Proceedings of the 2018 Winter Simulation Conference
M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, eds.

CYBER-PHYSICAL SIMULATION AND OPTIMAL MITIGATION FOR SHIPPING PORT OPERATIONS

Gabriel A. Weaver

Information Trust Institute
University of Illinois at Urbana-Champaign
1308 W Main Street
Urbana, IL 61801

Lavanya Marla

Industrial and Enterprise Systems Engineering
University of Illinois at Urbana-Champaign
104 S Mathews Ave
Urbana, IL 61801

ABSTRACT

Modern shipping ports *require* computer systems to accommodate an increasing number of port calls, larger vessel sizes, and tighter supply chains. Disruptions to assets on these networks have the potential to propagate to other critical infrastructures at great economic cost. Such disruptions may be introduced intentionally by adversaries that include nation states, organized crime, hacktivists, and insiders. *Area Maritime Security Committees (AMSCs)* must develop security plans to minimize disruptions' impact. This paper explores one way to couple a simulation of the flow of commodities through a shipping port with an optimization that minimizes the cost of disruptions to the port transportation system. Our intent is to enable stakeholders to run what-if scenarios, to understand the impact and effect of cyber-physical disruptions, and to optimally mitigate their effect. This research, based on ongoing fieldwork with Port Everglades and the USCG, hopes to improve security policies that integrate cyber and physical effects.

1 INTRODUCTION

Shipping ports are essential to global commerce and our way of life. According to a report by Martin Associates, the economic value of activity at the more than 360 sea and river ports in the USA was $4.6 trillion in 2014, more than a quarter of the country's GDP (Associates 2015). Modern port operations form an interconnected cyber-physical system consisting of a network of transportation and logistics systems, and associated information and communication systems, with the port as the connecting entity. Within modern ports, computer systems "operate machinery, vessel propulsion, and navigation systems; monitor and control safety and operate security cameras, gates, and communications systems; [and] track and enable vessel operators to control ballast" (Zukunft 2015). Ports *require* computer systems in order to accommodate an increasing number of port calls, larger vessel sizes, and tighter supply chains.

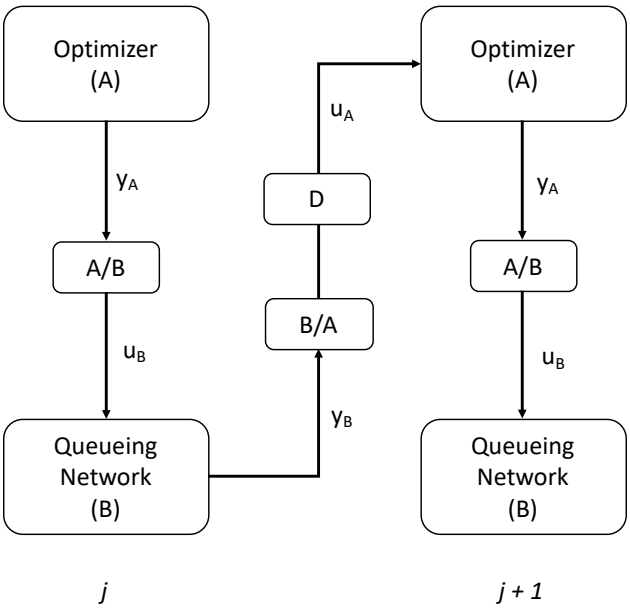
Increased dependence upon automation within shipping ports, combined with advanced intermodal logistics upon which just-in-time supply chains depend, makes research into cyber-physical systems within the Maritime domain a practical necessity. Efforts such as *Executive Order (EO)* 13636 (Order 2013), *Presidential Policy Directive (PPD)* 21 (Obama 2013), the *National Infrastructure Protection Plan Risk Management Framework (NIPP RMF)* (DHS 2013), the NIST Cybersecurity Framework (National Institute of Standards and Technology (NIST). 2014), and the USCG Cyber Strategy (Zukunft 2015) make understanding the interactions between the transportation and communications/IT sectors even more relevant.

Shipping ports are a nexus of critical infrastructure. Within a small geographic region, there are interactions between the Transportation, Communications/IT, and Energy Sectors. As such, shipping ports have become a valuable use case to explore simulation of cyber-physical systems. Researchers and practitioners need a better understanding of the interactions between and dependencies among critical infrastructure components. Ablon relates the lack of understanding of cyber-physical dependencies within the MTS to increased risk of attack. "The massive growth of networked and connected devices also increases

the attack surface, enable cyber physical effects, and impacts overall security ccosts. This is due in large part to an increased number of connected devices, a lack of emphasis on security, and little awareness of what is actually connected" (DiRenzo et al. 2017).

The integration of automation and security networks into shipping port operations motivates the need to model disruptions to cyber-physical systems within the MTS. Recent events such as Hurricane Harvey as well as the NotPetya ransomware attack highlight the variety of hazards faced by the MTS. The variety and combination of these disruptions motivates the need for *Area Maritime Security Committees (AMSCs)* to be able to mitigate and recover from cyber-physical disruptions or combinations thereof.

Borrowing from the co-simulation literature and multidisciplinary design optimization, this paper will explore the coupling of a numeric simulation of the flow of commodities through a shipping port with an analytic optimization module that re-designs routes and schedules to minimize the cost of disruptions to the port transportation system. The intent of this coupling is to enable AMSCs to understand the the *impact and effect* of cyber-physical disruptions (via the simulation module) while mitigating the effect of such disruptions in a manner that minimizes cost and time (via the optimization module). For example, Figure 1 illustrates a sequential coupling scheme between optimization and co-simulation modules.



$$
\begin{aligned}
u_A &= < K, O(k_u), D(k_u), EAT_{k_u}, LDT_{k_u}, D_l^{k_u}, \Delta_{delay}^{k_u}, \\
&\quad c_{ihj}^{k_u}, u_{ihj}^{k_u}, u_{ihj}, s_i, tt_{ihj}, G > \\
y_A &= < x_h^{k_u}, y_h^{k_u}, t_l^{k_u}, t_h^{k_u} > \\
u_B &= < A_i, B_i, c_i, N_i, K_i, G, P > \\
y_B &= < x_{ku} >
\end{aligned}
$$

Figure 1: The sequential coupling runs the optimizer A and queueing network B in sequence. At event j, outputs from the multicommodity schedule optimizer (y_A) are transformed via function A/B to inputs for the queueing system u_B. The queueing system simulates port operations until the time of event $j+1$ at which point the behavior trace and other outputs y_B will be transformed to inputs for the optimizer u_A. If $j+1$ is a disruption or mitigation event, module D will perturb some of these inputs (e.g. service time) according to the disruption. More details about the input/output vectors and transformation functions will be provided in sections for each module.

The simulation module enables stakeholders to experiment—through *what if* scenario analyses—with interactions between the availability of communications/IT services and the throughput of the shipping port transportation network. Using this module, researchers can understand the effect of disruptions to the port. Given a schedule of commodities and an infrastructure graph, this discrete time (DT) stochastic simulation computes a behavior trace that describes the flow of commodities through a shipping port's transportation system. Section 3 describes this module and how it may be used to model cyber-physical disruptions to the MTS.

The optimization module analytically computes a schedule for how to route multiple commodities with minimum cost. Unexpected disruptions due to changing environmental and adversarial conditions make determining optimal routes for commodities even more challenging. Therefore, this module implements a multicommodity optimal network flow algorithm to help stakeholders minimize the impact of disruptions in a cost-effective manner. The challenge of these approaches is to compute in a time and space-efficient manner. This analytic module uses discrete time to deterministically compute an optimal schedule to move commodities through the shipping port. Section 4 describes the formulation of this module used in this paper and how it might support decisions made by the AMSCs to prepare and recover from a disruption.

2 RELATED WORK

Current approaches for modeling port operations use approaches derived from operations research or discrete event simulation, and mostly consist of modeling the physical aspects of such operations. Moreover, research into modeling intelligent and adversarial behavior in the form of coordinated cyber (or physical) attacks appears limited in the shipping domain although techniques may be applicable from research in the Energy Sectorb (Sholander et al. 2006).

Several approaches to model automated ports within the academic literature include Discrete Event Simulation, Bayesian Networks (Tien 2017), Markov Models, Optimal Network Flow, and Petri Nets. Some of these methods, have been used to simulate cyber-physical disruptions (Ekelhart et al. 2015; Kotenko 2014; Banks et al. 2010; Wagner et al. 2015; Franqueira et al. 2009; Toutonji et al. 2012). Cimino et al. (2017) conducted a comprehensive study that models the effect of automation in a container terminal. They use the *Business Process Modeling Notation (BPMN)* to look at efficiencies introduced by smart technologies on harbor logistics. In addition, Zhu et al. (2010) use event-driven simulation and virtual reality to evaluate the utilization of a new automated container system design that included twin *Rail Mounted Gantry Cranes (RMG)* and quay cranes.

The academic literature suggests a number of approaches to documenting and modeling cross-infrastructure interactions of which cyber-physical interactions are one example. Specifically, the research areas of *Multidisciplinary Design Optimization (MDO)* (Martins and Lambe 2013) and co-simulation (Yi et al. 2016; Guo et al. 2014) provide formalisms to relate and propagate state across models of different critical infrastructures. As noted in a recent survey by Gomes et al. (2017), co-simulation is being studied across many heterogeneous communities and challenges in composition including managing causality, determinism, and dynamic changes to simulation structure. Different approaches to co-simulation include (but are not limited to) hybrid systems (Broman et al. 2015; Ni and Broenink 2012; Wang and Baras 2013), numerical analysis (Gu and Asada 2004; Kalmar-Nagy and Stanciulescu 2014), and differential algebra (Schweizer and Lu 2015). Some are even trying to develop frameworks and standards by which independent simulation modules may be composed (Broman et al. 2015; Gu and Asada 2004). Finally, several approaches have been taken to model cross-infrastructure disruptions including simulation, emulation, and Bayesian Networks (Tien 2017). Most relevant to simulating cyber-physical disruptions to shipping ports, is work done by Bou-Harb et al. (2017); Beaumont and Wolthusen (2017) and SANDIA and Bell Laboratories in Beyeler et al. (2004).

3 SIMULATION

As shown in Figure 1, a schedule of commodities is used to route information through a queueing network instantiated from graphical models of baseline operations. Unlike the optimization module, the simulation module can capture the effects of stochastic behavior on the movement of commodities as well as record resource utilization. The intent of the simulation module is to be able to look at the robustness of an optimal schedule with respect to stochastic behavior (and disruptions) as well as to understand the degree to which different optimal schedules (as there may be more than one) affect resource utilization within a

shipping port. This section provides an overview of the queueing model, and subsections detail models of baseline operations and simulation of cyber-physical disruptions.

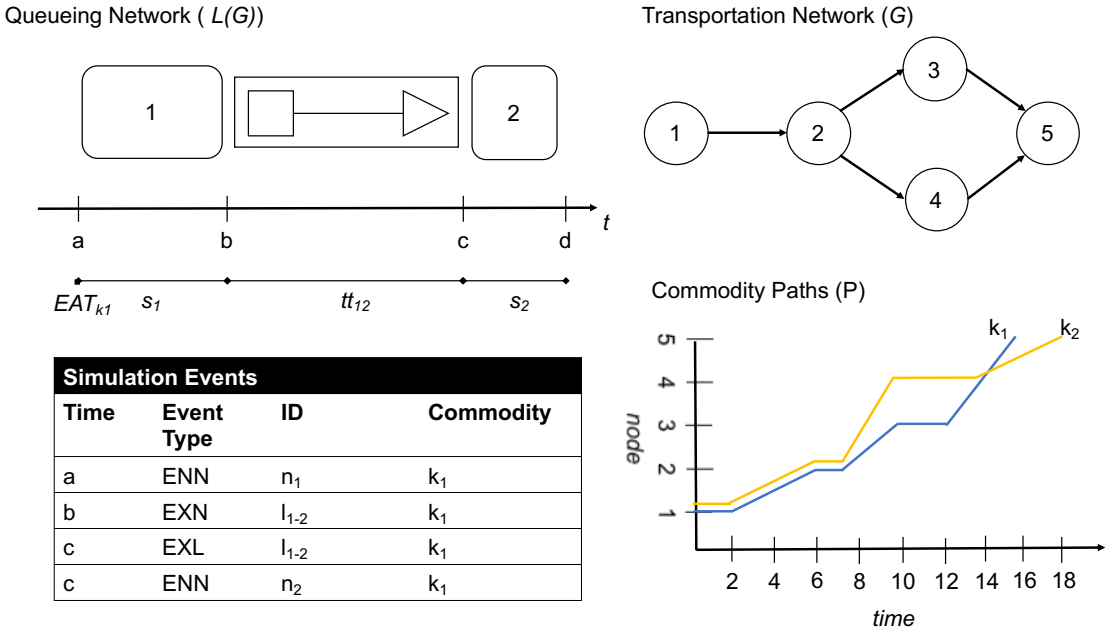
Inputs to the simulation module consist of a graph-based representation of the transportation network topology(G), a set of commodity units (K) that must be routed through this graph, and a set of paths (P) that commodities take through the network. In the current implementation, simulator inputs are encoded within JSON file formats for both the transportation network and commodity units as well as via a text-based format that encodes per-commodity unit paths. Table 1 provides an overview of simulation module inputs and outputs.

The input graph ($G = (V,A)$) is used to instantiate a queueing model $L(G) = (N,E)$ whose nodes $n \in N$ correspond to link entrance and exit buffers as shown in Figure 2. In addition to the transportation network topology, additional model parameters from the optimization module may be used to instantiate the service time distribution for each node in the queueing network (B_i), the number of parallel servers at a node (c_i), and the number of commodity units that can wait to be serviced at a node (N_i). More details about how the optimization model parameters might be used to instantiate model parameters are provided in Table 1. Commodity shipments (K) and paths (P) describe each of the commodities to be scheduled and their optimal path through the transportation network (G) respectively.

Given these inputs, the simulation propagates commodities through the queueing network via the process of *node transfer* and *link traversal* as described by Qu and Zhou (2017). Using this approach, the module schedules, processes, and computes cumulative counts for the following events: the number of commodities that have *ENtered (EN)* and *EXited (EX)* a link (L) or node (N). Commodities (K) are scheduled to flow relative to the optimal paths P. Figure 2 illustrates commodity shipment k_1 arriving at its source node ($O(k_1) = n_1$) at time $a = EAT_{k_1}$ (ENN), being serviced, and exiting the source node at time $b = a + s_{n_1}$. In general, $a \geq EAT_{k_1}$ and $b \geq a + s_{n_1}$. Upon exiting the node (EXN), the commodity is assumed to immediately enter the next link l on its path (ENL) where it is queued at the entrance node for that link l. In the process of *link traversal*, a commodity is removed from the entrance queue at time b and added to the exit queue at time $c = b + tt_l$. Although Figure 2 shows the commodity immediately

Table 1: Input and output variables for the simulation module. Simulation model parameters are based on Kendall's notation with slight modifications due to coupling with the optimization module. For example, A_i is defined with node arrival times for each commodity $k_u \in K$ rather than a distribution of arrival times. These variables are used by the co-simulation shown in Figure 1.

Simulation Input Variables (u_B)		
Parameter	Description	Relation to Optimization Module Parameters/Outputs
A_i	Arrival times for each commodity unit at a node in the queueing network.	Based on the commodity path $p_{k_u} \in P$.
B_i	The service time distribution at a node in the queueing network.	Based on the travel time/service times (s_i, tt_{ihj}) for corresponding edge or vertex in G
c_i	The number of parallel servers at a node in the queueing network.	Based on capacity of an edge (u_{ihj}) in G.
N_i	The number of commodity units that can wait to be serviced at a node.	Based on the capacity of an edge (u_{ihj}) in G.
K	The total number of commodity units that may be served.	Given by commodity shipments in K.
Simulation Output Variables (y_B)		
$< x_{ku} >$	A per-commodity unit state trajectory that relates the co-simulation time base T to one of the nodes in the queueing model.	



Simulation Events			
Time	**Event Type**	**ID**	**Commodity**
a	ENN	n_1	k_1
b	EXN	$l_{1\text{-}2}$	k_1
c	EXL	$l_{1\text{-}2}$	k_1
c	ENN	n_2	k_1

Figure 2: Given a transportation network G, a set of commodities K, and a set of commodity paths P, the simulation model schedules and processes commodity link arrival and link departure events. The link-based queueing network is instantiated from G by associating an entrance and exit queue with every edge in G. The relation between the timing of these events, as well as movement of commodities along optimal paths, is shown in the illustration above. For example, commodities $k_1, k_2 \in K$ both move through the network, but take different paths, the former going through node 3 while the latter through node 4.

exiting link l after link traversal, time $c \geq b + tt_l$, as commodities may wait to exit the link in the general case (e.g. due to downstream link capacity as mentioned by Qu and Zhou (2017)). In the process of *node transfer*, commodities are moved from the exit buffer of a node's incoming link to the entrance buffer of the node's outgoing link.

4 OPTIMIZATION

The multicommodity optimal network flow module computes an optimal way to deliver commodities through the MTS network. Table 2 provides an overview of different input model parameters for the ONF formulation. These parameters are used within Figure 1 to describe input and output variables within the co-simulation.

Given these inputs, the Optimal Network flow model seeks to find the schedule that minimizes the delay costs of shipments being delivered after the latest delivery time and the operating cost of travel of all shipments. The optimization formulation has been fully implemented using the Python bindings for the Gurobi Optimization Library (Gurobi Optimization 2015). The complete formulation has been omitted due to space constraints.

5 EXAMPLE APPLICATION AND RESULTS

The previous sections described the inputs, operation, and outputs of the simulation and optimization coupling. In this section, we apply this approach to an example of commodity flows within shipping ports. The first subsection begins with an overview of data sources and network models that are informed by extensive fieldwork with partner shipping ports. We adopt a layered network approach to document

dependencies between the Communications/IT and Transportation Sectors that could adversely affect the MTS. The second subsection provides a simple example of optimal mitigation in which commodity paths are recomputed as a result of a cyber-originating disruption to a drayage road. Finally, the third subsection describes some lessons learned and challenges encountered while implementing the coupled simulator/optimizer.

Table 2: Input and output variables for the optimization module. The module is implemented as a multicommodity network flow algorithm in which containers flow from a source to a destination node within the transportation network. These variables are used by the coupled optimizer-simulator shown in Figure 1.

Optimizer Input Variables (u_A)			
Parameter	Description	Parameter	Description
$K \subseteq \mathbb{N}$	The set of all commodities. For all $k \in K$, k_u denotes the u^{th} shipment of the k^{th} commodity ($u \in U \subseteq \mathbb{N}$).	$O(k_u)$	The source vertex of commodity shipment k_u.
$D(k_u)$	The destination vertex of commodity shipment k_u.	EAT_{k_u}	The *Earliest Arrival Time (EAT)* of a commodity shipment at its origin, $O(k_u)$.
LDT_{k_u}	The *Latest Delivery Time (LDT)* of a commodity unit to its destination, $D(k_u)$.	D_l^k	The demand for a commodity unit at an origin or destination vertex $l \in V[G]$.
$c_{ihj}^{k_u}$	The per commodity unit cost to use arc h.	u_{ihj}	The total capacity of an arc h, expressed in number of commodity units.
$u_{ihj}^{k_u}$	The per-commodity capacity of an arc h, expressed in number of commodity units.	s_i	The service time at location vertex i.
tt_{ihj}	The travel time along an arc, expressed in simulation time minutes.		
Optimizer Output Variables (y_A)			
$x_h^{k_u}$	Indicator variable, 1 if commodity unit k_u takes edge h.		
$y_h^{k_u}$	The number of commodity units that flow across edge h.		
$x_l^{k_u}$	Indicator variable, 1 if commodity unit k_u uses vertex l.		
$y_l^{k_u}$	The number of commodity units that flow through vertex l.		
P	A set of optimal paths for each commodity through G_{trans}, computed from previous output variables.		

5.1 Data Sources and Model Inputs

As discussed in previous sections, our coupling scheme depends upon a network model (G_{Trans}) to represent the *Maritime Transportation System (MTS)*. Moreover, the approach also depends upon commodity shipment schedules (K) that detail when various types of commodities arrive at a port. Through extensive fieldwork with partner shipping ports, models of baseline operations within shipping ports as well as dependencies between these operations and Communications/IT systems have been encoded.

First, the optimizer-simulator coupling requires a network model. Figure 3 illustrates dependencies between port automation systems and a simple transportation system. The intent of this model is to provide a simple but practical analysis of how disruptions to a cyber service may affect the MTS. Consider graph G in Figure 3 as a layered network whose components are partitioned according to the Communications/IT (G_{Cyber})

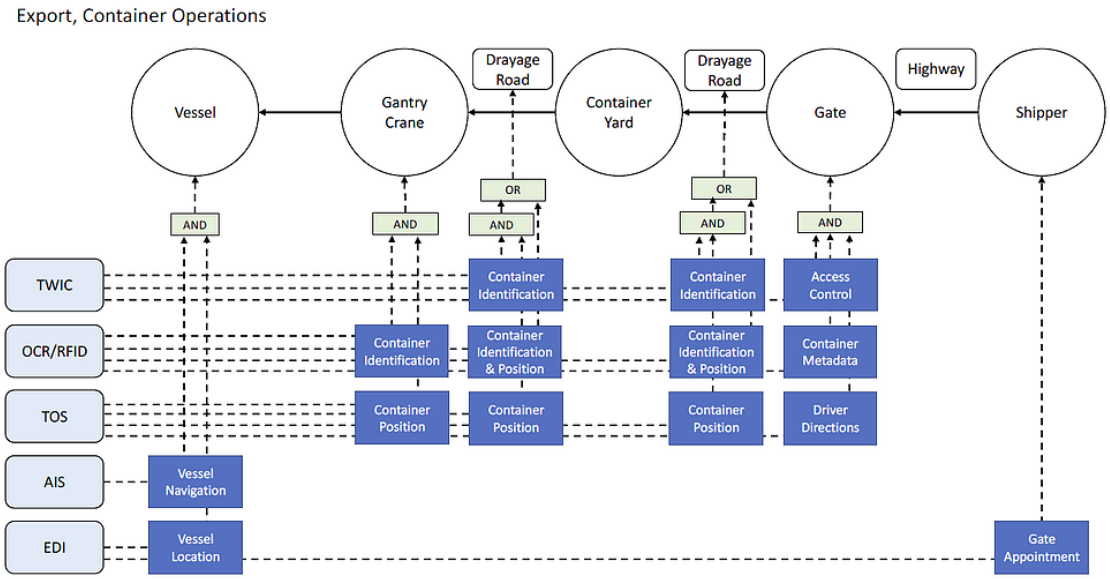


Figure 3: A cyber-physical model for container export operations as a layered network. The graph in the top row, shown in white, illustrates the flow of export commodities from a distribution center to a vessel. The leftmost column enumerates different systems provided by the Communications/IT infrastructure that are necessary for efficient operation. The latter is related to the former via data dependencies such that latencies in the availability of data within the cyber system affect service times in the intermodal transportation system.

and Transportation (G_{Trans}) Critical Infrastructure Sectors. The container operations model represented by G_{Trans} was developed based upon fieldwork as well as a recent report on emerging automation technologies in container operations by the United States *Department of Homeland Security (DHS)* (DHS. 2017).

Note that the dependencies encoded by edges from nodes in G_{Cyber} to G_{Trans} may be used by the disruptions module D (shown in Figure 1) to model how latencies within cyber services affect service times within the transportation network. Latencies resulting from disruptions within the cyber domain may be modeled as random variables or constants whose values represent the time delay introduced by the compromise or failure of that service. In general, delays may range from minutes (e.g. latencies within the *Terminal Operating System (TOS)*), to days (e.g. ransomware). This approach is not suitable to model all cyber disruptions. For example, the attack on the Port of Antwerp from 2011-2013, in which organized crime was able to alter TOS entries to illegally smuggle drugs, would require a model of data integrity, not a model that introduces latencies. Nonetheless, we believe that this approach is suitable for a wide variety of cyber-physical disruptions.

5.2 Example Disruption Scenario and Optimal Mitigation Results

We now provide a small example to demonstrate the operation of the coupled optimizer-simulator. In this scenario (based on feedback from operators) a disruption at the lanes connecting Gate to to Terminal B causes an increase in traffic at the entrance to that road. As a result, new trucks are effectively unable to use this road to reach the terminal. Such an occurrence may happen due to a lack of labor at a given time of day (e.g. lunchtime) or due to a disruption to gate operations caused by a ransomware attack (as shown in Figure 4. This example illustrates a scenario in which AMSC stakeholders could benefit from the ability to compute a new optimal route for commodities moving through the port following a disruption.

Figure 4 shows the simple queueing system for this scenario which consists of five nodes: a main road (Road), a shared Gate to access either of two terminals (Gate), Terminals A and B (TermA, TermB), and

the commodity shipments' destination (Sea). Trucks are assumed to carry a single *twenty-foot equivalent (TEU)* and arrive at the Road according to the times provided by the optimal commodity schedule. Per-link travel times are given by a normal distribution B_l whose mean is defined in terms of tt_l for each link $l \in A[G]$. For the results shown in Figures 5a, 5c, 5b, and 5d, a distribution is not used and instead travel times are deterministically set to tt_l. The effect of stochastic behavior on optimality of paths is a possible area of future research as is the mapping from optimizer outputs to simulator inputs. The number of parallel servers c at the entrance and exit buffers for each link is given by the capacity of that link. Finally, the per-node queue length for entrance and exit buffers must sum to the total capacity of the link. Finally, the size of the calling population for each queue is bounded by the number of commodities K.

The queueing model runs as normal, however callbacks to the optimizer could occur under conditions that indicate the occurrence (or clearing) of spillover. In the former case, an example condition could be when the ratio of queued trucks to queue length in the link exceeds 80%. In the latter case, a condition for spillover clearning could be when the same ratio drops below some threshold. When spillover occurs, the capacity of the corresponding link in the optimization (u_{ihj}) is adjusted to reflect the decreased capacity and new routes computed. In future implementations, these new routes would be followed until the point that the simulation indicates that the spillover has cleared at which point the link capacity is restored in the optimizer and routes re-calculated. The goal is to provide the best set of actions possible given a disruption (intentional or unintentional) to a *Captain Of The Port (COTP)*, Port Security Manager, or other stakeholders within an AMSC.

Per-link cumulative event counts from routing commodity shipments according an optimal schedule are shown in Figure 5a. Note that the capacity utilization of the road between Gate 2 and Terminal B exceeds the link capacity utilization threshold of 80% in Figure 5c. This could be due to (or exascerbated by) a disruption as discussed above. If desired, stakeholders could compute an optimal mitigation. In Figure 5b, traffic on link $2-4$ is rolled back to Gate 2 and routed via link $2-3$ while capacity on link $2-4$ is set to 0 to avoid congestion. In future implementations, one could also allow the traffic on link $2-4$ at the time of the disruption to clear out and subsequently adjust the capacity appropriately.

6 FUTURE WORK

While implementing the prototype, several lessons were learned and challenges discovered that set the stage for future research. First, there may be multiple conditions of interest that would invoke recomputing optimal commodity shipment schedules. Although the example in the previous section focused on a threshold of road capacity being exceeded, another condition might include when a certain threshold of non-optimal commodity movements is exceeded. Second, when the simulator forks to execute a new optimization cycle (corresponding to moving from iteration j to iteration $j+1$ in Figure 1), a variety of state must be saved to implement the B/A transformation. Due to space constraints, an in-depth discussion of the B/A and A/B mappings had to be excluded. Third, the simulation module discussed in this paper was a link-based simulation module and as such provided queues at link entrances and exits. Such an approach has been used to model spillback in a scalable manner by Qu and Zhou (2017). In general, looking at scalability of the simulation and optimization to larger graphs and sets of commodities is an item for future work. Moreover, more research into the effects of stochastic behavior within the simulator on the utility of paths produced by the optimizer needs to be conducted. In general, not all optimal schedules may be created alike as we observed different schedules that had different resource utilization profiles in the simulator. Finally, higher-fidelity models of communications/IT networks might allow us to study a broader class of disruptions.

7 CONCLUSIONS

Integrating the optimizer with the simulator provides a clean separation of concerns. The simulator enables one to understand the movement of containers through the system while accounting for resource usage

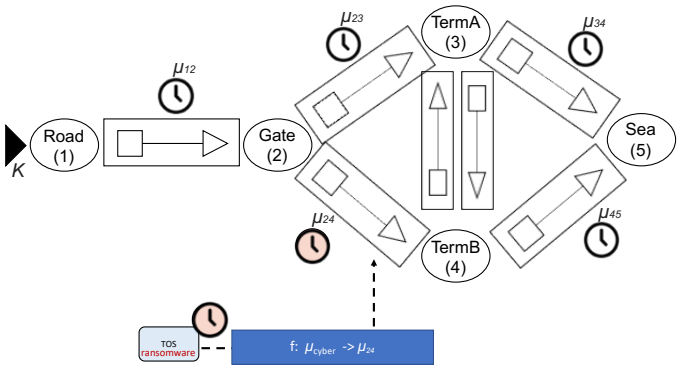
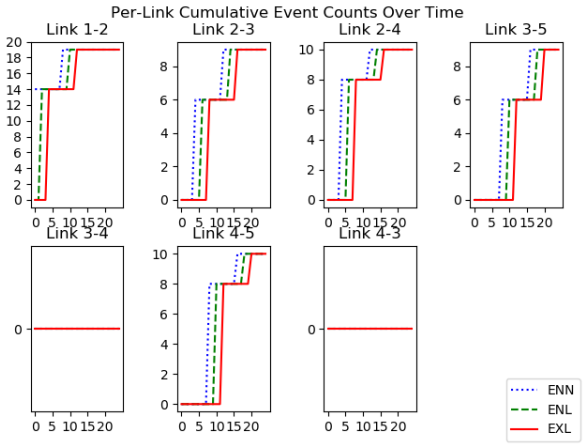
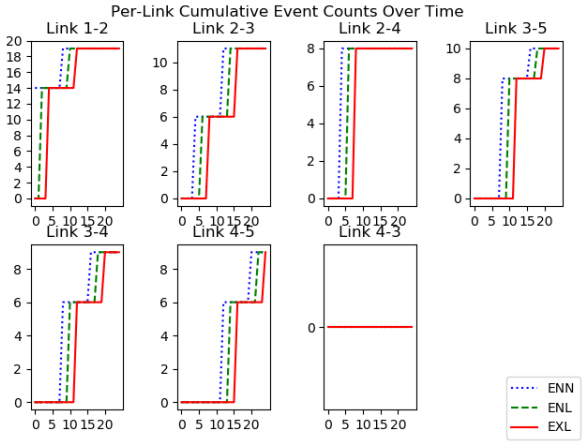


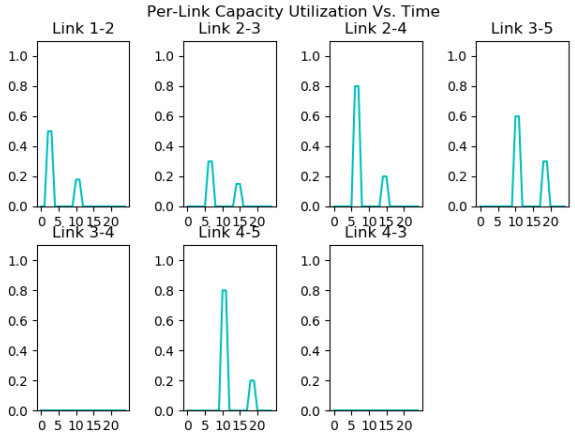
Figure 4: The link-based queueing model for this example scenario consists of five nodes. A disruption to the Gate's kiosk system could result in an increased number of trucks queueing at the entrance of the road to Terminal B.



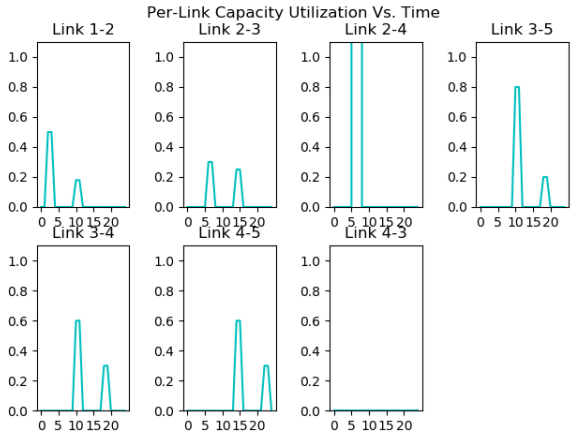
(a) The per-link cumulative event counts over time show the flow of commodities along the links in the network above.



(b) The per-link cumulative event counts over time for a utilization threshold has been exceeded. Commodities originally on link $2-4$ that caused the congestion are rolled back and rescheduled to travel over link $2-3$.



(c) At $t = 6$, the truck capacity threshold of 80% at link $2-4$ is exceeded. In this case, optimal paths were not recomputed.



(d) The per-link capacity utilization after recomputing optimal paths at $t = 6$ when the capacity utilization threshold of link $2-4$ was exceeded.

Figure 5: Cumulative commodity flows and capacity utilization computed by the coupled simulation/optimizer when run on Figure 4's transportation network.

such as percentage of servers used at any one point in time or the number of trucks queued (including spillover). In contrast, the optimizer cannot compute the resource utilization at any point in time, only that they are used within a given set of constraints. The optimizer, however, can compute the optimal schedule by which goods should be routed within capacity and time constraints. For example, a certain set of containers can arrive in the system no earlier than EAT_{k_u} and be delivered to its destination no later than LDT_{k_u}. The simulator cannot compute the optimality of paths taken. As such, we believe integrating an optimization with simulation provides a way to get the benefits of optimal routing as resource availability evolves within the simulation due to increased traffic flows, disruptions, or even mitigation or response actions. Such tools could be useful for developing mitigation and response plans in terms of quantifiable, capability targets as defined within DHS' *Threat and Hazard Identification and Risk Assessment (THIRA)* framework.

Shipping ports are a nexus of critical infrastucture. Within a small geographic region multimodal transportation systems intersect with increasingly automated shipping port operations. Given that environmental conditions as well as the capabilities of intelligent adversaries are increasing, stakeholders at local ports and regional AMSCs need the ability to develop and evaluate their security plans against the possibility of cyber-physical disruptions. This paper describes a coupling that allows practitioners to understand how cyber-physical disruptions affect the flow of commodities through the MTS (via a simulator) while simultaneously helping them to design security plans around optimal responses to such disruptions (via an optimizer). Such a capability is essential given the degree to which modern commerce depends upon the efficient and resilient operation of shipping ports.

ACKNOWLEDGMENTS

The material presented in this paper is based upon work supported in part by the U.S. Department of Homeland Security under Grant Award Number, 2015-ST-061-CIRC01 as well as the Herman M. Dieckamp Post-Doctoral Fellowship. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

REFERENCES

Associates, M. 2015. "The 2014 National Economic Impact of The U.S. Coastal Port System". Technical report, American Association for Port Authorities.

Banks, J., J. S. Carson, B. L. Nelson, and D. M. Nicol. 2010. *Discrete-Event System Simulation*. Fifth ed. Prentice Hall.

Beaumont, P., and S. Wolthusen. 2017. "Cyber-risks in maritime container terminals: Analysis of threats and simulation of impacts".

Beyeler, W. E., S. H. Conrad, T. F. Corbet, G. P. O'Reilly, and D. D. Picklesimer. 2004. "Inter-infrastructure modelingPorts and telecommunications". *Bell Labs Technical Journal* 9(2):91–105.

Bou-Harb, E., E. I. Kaisar, and M. Austin. 2017. "On the impact of empirical attack models targeting marine transportation". In *Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 5th IEEE International Conference on*, 200–205. IEEE.

Broman, D., L. Greenberg, E. A. Lee, M. Masin, S. Tripakis, and M. Wetter. 2015. "Requirements for hybrid cosimulation standards". In *Proceedings of the 18th International Conference on Hybrid Systems Computation and Control - HSCC '15*, 179–188.

Cimino, M. G., F. Palumbo, G. Vaglini, E. Ferro, N. Celandroni, and D. La Rosa. 2017. "Evaluating the impact of smart technologies on harbors logistics via BPMN modeling and simulation". *Information Technology and Management* 18(3):223–239.

DHS 2013. "National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience".

DHS. 2017. "Emerging Systems at Automated Container Terminals". Technical report, Department of Homeland Security NPPD OCIA.

DiRenzo, J., N. K. Drumhiller, and F. S. Roberts. 2017. *Issues in Maritime Cyber Security*. Westphalia Press.

Ekelhart, A., E. Kiesling, B. Grill, C. Strauss, and C. Stummer. 2015. "Integrating attacker behavior in IT security analysis: a discrete-event simulation approach". *Information Technology and Management* 16(3):221–233.

Franqueira, V. N., R. H. Lopes, and P. Van Eck. 2009. "Multi-step attack modelling and simulation (MsAMS) framework based on mobile ambients". In *Proceedings of the 2009 ACM symposium on Applied Computing*, 66–73. ACM.

Gomes, C., C. Thule, D. Broman, P. G. Larsen, and H. Vangheluwe. 2017. "Co-simulation: State of the art". *arXiv preprint arXiv:1702.00686*.

Gu, B., and H. H. Asada. 2004. "Co-simulation of algebraically coupled dynamic subsystems without disclosure of proprietary subsystem models". *Journal of dynamic systems, measurement, and control* 126(1):1–13.

Guo, L., Q. Zhu, P. Nuzzo, R. Passerone, A. Sangiovanni-Vincentelli, and E. A. Lee. 2014. "Metronomy: a function-architecture co-simulation framework for timing verification of cyber-physical systems". In *Proceedings of the 2014 International Conference on Hardware/Software Codesign and System Synthesis*, 24. ACM.

Gurobi Optimization, I. 2015. "Gurobi optimizer reference manual". *URL http://www. gurobi. com*.

Kalmar-Nagy, T., and I. Stanciulescu. 2014. "Can complex systems really be simulated?". *Applied Mathematics and Computation* 227:199–211.

Kotenko, I. 2014. "Multi-agent simulation of attacks and defense mechanisms in computer networks". *International Journal of Computing* 7(2):35–43.

Martins, J. R., and A. B. Lambe. 2013. "Multidisciplinary design optimization: a survey of architectures". *AIAA journal*.

National Institute of Standards and Technology (NIST). 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology (NIST).

Ni, Y., and J. F. Broenink. 2012. "Hybrid systems modelling and simulation in DESTECS: A co-simulation approach". *The 2012 European simulation and modelling conference*:32–36.

Obama, B. 2013. "Presidential policy directive 21: Critical infrastructure security and resilience". *Washington, DC*.

Order, E. 2013. "13636–Improving Critical Infrastructure Cybersecurity". *Federal Register* 78(33):11739.

Qu, Y., and X. Zhou. 2017. "Large-scale dynamic transportation network simulation: A space-time-event parallel computing approach". *Transportation research part c: Emerging technologies* 75:1–16.

Schweizer, B., and D. Lu. 2015. "Predictor/corrector co-simulation approaches for solver coupling with algebraic constraints". *ZAMM Zeitschrift fur Angewandte Mathematik und Mechanik* 95(9):911–938.

Sholander, P. E., J. L. Darby, J. M. Phelan, B. Smith, G. D. Wyss, A. Walter, G. B. Varnado, and J. M. Depoy. 2006. "Critical infrastructure systems of systems assessment methodology.". Technical report, Sandia National Laboratories.

Tien, I. 2017. "Bayesian network methods for modeling and reliability assessment of infrastructure systems". In *Risk and Reliability Analysis: Theory and Applications*, 417–452. Springer.

Toutonji, O. A., S.-M. Yoo, and M. Park. 2012. "Stability analysis of VEISV propagation modeling for network worm attack". *Applied Mathematical Modelling* 36(6):2751–2761.

Wagner, N., R. Lippmann, M. Winterrose, J. Riordan, T. Yu, and W. W. Streilein. 2015. "Agent-based simulation for assessing network security risk due to unauthorized hardware". In *Proceedings of the Symposium on Agent-Directed Simulation*, 18–26. Society for Computer Simulation International.

Wang, B., and J. S. Baras. 2013. "HybridSim: A modeling and co-simulation toolchain for cyber-physical systems". In *Proceedings - IEEE International Symposium on Distributed Simulation and Real-Time Applications*, 33–40.

Yi, T., L. Feng, W. Qi, C. Bin, and N. Ming. 2016. "Overview of the co-simulation methods for power and communication system". In *Real-time Computing and Robotics (RCAR), IEEE International Conference on*, 94–98. IEEE.

Zhu, M., X. Fan, H. Cheng, and Q. He. 2010. "Modeling and Simulation of Automated Container Terminal Operation.". *JCP* 5(6):951–957.

Zukunft, A. 2015. "United States Coast Guard Cyber Strategy". Retrieved on November 27, 2017 from http://www.overview.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf?ver=2016-10-13-122915-863.

AUTHOR BIOGRAPHIES

GABRIEL A. WEAVER is a Research Scientist at the Information Trust Institute at the University of Illinois at Urbana-Champaign. Currenly, Weaver is PI on a project via the *Critical Infrastructure Resilience Institute (CIRI)* to look at the economic impacts of cascading disruptions to shipping port infrastructure. Weaver holds a Ph.D from Dartmouth College and a B.A. in Classics and Mathematics, with a minor in Computer Science from the College of the Holy Cross. His email address is gweaver@illinois.edu.

LAVANYA MARLA received her PhD in Transportation Systems from the Massachusetts Institute of Technology, MS in Operations Research and Transportation from MIT, and a Bachelor of Technology from the Indian Institute of Technology, Madras. She is currently an assistant professor in the department of Industrial and Enterprise Systems Engineering at the University of Illinois at Urbana-Champaign. Prior to this, she was a Systems Scientist with the iLab Mobility Analytics group in the Heinz College at Carnegie Mellon University. Her research interests include robust resource allocation for large-scale systems, data-driven large-scale optimization with machine learning, real-time reconfigurability of networks, decision-making under uncertainty, and multi-agent systems; with applications in airline, logistics, emergency management and shared transportation systems. Her email address is lavanyam@illinois.edu.