Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Dynamic Lines of Collaboration in CPS Disruption Response

Hao Zhong[a], Shimon Y. Nof[a], Florin G. Filip[b]

[a] *PRISM Center & School of Industrial Engineering, Purdue University, West Lafayette, IN 47907, USA*
[b] *Romanian Academy, 125, Calea Victoriei, 71102 Bucharest-1, 3R The National Institute for R&D in Informatics – ICI, Bucharest, Romania*

Abstract: Cyber-physical systems (CPSs) are emerging future engineered systems with combined efforts in cybernetics and advanced physical components. They are often designed for large and mission-critical systems, e.g., smart grids. The continuous availability of functionality is one of the important concerns by CPS stakeholders. Currently CPSs are still vulnerable to major disruptions. In this research we design the Dynamic Lines for Collaboration (DLOC) protocol for responding to disruptions in CPS. DLOC utilizes current advantages in a centralized computing model, HUB-CI (high performance computing HUB with collaborative intelligence tools), and facility sensor networks deployed in physical and cyber domains with active middleware. Based on the hybrid centralized/distributed CPS structure, DLOC is hypothesized to be a better protocol for CPS disruption response than conventional centralized protocols. Experiments with an agent-based model are performed to test the DLOC effectiveness. The results indicate that by using DLOC protocol, CPS can have 12% lower emergency responder workload, 80% reduced subsystem downtime, 82% shorter disruption response time, and 30% increased link availability compared with the conventional centralized protocol. The performance advantages of DLOC over the common centralized methods demonstrate that a high performance computing center approach to disruption response is not sufficient. DLOC can also have a relatively higher information triage efficiency and increased robustness to network dynamics and information overload.

Keywords: Collaborative control; Incidence management; Multi-agent system; Sensor network

1. INTRODUCTION

Realizing the fact that cybernetics can provide better stability, performance, reliability, robustness, and efficiency to physical systems, cyber-physical system (CPS) is emerging, especially for large scale mission-critical infrastructures (Kim & Kumar, 2012). In spite of the rapid development of CPS, it is still difficult to maintain the availability of critical systems. For instance, disruptions in power grids have affected at least half million people in U.S. just between January to August, 2013 (EIA, 2013). CPS can have large volumes of data generated by sensors, but if these data flowing on the CPS network are poorly processed, decision makers, even with qualified expertise, become the bottlenecks for system control, particularly in emergent situations. Inefficient information triage has damaged the capability of CPS. For time-critical response tasks, disruption alerts have to reach the right response agent at the right time. Otherwise, disruptions will reduce the availability of CPS.

Considering the composition of CPS, disruptions will happen in both cyber space and physical devices. The objective of this research has been to design intelligent protocol for agents to handle disruptions in CPS. The agent network should be able to respond to both cyber and physical disruptions with efficiency. Besides, the collaboration among agents should also help to balance the workload of agents in CPS.

In this paper, the dynamic lines of collaboration (DLOC) protocol is developed. Agent-based modeling is simulated to show the advantages of applying DLOC for disruption response in CPS.

2. RELATED WORK

CPS implements sensor networks to acquire information from individual components and to monitor the entire system. Related research in cyber and physical sensor networks is reviewed in this section. Helpful studies about disruption response are also discussed.

2.1 Cyber and Physical Sensor Networks

The advanced progress in sensor networks promotes the development of CPS (Wu, *et al*., 2011). Heterogeneous sensors provide information about a CPS as observations for real-time control. Facility sensor network (FSN) is a network of sensors that physically deploys at production facilities (Ko, *et al*., 2010). FSN uses different sensors together to monitor the entire production processes. The active middleware for FSN is a key component for a successful deployment, which optimizes the communication channels and saves energy consumption (Jeong, *et al*., 2012). FSN can help industrial applications to have better reliability in communication, robustness to various interferences, fault tolerance, and the adaptation to different geometry of the production facility throughout which collaborating sensors are implemented. Error and conflict detection agents are developed to monitor and to prevent malfunctions in a system (Chen & Nof, 2012). Agents collaborate to share the

knowledge of tasks, dependency and historical errors. With communication capabilities, the agent network improves the ability to prevent errors and cascading failures.

Sensors are also deployed in cyber space. Virtual sensors are used to detect intrusions coming from computer networks (Kemmerer & Vigna, 2002). Firewalls and other security mechanisms are not sufficient for large networked systems. Some undefined attacks are out of the specifications by firewalls and thus introduce risks. Other attackers break into a protected area with identities stolen from legitimate users. Their attacks cannot be prevented by firewalls but can be sensed by their abnormal behaviors. For example, an intrusion detection system can activate alerts when a user starts to download data from a database s/he rarely accesses.

The availability of continuous functionality in CPS relies on sensor networks. CPS requires high assurance of the availability of deployed sensors and their links to provide lines of command and collaboration (LOCC; Velasquez, *et al*., 2010). Disruptions in CPS and the sensor networks should be handled as early as possible.

2.2 Disruption Response Protocols

In cyber and physical domains separately, researchers have developed algorithms to cope with disruptions. (1) The study on dispatching algorithms for emergency medical service (EMS) is an ongoing work in operations research. Several articles have tried to formulate mathematical models to minimize the response time in a dynamic environment (Ghiani, *et al*., 2003). Simulation-based approaches are also popular since more factors (e.g., client priority, resource availability) can be considered in a complex network of emergency response vehicles (Gnanasekaran, *et al*., 2013). These methodologies ignore the role of communication channels in the response network. The links can be broken and need to be repaired quickly. (2) The design of disruption-tolerant networks (DTNs) is an active area of research which focuses on communication challenges in intermittently connected networks due to less reliable channels (Khabbaz, *et al*., 2012). Architecture design, routing, flow control, cooperative schemes, etc. are all active topics for DTN. A prominent approach to deal with disruptions is through the collaboration of faulty but redundant nodes in the network (Nof, *et al*., 2009). However, DTN does not provide mechanisms to fix link ruptures in the physical layer.

CPS needs the availability in both cyber and physical domains. Related research in both vehicle routing and DTN provide helpful guidelines for the design of CPS disruption response protocols.

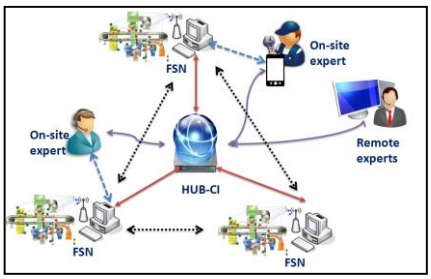


Fig. 1 Disruption Response Architecture in CPS

3. DYNAMIC LINES OF COLLABORATION

In this section, the framework of disruption response for CPS and the DLOC protocol are described.

3.1 Disruption Response Architecture in CPS

In emerging large-scale industrial systems, centralized data centers are often used to process big data for daily operations. The HUB-CI (high-performance computing hub with collaborative intelligence tools) approach is proven to be useful in e-work (Seok & Nof, 2011; Zhong & Nof, 2013). With the help of centralized HUB-CI and distributed FSN, the architecture for disruption response can be more collaborative, as shown in Fig. 1. The HUB-CI computing resource serves as an advanced version of data center. The sensor networks at each subsystem can also have multiple channels for interactions. Each FSN is connected not only to the centralized HUB-CI, but also with human experts in the production locations and other FSNs within the ranges enabled by the wireless communications. Disruption response agents working in the production site are equipped with smart handsets or wearable devices, so they can receive information from HUB-CI and have direct communication with local FSNs. The disruption response architecture can be defined as:

$$DRA := < S, A, E > \quad (1)$$

where DRA is the entire response architecture; S is a set of subsystems implemented with FSNs; A is a set of disruption responders ($x_j \in A$), and E is the set of links in the network enabled by CPS communication channels. Whenever an element of S or E has a disruption, elements of A are assigned to resolve the problem if the communication channels (E) are still available.

To study disruption response in this CPS model, the following assumptions are made:
1) Disruption. Two types of disruptions can happen in the CPS: subsystem malfunctions, and link ruptures.
2) Detection. For each FSN in the network, the FSN middleware can monitor the status of its connected links and subsystems.
3) Security. The disruptions are caused by errors or external attacks. Subsystems and links will not produce fake data if they are functioning. Disruption response agents are all trusted, and they will not be compromised by attackers and they are able to fix disruptions in required time.
4) Repairs. A broken link can only be repaired by two agents at both ends of the link, whereas subsystem malfunction can be handled by a single agent.
5) Workload. The workload for handling each disruption can be estimated by the middleware of FSN, so an appropriate responder can be assigned.
6) Agents. Response agents are classified into several ranks according their expertise of handling disruptions.
7) Ruptures. As shown in Fig. 1, the communication links are not the same. The risk of rupture is modeled in Eq. 2 according to the dynamics in wireless and wired networks:

r(FSN, FSN) > r(FSN, On-site agent) > r(HUB-CI, On-site agent) > r(FSN, HUB-CI) > r(HUB-CI, Remote expert) (2)

3.2 Protocol for Dynamic Lines of Collaboration

To respond to disruptions effectively, the communication of response agents should establish dynamic lines of collaboration (DLOC) to mitigate the risk of lost information and overloaded agents in *DRA*. DLOC protocol should (1) maintain a high connectivity and (2) schedule responses according to workload. The two features assure that messages of disruptions should be routed to the best responders. The formal definition of CPS disruption response with DLOC protocol is defined by a Petri net (see Fig. 2):

$$DRN := < P, T, F > \quad (3)$$

where *DRN* is the Petri net for disruption response; P is the set of states in CPS, T is the set of transitions; F is the set of flow relations. CPS subsystem S_i has normal operation in state P_1. If a disruption occurs (T_1 or T_2), the FSN of S_i will detect states P_2 or P_3 and issue alerts to inform response agents (by T_3). If the disruption is malfunction, only one agent is required; if the disruption is link rupture, two agents are required. $F(P_4 \rightarrow T_3)$ enables the allocation of multiple agents. After T_4 repair process, S_i is back to normal operation and agents are back to waiting state.

T_3 is the core part of DLOC protocol. It allocates responders to different disruptions by delivering messages. The contents of a message in T_3 should contain all information for a successful delivery. An example is shown in Fig. 3.

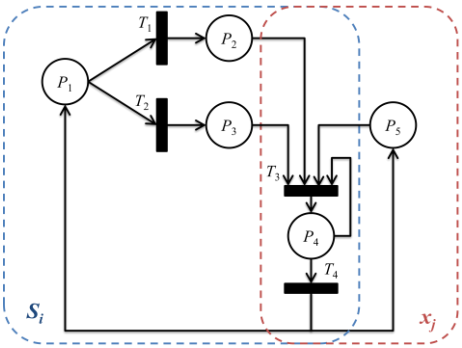
In Fig. 3, the alert is issued by the middleware of the FSN monitoring a drilling machine. The message contains the original time when the disruption has been detected. It also indicates that this event can be handled by a lowest-ranked agent and it will take him/her about 10 minutes to fix the problem. If the message is finally delivered to a higher ranked responder, the time required to resolve the problem may be shorter. Detailed information about this disruption is addressed at the end of the message. The workload and minimal level of agent required is estimated by software tools that are pre-downloaded from HUB-CI servers.

Disruption alerts have to be delivered on the intermittently connected network to responders ($F(P_2 \rightarrow T_3)$, $F(P_3 \rightarrow T_3)$, and $F(P_5 \rightarrow T_3)$). The detailed sequence is shown in Fig. 4. A CPS is a hybrid centralized/distributed network. There are several FSNs connected with subsystems and only one HUB-CI is required. Fig. 4 shows a disruption that happens to one FSN and the aftermath procedure of delivering alerts. Each FSN middleware stores a routing table of the entire network, which is downloads from HUB-CI frequently to keep current the routing information (step a). At the same time, if disruptions are detected, the events need to be reported to HUB-CI to update the network map (step b). The FSN uses updated information form HUB-CI to construct the route to the best expert (step c). If the HUB-CI is not reachable, the FSN has to use its own network discovery capabilities to find a route to an expert (steps d, b' and c'). If no responder is found, the subsystem waits in error status (step e). This operation is the FSN part of the DLOC protocol.

The decision on which agent to choose (step c in Fig. 4) is based on the knowledge of the expertise of the agent, the location of the agent, and the requirements to handle the disruption. Agent's workload is minimized in the following function to select the best responder:

$$\text{MIN } Z = W(x_j) \times \text{EXP}(L(x_j) - L_0),\ L(x_j) \geq L_0 \quad (4)$$

where x_j is a responder in the emergency response department ($x_j \in A$); $W(x)$ is the estimated workload (hour) of x_j to accomplish a given task (including the travel time from the agent's current location to the disruption site and the time to solve the problem); $L(x_j)$ is the expertise level of agent x_j; L_0 is the minimal level required to handle the unplanned event ($L(x)$ must be larger than L_0); and Z is a weighted workload, serving as the objective function. The optimization problem



P_1: subsystem normal operation
P_2: link broken
P_3: subsystem down
P_4: responder(s) allocated
P_5: responder waiting
T_1: link rupture
T_2: malfunction
T_3: responder allocation
T_4: repair process

Fig. 2 Petri Net of DLOC in CPS Disruption Response

Source:	Drilling machine#1
Message id.:	12
Issue time:	10:23:23, Oct.23, 2013
Minimal expertise level required:	1
Estimated workload:	10min
Message body:	Main motor overheat.

Fig. 3 The Structure of an Example Alert

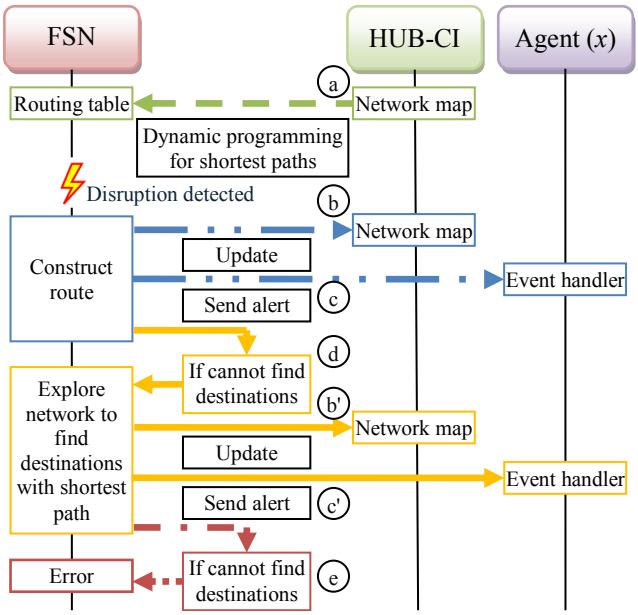


Fig. 4 Sequence Diagram of Alert Delivery ($F(P_2 \rightarrow T_3)$, $F(P_3 \rightarrow T_3)$, and $F(P_5 \rightarrow T_3)$)

can be solved in linear time by enumerating the responders.

The exponential function (Eq. 4) is used so the protocol tries to find an agent at the same level of the request. The cost of finding a higher ranked agent is set to grow fast, so that (1) higher ranked agents will not be overloaded; (2) information triage is more efficient by the most available agents.

As indicated in assumption 4 (repair), a link rupture needs to be repaired by two agents at each end. The DLOC protocol should allocate a second agent after the first one is allocated ($F(T_3 \rightarrow P_4)$ and $F(P_4 \rightarrow T_3)$). As shown in Fig. 5, when an agent starts to process an alert, it will move to the requesting FSN (step i). Depending on the alert type, the agent (1) repairs a subsystem malfunction alone; (2) repairs a link to HUB-CI with remote experts, or (3) repairs an inter FSN link with one of its peers (step ii). It is likely to have no expert available at the other end of a broken link. The first arriving expert can request another expert through HUB-CI to move to the desired location (step iii). A FSN can have multiple disruptions at the same time, so a local expert aside a FSN might not be available for repairing a specific link. The collaboration protocol enforces an expert to wait until the experts on both sides of the link are available to work together before a timeout (step iv). If an expert waits too long and exceeds the timeout, s/he will give up the current task and leave the FSN with the link unrepaired (step v).

In the entire DLOC protocol, there are three types of message delivery: (1) from a FSN to the HUB-CI with link status updates (step b in Fig. 4), (2) from the source of disruption to a responder (step c in Fig. 4), and (3) from one agent to another agent for a request of collaboration (step iv in Fig. 5). During an emergent situation, the network has to ensure timely delivery. To calculate the most reliable route, the following optimization problem needs to be solved to minimize the total risk of disconnection:

$$\min y = \sum_j \sum_i X_{ij} r(i,j), \quad i,j = 1 \ldots |S| + |A| \tag{5}$$

s.t.:

$$\begin{cases} 1, & \text{if agent } i \text{ is the start} \\ -1, & \text{if agent } i \text{ is the end} \\ 0, & \text{otherwise} \end{cases}$$

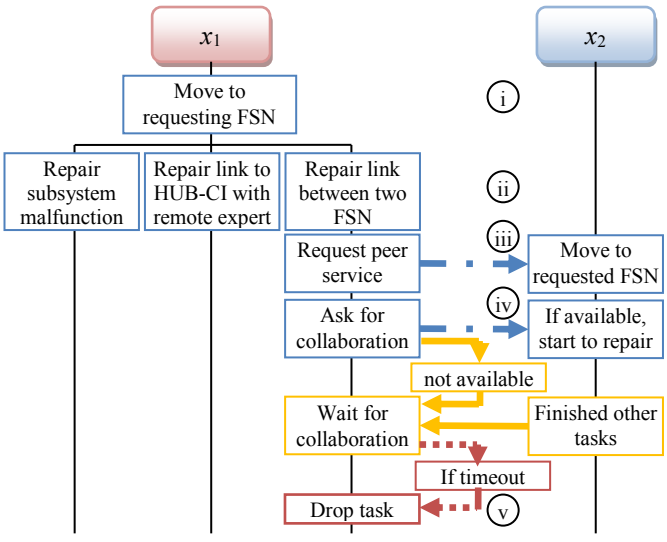


Fig. 5 Sequence Diagram of Handling Unplanned Event ($F(T_3 \rightarrow P_4)$ and $F(P_4 \rightarrow T_3)$)

where $r(i, j)$ is the risk of disconnection of the link from node i to node j. The value is 1 for a broken link, and for a connected link without any risk is 0. The probability can be estimated based on the type of link according to assumption 7 (ruptures) with Eq. 2. X_{ij} is a decision variable that equals 1 when the link is used to deliver a message, otherwise 0; and y is the total risk; it is the objective function. This optimization can be solved by a shortest path algorithm with computational complexity $O(|E| + (|S|+|A|)\log(|S|+|A|))$.

Timeouts used in DLOC are crucial in disruption response task administration (Ko & Nof, 2012). If a resource fails to respond to a call, the protocol quickly finds backup plans. In order to prevent a long waiting time, every request in the system has to abide by a timeout limitation. A subsystem will be considered malfunctioning after a timeout when the HUB-CI is querying it. The abnormal behavior will trigger an alert of disruption by the HUB-CI to be solved by responders.

4. CASE STUDY

A CPS e-manufacturing plant is simulated to verify DLOC. The plant has several subsystems, and each subsystem implements a FSN with active middleware monitoring the entire unit. The HUB-CI server is located away from any production facility. Only Internet cables are used to connect HUB-CI with FSNs. All disruption response agents are equipped with smart devices to receive alerts from HUB-CI and FSNs. The agent-based model of the CPS is coded in *AnyLogic* software. The lines represent links between agents. If two FSNs are close together, less than a threshold, a wireless link between them is established. Each FSN and response agent has a link to the HUB-CI. Responders are connected to FSNs when they are close enough.

To show the advantages of DLOC, the DLOC protocol is compared with a conventional centralized disruption response protocol (P_c). By P_c, each alert of a disruption will be sent to the HUB-CI. HUB-CI schedules responders to each event to repair a broken link or a malfunction. The experiments with DLOC and P_c have the same facility layout and the same random events enforced by the same seeds for generating pseudorandom numbers. A summary of experimental design parameters is shown in Table 1.

Fig. 6 shows the comparisons of DLOC and P_c on subsystems downtime rate (η), agent busy rate (ρ), disruption response time (T), link availability (μ) and robustness. Those measurements show the efficiency of a disruption response system fulfilling the requirements of communication capacity, response earliness, information sharing, and reliability of channels (Kim *et al.*, 2007). Other efficiency measurements on regulations and human factors are out of the scope of DLOC protocol, for this phase of research.

As shown in Fig. 6 (a) and t-test for ^{1}H in Eq. 7 and Table 2, the simulated CPS has less failed subsystems when using DLOC protocol (η_1; on average 3.1% of all subsystems through a year) than using the centralized protocol P_c (η_2; on average 14.7%).

Table 1. Simulation Experimental Design Parameters

Parameter	Value
Disruption response agent level 1	5
Disruption response agent level 2	3
Disruption response agent level 3	1
Number of subsystems	10
Number of HUB-CI	1
Simulation length (single replication)	1 year
Subsystem malfunction rate	10/ year
Link rupture base rate (p)	150/year
Rupture rate of links between FSNs ($0.5p$)	75/year
Rupture rate of links between FSN and HUB-CI ($0.3p$)	45/year

For each subsystem malfunction, it takes longer time to wait for responders to fix the problem in CPS with P_c (t_2; on average 146.4 hours in Fig. 7(c)). t-test for ^{3}H in Eq. 7 and Table 2 show the response time in CPS with DLOC is less (t_1; on average 25.7 hours). The difference is because using DLOC the entire CPS maintains more available lines of communication and efficient information triage to responders. Fig. 6(b) shows difference of workload for disruption response agents between systems with DLOC and P_c. On average, all agents are busy 80% of the time in the settings of P_c (ρ_2). The DLOC protocol helps to reduce the workload of agents (ρ_2; on average 57%) while making more timely responses to disruptions in CPS as shown in t-test on hypothesis ^{2}H in Eq. 7 and Table 2. The availabilities of links in DLOC and P_c (μ_1 and μ_2) shown in Fig. 6(d) indicate that DLOC can increase the link availability from P_c, confirmed by ^{4}H test in Eq. 7 and Table 2. Another important concern of disruption response system is about how sensitive the response performance is to intermittently connected network. As shown in Fig. 6(c), when the link rupture rate (p) is set to be higher, the time for disruption response (t) typically grows larger. To compare the difference between DLOC and P_c a linear regression model is constructed as shown in Eq. 7. Hypothesis ^{5}H tests whether there is a difference between the growth rates (β_1) of response time in the two protocols. According to the t-test in Table 3, the DLOC keeps the disruption response in relatively constant time.

Fig. 6(c) shows that a system with DLOC is robust to network dynamics. The links rupture rate (p) also indicates the volume of information generated in the system. Each rupture will trigger a request to fix the link. Although centralized computing facility, e.g., HUB-CI, has high computing capabilities, the information overload can still drag performances due to defects in the protocol control. With the same settings of system and network structure of a CPS, just by changing the collaboration process to DLOC protocol, disruption response performances can be improved.

5. CONCLUSIONS AND FUTURE WORK

Control protocol design for CPS' disruptions handling is detrimental. In emerging CPS, facility sensor networks can enable wired and wireless communication channels for an integrated system of cyber elements and physical devices. The HUB-CI gives centralized computing capabilities, but it is not sufficient for disruption response under time pressure. To assure the effectiveness of disruption response in CPS, Dynamic Lines of Collaboration (DLOC) protocol is developed. DLOC is a hybrid centralized/distributed coordination protocol that takes advantage of the adequate

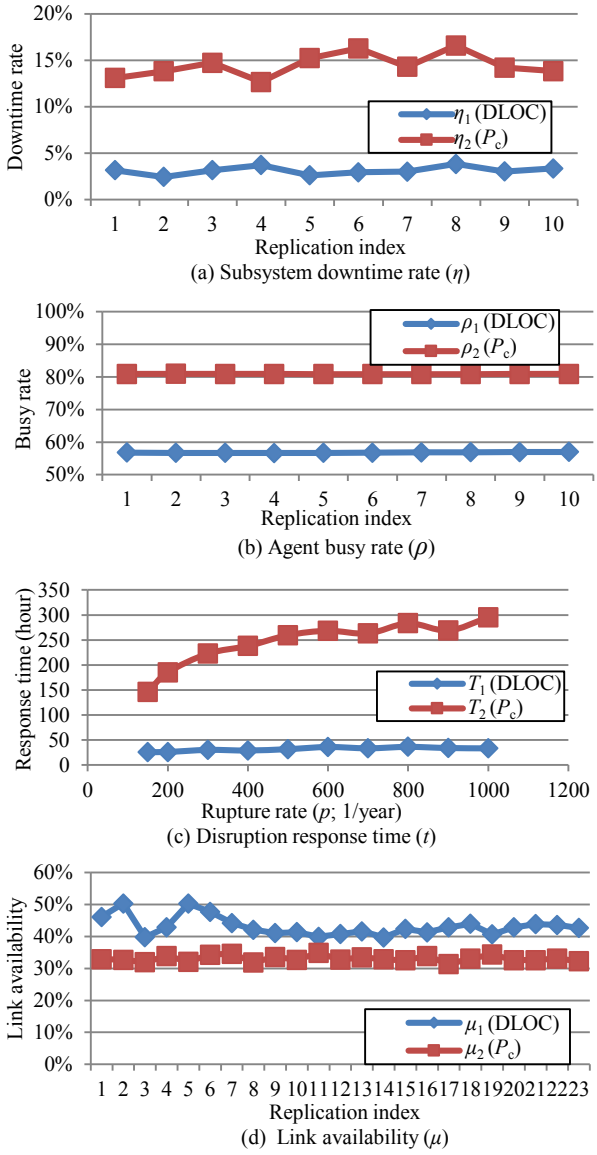


Fig. 6 Experiments Results

links enabled by FSNs and the high computing capability in HUB-CI. By using DLOC, disruption response systems can outperform conventional systems using centralized protocols (often used in systems with datacenters and cloud services). Through agent-based modeling six significant advantages are observed for DLOC compared with a centralized approach: Reduced (1) system downtime, (2) disruption response time, (3) human workload, (4) information overload; Improved: (5) link availability, and (6) robustness to network dynamics. Compared with other approaches for CPS disruption response, the developed method has the following characteristics, as summarized in Table 4.

Availability in mission-critical CPS is one of the most significant factors considered by stakeholders and users. Many CPSs (e.g., power grids, air transportation systems) are considered as critical resources for human safety, beyond just being profit generators. The new DLOC protocol can help maintain a high availability of CPS to high priority users. In this approach, the capability of timely response and recovery is enabled by the correct integration of sensor networks and

$$t_2 - t_1 = \beta_1 p + \beta_0 \quad (6)$$

$$^1H_0: \eta_1 - \eta_2 = 0;\ ^1H_a: \eta_1 - \eta_2 < 0$$
$$^2H_0: \rho_1 - \rho_2 = 0;\ ^2H_a: \rho_1 - \rho_2 < 0$$
$$^3H_0: t_1 - t_2 = 0;\ ^3H_a: T_1 - T_2 < 0 \quad (7)$$
$$^4H_0: \mu_1 - \mu_2 = 0;\ ^4H_a: \mu_1 - \mu_2 > 0$$
$$^5H_0: \beta_1 = 0;\ ^5H_a: \beta_1 \neq 0$$

Table 2 T-Tests on Experiments Results (alpha = 0.05)

Variable	Sample size	Mean	SD	p value	Decision
η_1	10	0.031	0.004	0.000	Reject $^1H_0$
η_2	10	0.147	0.014		
ρ_1	10	0.568	0.001	0.000	Reject $^2H_0$
ρ_2	10	0.809	0.000		
t_1	1000	25.7	16.5	0.000	Reject $^3H_0$
t_2	1000	146.4	102.0		
μ_1	23	0.431	0.030	0.000	Reject $^4H_0$
μ_2	23	0.331	0.009		

Table 3 T-Test on Slop (alpha = 0.05)

Slop	Sample size	Value	SE	p value	Decision
β_1	10	0.131	0.023	0.001	Reject $^5H_0$

HUB-CI computing facilities. DLOC protocol further improves the ability of handling disruptions.

In the near future, increasingly more complex CPSs will be implemented all over the world. Managing the availability together with other functionality and security requirements is an important challenge that needs to be studied. System integrators and system operators need to have clear policies, mechanisms, and protocols to assure the correct establishment and operation of CPSs. Future directions include applying DLOC protocol and collaborative intelligence algorithms in CPS to reduce the risk of system malfunction and internal/external attacks when CPS is dynamically evolving. The availability of interoperating different CPSs, e.g., power grids, water supply, and metropolitan networks, is a vital research direction.

ACKNOWLEDGEMENT

Research reported here is supported by the PRISM Center for Production, Robotics, and Integration Software for Manufacturing & Management. The LOCC principle of CCT, Collaborative Control Theory, began with security projects supported by INDOT, Indiana Department of Transportation.

REFERENCES

Chen, X. W. & Nof, S. Y. (2012). Agent-based error prevention algorithms. *Expert Systems with Applications*, 39(1), pp. 280-287.

Energy Information Administration, U.S. (EIA) (2013). Table B.1 Major Disturbances and unusual occurrences, year-to-date. *Electric Power Monthly*. Retrieved from: www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_b_1

Ghiani, G., Guerriero, F., Laporte, G., Musmanno, R. (2003). Real-time vehicle routing: solution concepts, algorithms and parallel computing strategies. *European Journal of Operational Research*, 151, pp.1-11.

Gnanasekaran, A. M., Moshref-Javadi, M., Zhong, H., Moghaddam, M., Lee, S. (2013) Impact of Patients Priority and Resource Availability in Ambulance Dispatching. *ISERC 2013*.

Jeong, W., Ko, H., Lim, H., & Nof, S. (2013). A protocol for processing interfered data in facility sensor networks. *Int. J. Adv. Manuf. Technol*., 67(9-12), pp. 2377-85.

Khabbaz, M. J., Assi, C. M. Fawaz, W. F. (2012) Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. *IEEE Com. Surveys & tutorials*, 14(2), pp. 607-640.

Kim, J. K., Sharman, R., Rao H. R., Upadhyaya, S. (2007). Efficiency of critical incident management systems: instrument development and validation, *Decision Support Systems*, 44. pp. 235-250.

Kim, K. & Kumar, P. R. (2012) Cyber-physical systems: a perspective at the centennial, *Proc. of IEEE*, 100, pp. 1287-1308

Ko, H., & Nof, S. Y. (2010). Design of collaborative e-service systems. In G. Salvendy, & W. Karwowski, *Introduction to Service Engineering* (pp. 227-252). Wiley.

Ko, H.S. and Nof, S.Y. (2012), Design and application of task administration protocols for collaborative production and service systems. *International Journal of Production Economics*, 135, pp. 177-189.

Nof, S. Y., Liu, Y., Jeong, W. (2009). Fault-tolerant timeout communication protocol with sensor integration. *United States Patent*, No. 7,636,038 B1.

Seok, H., & Nof, S. (2011). The HUB-CI initiative for cultural, education and training, and healthcare networks. *21st Int. Conf. Production Research.* Stuttgart, Germany.

Velasquez, J.D., Yoon, S.W., Nof, S.Y. (2010). Computer-based collaborative training for transportation security and emergency response, *Comp. in Ind.*, 61(4), 380-389.

Wu, F., Kao, Y., Tseng, Y. (2011). From wireless sensor network towards cyber-physical systems, *Pervasive and Mobile Computing*, 7(4), pp. 397-413.

Zhong, H., & Nof, S. (2013). Collaborative design for assembly: the HUB-CI model. *22st Int. Conf. Production Research*. Iguassu Falls, Brazil.

Table 4 Comparison of Disruption Response Protocols for CPS

Protocol Approach	Protocol Assumptions	Advantages	Limitations
Vehicle routing in EMS (Ghiani, *et al*., 2003; Gnanasekaran, *et al*., 2013)	Persistently connected networks; request of services can always reach the dispatching center; dynamic vehicle location and travel/service time.	Minimizes response time; efficient use of vehicles; optimal location of vehicles prepared for emergencies.	Communication channels are critical, yet there no methods for routing in disrupted networks.
Disruption-tolerant networks (Khabbaz, *et al*, 2012; Nof, *et al*., 2009)	Intermittently connected networks due to disruptions in extreme environments; distributed sensors need to transmit message to a base station.	Tolerate link delays and disruptions; improved reliability in routing congestion resolution; and cooperation between agents.	No strategy for repair; no methods of removing deprecated messages.
DLOC for disruption response in CPS (the current research)	Link ruptures and subsystem malfunctions in CPS will call for repair if a communication line to response team, or teams, is (are) available.	Minimizes system down time and disruption response time; increased link availability; and effective and efficient deployment of response team.	Only responds to disruption incidences; not proactive.