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

AN AGENT-BASED SIMULATION FRAMEWORK FOR SUPPLY CHAIN DISRUPTIONS AND FACILITY FORTIFICATION

Xueping Li
Rodney Kizito

Department of Industrial and Systems Engineering
University of Tennessee
Knoxville, TN 37996, USA

Taynara I. Paula

Institute of Industrial Engineering and Management
Federal University of Itajubá
Itajubá, MG 37500-903, BRAZIL

ABSTRACT

Fortifying facilities within a supply chain network can mitigate facility failures caused by disruptions. In this study we build an agent-based simulation model to study the *r*-interdiction median problem with fortification (RIMF), considering two types of facility disruptions: naturally-caused and human-caused disruptions. The objective of this study is to develop a simulation model that analyzes facility disruption and fortification as a repeated Stackelberg competition, where fortification decisions are made anticipating disruptions. The most important facilities - those with the largest demand coverage - are fortified, while the next most important facilities - those not fortified due to fortification resource limitations - are successfully disrupted. In addition, the study provides event-by-event updates of the fortifying, disrupting, and recovering processes, as well as how these events affect the total network cost over the course of the simulation; thus paves the way for a future study on how to make optimal fortification decisions.

1 INTRODUCTION

Facilities within supply chain networks are vulnerable to natural and human-caused disruptions. These disruptions can cause facility failure, leading to severe consequences for the overall supply chain network. Among the types of disruptions that may occur are random naturally-caused attacks (floods, hurricanes, earthquakes, etc.) and human-caused attacks (cyber-attacks, terrorist strikes, etc.). Disruptions can be extremely costly due to the effects they have on production time and incurred transportation costs. In this study, incurred transportation costs occur when a distributor (facility) fails as the result of a disruption. The demand points covered by the failed facility are re-assigned to the closest, in terms of distance, currently operational distributor within the network leading to incurred transportation costs.

To mitigate the risk of disruptions, facilities are fortified in a manner that negates failure from human-caused attacks; however, naturally-caused attacks can not be negated by fortification. Examples of fortification resources against human-caused attacks are advanced facility security systems, enhanced malware protections software, elaborate forts around facilities, etc. The *r*-interdiction median problem with fortification (RIMF) (Church and Scaparra 2007) assumes that a network of P operating facilities has enough resources to protect Q of the P facilities, in order to anticipate worst-case losses when R of the P facilities fail due to disruptions. The objective of this study is to develop an agent-based simulation model to simulate a repeated Stackelberg competition between the fortifying of the most important facilities against disruptions, thus anticipating worst-case losses, and experiencing successful disruptions to the next most important facilities which are not fortified. The simulation is performed for a 10-year duration. The following section provides background to this study.

2 BACKGROUND

This section provides some background to this study. The model is developed to analyze supply chain disruptions and this section provides an explanation on what disruptions are and the impact disruptions have on supply chains. The Stackelberg competition, which the model in this study imitates, is explained. In addition, the p-median problem and RIMF model are detailed, and are used in this study to establish which facilities serve as distributors and which distributors are fortified respectively.

2.1 Supply Chain Disruptions

According to Snyder et al. (2016), disruptions are unexpected events that cause a supplier or other elements within a supply chain to stop functioning, completely or partially, for a certain amount of time. For example, when a disruption affects a supplier, the supplier cannot provide any goods during the disruption period. Such a situation can cause economic losses for a company and must thus be prevented or reduced in terms of occurrence probability. Supply chain disruptions exist as long as supply chains are present, but according to Snyder et al. (2016), the interest in this subject has increased in the past decade due to four main reasons: (1) several high profile events, such as the terrorist attacks of September 11 in 2001, the west-coast port lockout in 2002 and hurricane Katrina in 2005, that brought disruptions to public attention; (2) the vulnerability to disruptions of the just-in-time (JIT) philosophy; (3) the global growth of supply chains, in which suppliers are located in politically or economically unstable regions making them increasingly prone to human-caused disruptions; (4) the critical momentum the topic has gained in academia and industry.

The impact of facility disruptions should be taken into account during the initial design of a network. However, relocating facilities, changing suppliers, or reconfiguring networks can lead to many expenses. An alternative is to enhance the reliability of existing network infrastructure through efficient investments in protection and security measures Snyder et al. (2006); these protection and security measures serve as the fortification resources in this study. Choosing which facilities within a network should be protected (fortified) has led researchers to develop various fortification models.

2.2 Stackelberg Competition

Stackelberg (Von Stackelberg 1952) introduced the leader-follower game: a static two-level optimization model where one player acts as a leader and the rest act as followers. In such games, the objective is to find an optimal strategy for the leader, assuming the followers will react to the leader's actions in such a rational way that they can optimize their own objective functions (Nie and Zhang 2008). Network interdiction problems can be treated as a leader-follower game, where the leader tries to disrupt the network through interdictions and the follower then attempts to maximize flow or minimize transportation costs within the resulting disrupted network Snyder et al. (2016).

2.3 Fortification Models

The RIMF model serves as the baseline fortification model Zhang et al. (2018). RIMF addresses the option of fortifying the most important infrastructures against worst-case interdiction Gong et al. (2016). The model is based upon the classic p-median problem and assumes that the efficiency of the network is measured in terms of accessibility or service provision costs (Scaparra and Church 2008). Sections 2.3.1 and 2.3.2 describe the p-median and the RIMF problems respectively.

2.3.1 P-median Problem

The p-median problem is a classic facility location problem that focuses on optimizing facilities chosen as "open" within a network, while minimizing the total distance traveled in the network. Given a network of demand points, P number of facilities are open from all potential facilities. Let $I = \{1...a\}$, where a is the total number of potential facilities in the network. Let $J = \{1...b\}$ where b is the total number of

demand points in the network. Let $C = [c_{ij}]$ be an $a \times b$ matrix of transportation costs from a potentially open facility i to a demand point j in the network; the distances between the potentially open facilities and the demand points serve as the transportation costs in the $a \times b$ distance matrix. The objective of the p-median problem is to locate P facilities to open that minimize the transportation cost (weighted distance) between demand points and the nearest selected facilities (Daskin and Maass 2015). Let x_{ij} and y_i denote binary decision variables defined as follows:

$$x_{ij} = \begin{cases} 1 & \text{if the facility at } i \text{ is assigned to meet the demand at } j \\ 0 & \text{otherwise} \end{cases}$$

$$y_i = \begin{cases} 1 & \text{if a facility located at } i \text{ is open} \\ 0 & \text{otherwise} \end{cases}$$

The complete p-median problem is modeled as follows:

$$\text{Minimize} \quad \sum_{i \in I} \sum_{j \in J} c_{ij} x_{ij} \tag{1}$$

$$\text{Subject to:} \quad \sum_{i \in I} x_{ij} = 1, j \in J \tag{2}$$

$$\sum_{i \in I} y_i = P \tag{3}$$

$$x_{ij} \leq y_i, i \in I, j \in J \tag{4}$$

$$x_{ij} \in \{0,1\}, i \in I, j \in J \tag{5}$$

$$y_i \leq y_i, i \in I \tag{6}$$

where the objective function (1) minimizes the total cost. Constraint (2) ensures that all demand point within the network are assigned to an open facility. Constraint (3) ensures that there are exactly P facilities open within the network. Constraint (4) ensures that demand points are only assigned to one of the P opened facilities. Constraints (5) and (6) ensures the decision variables are binary. The opened P facilities serve as the distributors within the network. The most important of these P facilities are fortified.

The p-median problem has been largely used in application settings where optimizing consumer access to supply centers is the primary objective. However, if some of the facilities suffer any kind of disruption, customers will have to receive shipments from facilities that are further away, which can have costly implications (Scaparra and Church 2008). In order to reduce the impact of disruptions, Church and Scaparra (2007) proposed the r-interdiction median problem with fortification.

2.3.2 RIMF Model

RIMF is an integer-linear programming model that identifies the most effective way of allocating protective resources among the facilities of an existing but vulnerable network. The objective is to minimize the impact of the most disruptive attack to the R unprotected facilities (Scaparra and Church 2008).

According to Scaparra and Church (2008), the RIMF can be seen as a game involving sequential decisions of two players: (1) a facility planner, the "defender" in the game, first decides which Q facilities to fortify so that the network operates as efficiently as possible in case of interdiction; (2) an interdictor, the "attacker" in the game, then attempts to reduce the network's efficiency as much as possible by hitting R unprotected facilities. The RIMF assumes that the network defender has resources to protect Q facilities, whereas the interdictor has resources to attack up to R facilities, where $Q+R \leq P$. The following interdiction and assignment variables are used in the RIMF model, where Z_j and S_j represent the upper level fortification

and the lower-lever interdiction variables respectively, and Y_{ij} represents user choices Snyder et al. (2006), Scaparra and Church (2008).

$$Z_j = \begin{cases} 1 & \text{if a facility located at } j \text{ is fortified} \\ 0 & \text{otherwise} \end{cases}$$

$$S_j = \begin{cases} 1 & \text{if the facility located at } j \text{ is fails due to interdiction} \\ 0 & \text{otherwise} \end{cases}$$

$$Y_{ij} = \begin{cases} 1 & \text{if the demand at } i \text{ is assigned to a facility at } j \\ 0 & \text{otherwise} \end{cases}$$

In addition, the formulation uses the set $T_{ij} = \{k \in J | d_{ik} > d_{ij}\}$, that is defined for each customer i and facility j, and represents the set of existing sites (excluding j) that are farther than j is from i; d represents the distance. Thus, the RIMF can then be modeled as follows Snyder et al. (2006):

$$\text{Minimize} \quad H(\mathbf{z}) = \max \quad \sum_{i \in I} \sum_{j \in J} h_i d_{ij} Y_{ij} \tag{7}$$

$$\text{Subject to:} \quad \sum_{j \in J} Z_j = Q, \quad Z_j \in \{0,1\} \quad \forall j \in J \tag{8}$$

$$\sum_{j \in J} Y_{ij} = 1 \quad \forall i \in I \tag{9}$$

$$\sum_{j \in J} S_j = R \tag{10}$$

$$\sum_{h \in T_{ij}} Y_{ih} \leq S_j \quad \forall i \in I,\ j \in J \tag{11}$$

$$S_j \leq 1 - Z_j \quad \forall j \in J \tag{12}$$

$$S_j \in \{0,1\} \quad \forall j \in J \tag{13}$$

$$Y_{ij} \in \{0,1\} \quad \forall i \in I,\ j \in J \tag{14}$$

There are exactly Q fortification resources allocated (8) to minimize the highest possible level of weighted distances (transportation costs) - represented by H in Eq. (7) - caused by the loss of R of the P facilities. h_i is a measure of demand at i in Eq. (7). Constraint (9) ensures that each demand point is assigned to a facility after interdiction; (10) ensures that only R facilities can be interdicted; (11) guarantees that each demand point is assigned to the closest open facility after interdiction; (12) prevents the interdiction of a protected (fortified) facility; (13) and (14) represents the binary requirements for the interdiction and assignment variables respectively. An interdiction in RIMF equates to a disruption and an open facility equates to a distributor in this study. Interdiction can only occur on the opened facilities within the network in this study. The following section defines the problem this study addresses.

3 PROBLEM DEFINITION

This section defines the problem in this study. The supply chain network used in the model, as well as how p-median problem is used to help develop the network, is described. The disruptions, fortification and recovery aspects of the model are also described.

3.1 Supply Chain Network

The p-median problem is used as the base of the supply chain network design in this study. Given a total number of demand points $I = \{1,2,\ldots,i\}$ in a supply chain network, the objective is to choose $P = \{1,2,\ldots,j\}$ of these points to open as distributors within the network. The p-median problem is used to select these P distributors. Each demand point I has a demand $D = \{d_{11},d_{12},\ldots,d_{ij}\}$ that is supplied by a selected distributor. Each distance from a demand point to a selected distributor has a transport cost of C, where $C = \{c_{11},c_{12},\ldots,c_{ij}\}$.

3.2 Disruptions: Human and Naturally-caused Attacks

The human-caused attacks are represented as $A = \{a_1,a_2,\ldots,a_l\}$, where $l =$ total number of human-caused attack over the simulation period. These attacks happen at occurrences $O = \{o_1,o_2,\ldots,o_v\}$ where v denotes the total number of human-caused attack occurrences over the entire simulation period. Moreover, the attack occurrences have exponentially distributed interarrival times, with mean λ_1, between each occurrence. In addition, the number of human-caused attacks A that happen at each attack occurrence O are discrete uniformly distributed. Human-caused attacks target the distributors that would cause the most damage to the network if failed. Targeted distributors that are fortified are protected against the human-caused attacks, while targeted distributors that are not fortified are disrupted (fail) as a result of the human-caused attacks. The damage is determined by the total incurred transportation costs, which occur as a result of re-assigning demand points covered from each failed distributor to the closest distributor that is still operational. This study assumes a human-caused attack leads to total disruption (failure) of the distributor and does not consider severity levels of the attack.

N total naturally-caused (random) attacks occur over the duration of the simulation period. Naturally-caused attacks target the distributors randomly and occur with exponentially distributed interarrival times, with mean λ_2, between each attack. Naturally-caused attacks are unaffected by fortification and will always result in a failure of the targeted distributor. We make such an assumption to account for situations such as hurricanes that are "non-avoidable". The exponential distribution is used for both types of attack occurrences due to its memoryless property, thus every attack instance has the same distribution regardless of how much time has passed.

3.3 Distributor Fortification

The RIMF problem is used to decide the fortification of distributors in this study. Given a limit of K fortification resources, Q of the P distributors are chosen for fortification. The choice of which distributors are fortified depends on which fortified group of distributors minimizes the total damage to the network if the distributors were to fail due to human-caused attacks. We assume fortification has a 95% success rate. In addition, the RIMF problem in this study assumes the following: (1) one fortification resource is given to one distributor and thus $K = Q$; (2) fortification only protects against human-caused attacks; (3) the total number of fortified distributors is less than the number of open distributors $Q < P$; (4) the number of available fortification resources is equal to the minimum number of possible human-caused attacks at each attack occurrence. In addition, this study assumes there is no cost for fortification resources, and that fortification resources and fortified distributors are reset after each human-caused attack occurrence.

3.4 Distributor Recovery

Following a disruption (failure) by a human or naturally-caused attack, a distributor can be down for a certain period, e.g., uniformly distributed 1-4 months. After the down period, distributors are able to recover. The recovery of a failed distributor takes a certain time, e.g., a uniformly distributed time between 1 and 8 months; this recovery period occurs immediately following the down period. Overall, a failed distributor can be non-operational (down period + recovery time) for a duration of time, e.g., 2-12 months

before returning to an operational state. During the non-operational period, the demand previously assigned to the distributor is re-assigned to the closest open distributor within the network that is operational. Once a distributor has recovered, its originally assigned demand is re-assigned to the distributor as was in the initial network. The following section explains the configuration of the simulation model.

4 SIMULATION CONFIGURATION

The analysis starts with solving the p-median problem. A dataset that includes 100 demand points within the continental United States is utilized. The dataset provides the longitude and latitude coordinates of each point, as well the demand for each point. From these potential points, $P = 20$ are established as the distributors within the network. A distance matrix is then created and represents the transportation costs for the $a \times b$ matrix C. The solution to the p-median problem yielded the locations (longitude and latitude) of the P distributors for the network, the demand points assigned to each distributor and the total demand covered by each distributor. The total demand covered is a summation of the demand from each demand point assigned to the distributor, including the demand of the distributor itself.

An initial network is developed using a dataset of 100 demand points (defined as customers in the analysis) and 20 distributors. The AnyLogic simulation software is used. The GIS location map feature of AnyLogic is used for the locating of the customers and distributors based of longitude and latitude coordinates. Figure 1 displays the network as it appears in the GIS feature on the Unites States map. The red items represent the distributors, the teal items represent the customers, and the blue lines represent the distance from distributor to customer as computed in the distance matrix C.

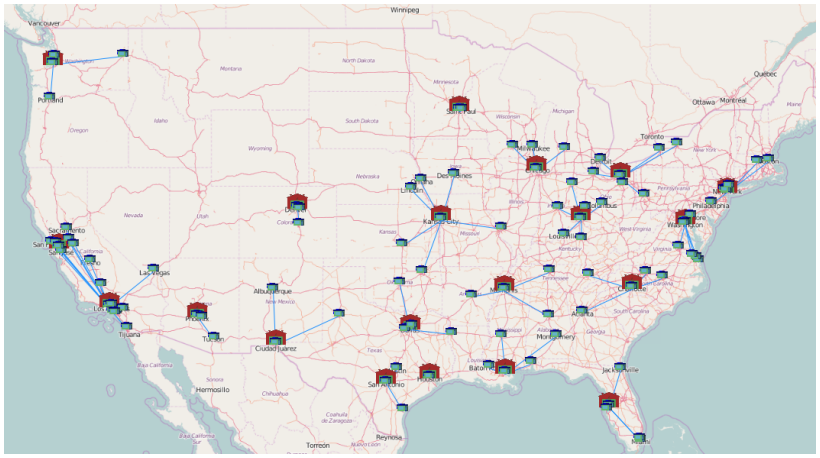

Figure 1: An initial state of the supply chain network.

4.1 Model Agents

The proposed simulation model is created using agent-based modeling. Several model components such as functions, events, and a state chart are incorporated to ensure the model executes accurately. Events are used to schedule actions within the model. A state-charts defines the behavior of events and assigns transitions between different statuses/states of the model's agents.

4.1.1 Main Agent

The main agent of the model contains all components of the model such as other agents, functions, events, parameters and data/statistics. The main agent serves as the entry point of an AnyLogic model, which connects all other components of the model. Figure 2 displays the components of the main agent, noted by the underlined *Main* text. The "*customers*" agent represents the the population of demand points

within the network and the "*distributors*" agent represents the population of distributor facilities within the network. The main agent contains the five functions of the model: (1) "*setDistributor*" assigns an initial distributor to each customer based on distance proximity and re-assigns customers if the distributor fails; (2) "*getImportanceScore*" determines how important each distributor is to the network by summing the total customer demand covered by a distributor; (3) "*getTransportationCost*" determines the cost for a distributor to supply a customer based on the distance between the distributor and customer points; (4) "*fortifyImportant*" ensures that the most important distributors are fortified against human-caused attacks; (5) "*attackImportant*" ensures that human-caused attacks target the most important distributors within the network. The main agent also contains the 3 events that occur in the model: (1) "*fortifydistributor*" initiates the fortification process and limits the number of fortification resources available; (2) "*startNaturalAttacking*" initiates the naturally-caused attacks and ensures these attacks randomly target the distributors; (3) "*startAttacking*" initiates the human-caused attacks and ensures the number attacks per occurrence are discrete uniformly distributed. The "*TransportationCost*", a statistic of the model, computes the total transportation cost of the network throughout the simulation's duration.[6pt]

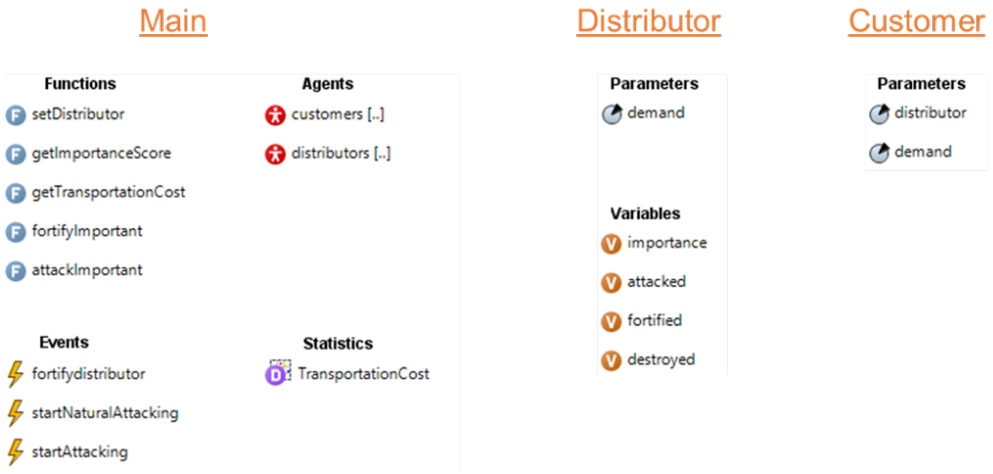

Figure 2: Main, Distributor and Customer agent components.

4.1.2 Customer Agent

The customer agent contains a population of 100 customers and is defined in the GIS environment according to the latitudes and longitudes of the dataset; AnyLogic allows for creation of a single or population of customers under one customer agent. Figure 2 displays the components of the customer agent, noted by the underlined *Customer* text. This agent has two parameters: "*distributor*" and "*demand*"; parameters are characteristics of an agent in AnyLogic. The "*distributor*" parameter is used to define which distributors will be responsible for supplying the customers. These distributors are the chosen $P = 20$ from the p-median problem. The "*demand*" parameter indicates the demand requirements for each customer.

4.1.3 Distributor Agent

The distributor agent contains a population of 20 distributors and is defined in the GIS environment according to the p-median problem; AnyLogic allows for creation of a single or population of distributors under one distributor agent. Figure 2 displays the components of the distributor agent, noted by the underlined *Distributor* text. This agent has a "*demand*" parameter, 4 variables, and a state chart. The "*demand*" parameter indicates how much demand each distributor is responsible for within the network; this is the total of all demand from the demand points assigned to a distributor. The "*importance*" variable is used to compute the importance of a distributor, which is determined based on the the total demand the distributor is

responsible for within the network; the more demand a distributor is responsible for, the more important the distributor. Human-caused attacks target the most important distributors because such distributors failing causes the most damage to the network. The "*attacked*" variable is a boolean variable, where TRUE signifies that the distributor was targeted by a human-caused attack and FALSE if the distributor was not targeted. Similarly, the "*fortified*" and "*destroyed*" variables are also boolean. A TRUE signifies that the distributor was successfully fortified/defended against a human-caused attack and FALSE if the fortification was not successful for the "*fortified*" variable; fortification has a 95% success rate, meaning the "*fortified*" variable will result in a TRUE - distributor is fortified/defended from the targeted human-caused attack - 95% of the time. A TRUE signifies the distributor was successfully hit/destroyed by a human-caused attack and FALSE otherwise for the "*destroyed*" variable. As displayed in the state chart in figure 3, a distributor can have 4 different statuses/states: *Working*, *Defended*, *Destroyed* and *Recovering*.

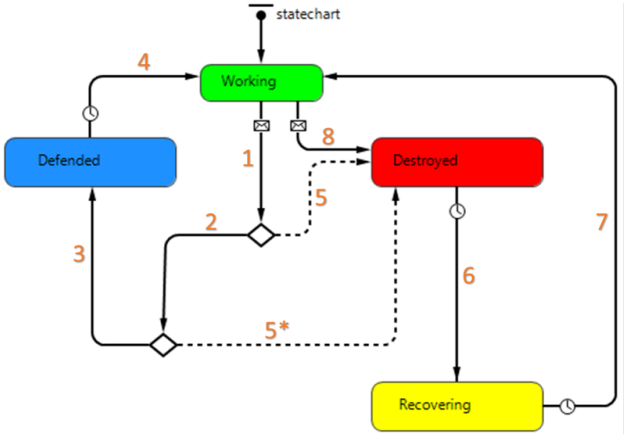

Figure 3: Distributor agent State-chart.

All distributors begin as *Working*. When a human-caused attack targets a distributor (indicated as '1' on state chart), the distributor can transition to the *Defended* state or the *Destroyed* state depending on the condition of the "*fortified*" variable. If the "*fortified*" variable is TRUE (indicated as '2' on state chart) for that attacked distributor, then the distributor transitions to the *Defended* state (indicated as '3' on state chart) and transitions back to the original *Working* state (indicated as '4' on state chart). If the "*fortified*" variable is FALSE (indicated as '5' on state chart) for that attacked distributor, then the distributor transitions to the *Destroyed* state for the down period. Since fortification has a 95% success rate for TRUE, if fortification fails then the distributor transitions to the *Destroyed* state (indicated as '5*' on state chart). From the *Destroyed* state, the distributor transitions to the *Recovering* state after the 1-4 month down period (indicated as '6' on state chart). From the *Recovering* state, the distributor transitions back to the *Working* state after the 1-8 month recovery period and the network is reset to account for the re-opened distributor (indicated as '7' on state chart). If the attack was naturally-caused, then the distributor transitions to the *Destroyed* state (indicated as '8' on state chart) since fortification does not effect naturally-caused attacks.

4.2 Simulation Description

The simulation model is created to demonstrate the problem over a 10-year duration. The model is created using the AnyLogic software. The network displayed in figure 1 remains as displayed until the first attack occurrence. When this attack occurrence happens, there are 3 fortification resources utilized to protect the most important distributors; these are the distributors the attacker will target by logic of the model. The attack occurs with a discrete uniformly distributed number of human-caused attacks with a minimum of 3 and a maximum of 8 human-caused attacks. One of two scenarios can thus occur.

4.2.1 Scenario 1

The number of human-caused attacks from the attack occurrence is 3. In this scenario, the 3 targeted distributors, which would be the most important 3, would all be fortified and protected from the attack. No damages are experienced by the network in this scenario unless a naturally-caused attack also occurs in the same moment. Fortification only protects against human-caused attacks, so if a naturally-caused attack was to randomly occur at the same moment as the human-caused attack, the distributor targeted by the naturally-caused attack would thus be disrupted (fail) and the network would re-assign the customer demand covered by the disrupted distributor in a manner that minimizes the incurred transportation costs.

The naturally disrupted distributor, if any, will recover based on the recovery time frame. If another attack occurrence of 3 human-caused attacks happens, then the same fortification process described will repeat. If another naturally-caused attack happens while the previously naturally disrupted distributor is still down, then another currently operating distributor will be randomly targeted and naturally disrupted.

4.2.2 Scenario 2

The number of human-caused attacks at the attack occurrence is greater than a certain threshold, e.g., 3. In this scenario, if the number of human-caused attacks equals 4, then the 3 most important distributors will be fortified and protected from the attack but the 4^{th} most important distributors would be disrupted. If the number of human-caused attacks equal 5, then the 4^{th} and 5^{th} most import distributors would both be disrupted, and so on. Similar to scenario 1, the network would then re-assign the customer demand covered by the disrupted distributor(s) in a manner that minimizes the incurred transportation costs. The naturally-caused attack effects are as described in scenario 1 in the case a naturally-caused attack is to also occur in the same moment as the human-caused attacks. The naturally disrupted distributor, if any, will follow the same recovery process as described in scenario 1. The distributor(s) disrupted by the human-caused attacks will recover based on the same time frame as the naturally disrupted. If another attack occurrence with ≥ 4 human-caused attacks happens while the distributor(s) disrupted by the human-caused attacks are still down, then 1 (if 4 human-caused attacks) or 2 (if 5 human-caused attacks), and so on, distributor(s) will go down from those currently operating; 3 distributors will again be fortified from the other 3 human-caused attacks. The attacks will again target the most important distributors in the network, excluding the currently down (disrupted) distributors from the previous attack occurrence. The following section presents and discusses the results of the simulation.

5 RESULTS AND DISCUSSION

We provide a part of the results for the 10-year simulation in Table 1. The "Simulation Period" column indicates the time of an event during the 10-year duration. Results for human-caused attacks and the naturally-caused attacks are both displayed. The time at which the distributors are attacked is provided, as well as the time at which the attacked distributors recover and become operational again. The "Transportation Cost" column indicates the total network cost at the conclusion of each event. Each year begins with the 3 most important, and currently operational, distributors fortified. For example, year 0 begins with distributor 1, 16 and 19 fortified. The limitation of fortification resources ensures that only 3 distributors are fortified. At this point the network has yet to be affected by any disruptions, thus the total cost of the network is at the p-median solution amount of 482241.3. Year 0 has 1 naturally-caused attack occurrence at the 0.10 mark (January, Year 0) at which distributor 10 is randomly targeted and disrupted. Year 0 has 1 human-caused attack occurrence at the 0.20 mark (February, Year 0) at which 3 human-caused attacks happen. These attacks successfully disrupted (cause to fail) distributors 13, 11 and 7; these distributors were the 4th, 5th and 6th most important distributors within the network at the 0.20 mark. As each of the 4 disrupted distributors are attacked, the total cost of the network increases as seen at the end of the 0.10 and each of the 0.20 marks. Distributor 10 recovers and is operational again at the 0.78 mark (September, Year 0). As a result, the total cost of the network decreases from 770487.8 at 0.20 mark to 675291.2 at

the 0.78 mark. Distributors 11 and 13 recover and become operational again at the 0.81 (September, Year 0) and 0.96 (November, Year 0) mark. As a result, the total cost of the network continues to decrease.

Table 1: An illustration of the results table (partial). The complete table can be visualized in: https://docs.google.com/spreadsheets/d/1Pups3phoacNIgeUo9X1MJ3UkwnJYH-ZbBuowOEec0oI/edit?usp=sharing

Simulation Period	Distributor Status				Transportation Cost
	Fortified	Human-caused Attacked	Naturally-caused Attacked	Recovered	
0.00	1				482241.3
0.00	16				
0.00	19				
0.10			10		577437.9
0.20		13			627069.7
0.20		11			706051.3
0.20		7			770487.8
0.78				10	675291.2
0.81				11	596309.6
0.96				13	546677.8
1.00	1				
1.00	16				
1.00	19				
1.02				7	482241.3
1.10			10		577437.9
1.35		11			656419.5
1.35		7			720856.0
1.44			2		1038745.2
1.64			17		1083445.2
2.00	1				
2.00	4				
2.00	15				
2.09				11	973142.3
2.10				10	874302.9
2.11				7	809866.5
2.61				2	523298.5
2.65		13			576879.0
2.65		7			641315.4
2.65		10			740154.8
2.65		19			820506.6
2.65		16			940371.5
2.80				17	891722.8

Distributor 7 recovers and is operational again at the 1.02 mark (January, Year 1) at which point all previously disrupted distributors within the network are fully operational and the total network cost returns to original amount of 482241.3. Whereas year 0 only experienced 6 human-caused attacks (3 fortified against and 3 successfully disrupting distributors), year 2 experienced 8 that disrupted distributors 13, 7, 10, 19 and 16; the other 3 attacks that targeted distributors 1, 4 and 15 were negated due to fortification. Per the human-caused attack limitations, 8 human-caused attacks are the maximum possible at an attack occurrence. Thus year 2 experienced the maximum possible human-caused attacks. Whereas year 0 experienced only 1 naturally-caused attack, year 1 experienced 3 such attacks at the 1.10 (January, Year 1), 1.44 (May, Year 1)

and 1.64 (July, Year 1) marks. These three attacks randomly targeted distributors 10, 2 and 17 respectively. The total network cost reaches its highest value of 2319076.6 at the 7.42 mark (May, Year 7) due to the 6 attack occurrences and 11 total successful human-caused attacks between the start of year 6 (6.00 mark) and the 7.42 mark. During this period there were 2 naturally-caused attacks as well. By the 7.42 mark, only 5 of the 13 disrupted distributors had recovered, leaving the network with only 12 of its 20 distributors operational. The simulation period concludes at the end year 9 with a total network cost of 1008729.7.

Figure 4 displays the transportation cost over the duration of the simulation. The graph shows increases and decreases in the transportation cost over the simulation duration but does not show a steady single trend. This is due to the uniform distribution of the number of human-caused attacks at each attack occurrence. For a constant increasing trend in transportation cost to occur, the number of human-caused attacks would have to also increase at each attack occurrence, leading to an increase in disrupted distributors each year. If each attack occurrence resembled scenario 1, then the graph would show a constant stable trend for transportation cost because all human-caused attacks would be fortified against. The decreasing intervals on the graph are from years where the transportation cost savings from recovering distributors outweighs the transportation cost increases from disrupted distributors. The spikes seen in year 6 and 8 are representative of the larger than average number of human-caused attacks occurring in those two years. The following section highlights the conclusions reached from this study.

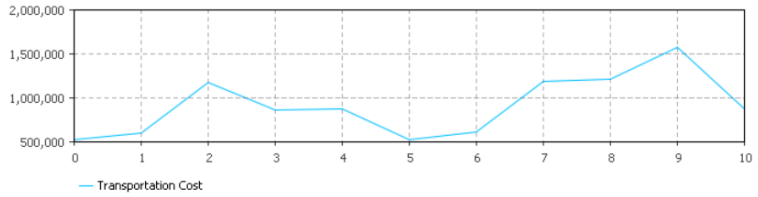

Figure 4: Transportation cost over simulation period.

6 CONCLUSION

This study develops an agent-based simulation model to analyze the effects of facility disruption and fortification on total system costs within a supply chain network. The simulation provides event-by-event updates of fortifying, attacking and recovering processes, as well the affects by such events on total system costs over the 10-year simulation period. The total system cost obtained from the simulation provides insights as to what incurred costs to expect over the simulation period given the occurrence of disruptions within the network, and how fortification can reduce the worst-case losses in such situations. In this study, the "defender" (fortifier) and "attacker" (human-caused disruptions) game follows a repeated Stackelberg competition model, where fortification decisions are made by anticipating disruptions to occur to the most important facilities, while attacks will be successfully carried to the next most important facilities which are not fortified; thus an equilibrium is achieved. This is based on the availability of fortification information to the attackers and the sequential moves by the players. However, in reality, it is much more complicated. First of all, fortification information may not be made public. Secondly, "defenders" and "attackers" may not act sequentially. Moreover, their strategies may change over time. For example, a "defender" may choose to fortify a facility if it has not been attacked for a certain time (thus anticipates an incoming attack) or vice versa. Thirdly, an "attacker" may or may not know the outcome (damage done to the network) of disrupting a certain distributor in advance of targeting the distributor. In addition, this study assumes no fortification cost and instead limits the number fortification resources to the minimum number of human-caused attacks. This study also assumes that all disruptions lead to total failure of a distributor and does not consider disruption severity levels. These assumptions will not be the case in reality as fortification resource costs can greatly effect how many resources the "defender" has available, and severity of disruptions impacts whether a distributor is deemed completely disrupted (failed) or damaged but still operational. A damaged but still operational distributor would not require re-assignment of its covered

demand to another distributor, thus negating incurred transportation costs. These scenarios are notoriously challenging to model and solve through traditional game theory and stochastic programming approaches. Agent-based models seem to be able to tackle these problems, although challenges remain such as how to obtain optimal fortification decision policies through simulation. Future research will be carried out to extend the proposed RIMF simulation framework to address these challenges.

ACKNOWLEDGMENTS

The author (T. I. Paula, Fellow CAPES / PDSE / Process Nº 88881.132477/2016-01) would like to express her gratitude to CAPES for its support to this research.

REFERENCES

Church, R. L., and M. P. Scaparra. 2007. "Protecting Critical Assets: The r-Interdiction Median Problem with Fortification". *Geographical Analysis* 39(2):129–146.

Daskin, M. S., and K. L. Maass. 2015. "The p-Median Problem". In *Location Science*, 21–45. Springer, Cham.

Gong, X., Z. Zheng, and X. Zhang. 2016. "Interdiction and Fortification Problem of Supply System Based on Preferential Attachment". In *2015 Chinese Automation Congress*, 2229–2236. Wuhan, China.

Nie, P. Y., and P. A. Zhang. 2008. "A Note on Stackelberg Games". In *Chinese Control and Decision Conference (CCDC 2008)*, 1201–1203. Yantai, Shandong, China.

Scaparra, M. P., and R. L. Church. 2008. "A Bilevel Mixed-Integer Program for Critical Infrastructure Protection Planning". *Computers and Operations Research* 35(6):1905–1923.

Snyder, L. V., Z. Atan, P. Peng, Y. Rong, A. J. Schmitt, and B. Sinsoysal. 2016. "OR/MS Models for Supply Chain Disruptions: A Review". *IIE Transactions* 48(2):89–109.

Snyder, L. V., M. P. Scaparra, M. S. Daskin, and R. L. Church. 2006. "Planning for Disruptions in Supply Chain Networks". In *Tutorials in Operations Research: Models, Methods, and Applications for Innovative Decision Making*, Chapter 9, 234–257. INFORMS.

Von Stackelberg, H. 1952. *The Theory of the Market Economy*. London: Oxford University Press.

Zhang, X.-y., Z. Zheng, K.-y. Cai, and S. Yang. 2018. "A Fortification Model for Decentralized Supply Systems and Its Solution Algorithms". *IEEE Transactions on Reliability* 67(1):381–400.

AUTHOR BIOGRAPHY

XUEPING LI is an Associate Professor of Industrial and Systems Engineering and the Director of the Ideation Laboratory (iLab) and co-Director of the Health Innovation Technology and Simulation (HITS) Lab at the University of Tennessee - Knoxville. He holds a Ph.D. from Arizona State University. His research areas include complex system modeling, simulation and optimization, information assurance, scheduling, supply chain management, data analytics, and health systems engineering. He is a member of IIE, IEEE, ASEE and INFORMS. His e-mail address is Xueping.Li@utk.edu, and his web address is http://web.utk.edu/ xli27/.

RODNEY M. KIZITO is a Ph.D. student in the department of Industrial and Systems Engineering at the University of Tennessee - Knoxville. He holds an M.S. from the University of Arkansas. His research areas include data analytics, energy system modeling, simulation and optimization. His e-mail address is rkizito@vols.utk.edu.

TAYNARA I. PAULA is a Ph.D. student in the Institute of Industrial Engineering and Management at the Federal University of Itajubá. She holds a M.S. in Industrial Engineering also from the Federal University of Itajubá. Her research areas include multi-objective optimization, design of experiments and multivariate analysis. Her e-mail address is taynaraincerti@gmail.com.