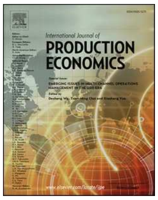
Contents lists available at ScienceDirect

International Journal of Production Economics

journal homepage: http://www.elsevier.com/locate/ijpe



Strategic lines of collaboration in response to disruption propagation (CRDP) through cyber-physical systems

Win P.V. Nguyen [*], Shimon Y. Nof

PRISM Center and School of Industrial Engineering, Purdue University, United States of America

ARTICLE INFO

Keywords:
Collaborative control
Collaborative response
Cyber-physical systems
Disruption propagation
Disruption response
Team formation

ABSTRACT

Recent developments in modern cyber-physical systems (CPSs) have allowed greater levels of intelligence and flexibility. The high levels of interactions and interdependencies in CPSs, however, also increase their vulnerabilities to external attacks and internal malfunctions. Disruptions in one cluster of a CPS can propagate to another cluster, eventually compromising the entire CPS if protective mechanisms and preparations are insufficient. The economic impacts are immediately local, but will become global should response mechanisms prove insufficient. Ensuring CPS resilience against disruption propagation requires the appropriate strategic preparation of response mechanisms, which is studied in this article. Recent work in CPS disruption response, notably the Collaborative Response to Disruption Propagation (CRPD) framework, has established the foundations for modeling and comprehension of the disruption response problem. Building upon the CRDP framework, this research introduces the Collaborative Response to Disruption Propagation/Strategic Lines of Collaboration (CRDP/SLOC) to investigate the effects of selecting different response agent teams to tackle disruptions. This selection is a strategic decision that cannot be altered once the disruptions begin, and thus needs to be guided by an appropriate collaborative control principle, called the SLOC principle. The SLOC principle analyzes the network structure, incorporates disruption propagation knowledge, and evaluates the strategic compatibility of the response agent teams to guide the selection and preparation process. The CRDP/SLOC model is validated using a set of experiments with different factors. These experiments indicate that the teams selected with the SLOC principle outperform the baseline teams in terms of response performance and resilience.

1. Introduction

1.1. *Motivations for this work*

Unexpected disruptive events during recent decades have drawn increasing attention to the concept of resilience in cyber-physical systems (CPSs) and complex networks: Networks of information, supply, computers, manufacturing, utility, transportation, and other infrastructure (Crucitti et al., 2004). The complex interactions and interdependencies of a CPS, while enabling greater economic growth and better quality of services, also allow the locally-occurring disruptions to propagate to other parts and subsystems of the CPS. For example, computer networks and sensor networks are vulnerable to propagating malware and informational errors, which can compromise the quality and/or functionality of the networks (Snediker et al., 2008; Kim et al., 2015; Liu et al., 2016). Advanced supply networks and manufacturing networks are also vulnerable to disruptions and disruption propagation, where disruptions in one node can negatively affect preceding and succeeding nodes, due to unfulfilled demands and/or supplies (Reyes Levalle and Nof, 2015b; 2015a, 2017; Reyes Levalle, 2018). External disruptions, such as natural disasters and cyber-attacks, can disrupt the production of certain raw materials and intermediate production steps; damage or destroy infrastructure, which can negatively impact manufacturing processes and product quality (Day, 2014; Gong et al., 2014). Internal disruptions, such as demand/supply uncertainties, human errors, equipment and machinery breakdowns, can also affect the performance of advanced supply networks and manufacturing networks (Sajadi et al., 2011). Disruptions within a CPS can also propagate between the physical layer (hardware, machinery, robots, tools, autonomous vehicles, drones, other physical connectors, etc.); and the cyber layer (software agents, automatic control and decision algorithms and protocols, communication protocols, etc.) of the CPS. This propagation of disruptions between the different CPS layers occur because of the high interdependency and interconnectedness between these layers.

[*] Corresponding author.
E-mail addresses: nguyen41@purdue.edu (W.P.V. Nguyen), nof@purdue.edu (S.Y. Nof).

https://doi.org/10.1016/j.ijpe.2020.107865
Received 18 November 2019; Received in revised form 27 June 2020; Accepted 5 July 2020
Available online 11 July 2020

For example, unforeseen errors and conflicts in the physical layer can cause software exceptions and crashes in the cyber layer, which can then propagate and affect other components of the physical layer.

The challenge of ensuring resilience in CPSs requires the effective planning and preparation of response mechanisms to disruption propagation. Proper preparation of response mechanisms is particularly important because of the involvement of advanced, flexible manufacturing equipment and complex machinery. The economic impacts of disruptions, both short-term and long-term, can be devastating (Nguyen and Nof, 2019). Disruptions of supply in supply networks can lead to downstream raw materials and intermediate components shortage, which in turn lead to disruptions of demand affecting upstream productions and revenues (Nguyen and Nof, 2018). Cyber-attacks on information networks and computer service networks can lead to short-term losses due to leaks and compromises of sensitive information as well as service denials, long-term equipment damage, loss of customer's trust, and loss of strategic advantages (Zhong and Nof, 2015, 2020). The planning of response to disruption propagation is also challenged by the size and complexity of the CPSs and complex networks involved, requiring cyber-augmented planning and management to effectively coordinate response activities (Snediker et al., 2008).

To ensure the resilience of CPSs, appropriate preparation of disruption response resources is necessary. The presence of response can not only remove the disruptions, but also prevent the potential propagation that would have occurred (Nguyen and Nof, 2019). For example, eliminating a supply disruption at a supply network's node (firm/company) not only benefits the concerned node, but also prevents the propagating/cascading effects of the shortage to its successor nodes (customers). Timely response to disruptions is critical to ensure CPS resilience, because late and/or insufficient responses can allow disruptions to propagate beyond the capability of the response resources. However, timely disruption response is often difficult to achieve because the exact time and location of the disruption occurrences are usually not known to the response resources ahead of time. Therefore, appropriate strategic preparation and deployment of response resources are necessary to ensure the resilience of CPSs, and this challenge is addressed in this work.

1.2. The CRDP/SLOC model

In this work, the Collaborative Response to Disruption Propagation via the Strategic Lines of Collaboration (CRDP/SLOC) model, which is an original contribution, is introduced to illustrate the effects of strategic preparation of response resources against disruption propagation on a CPS. The CRDP/SLOC model expands upon the general framework CRDP of Nguyen and Nof (2019) by providing insights into the impacts of the strategic decisions of preparing response resources before disruptions occur. The second original contribution is the development of the Strategic Lines of Collaboration (SLOC) principle that guides the strategic preparation and allocation of disruption response resources. The SLOC principle specifies the network structure analysis of the CPS concerned, the incorporation of disruption propagation understanding into the analysis, and the evaluation of strategic compatibility of the possible teams of response agents. This work is the continuation of the CRDP work, and is inspired by the SmaRTA, Smart Response-Task Allocation project as well as the Dynamic Lines of Collaboration (DLOC) model (Zhong et al., 2014; Zhong and Nof, 2015, 2020; Zhong, 2016; Nguyen and Nof, 2018, 2019). The CRDP/SLOC model and its accompanying analytics and principles are designed to be general, and can be adapted for different specific applications and problems.

In CRDP/SLOC, the CPS, referred to as the client network, is represented as a network of directed and weighted edges, with the nodes representing the components and subsystems of the CPS and the edges representing the connections between the nodes and the potential disruption propagation directions. The nodes are subjected to initial disruptions. Any potential disruption propagation directions are modeled as directed and weighted edges between the nodes. This network modeling approach generalizes the disruptions and their propagation, allowing CRDP/SLOC to be applied to different CPS contexts and applications. A centrally controlled team of response agents collaborate to remove/repair the disruptions and to prevent immediate propagation of disruptions. The main modeling difference from the original CRDP model is that this team of response agents is selected from a collection of multiple different teams, each with different response agents that have different response capabilities.

The SLOC principle is then introduced to guide the team selection process, which is a strategic decision that cannot be altered once the disruptions occur. The structure of the client network is analyzed, and the knowledge of the disruption propagation mechanisms is incorporated into the SLOC analysis. Then, the strategic value of each node is computed, which provides information for the strategic compatibility evaluation of all response teams. Then, the most appropriate team(s) is selected to stand by against potential disruptions. To validate the CRDP/SLOC model and the SLOC principle, a set of experiments with three different random network models is performed. The experiments show that the application of the SLOC principle leads to better response performance of the selected agent team, which results in higher resilience of the CPS under disruption.

The remainder of the article is organized as follows: Section 2. Background with the literature review of related work and previous work; Section 3. Methodology and Theory of the CRDP/SLOC model, the network analysis, the disruption propagation analytics, and the Strategic Lines of Collaboration principle; Section 4. Experiments, Results, and Discussions with the set of experiments and results; Section 5. Conclusion and Discussion. The abbreviations are listed in Table 1.

2. Background

In this section, the relevant previous work is discussed. This review is not exhaustive and is intended to provide an overview of recent research surrounding response to disruption propagation in CPSs; disruption response mechanisms; disruption response strategies, analytics, and protocols.

Cyber-physical systems (CPSs) typically consist of multiple subsystems and components, both physical and cyber. Due to the complex relationship and interconnection between the subsystems, CPSs can be modeled as complex networks, with the subsystems and components represented as nodes, and their connections/relationships represented as edges. In production networks or supply networks, nodes can represent companies, factories, and facilities, and edges can represent demand/supply relationship. In information networks and computer networks, nodes can represent servers, computers, clients, and users, and edges can represent connections and information exchanges. In manufacturing networks, nodes can represent machines and departments, and edges can represent flows of raw materials, intermediate products, final products, and information. Within the context of CPSs and networks, Nguyen and Nof (2019) define disruptions as "Any unexpected, and often negative, changes to any entity in the network, including but not limited to: the nodes, the attributes of the nodes, the edges, and the attribute of the edges". It is noted that the specific nature

Table 1
Abbreviations.

CMN	Cyber-augmented Manufacturing Networks
CPS	Cyber-physical system
CRDP	Collaborative Response of Disruption Propagation
DLOC	Dynamic Lines of Collaboration
FCFS	First-come-first-serve
MATW	Minimizing additional task workload
MNDP	Minimizing neighboring disruption propagation
SLOC	Strategic Lines of Collaboration
SPT	Shortest processing time

and mechanisms of the disruptions are highly dependent on the CPS of interest and the modeling decisions of the concerned researchers.

One type of CPS disruption is the removal of nodes and/or edges from the network (Barabasi and Albert, 1999; Albert et al., 2000; Shen et al., 2012; Shen, 2013; Wang et al., 2017). The node/edge removal disruptions are highly related to graph theory and network theory and the concepts of node degree and degree distribution. A class of complex network, the scale-free network, is observed to be highly resistant against this type of disruption (Albert et al., 2000), yet less resistant to disruptions that propagate through the network due to the lower characteristic path length. Several algorithms and allocation protocols are developed to select node/edge removal disruptions to optimize certain objectives, such as maximizing the number of graph components and minimizing the largest component size (Shen et al., 2012; Shen, 2013).

An important type of disruption focuses on a pre-defined set of attributes of the nodes and edges of the CPS. This set of attributes can be freely designed, which enables researchers to model the actual CPSs and their mechanisms accurately. In production networks and supply networks, node attributes can reflect a node's production capability and inventory level, while edge attributes can reflect the demand/supply statuses between nodes. One type of disruption reduces the production capability of the nodes, affecting succeeding nodes, and these disruptions are propagated through the network if not properly contained (Reyes Levalle and Nof, 2015b; 2015a, 2017; Reyes Levalle, 2018). Such disruptions reduce the production capability of succeeding nodes, requiring these nodes to have contingent supply/inventory, affecting the nodes downstream (Seok et al., 2016). In road/traffic networks, disruptions are concerned with the attribute traffic density (Zhang, Gier, & Garoni, 2014). An important type of disruption is concerned with the attribute failure status of the CPS's nodes and edges (Zhong et al., 2014; Zhong & Nof, 2015, 2020; Zhong, 2016), which targets both nodes and edges, then propagates to neighboring nodes and edges, and this propagation cycle continues.

Various research also investigates different disruption propagation mechanisms. For example, the load-based mechanism (Motter and Lai, 2002) involves disruptions that reduce the load of the neighboring nodes, and nodes with insufficient load are removed from the network, the cycle repeats itself to the point of equilibrium (Yin et al., 2016). The load-based disruption can be generalized using pre-defined relationships and functions for individual nodes (Guariniello and DeLaurentis, 2017). Other research investigating disruption propagation includes the works of Crucitti et al. (2004); Buzna et al. (2007); Swift (2008); Buldyrev et al. (2010); Chaoqi et al. (2017a, 2017b); and Chaoqi et al. (2018). It is observed that the mechanisms of disruption propagation are specific to the applications and problems of concern to the researchers. In undirected networks, disruptions generally propagate through the neighboring connections of the nodes, whereas in directed networks, disruptions generally propagate downstream through the directions of the edges.

To prevent, eliminate, and/or reduce disruptions, response mechanisms are often deployed. The response activities are often controlled and coordinated by response strategies and protocols. One response strategy is concerned with gradually increasing the response resource allocation in accordance with the disruption status of the nodes (Buzna et al., 2007). Against load-based disruption, a response strategy involving balancing energy loads of nodes is developed (Chaoqi et al. (2017a, 2017b; Chaoqi et al., 2018). Both centralized and decentralized algorithms have been investigated and compared in preventing errors and conflicts (Chen and Nof, 2012; Landry et al., 2013). In supply networks, response mechanisms can include both agent-based and semi-centralized decision making to re-route supply/demand (Reyes Levalle and Nof, 2015b; 2015a, 2017; Reyes Levalle, 2018). One response mechanism involves agents traveling to the nodes to perform the repair operations (Zhong et al., 2014; Zhong and Nof, 2015; Zhong, 2016), and the agents are supported by the centrality-based allocation strategy and advanced online scheduling protocols.

The CRDP/SLOC model is an extension of the CRDP model developed by Nguyen and Nof (2019) and is related to the Cyber-augmented Manufacturing Networks (CMN) (Nguyen and Nof, 2018). Both CRDP and CRDP/SLOC are also related to the Dynamic Lines of Collaboration (DLOC) principle developed by Zhong and Nof (2015) and the Emergent Lines of Collaboration and Command (ELOCC) principle developed by Velasquez et al. (2010). Both CRDP and DLOC specifically address the challenge of coordinating response activities to tackle disruption propagation, whereas ELOCC addresses the coordination of collaboration during emergencies. In the DLOC research, the CPSs concerned are modeled as unweighted and undirected networks, with the response agents traveling to repair disrupted nodes. The DLOC response strategies include centrality-based depot allocation protocol, activity-based online scheduling protocol, and auxiliary lines edge rewiring protocol. In the CMN work (see Table 2) the CPSs concerned are modeled as weighted and directed manufacturing networks, and the response strategies include employing network analytics, disruption analytics, and flow analytics to support response decisions. In the CRDP work, the CPSs concerned are modeled as weighted and directed networks, with response agents having the capability to remove disruptions, as well as preventing immediate disruption propagation. The CRDP's main contribution was the analysis of the response-disruption interaction, and the CRPD response strategy emphasizes this interaction to enhance the response activities. All the aforementioned work provides a concrete foundation and important research directions for the development of CRDP/SLOC. The summary and comparison of the related preceding work are provided in Table 2.

From the literature survey, there is limited investigation on the interaction effect between the CPS and the response mechanisms. Based on the CRPD framework, this interaction effect belongs to the category of client-response interaction, which governs the important relationships between the CPS and the response mechanisms. It is observed that both CRDP and DLOC focus more on the dynamic aspect, i.e., the online scheduling protocol of the response activities, and do not discuss the strategic aspect of preparation and configuration of the response mechanisms to tackle disruption propagation. This knowledge gap is addressed by the CRDP/SLOC model and the accompanying SLOC principle, which are discussed in the next section.

Table 2
Summary and comparison of preceding work of CRDP/SLOC.

Model	CPS type	Dynamic response strategy/protocol	Strategic response strategy/protocol
DLOC[a]	Unweighted, undirected network Application: General complex network	Online scheduling protocol: Nearest neighbor	Limited: Centrality-based depot allocation
DLOC[b]		Online scheduling protocol: activity-based; Edge rewiring: Auxiliary links	
CMN[c]	Weighted, directed network Applications: Manufacturing/production/supply network	Online scheduling protocol: Based on analytics	Very limited: Offline analytics of network, disruption, flow
CRDP[d]	Weighted, directed network Application: General complex network	Online scheduling protocol: minimizing neighboring disruption propagation, minimizing additional task workload	None
CRDP/SLOC [this work]			Significantly expanded: Network analysis, disruption propagation analytics, SLOC

[a] (Zhong and Nof, 2015).
[b] (Zhong, 2016).
[c] (Nguyen and Nof, 2018).
[d] (Nguyen and Nof, 2019).

3. Methodology and Theory

3.1. The CRDP/SLOC model – framework and formulation

In this section, the CRDP/SLOC model is presented (Fig. 1). The 3 main components of CRDP/SLOC are defined based on the CRDP general framework: D1 – the client network; D2 – the response teams; and D3 – the disruption propagation. In addition, the SLOC principle is developed to guide the strategic selection and preparation of the response teams. Component D1, the client network, represents the CPS concerned. Within the scope of this work, the client network is a network of unweighted nodes with directed and weighted edges. The nodes represent the subsystems of the CPS, which are subjected to disruptions represented by 0 and 1 binary values. Any possible disruption propagation directions between nodes are modeled as directed edges. Component D2, the set of response teams, consists of response teams that can be deployed to tackle the disruptions and their propagations. For each disruption scenario, one response team can be selected and deployed to tackle the disruptions and their propagation. Component D3 consists of the disruptions, which occur initially, target the nodes, and propagate throughout the client network through the directions of edges. Within the scope of the CRDP/SLOC model, the disruptions are assumed to occur initially, only in nodes, and can propagate within the client network through the directions and weights of the edges. Should edge disruption modeling be required, the CRDP/SLOC model can be applied by converting the edges to new nodes that reflect the relevant attributes of the original edges, as necessary. Then new edges can be created to reflect the relationship between the original nodes and original edges (Nguyen and Nof, 2019).

The edges of the triangle represent the interaction between the main components: E12 – the client-response interaction; E13 – the client-disruption interaction; and E23 – the response-disruption interaction. Based on the CRDP framework, this work defines the interaction as follows. Edge E12 represents the interaction between the client network and the response team, which specifies that each response team consists of a number of response agents, and each response agent can repair a disrupted node. Edge E13 represents the interaction between the client network and the disruption propagation: Disruptions propagate through the directions and the weights of the edges of the client network. Edge E23 represents the interaction between response teams and the disruptions, in that the effect of response removes the disruption and prevents ongoing disruption propagation; which limits the disruption propagation.

The main difference between the CRDP/SLOC model and the original CRDP model is in addressing the problem of selecting and preparing a response team (out of a set of response teams) to tackle the given disruptions. Each response team has a different capability, and its performance is not known unless the computationally expensive simulation is performed. Thus, the Strategic Lines of Collaboration (SLOC) principle, discussed in detail in the subsection below, is developed to guide this selection and preparation process. Following the SLOC principle, the structure of the client network is analyzed, and the knowledge of the disruption propagation mechanisms is incorporated into the analysis. This analysis is extended to compute the strategic value of each node is computed, and each team's strategic compatibility is computed. Then, the most appropriate team(s) is selected to standby for response against

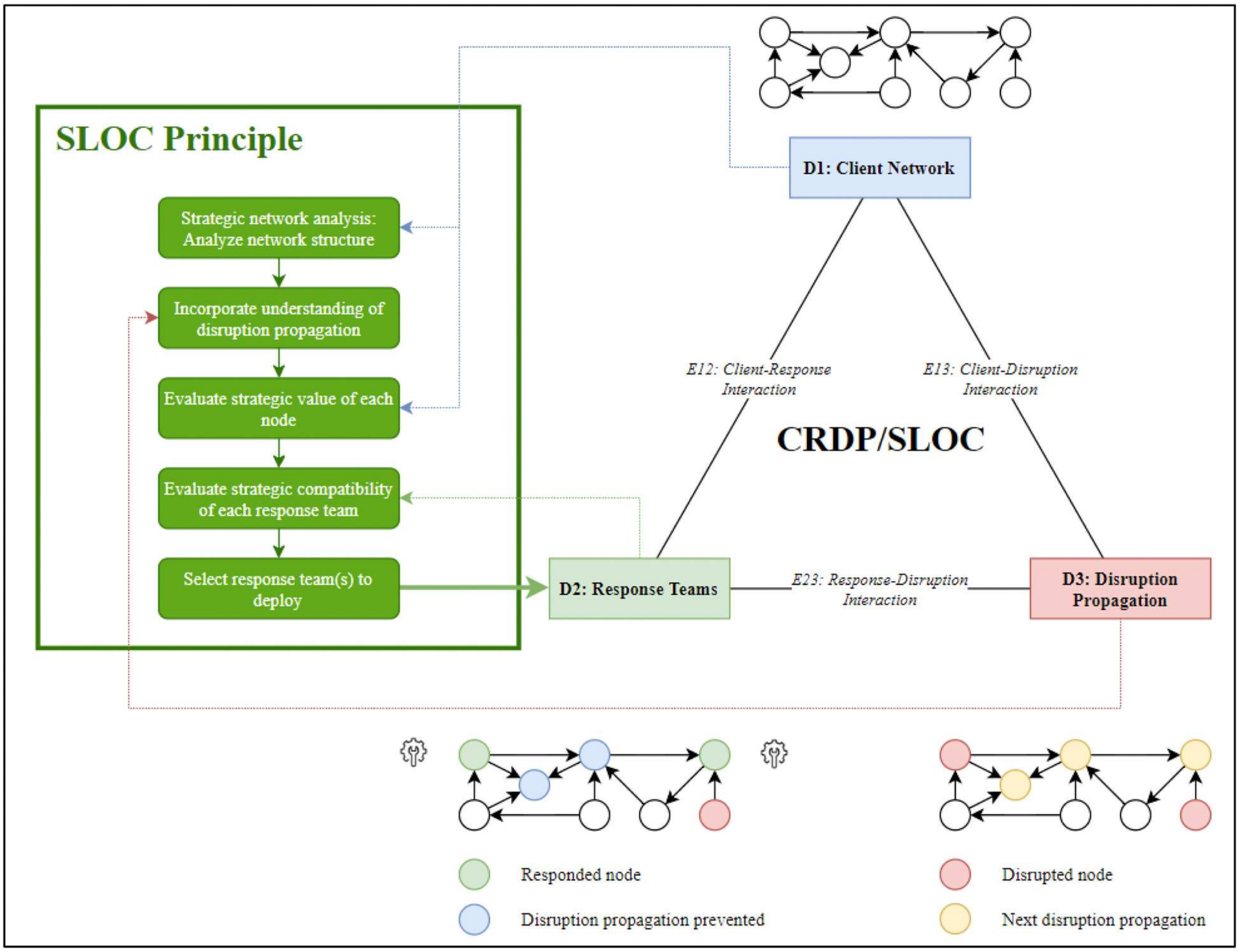

SLOC Principle
Strategic network analysis: Analyze network structure
Incorporate understanding of disruption propagation
Evaluate strategic value of each node
Evaluate strategic compatibility of each response team
Select response team(s) to deploy
D1: Client Network
D2: Response Teams
D3: Disruption Propagation
E12: Client-Response Interaction
E13: Client-Disruption Interaction
E23: Response-Disruption Interaction
CRDP/SLOC
Responded node
Disruption propagation prevented
Disrupted node
Next disruption propagation

Fig. 1. The CRDP/SLOC model.

potential disruptions.

The summary of the CRDP/SLOC model, per the CRDP framework, is provided next in Table 3.

The SLOC principle, which is one original contribution of this work, is developed to analyze the CRDP/SLOC model and to guide the response team selection and preparation process. The first step is to analyze the client network's structure and calculate the distance matrix and the nodes' out-degrees (the total number of outgoing edges of each node). Then, the understanding of disruption propagation, based on E13, is utilized to analyze the disruption propagation patterns and behavior. This information is used to estimate the strategic values of each node. Even though the client network contains unweighted nodes, the nodes with more outgoing nodes (both at the local-level and network-level), if disrupted, are more likely to propagate disruptions. Using the strategic values of the nodes, each response team's strategic compatibility with the client network is calculated using their response requirement matrices as specified by E12. Finally, a response team is selected to respond to the disruptions. The details of the SLOC principle are explained in subsection 3.2.

The CRDP/SLOC model is simulated through the use of C# and a discrete-event simulation programming, which culminates in the Teamwork Integration Evaluator/Collaborative Response to Disruption Propagation/Strategic Lines of Collaboration (TIE/CRDP/SLOC) software. The terms and their attributes are defined in Table 4.

The entities and attributes provided in Table 4 are necessary to satisfy the CRDP/SLOC model requirements as introduced in Table 3. The entities of interest in the system include the nodes, edges, response teams, response agents, and disruptions. The attributes are characteristics of the entities. The entities and attributes are either input entities, input attributes, dynamic attributes, or derived attributes. The input entities and input attributes are given by the user or the case study and remain unchanged throughout the simulation. The derived attributes are derived from the input entities and input attributes, and also remain unchanged throughout the simulation. The main difference between the CRDP/SLOC modeling and the CRDP modeling is the addition of the set of response teams TL, and the adjustment of the dynamic variables $NOS(n,t)$, $NAA(n,t)$, $NFCFS(n,t)$, $EDPS(e,t)$, and $ABS(a,t)$. The addition of TL allows CRDP/SLOC to model the impact of choosing different response teams on the resilience of the CPS. The adjustment of the dynamic variables also enables the analysis of the SLOC principle. The other items of the CRPD/SLOC modeling, including the discrete events, simulation logic, and performance metrics, follow the original CRDP modeling (Nguyen and Nof, 2019), with the adjustment of the dynamic variables taken into account. Readers are referred to Nguyen and Nof (2019) for further elaboration and details. The important performance metrics of CRDP/SLOC are listed in Table 5 for reference.

The next subsection discusses the SLOC principle, which analyzes the CRDP/SLOC model and guides the selection of the response team.

Table 3
Summary of the CRDP/SLOC model.

Aspect	Features	Details
CRDP/SLOC components	D1 – Client network	The CPS represented as a network of unweighted nodes with directed and weighted edges.
	D2 – Response teams	The set of response teams, in which one team is selected to respond to the disruptions. Each response team consists of response agents that can be assigned to repair disrupted nodes.
	D3 – Disruption propagation	Initial disruptions that target nodes and propagate through the edges.
CRDP/SLOC interactions	E12 – Client-response interaction	Each response agent can have a different response time for different nodes of the client network. This information is presented by a response requirement matrix.
	E13 – Client-disruption interaction	Disruptions can propagate through the directions and weights of the edges of the client network.
	E23 – Response-disruption interaction	The existence of response activities removes and prevents the effects of disruptions and disruption propagation.
Comparison to the original CRDP model	The response team selection problem	For a simulation instance, a single response team is selected (from the set of response teams) to respond to the disruptions.
	SLOC – client network analysis	The network structure of the client network is analyzed and node-level analytics are computed.
	SLOC – disruption propagation analysis	The disruption propagation analysis is performed to provide information on the disruption propagation pattern.
	SLOC – client network strategic analysis	Using the information from the client network analysis and disruption propagation analysis, each node's strategic value is computed.
	SLOC – response team strategic compatibility analysis	Then, each response team's strategic compatibility is evaluated.

3.2. The Strategic Lines of Collaboration (SLOC) principle

The SLOC principle is a collaborative control principle that addresses the strategic selection and preparation of a team of agents for the CRDP model. The SLOC principle consists of five steps. The first step involves the structure analysis of the client network. The second step incorporates the knowledge regarding the disruption propagation mechanisms into the network structure analysis. The third step utilizes the analytics created from the second step to evaluate the strategic value of each node. The fourth step then extends the analysis to evaluate the strategic compatibility of each response team. The fifth step then selects the most appropriate response team to be on standby to respond against disruptions.

The first step of the SLOC principle involves the analysis of the client network, which is presented as follows.

A node n's set of incoming/preceding neighboring nodes $NINL(n) \subset NL$ is formally defined as

$$NINL(n) = \{n_i \neq n \in NL : \exists e = (n_i, n) \in EL\} \tag{1}$$

A node n's set of outgoing/preceding neighboring nodes $NONL(n) \subset NL$ is formally defined as

$$NONL(n) = \left\{n_j \neq n \in NL : \exists e = \left(n, n_j\right) \in EL\right\} \tag{2}$$

A node n's set of incoming/preceding edges $NIEL(n) \subset EL$ is formally defined as

$$NIEL(n) = \left\{e = \left(n_i, n_j\right) \in EL : n_j \equiv n\right\} \tag{3}$$

A node n's set of outgoing/succeeding edges $NOEL(n) \subset EL$ is formally defined as

$$NOEL(n) = \left\{e = \left(n_i, n_j\right) \in EL : n_i \equiv n\right\} \tag{4}$$

Suppose a $CN = (NL, EL)$ is given with all determined values for all $EDPT(e)$, and a node n_d is selected as the only node disrupted initially, meaning at $t = 0, NOS(n_d, 0) = 0$ and $NOS(n, 0) = 1, \forall n \in NL - \{n_d\}$, with no response agents available, meaning $AL = \varnothing$. It is observed that

$$NOS\left(n_j, EDPT(e)\right) = 0, \forall e = \left(n_i, n_j\right) \in NOEL(n_d) \tag{5}$$

Table 4
Entities and basic attributes of the CRDP/SLOC model.

Type	Entity/Attribute and Explanation	Corresponds to
The following entities are defined for the CRDP/SLOC model		
Input	$CRDP/SLOC = (CN, TL, DNL)$	CRDP model
Input	$CN = (NL, EL)$ The client network, subjected to disruptions.	D1
Input	$NL = \{n_0, n_1, n_2 \ldots\}$ The set of nodes in the client network.	D1
Input	$EL = \{e_0, e_1, e_2 \ldots\}$ The set of weighted and directed edges, which represent the directions and time taken for disruptions to propagate from one node to other nodes connected to it.	D1
Input	$TL = \{(AL_0, RRM_0), (AL_1, RRM_1), \ldots\}$ The set of response agent teams with the corresponding response requirement matrices. For each experiment replication, only one team to standby for response. Each team has a response requirement matrix towards the client network. For example, AL_0 follows RRM_0, and AL_1 follows RRM_1.	D2
Input	$AL = \{a_0, a_1, a_2 \ldots\}$ The team of weighted response agents, which is responsible for responding to disruptions. For a simulation instance, a team *AL*is selected from the set *TL* to respond to the disruptions, and its agents are deployed to tackle the disruptions and their propagation.	D2
Input	$RRM = (r_{i,j}) \in \mathbb{R}_{>0}^{\lvert AL \rvert \times \lvert NL \rvert}$ The response requirement matrix, whose rows correspond to the agents in *AL*, and columns correspond to the nodes in *NL*. $r_{i,j}$ indicates the time taken for agent *i*to respond to a disruption affecting node *j*.	E12
Input	$DNL \subset NL$ The set of nodes subjected to initial disruptions.	D3
The following attributes are defined for each node $n \in NL$		
Dynamic	$NOS(n, t) \in \{0, 1\}$ The operational status of node *n* at time *t*. $NOS(n, t) = 1$ means the node is not disrupted at time *t*. $NOS(n, t) = 0$ means the node is disrupted at time *t* and can propagate disruptions to its successor nodes.	E13
Dynamic	$NAA(n, t) \in AL$ Node *n*'s currently assigned response agent for responding to its disruption at time *t*.	E23
Dynamic	$NFCFS(n, t) \in \mathbb{R}_{\geq 0}$ Node *n*'s last disrupted time, at time *t*, which is used in the first-come-first-serve scheduling protocol.	E13
The following attributes are defined for each edge $e = (n_i, n_j) \in EL$		
Input	$EDPT(e) \in \mathbb{R}_{>0}$ Edge *e*'s disruption propagation time, which is equivalent to edge *e*'s weight. Suppose node n_i is disrupted at time *t*, then at time $t + EDPT(e)$, node n_j will become disrupted if both node n_i and node n_j have not been responded to by an agent. If $EDPT(e) = 0$, both n_i and n_j can be treated as the same node, and their response requirement in *RRM*should be updated accordingly.	E13
Dynamic	$EDPS(e, t) \in \{0, 1\}$ Edge *e*'s disruption propagation status at time *t*, mainly used for simulation of disruption propagation. $EDPS(e, t) = 1$ means the disruption propagation along edge *e* will occur as planned. $EDPS(e, t) = 0$ means the disruption propagation is halted, due to the intervention of an agent.	E13
The following attributes are defined for each agent $a \in AL$:		
Dynamic	$ABS(a, t) \in \{0, 1\}$ Agent's busy status at time *t*. $ABS(a, t) = 0$ means the agent is idle, and $ABS(a, t) = 1$ means the agent is busy (currently responding to a disruption).	D2
Simulation-specific parameters are defined for the CRDP model:		
Dynamic	*t*The current time of the simulation.	Simulation
Dynamic	t_{last}A variable mainly used for recording performance metrics.	Simulation
Input	*simLen*Simulation length. Once $t = simLen$ or $\sum_n^{NL} NOS(n) = \lvert NL \rvert$, the simulation ends.	Simulation
Input	*selPro*Selected protocol for the replication.	E23

Table 5
The CRDP/SLOC performance metrics.

System performance metric	Explanation
rF	For each experiment, *rF*, the recovery fraction, is defined as the fraction of the replications where the system fully recovers from the disruption propagation. Higher values of *rF*are preferred.
rT	For each replication, *rT*, the recovery time, is defined as the time taken for the agent network to fully recover the client network. When all nodes are at full operational status, disruptions are non-existent and no longer occur, and the simulation ends. Lower values of *rT*are preferred. $if(NOS(n, t) = 1 \forall n \in NL)\ rT \leftarrow t, else\ rT \leftarrow simLen$
tPL	For each replication, *tPL*, the total performance loss, is defined as the over-time average fraction of nodes that are disrupted. Lower values of *tPL* are preferred. $tPL = \frac{\int_{t=0}^{simLen} pL(t) dt}{simLen}$ $pL(t) = \sum_n^{NL} \frac{1 - NOS(n, t)}{\lvert NL \rvert} at\ t$
mDPF	For each replication, *mDPF*, the maximum disruption propagation fraction, is defined as the largest fraction of the client network that was ever disrupted. Lower values of *mDPF*are preferred. $mDPF = \max_t pL(t)$

This property is true because the disrupted node n_d is the only cause of disruption. It is noted that, however, certain nodes $n_j \in NONL(n_d)$ may be disrupted earlier than the expected value of $EDPT(e)$ if a shorter disruption propagation path exists from n_d to that node n_j.

The second step of the SLOC principle incorporates the knowledge regarding the disruption propagation mechanisms to the network structure analysis. Based on this step, the neighboring disruption analytic $NNDA(n) \in \mathbb{R}$ is defined as

$$NNDA(n) = \sum_{n_j}^{NONL(n)} 1 \Big/ \min_{e=(n,n_j)} \{EDPT(e)\} \tag{6}$$

The $NNDA(n)$ analytic provides information regarding the local-level impact of a disruption affecting node *n*. The value of $NNDA(n)$ increases with a higher number of outgoing edges, or $\lvert NOEL \rvert$, and with lower weight for each edge $e \in NOEL(e)$. The formula also addresses the case where multiple edges exist from *n* to n_j, and $NNDA(n)$ only considers the shortest edge. Compared to network-level analytics, $NNDA(n)$ is more limited in terms of information provided, but requires less computational power to calculate, which is complexity $O(\lvert EL \rvert)$.

An analytic more advanced than $NNDA(n)$ would consider the network-level aspect of disruption propagation. Based on the observation that disruptions propagate from one node n_i(if n_i is the only disrupted node initially) to another node n_j through the shortest path from n_i to n_j; the shortest-path matrix $SPM = (d_{i,j}) \in \mathbb{R}_{\geq 0}^{\lvert NL \rvert \times \lvert NL \rvert}$ can be computed to assist with the calculation of network-level analytics. The matrix *SPM* can be computed efficiently using the Floyd-Warshall algorithm (Floyd, 1962) with complexity $O(\lvert NL \rvert^3)$. Each entry is defined as $SPD(n_i, n_j) \equiv d_{i,j} \in \mathbb{R}_{\geq 0}$ representing the shortest-path distance from node n_i to node n_j, with the edge directions applied and edge weights represented by $EDPT(e)$. If no such path exists, $SPD(n_i, n_j) = null$, and $1/SPD(n_i, n_j) = 0$. Using the shortest-path distance matrix, the harmonic centrality analytic $NHCA(n) \in \mathbb{R}$ is defined as

$$NHCA(n) = \sum_{n_j \neq n}^{NL} 1 \Big/ SPD(n, n_j) \tag{7}$$

The $NHCA(n)$ analytic provides information regarding the network-level impact of a disruption affecting node *n*. The value of $NHCA(n)$ increases if node *n* is closer to more nodes. The formula of $NHCA(n)$ also addresses the case where multiple edges exist between one pair of nodes, in that only the shortest path is considered in the calculation. Compared to the local-level analytic *NNDA*(n), *NHCA*(n) provides more information regarding disruption propagation risk, but requires more computational power to calculate.

The main limitation of both *NNDA*(n) and *NHCA*(n) is that their disruption propagation analyses do not consider the performance metrics used to evaluate a problem instance. While *NHCA*(n) can provide a relative ranking between nodes, the proportional differences in values of *NHCA*(n) between nodes may not reflect the actual differences with respect to the performance metrics ***tPL*** and ***mDPF***. To address these limitations, the second step of the SLOC principle is to incorporate the network-level understanding of disruption propagation.

To address the total performance loss metric ***tPL***, the rate of disruption propagation analytic *NRDPA*$(n) \in \mathbb{R}$ is defined as

$$NRDPA(n) = \frac{\int_{t=0}^{t=\max\limits_{n_i,n_j\in NL} SPD(n_i,n_j)} \left|\left\{n_j \in NL : SPD(n,n_j) \leq t\right\}\right| dt}{\max\limits_{n_i,n_j\in NL} SPD(n_i,n_j)} \tag{8}$$

The analytic *NRDPA*(n) aggregates the rate of increasing total performance loss of the CPS if node n is the sole initially disrupted node with no response agents present. To address the maximum disruption propagation fraction metric ***mDPF***, the maximum disruption propagation analytic *NMDPA*$(n) \in \mathbb{R}$ is defined as

$$NMDPA(n) = \frac{\left|\left\{n_j \in NL : SPD(n,n_j) \neq null\right\}\right|}{\max\limits_{n_i,n_j\in NL} SPD(n_i,n_j)} \tag{9}$$

The analytic *NMDPA*(n) considers the maximum damage a disruption affecting node n can cause. Both *NRDPA*(n) and *NMDPA*(n) overcome the limitation of *NHCA*(n) that tends to give a higher weight to nearby nodes n_j with extremely close proximity to n due to $1/\ SPD(n,n_j)$ formula. A simple 3-node example is provided in Fig. 2.

The third step of the SLOC principle computes the strategic values for each node. A node n's strategic value $NSV(n) \in \mathbb{R}$ is selected from $NNDA(n), NHCA(n), NRDPA(n), NMDPA(n)$ or a function combining these four indices. This decision is left open to individual cases and scenarios, depending on the available information and computational resources.

The fourth step of the SLOC principle evaluates the strategic compatibility of each agent team. A team of agents is defined as $AL = \{a_0, a_1, \dots\}$ with each agent a_i capable of responding to a disruption affecting node n_j after a period of time $RRM(i,j)$, which considers two integer arguments. An alternative notation for $RRM(i,j)$ is $RRM(a_i, n_j)$.

An agent a's estimated effectiveness index $AEI(a)$ towards the client network is defined as

$$AEI(a) = \sum_{n}^{NL} \frac{NSV(n)}{RRM(a,n)^* \sum_{n_o}^{NL} NSV(n_o)} \tag{10}$$

Aggregating all agents of a team, the team AL's strategic compatibility index $TSCI(AL) \in \mathbb{R}$ is defined as

$$TSCI(AL) = \sum_{a}^{AL} \frac{AEI(a)}{|AL|} = \sum_{a}^{AL}\sum_{n}^{NL} \frac{NSV(n)}{|AL|^* RRM(a,n)^* \sum_{n_o}^{NL} NSV(n_o)} \tag{11}$$

The index $TSCI(AL)$ estimates the total effectiveness of a particular team of response agents, given a certain selected method of deciding $NII(n)$, the team's RRM, and the client network NL.

The final step of the SLOC principle is to select the appropriate response team AL or a limited set of AL, based on the evaluation of $TSCI(AL)$. Higher values of $TSCI(AL)$ would indicate higher strategic compatibility.

4. Experiments, results, and discussions

In this section, experiments are conducted to illustrate the different network analytics and response team preparation protocols with respect to three types of random network models: Barabasi-Albert (Albert and Barabasi, 2002), Erdos-Renyi (Erdös and Rényi, 1959), and Watts-Strogatz (Watts, 2002). The details of the experiments are as follows (Table 6).

The three random network models above are used for the client network, with 100 replications each, each created with 100 nodes and 200 edges. A detailed comparison of the three random network models can be found in the work of Albert and Barabasi (2002). These three random network models can approximate current and emerging CPSs and complex systems with certain accuracies (Chen and Nof, 2012; Zhong and Nof, 2015), and are therefore appropriate network models for these numerical experiments. The Barabasi-Albert networks are created with 2 initial nodes, and the growth rate of 2 edges per new node, until 200 edges are reached. The Erdos-Renyi networks are created with the same number of nodes and number of edges, and only fully connected

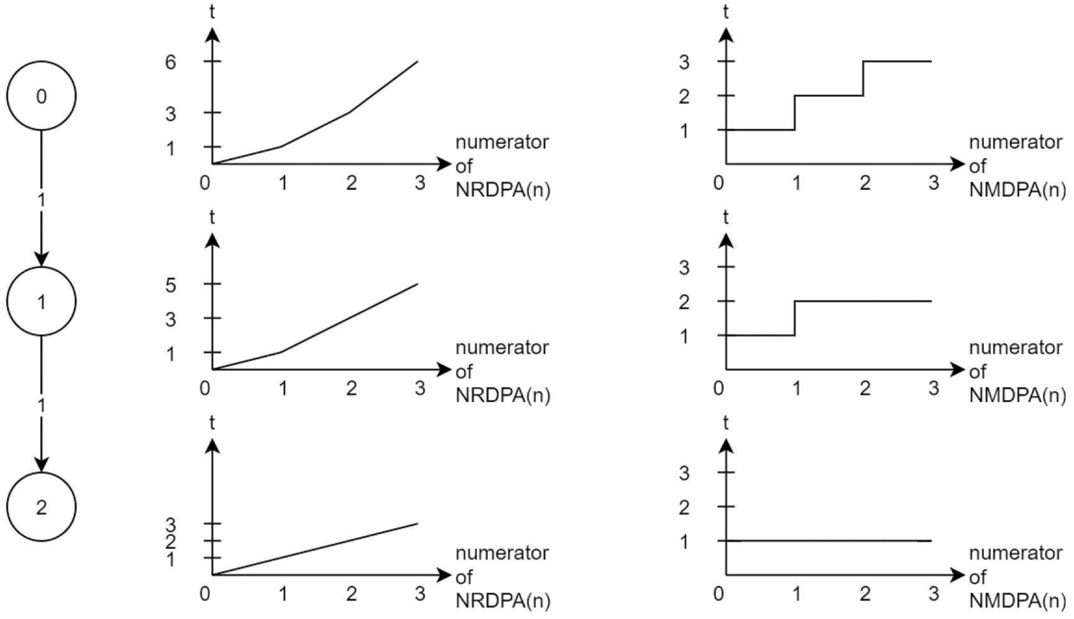


Fig. 2. Example of NRDPA(n) and NMDPA(n).

Table 6
Details of the experiments.

Factor	# variations	Details
Client network	3	Barabasi-Albert random network vs Erdos-Renyi random network vs Watts-Strogatz random network, all 100-node and 200-edge.
Agent network	4	Random team selection vs low strategic compatibility vs medium strategic compatibility vs high strategic compatibility
Disruption scenario	1	25 initial disruptions
Online response protocols	4	FCFS (baseline) vs SPT (baseline) vs MNDP vs MATW, based on (Nguyen and Nof, 2019)

networks are selected. The Watts-Strogatz networks are created with mean degree 4, and rewiring probability of 0.5. Because the three random network models used are undirected and unweighted networks, adjustments are required to match the requirements of the CRDP model. For each undirected and unweighted edge, there is a 2/3 probability for an edge to be unidirectional, and 1/3 probability for an edge to be converted to two directed edges of opposite directions. Each directed edge e receives a weight $EDPT(e)$ ranging from 0.5 to 1.5, uniformly distributed. With respect to disruption propagation, 25 initial disruptions are selected randomly based on a uniform distribution. The parameters of 10 agents and 25 initial disruptions for the 100-node networks are selected based on previous work (Nguyen and Nof, 2019).

Four online response protocols for the agents are applied, based on (Nguyen and Nof, 2019): First-come-first-serve protocol, FCFS, prioritizing disruptions that occur earlier; Shortest processing time protocol, SPT, prioritizing disruptions that can be addressed quickly with a selected idle agent; Minimizing neighboring disruption propagation protocol, MNDP, prioritizing disruptions that can spread quickly to undisrupted nodes; Minimizing additional task workload, MATW, a generalization of the MNDP protocol in considering the propagation of the task workload.

With respect to the response teams, a pool of 1000 teams are created, each of 10 response agents. Each team receives an across-agent-variation index $AAVI(AL)$with random distribution $UNIF(0,1)$, which determines the degree of variation between agents. Additionally, each agent receives an across-node-variation index $ANVI(a)$ with random distribution $UNIF(0,1)*AAVI(AL)$, which determines the degree of variation in terms of response time for that agent to the different nodes. Then, for each agent, the unnormalized response time $URT(a,n)$ for each node (out of 100) is generated with random distribution $UNIF(1,1+ANVI(a))$. Then, the unnormalized response time is normalized so that the average response time across all nodes for each agent is equal to 1. This procedure results in the creation of diverse teams and uniform teams. The diverse teams have higher values of $AAVI(AL)$ and have more diverse agents, whereas the uniform teams have lower values of $AAVI(AL)$ and have more uniform agents. The more diverse agents have higher values of $ANVI(a)$ and tend to have a wider range of response times across all nodes, whereas the uniform agents have lower values of $ANVI(a)$ and tend to have similar values of response times. The variability resulting from $AAVI(AL)$ and $ANVI(a)$ affects the response requirement matrix RRM, which affects $AEI(a)$, and ultimately affects $TSCI(AL)$. All agents, however, are assumed to have an average response time of 1 across all nodes, thus, all teams are economically balanced, but are not necessarily equal in terms of strategic compatibility. Simulating the full CRDP model with 1000 provided teams would be computationally expensive. Therefore, the SLOC principle is applied to guide the team selection decision. The first four steps of the SLOC principle are applied, resulting in the $TSCI(AL)$ for the 1000 provided teams. For this set of experiments, four groups of $TSCI(AL)$ are selected: A high-compatibility group, which consists of the top 10 teams based on $TSCI(AL)$ ranking; a medium-compatibility group, which consists of the middle 10 teams; a low-compatibility group, which consists of the lowest 10 teams; and a random group of 10 teams (selected randomly, uniformly from the set of 1000 provided teams).

Four performance measures listed in Table 5 are used. The recovery fraction, *rF*, is the fraction of the experiment replication where the client network is fully recovered from the disruptions and is returned to normalcy. The recovery time, *rT*, represents the total time taken for the disruptions to be fully removed from the client network. If the client network fails to recover within the prescribed simulation time, a large penalty value of 50 is applied. Both *rF*and *rT* are important recovery resilience metrics that indicate the effectiveness of the response activities and team configuration decisions. The total performance loss, *tPL*, represents the total over-time loss of performance due to disruptions of the client network. The metric *tPL*is relevant when the CPS is required to continue functioning during disruptions. The maximum disruption propagation, *mDPF*, represents the highest performance loss that occurs during an experiment replication. This metric is relevant when long-term damages are expected from disruptions, even after the disruptions are removed. Examples include loss of sensitive information, unrecoverable damages, and wear and tear.

Comparisons between strategic compatibility levels are provided in Fig. 3 and Table 7.

The high strategic compatibility teams significantly outperform the other three team types: 12.7%–15.6% improved recovery fraction, 7.3%–8.5% reduced recovery time, 9.6%–12.4% reduced total performance loss, and 5.5%–8.8% reduced maximum disruption propagation. Overall, the high strategic compatibility teams are proven to provide the best performance with statistical significance, followed by either randomly selected teams or medium strategic compatibility teams, then by the low strategic compatibility teams. The next comparisons are between strategic compatibility levels and online response protocols (Fig. 4, and Table 8).

When FCFS protocol is employed, high strategic compatibility teams provide 0.6%–1.3% reduced total performance loss and 1.3%–3.7% reduced maximum disruption propagation. This result is explained by the very low effectiveness of FCFS protocol in preventing the propagation of disruptions. With SPT protocol, the usage of high strategic compatibility teams significantly improves the resilience of the client network: 161%–1540% increased recovery fraction, 13.4%–18.9% reduced recovery time, 18.2%–26.9% reduced performance loss, and 11.6%–18% reduced maximum disruption propagation. It can be concluded that the SPT protocol highly depends on the appropriate strategic preparation of agent teams. With MNDP protocol, usage of high strategic compatibility teams provides a statistically significant improvement in resilience: 6.8%–11.2% increased recovery fraction, 5.3%–10.5% reduced recovery time, 7.6%–12.2% reduced performance loss, and 4.6%–5.2% reduced maximum disruption propagation. With MATW protocol, the high strategic compatibility teams provide statistically significant better resilience: 3.6%–5.8% reduced recovery time, 6.5%–11.6% reduced total performance loss, and 2.1%–7.7% reduced maximum disruption propagation. The lower improvement from employing high compatibility teams can be partially explained by the high effectiveness of the online response protocol MATW.

The experiment results indicate that using high strategic compatibility teams provides superior performance relative to other team types, demonstrating the effectiveness of employing the SLOC principle in strategic preparation of agent teams. The higher performance is most notable with the use of SPT online response protocol, followed by MNDP, then by MATW. It is also noted that using medium strategic compatibility teams is at about the same level of performance as the randomly selected teams.

5. Conclusion and Discussion of applications

Disruption propagation prevention and control can have significant social and economic value in the design of CPS. In the context of

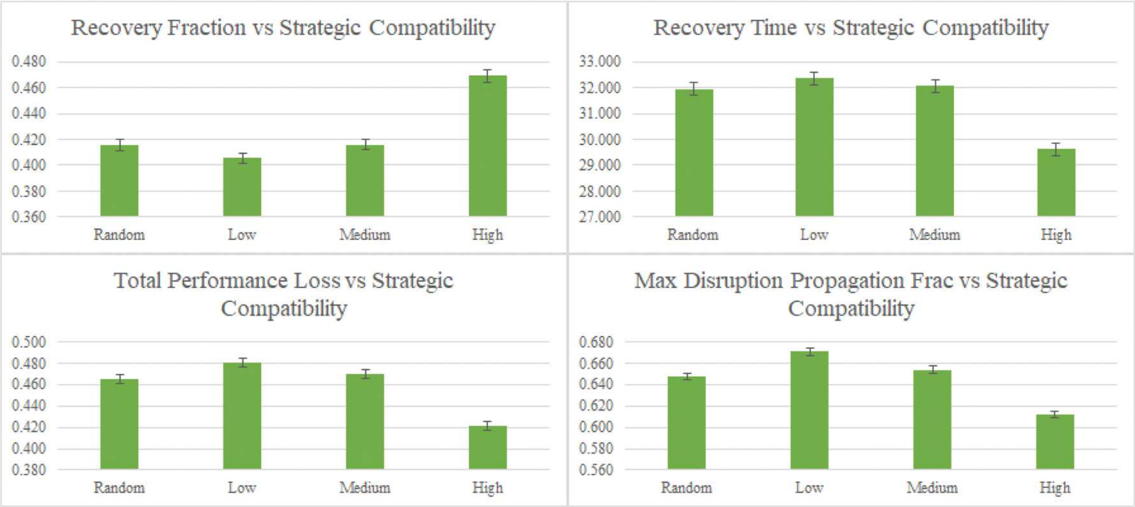


Fig. 3. Comparison chart of strategic compatibility levels (with 95% confidence intervals).

Table 7
Comparison table of strategic compatibility levels.

Strategic Compatibility	Recovery Fraction *rF*	Recovery Time *rT*	Total Performance Loss *tPL*	Maximum Disruption Propagation Fraction *mDPF*
Random	0.416	31.941	0.465*	0.647*
Low	0.405*	32.368	0.480	0.671*
Medium	0.416	32.055	0.469	0.654*
High	**0.469*** (+12.74%)	**29.628*** (−7.24%)	**0.421*** (−9.46%)	**0.612*** (−5.41%)

*: indicates statistical significance at.$\alpha = 0.05$
Best values of a metric are **bolded**, and compared with next best values.

Collaborative Control Theory, the Collaborative Response against Disruption Propagation/Strategic Lines of Collaboration (CRDP/SLOC) is introduced as an expansion of the CRDP framework, analyzing the effects of strategic preparation of teams of response agents against disruption propagation damaging a CPS. The new SLOC principle is developed and introduced as a general and adaptable collaborative control principle to design and select the appropriate strategic decisions in preparation against disruption propagation. The CRDP/SLOC model is validated using a set of experiments with three different random network models, four agent team selection protocols (with one protocol based on the SLOC principle), and four online response protocols. The developments of the CRDP/SLOC model and the SLOC principle for strategic selection of response agent teams are contributions to the research area of disruption propagation response in general, and in CPSs design in particular. The development of the CRDP/SLOC model demonstrates the generality of the CRDP framework to model collaboration response activities to tackle disruption propagation and furthering research in CPS resilience. Specifically, the SLOC principle addresses one important research direction of the CRDP model, the long-term value of strategic preparation and analytical decision-making. By applying complex network representation, the SLOC principle can be adapted to different types of CPSs and different disruption mechanisms, disruption propagation mechanisms, response mechanisms, and strategic preparation types. Practitioners, however, should employ robust validation in adapting the SLOC principle to significantly different cases.

From the results of this research, the following recommendations are made to managers, supervisors, and coordinators of CPSs and complex networks, e.g. production networks, supply networks, and information networks:

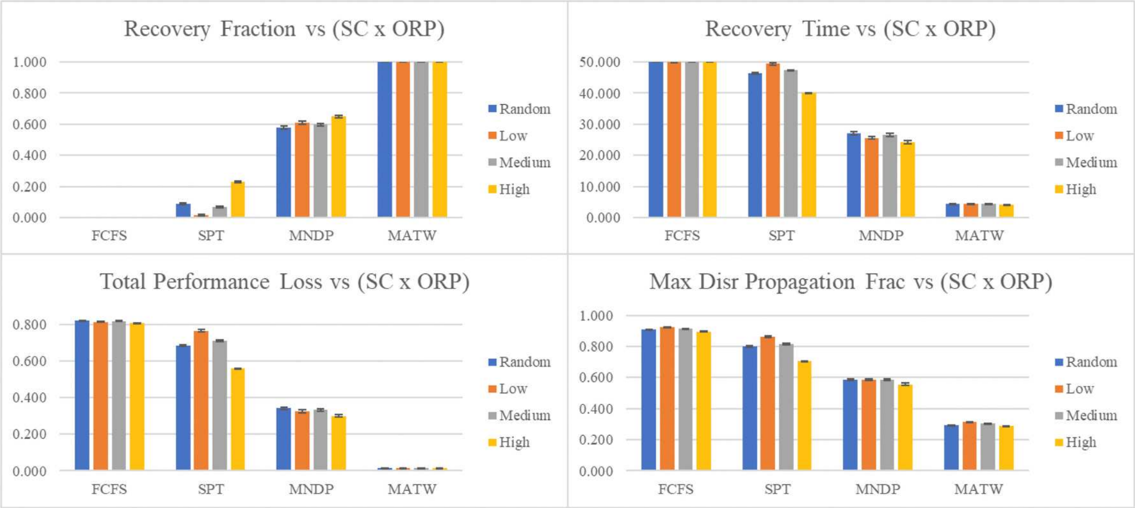


Fig. 4. Comparison chart of strategic compatibility levels and online response protocols (with 95% confidence intervals).

Table 8
Comparison table of strategic compatibility levels and online response protocols.

SC	RP	*rF*	*rT*	*tPL*	*mDPF*	*RP*	*rF*	*rT*	*tPL*	*mDPF*
Rand	FCFS	0.000	50.000	0.820	0.908*	MNDP	0.577*	27.121*	0.342	0.587
Low	FCFS	0.000	50.000	0.814*	0.924*	MNDP	0.608	25.636*	0.325	0.584
Med	FCFS	0.000	50.000	0.819	0.913*	MNDP	0.597	26.574*	0.332	0.584
High	FCFS	0.000	49.981	**0.809***	**0.895***	MNDP	**0.649***	**24.270***	**0.300***	**0.557***
				(−0.06%)	(−1.43%)		(+6.74%)	(−10.5%)	(−7.69%)	(−4.62%)
Rand	SPT	0.087*	46.33*	0.684*	0.799	MATW	1.000	4.306	0.015	0.295*
Low	SPT	0.014*	49.43*	0.765*	0.861*	MATW	1.000	4.408*	0.016	0.313*
Med	SPT	0.068*	47.31*	0.711*	0.815	MATW	1.000	4.335	0.016	0.304*
High	SPT	**0.227***	**40.11***	**0.559***	**0.706***	MATW	1.000	**4.152***	**0.014***	**0.289***
		(+161%)	(−13.4%)	(−18.3%)	(−11.6%)			(−3.58%)	(−6.65%)	(−2.03%)

* indicates statistical significance at.$\alpha = 0.05$
SC = strategic compatibility, RP = response protocol, Rand = random, Med = medium.
Best values of a metric of a category when comparing strategic compatibility are **bolded**, and compared with next best values.

(1) The CRDP framework is recommended for managers and supervisors. The framework can be applied to further develop their comprehensive understanding of disruptions, disruption propagation, and response to disruptions, and how these components interact with each other.
(2) Then, the SLOC principle can be applied to support the preparation of strategic resources against different disruption propagation scenarios. The strategic preparation should be accompanied by the use of advanced collaborative coordination protocols to coordinate response activities, in order to achieve better system resilience.

At this stage of research, the CRDP/SLOC model is limited in terms of disruption occurrence modeling and response activities modeling. Another limitation is the assumption of homogeneous node types and disruption types used in the network model. Although strategic compatibility with the client network has been discussed in this work, the synergy of the strategic decisions and the tactical (on-line) decisions has not been explored. Therefore, further research is recommended in the following directions:

(1) New collaboration mechanisms among response agents/teams in response to disruption propagation.
(2) Consideration of different node types and disruption types, and adapting the team preparation protocols and team coordination protocols accordingly.
(3) Generalization of collaborative control principles for disruption propagation response.
(4) The modeling of disruption detection activities, disruption prevention activities, in addition to repair.
(5) Development of advanced analysis and protocols to further support the team formation and reconfiguration decisions.
(6) Exploration and analysis of the synergy and counter-synergy between the strategic team preparation decisions and the tactical (on-line) response decisions.

Declaration of competing interest

None.

Acknowledgment

This research is supported in part by the PRISM Center for Production, Robotics, and Integration Software for Manufacturing & Management at Purdue University. This research is also supported by BARD project Grant# IS-4886-16 R, "Development of a Robotic Inspection System for Early Identification and Locating of Biotic and Abiotic Stresses in Greenhouse Crops" with Co-PIs A. Bechar (ARO, Israel); Y. Tao (UMD); and S.Y. Nof. This research is also a part of the National Science Foundation's Award 1839971 Future of Work at the Human-Technology Frontier program, Collaborative Research: Pre-Skilling Workers, Understanding Labor Force Implications and Designing Future Factory Human-Robot Workflows Using a Physical Simulation Platform.

References

Albert, R., Barabasi, A.L., 2002. Statistical mechanics of complex networks. Rev. Mod. Phys. 74 (1), 47–97. https://doi.org/10.1103/RevModPhys.74.47.

Albert, R., Jeong, H., Barabasi, A.L., 2000. Error and attack tolerance of complex networks. Nature 406 (6794), 378–382. https://doi.org/10.1038/35019019.

Barabasi, A.L., Albert, R., 1999. Emergence of scaling in random networks. Science 286 (5439), 509–512. https://doi.org/10.1126/science.286.5439.509.

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S., 2010. Catastrophic cascade of failures in interdependent networks. Nature 464 (7291), 1025–1028. https://doi.org/10.1038/nature08932.

Buzna, L., Peters, K., Ammoser, H., Kuhnert, C., Helbing, D., 2007. Efficient response to cascading disaster spreading. Phys. Rev. E - Stat. Nonlinear Soft Matter Phys. 75 (5 Pt 2), 056107 https://doi.org/10.1103/PhysRevE.75.056107.

Chaoqi, F., Ying, W., Kun, Z., Yangjun, G., 2018. Complex networks under dynamic repair model. Phys. Stat. Mech. Appl. 430, 323–330. https://doi.org/10.1016/j.physa.2017.08.071.

Chaoqi, F., Ying, W., Xiaoyang, W., 2017a. Research on complex networks' repairing characteristics due to cascading failure. Phys. Stat. Mech. Appl. 482, 317–324. https://doi.org/10.1016/j.physa.2017.04.086.

Chaoqi, F., Ying, W., Yangjun, G., Xiaoyang, W., 2017b. Complex networks repair strategies: dynamic models. Phys. Stat. Mech. Appl. 482, 401–406. https://doi.org/10.1016/j.physa.2017.04.118.

Chen, X.W., Nof, S.Y., 2012. Conflict and error prevention and detection in complex networks. Automatica 48 (5), 770–778. https://doi.org/10.1016/j.automatica.2012.02.030.

Crucitti, P., Latora, V., Marchiori, M., 2004. Model for cascading failures in complex networks. Phys. Rev. E - Stat. Nonlinear Soft Matter Phys. 69 (4 Pt 2), 045104 https://doi.org/10.1103/PhysRevE.69.045104.

Day, J.M., 2014. Fostering emergent resilience: the complex adaptive supply network of disaster relief. Int. J. Prod. Res. 52 (7), 1970–1988. https://doi.org/10.1080/00207543.2013.787496.

Erdös, P., Rényi, A., 1959. On random graphs, I. Publ. Math. 6, 290–297 doi:citeulike-article-id:4012374.

Floyd, R.W., 1962. Algorithm 97: shortest path. Commun. ACM 5 (6), 345. https://doi.org/10.1145/367766.368168.

Gong, J., Mitchell, J.E., Krishnamurthy, A., Wallace, W.A., 2014. An interdependent layered network model for a resilient supply chain. Omega 46, 104–116. https://doi.org/10.1016/j.omega.2013.08.002.

Guariniello, C., DeLaurentis, D., 2017. Supporting design via the system operational dependency analysis methodology. Res. Eng. Des. 28 (1), 53–69. https://doi.org/10.1007/s00163-016-0229-0.

Kim, Y., Chen, Y.-S., Linderman, K., 2015. Supply network disruption and resilience: a network structural perspective. J. Oper. Manag. 33–34, 43–59. https://doi.org/10.1016/j.jom.2014.10.006.

Landry, S.J., Chen, X.W., Nof, S.Y., 2013. A decision support methodology for dynamic taxiway and runway conflict prevention. Decis. Support Syst. 55 (1), 165–174. https://doi.org/10.1016/j.dss.2013.01.016.

Liu, W.P., Liu, C., Yang, Z., Liu, X.Y., Zhang, Y.H., Wei, Z.X., 2016. Modeling the propagation of mobile malware on complex networks. Commun. Nonlinear Sci. Numer. Simulat. 37, 249–264. https://doi.org/10.1016/j.cnsns.2016.01.019.

Motter, A.E., Lai, Y.C., 2002. Cascade-based attacks on complex networks. Phys. Rev. E - Stat. Nonlinear Soft Matter Phys. 66 (6 Pt 2), 065102 https://doi.org/10.1103/PhysRevE.66.065102.

Nguyen, W.P.V., Nof, S.Y., 2018. Resilience informatics for cyber-augmented manufacturing networks (CMN): centrality, flow and disruption. Stud. Inf. Contr. 27 (4), 377–384. https://doi.org/10.24846/v27i4y201801.

Nguyen, W.P.V., Nof, S.Y., 2019. Collaborative response to disruption propagation (CRDP) in cyber-physical systems and complex networks. Decis. Support Syst. 117, 1–13. https://doi.org/10.1016/j.dss.2018.11.005.

Reyes Levalle, R., 2018. Resilience by Teaming in Supply Chains and Networks. Springer Automation, Collaboration, and E-Services (ACES) series.

Reyes Levalle, R., Nof, S.Y., 2015a. A resilience by teaming framework for collaborative supply networks. Computers &Sa Industrial Engineering 90, 67–85. https://doi.org/10.1016/j.cie.2015.08.017.

Reyes Levalle, R., Nof, S.Y., 2015b. Resilience by teaming in supply network formation and re-configuration. Int. J. Prod. Econ. 160, 80–93. https://doi.org/10.1016/j.ijpe.2014.09.036.

Reyes Levalle, R., Nof, S.Y., 2017. Resilience in supply networks: definition, dimensions, and levels. Annu. Rev. Contr. 43, 224–236. https://doi.org/10.1016/j.arcontro1.2017.02.003.

Sajadi, S.M., Esfahani, M.M.S., Sorensen, K., 2011. Production control in a failure-prone manufacturing network using discrete event simulation and automated response surface methodology. Int. J. Adv. Manuf. Technol. 53 (1–4), 35–46. https://doi.org/10.1007/s00170-010-2814-0.

Seok, H., Kim, K., Nof, S.Y., 2016. Intelligent contingent multi-sourcing model for resilient supply networks. Expert Syst. Appl. 51, 107–119. https://doi.org/10.1016/j.eswa.2015.12.026.

Shen, S.Q., 2013. Optimizing designs and operations of a single network or multiple interdependent infrastructures under stochastic arc disruption. Comput. Oper. Res. 40 (11), 2677–2688. https://doi.org/10.1016/j.cor.2013.05.002.

Shen, S.Q., Smith, J.C., Goli, R., 2012. Exact interdiction models and algorithms for disconnecting networks via node deletions. Discrete Optim. 9 (3), 172–188. https://doi.org/10.1016/j.disopt.2012.07.001.

Snediker, D.E., Murray, A.T., Matisziw, T.C., 2008. Decision support for network disruption mitigation. Decis. Support Syst. 44 (4), 954–969. https://doi.org/10.1016/j.dss.2007.11.003.

Swift, A.W., 2008. Stochastic models of cascading failures. J. Appl. Probab. 45 (4), 907–921. https://doi.org/10.1239/jap/1231340223.

Velasquez, J.D., Yoon, S.W., Nof, S.Y., 2010. Computer-based collaborative training for transportation security and emergency response. Comput. Ind. 61 (4), 380–389. https://doi.org/10.1016/j.compind.2009.12.007.

Wang, T.Y., Zhang, J., Sun, X.Q., Wandelt, S., 2017. Network repair based on community structure. Epl 118 (6). https://doi.org/10.1209/0295-5075/118/68005.

Watts, D.J., 2002. A simple model of global cascades on random networks. Proc. Natl. Acad. Sci. U. S. A. 99 (9), 5766–5771.

Yin, R.R., Liu, B., Liu, H.R., Li, Y.Q., 2016. Research on invulnerability of the random scale-free network against cascading failure. Phys. Stat. Mech. Appl. 444, 458–465. https://doi.org/10.1016/j.physa.2015.08.017.

Zhang, L., Gier, J.d., Garoni, T.M., 2014. Traffic disruption and recovery in road networks. Phys. Stat. Mech. Appl. 401, 82–102. https://doi.org/10.1016/j.physa.2014.01.034.

Zhong, H., 2016. Dynamic Lines of Collaboration in E-Work Systems (Ann Arbor : ProQuest Dissertations & Theses).

Zhong, H., Nof, S.Y., 2015. The dynamic lines of collaboration model: collaborative disruption response in cyber–physical systems. Comput. Ind. Eng. 87, 370–382. https://doi.org/10.1016/j.cie.2015.05.019.

Zhong, H., Nof, S.Y., 2020. Dynamic Lines of Collaboration: Disruption Handling & Control. Springer Automation, Collaboration, and E-Services (ACES) series.

Zhong, H., Nof, S.Y., Filip, F.G., 2014. Dynamic lines of collaboration in CPS disruption response. IFAC Proceedings Volumes 47 (3), 7855–7860. https://doi.org/10.3182/20140824-6-ZA-1003.02403.