hardware design: exploiting algorithmic resilience for energy efficiency. In *Proceedings of the 47th Design Automation Conference* (DAC'10)*, June 13-18, 2010, Anaheim, California, USA*, pp. 555-560.
[24] Verma, N., Lee, K. H., Jang, K. J., & Shoeb, A. (2012, March). Enabling system-level platform resilience through embedded data-driven inference capabilities in electronic devices. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* pp. 5285-5288.
[25] Wang, Z., Schapire, R. E., & Verma, N. (2015). Error Adaptive Classifier Boosting (EACB): Leveraging Data-Driven Training Towards Hardware Resilience for Signal Inference. *IEEE Transactions on Circuits and Systems I: Regular Papers, 62*(4), 1136-1145.
[26] Abdallah, R., & Shanbhag, N. R. (2013). Error-resilient systems via statistical signal processing. In *Proc. 2013 IEEE Workshop on Signal Processing Systems (SiPS),* pp. 312-317.

[27] Schneider, F. B. (Ed.). (1999). *Trust in cyberspace*. National Academies Press.
[28] Lin, H. S., & Goodman, S. E. (Eds.). (2007). *Toward a safer and more secure cyberspace*. National Academies Press.
[29] Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, *54*(8), 1245-1265.
[30] Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2007). *Resilience Engineering: Concepts and Precepts*. Ashgate Publishing, Burlington, VT.
[31] Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal*, **3**(2), 181-191.
[32] Hollnagel, E., & Fujita, Y. (2013). The Fukushima disaster – Systematic failures as the lack of resilience. *Nuclear Engineering and Technology*, **45**(1), 13-20.
[33] Zhou, H., Wan, J., & Jia, H. (2010). Resilience to natural hazards: a geographic perspective. *Natural Hazards*, **53**(1), 21-41.
[34] Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, **121**, 90-103.
[35] Youn, B. D., Hu, C., & Wang, P. (2011). Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design*, **133**(10), 101011.
[36] Yodo, N., & Wang, P. (2016). Resilience modeling and quantification for engineered systems using Bayesian networks. *Journal of Mechanical Design*, **138**(3), 031404.
[37] Hu, Z., & Mahadevan, S. (2016). Resilience Assessment Based on Time-Dependent System Reliability Analysis. *Journal of Mechanical Design*, **138**(11), 111404.
[38] Bruneau, M., & Reinhorn, A. (2007). Exploring the concept of seismic resilience for acute care facilities. *Earthquake Spectra*, **23**(1), 41-62.
[39] Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Framework for analytical quantification of disaster resilience. *Engineering Structures*, *32*(11), 3639-3649.
[40] Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety*, **36/37**, 23-31.
[41] Ayyub, B. M. (2015). Practical Resilience Metrics for Planning, Design, and Decision Making. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, *1*(3), 04015008.
[42] Khabbaz, M. J., Assi, C. M., & Fawaz, W. F. (2012). Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges. *IEEE Communications Surveys & Tutorials*, *14*(2), 607-640.
[43] Miu, A., Balakrishnan, H., & Koksal, C. E. (2005, August). Improving loss resilience with multi-radio diversity in wireless networks. In *Proceedings of the 11th annual International Conference on Mobile Computing and Networking*, pp. 16-30.
[44] Lei, J. J., & Kwon, G. I. (2010). Reliable Data Transmission Based on Erasure-resilient Code in Wireless Sensor Networks. *TIIS Transactions on Internet & Information Systems*, *4*(1), 62-77.
[45] Huang, Y., Gao, Y., Nahrstedt, K., & He, W. (2009, June). Optimizing file retrieval in delay-tolerant content distribution community. In *Proc. 29th IEEE International Conference on Distributed Computing Systems (ICDCS'09)*. pp. 308-316.
[46] Cohen, R., Erez, K., Ben-Avraham, D., & Havlin, S. (2000). Resilience of the Internet to random breakdowns. *Physical review letters*, *85*(21), 4626.

[47] Çetinkaya, E. K., Broyles, D., Dandekar, A., Srinivasan, S., & Sterbenz, J. P. (2013). Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach. *Telecommunication Systems*, *52*(2), 751-766.

[48] Rohrer, J. P., Jabbar, A., & Sterbenz, J. P. (2014). Path diversification for future internet end-to-end resilience and survivability. *Telecommunication Systems*, *56*(1), 49-67.

[49] Paul, G., Sreenivasan, S., & Stanley, H. E. (2005). Resilience of complex networks to random breakdown. *Physical Review E*, *72*(5), 056130.

[50] Sun, F., & Shayman, M. A. (2007). On pairwise connectivity of wireless multihop networks. *International Journal of Security and Networks*, *2*(1-2), 37-49.

[51] Shirazi, F., Diaz, C., & Wright, J. (2015, October). Towards measuring resilience in anonymous communication networks. In *Proc. the 14th ACM Workshop on Privacy in the Electronic Society*, pp. 95-99.

[52] Pradhan, S., Dubey, A., Levendovszky, T., Kumar, P. S., Emfinger, W. A., Balasubramanian, D., Otte, W., and Karsai, G. (2016) Achieving resilience in distributed software systems via self-reconfiguration. *Journal of Systems and Software*, **122**: 344-363.

[53] Sheffi, Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. MIT Press.

[54] Hohenstein, N. O., Feisel, E., Hartmann, E., & Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: a systematic review and paths for further investigation. *International Journal of Physical Distribution & Logistics Management*, *45*(1/2), 90-117.

[55] Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: definition, review and theoretical foundations for further study. *International Journal of Production Research*, *53*(18), 5592-5623.

[56] Ivanov, D., Mason, S. J., & Hartl, R. (2016). Supply chain dynamics, control and disruption management. *International Journal of Production Research*, *54*(1), 1-7.

[57] Chopra, S., Reinhardt, G., & Mohan, U. (2007). The importance of decoupling recurrent and disruption risks in a supply chain. *Naval Research Logistics*, *54*(5), 544-555.

[58] Snyder, L. V., & Daskin, M. S. (2005). Reliability models for facility location: the expected failure cost case. *Transportation Science*, *39*(3), 400-416.

[59] Li, X., & Ouyang, Y. (2010). A continuum approximation approach to reliable facility location design under correlated probabilistic disruptions. *Transportation research part B: methodological*, *44*(4), 535-548.

[60] Yang, Y., & Xu, X. (2015). Post-disaster grain supply chain resilience with government aid. *Transportation research part E: logistics and transportation review*, *76*, 139-159.

[61] Seok, H., Kim, K., & Nof, S. Y. (2016). Intelligent contingent multi-sourcing model for resilient supply networks. *Expert Systems with Applications*, *51*, 107-119.

[62] Spiegler, V. L., Naim, M. M., & Wikner, J. (2012). A control engineering approach to the assessment of supply chain resilience. *International Journal of Production Research*, *50*(21), 6162-6187.

[63] Hu, Y., Li, J., & Holloway, L. E. (2013). Resilient control for serial manufacturing networks with advance notice of disruptions. *Systems, Man, and Cybernetics: Systems, IEEE Transactions on*, *43*(1), 98-114.

[64] Hishamuddin, H., Sarker, R. A., & Essam, D. (2013). A recovery model for a two-echelon serial supply chain with consideration of transportation disruption. *Computers & Industrial Engineering*, *64*(2), 552-561.

[65] Mari, S. I., Lee, Y. H., Memon, M. S., Park, Y. S., & Kim, M. (2015). Adaptivity of complex network topologies for designing resilient supply chain networks. *International Journal of Industrial Engineering*, *22*(1), 102-116.
[66] Wang, Y. System resilience quantification for probabilistic design of Internet-of-things architecture. In *Proceedings of the ASME 2016 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference (IDETC/CIE2016), August 21-24, 2016, Charlotte, North Carolina, USA*, Paper No. DETC2016-59426.
[67] Network simulator ns-2. Available at http://www.isi.edu/nsnam/ns/