applied sciences

MDPI

Article

# An Epistemic Utility-Theoretic Model in Fortifying Oil-and-Gas Production Networks

**Mustafa Alassad [1], Hamzeh Davarikia [2,*] and Yupo Chan [1]**

[1] Department of Systems Engineering UA at Little Rock, Little Rock, AR 72204, USA; mmalassad@ualr.edu (M.A.); yxchan@ualr.edu (Y.C.)
[2] Department of Engineering and Computer Science, McNeese State University, Lake Charles, LA 70605, USA
* Correspondence: hdavarikia@mcneese.edu

Received: 2 February 2020; Accepted: 29 February 2020; Published: 2 June 2020


**Abstract:** Oil-and-gas networks are systems of pumps and pipelines that are exposed to heterogeneous threats. Accordingly, hardening strategies against malicious attacks are needed in today's geopolitical climate. In this paper, a tri-level leader–follower–operator game is established for determining the optimal fortification tactics to protect the critical assets considering the petroleum firm limited resources. We additionally consider defender options beyond outright fortification including tactics often adapted in the fog of war, such as deception. These are mathematically modeled under shared cognition concepts. The proposed model assumes a trial-and-error learning process to gradually discover effective defense strategies. These strategies may include a network defender projecting false information in the media or on the front lines to deceive the aggressor. The resulting mixed-integer nonlinear programming problem is decomposed into a master problem associated with deception and sub-problem as response strategies. A column-and-constraint generation solution duly takes into account the defender–operator and attacker–operator interactions. Further, linearization techniques are applied to reformulate the problem into a mixed-integer linear problem. Our studies performed on the part of the Iraq oil-and-gas network and computational results verified that the deception concept is much more effective than fortification, where the cost of attackers damages diminished significantly without substantial resources commitment on the part of the defender.

**Keywords:** deception; epistemic utility theory; information value theory

## 1. Introduction

The opposite of fortifying a network is the network interdiction, which in the security sense, has a meaning of destroy, cut, or damage by ground or aerial firepower. The attacker activities are modeled in many studies using a variety of optimization approaches in which the attacker damages the network's assets to stop the network's functionality. For example, in a petroleum network, the most important assets are the production sources, pipelines, pump stations, and so on [1]. Each of these components is critical to the petroleum industry and their safety is still a priority for companies, governments, and host communities. For example, many countries' petroleum networks are under attack, such as Nigeria, Saudi Arabia, the USA, and Canada [2]. The greatest necessity is to model and examine network vulnerability and reliability under terrorist attacks due to network importance, especially when there is a war to destabilize the whole environment [3]. Many reasons would encourage the defender for modeling such as limited resources, prioritizing the network's components based on their capacity, length of pipelines, and the amount of produced oil or natural gas. In this regard, such a model was investigated by Snyder and Daskin [4]. The authors studied a reliable supply chain design to dispatch petroleum products. They developed the network reliability and security plans for a single source and single commodity network. Maximizing survivability and source–sink reliability using a

probabilistic solution discovery algorithm (PSDA) was proposed by [5], whereby PSDA can be readily applied to solve the all-terminal network's reliability allocation problems.

This research aims to apply the leader–follower game theory and shared cognition concepts in a real oil-and-gas infrastructure system. It is often implicitly assumed that game players are aware of the game structure, utility, outcomes, and also aware that other players aware of this. This information is called common knowledge [6] and is subtly distinct from mutual knowledge, which is known just about the state of the game, but not about other players' awareness. Chan [7] suggested a Stackelberg game where the leader (defender) would minimize the operational cost, and the follower (the aggressor) would inflict damage to maximize the operational cost and so on. The Max–Min two-person zero-sum game is one of the classical methods for solving the game theory problems; when playing it out in real-time, an attacker will move first, and the defender will respond by hardening the relevant attacked assets [8,9].

According to Cannon-Bowers and Salas [10], the concept of shared cognition helps to explain the role of information in the team and organizational performance. Many other theories address this concept and are presented within this paper. The central premise of Truth-Default Theory (TDT) is that people tend to believe others and that this "truth-default" is adaptive. TDT highlights contextualized communication content in deception findings over nonverbal performances linked with reaction, arousal, strategic self-presentation, or cognitive effort [11,12]. Deceptive information was investigated by Levine et al. [13], where the authors stated that deceptive information would result in non-availability of precise and comprehensive data at the right time, leading to unproductive process organization, increased project cost, and distribution delay—just the negative attributes that one would like to impart upon an intruder. Social media applications have proposed many deception concepts without formal mathematical modeling [14].

As an oil-and-gas company, the most prominent challenge today is obtaining the most effective strategies for defending the operation network and validate the model results with real-world operations. Aside from outright fortification, disseminating false information for protecting the network is a positive strategy; for example, the company can consider when he is lacking hardening resources, whereby it can at least deceive the attacker into attacking fewer essential facilities. However, in this kind of strategy, we have a lot of questions to answer such as how much false information is required to generate? Which asset appears to be most important? Can we implement an idea of the deception concept to reduce attacker damages? These questions seem to be hard to answer, and we feel that existing research answers them partially. We hope that the lack of resources of deception introduced in this paper could prevent the attacker from the network core facilities. Our research targeted one of the most critical infrastructure networks in Iraq, where a war is ongoing with terrorists such as ISIS, who are burning all infrastructure and government resources. We recognize the many dimensions of gaming beyond outright fortification, including tactics often adapted in the fog of war, such as deception. This is modeled mathematically under the shared cognition concept. In practice, it could be as easy as burning crude oil for building huge smoke and to prevent a pilot's clear vision, where the defender is considered to project false information to deceive the aggressor. In addition, we considered another hardship where there is not enough budget to provide real protection. Our model proposed a model based on the tri-level and bi-level programming concepts, where the defender/attacker/operator and the attacker/defender have a different objective in mind. The defender can deflect the attacker's attention from the significant assets in the network by hardening the oil-and-gas facilities, pump stations, and pipelines.

In this paper, we applied hardening and deception methods under limited resources to minimize network damages. The developed optimization problem has the Mixed-Integer Linear Programming format, in which an efficient solution strategy can be pursed to seek the optimum point. It is essential to estimate the value of hardening as well as that associated with deception strategy, representing new findings not reported in the literature. Cost-saving provides the valuation of our model. By experimenting with the number of hardened facilities and deception, the defender can

see how many of such resources are required to deviate the attacker from the most critical assets. The petroleum firm must find her optimal plan including both of the hardening and deception whereby the attacker will see only one fortification strategy, not separated actions. We also propose measuring the value of deception mathematically during gameplay, which has not done before in the literature. Calculating the amount of saving in dollars is of great importance to the government and companies, who can now adopt judicious, cost-effective steps to prevent malicious attacks based on their valuation.

In summary, the highlights of our contributions are: (1) providing the scientific basis for posturing and deception in terms of shared cognition and epistemic utility functions; (2) quantifying the value of deception in a game-theoretic context; (3) modeling an active defender to limit the attackers intrusions; and (4) implementing them on a real-world petroleum network.

The paper is started with the problem definition. Section 2 will discuss the model formulation and challenges of the leader–follower game theory or the defender–attacker–operator interactions, including implementing the deception concept and production and consumption allocations. Section 3 will explore solutions strategies, which will be executed to assess the validity of the model and the results. Section 4 contains the conclusion which verifies that the model works as intended and that the modeling results agree with available empirical data, followed by recommendations for future work. Appendix A summarizes the model variable notations for the reader's convenience. Appendix B monitors the linearization methods of nonlinear terms within the model.

## 2. Model Formulation

*Tri-Level Defender-Attacker–Operator Problem*

In our tri-level defender-attacker–operator problem, Equations (1)–(13), all parties seek to optimize the transportation cost of the produced crude oil and natural gas liquids (NGL) from the production facilities to the demand nodes. The modeled oil/gas network compromises the pump stations for the crude oil and the direct pipelines for the NGL. Moreover, the limits of production and pipeline capacities are considered. Figure 1 demonstrates the interaction among the players in the tri-level game, wherein the first level problem, Equations (2)–(5), the defender plans the hardening and false information propagation.

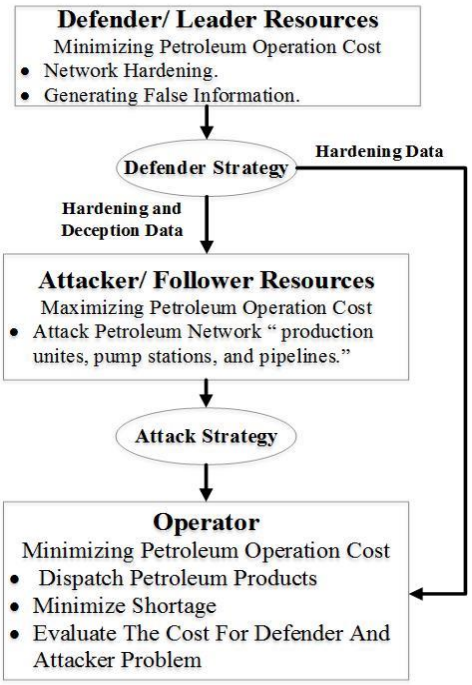


**Figure 1.** Tri-level model presentation; with defender, attacker, and operator interactions.

A distinguishing of the feature of our model is the explicit recognition of the importance information plays in such a competitive game, as shown in our discussions on shared cognition and epistemic knowledge, where such information is generated at the defender model. Specifically, the defender would release some false information, do specific actions, and pretend that information/actions are classified, or are real strategies, by way of posturing or side information. When applied on top of hardening, this strategy can deflect the attacker from its intended target toward a protected target, resulting in depleting the adversary's limited resources without any compromise on the oil/gas network. In the second-level problem, Equations (6)–(8), while the attacker believes in spending resources to elicit intelligence from the defender, he makes his strategies based upon the received data, without knowing that he is buying false information. The model demonstrates the intricate relationship between game and information within the first and second-level of the tri-level problem, namely the leader and follower levels. The defender and attacker employ the third-level operator problem, Equations (9)–(13), for evaluating their strategies, to ensure they optimized their interests, and dispatch their products to the demand points.

The objective function, Equation (1), optimizes the entire system operating cost (OC), including transportation in the first part and the shortage cost in the second part of the equation. The defender and the operator are seeking to minimize the OC with respect to the decision variables in the sets $\boldsymbol{\Gamma}^O$ and $\boldsymbol{\Gamma}^O$, respectively, while the attacker maximizes the OC sought by the decision variables in the set $\boldsymbol{\Gamma}^A$. Note that Appendix A summarizes the model variable notations for the reader's convenience.

$$\min_{\Gamma^D} \max_{\Gamma^A} \min_{\Gamma^O} \left( \sum_{ij,p} C^T_{ijp} x_{ijp} + \sum_{i,p} C^{Sh}_{ijp} U_{ip} \right) \tag{1}$$

Subject to

$$\psi^{DF}_{ij} = \left(\psi^D_{ij} + \psi^F_{ij}\right) - 2\psi^D_{ij}\psi^F_{ij}\ ;\ \forall ij \tag{2}$$

$$\phi^{DF}_{i} = \left(\phi^D_{i} + \phi^F_{i}\right) - 2\phi^D_{i}\phi^F_{i}\ ;\ \forall i \tag{3}$$

$$\sum_{ij} \psi^D_{ij} + \sum_{i} \phi^D_i \le B^D \tag{4}$$

$$\sum_{ij} \psi^F_{ij} + \sum_{i} \phi^F_i \le B^F \tag{5}$$

Subject to

$$\psi^A_{ij} \le 1 - \psi^D_{ij};\ \forall i \tag{6}$$

$$\phi^A_i \le\ 1 - \phi^D_i;\ \forall i \tag{7}$$

$$\sum_{ij} \psi^A_{ij} + \sum_{i} \phi^A_i \le B^A \tag{8}$$

Subject to

$$\sum_{j\in\delta^+(i)} h_{ijp} x_{ijp}\left(1-\psi^A_{ij}\right) - \sum_{j\in\delta^-(i)} h_{jip} x_{jip}\left(1-\psi^A_{ji}\right) = S_{ip} - D_{ip} + U_{ip}\ ;\ \forall i,p\ :\left(\lambda_{ip}\right) \tag{9}$$

$$\sum_{j} x_{ijp} \le v_{ip}\left(1-\phi^A_i\right)\ ;\ \forall i,p\ :\left(\mu^n_{ip}\right) \tag{10}$$

$$0 \le x_{ijp} \le \overline{x_{ijp}}\left(1-\psi^A_{ij}\right)\ ;\ \forall ij,p\ :\left(\mu^a_{ip}\right) \tag{11}$$

$$0 \le S_{ip} \le \overline{S_{ip}}\left(1-\phi^A_i\right)\ ;\ \forall i,p\ :\left(\mu^s_{ip}\right) \tag{12}$$

$$0 \le U_{ip} \le \overline{U_{ip}}\ ;\ \forall i,p\ :\left(\mu_{ip}^{sh}\right) \tag{13}$$

where

$$\Gamma^D = \left\{\psi_{ij}^{DF}, \psi_{ij}^{D}, \psi_{ij}^{F}, \phi_i^{DF}, \phi_i^{D}, \phi_i^{F}\right\},\ \Gamma^A = \left\{\psi_{ij}^{A}, \phi_i^{A}\right\},\ \Gamma^O = \left\{x_{ijp}, U_{ip}, S_{ip}\right\}$$

The deception strategy for the pipelines and nodes is modeled on Constraints (2) and (3) respectively, which allows the defender to pass the true-false information about the hardening strategy to the attacker. Utilizing this kind of posturing is to deceive the attacker with uncertainty. In practice, propagating fake information about the network is reasonable when the defender is suffering from limited defending resources; for example, burning crude oils and creating clouds of smoke. This strategy is very helpful when a pilot is trying to attack. We are not going to dive into detail. Table 1 shows the performance of these equations. For example, in the first two cases, the assets are unprotected ($\psi_{ij}^{D}/\phi_i^{D} = 0$). However, when the defender decides to deceive the attacker, the false information about the protection status of the facilities should equal to ($\psi_{ij}^{F}/\phi_i^{F} = 1$). On the other hand, when ($\psi_{ij}^{F}/\phi_i^{F} = 0$) the attacker will get the true information about the protection plans ($\psi_{ij}^{DF} = \psi_{ij}^{D}$ and $\phi_i^{DF} = \phi_i^{D}$). Constraints (2) and (3) have nonlinear terms that need linearization as illustrated in Appendix B.

**Table 1.** Deception plan for nodes ($i$) and pipelines ($i$, $j$).

| Case No. | $\psi_{ij}^{D}/\phi_i^{D}$ | $\psi_{ij}^{F}/\phi_i^{F}$ | $\psi_{ij}^{DF}/\phi_i^{DF}$ |
|---|---|---|---|
| Case 1 | 0 | 0 | 0 |
| Case 2 | 0 | 1 | 1 |
| Case 3 | 1 | 0 | 1 |
| Case 4 | 1 | 1 | 0 |

Constraints (4) and (5) are used to control the defender fortification and deception resources, respectively. Notice that these resources refer to the number of trials in hardening a facility and the number of trials and posturing gestures in propagating false information to the adversary. We adopt these parametric resources to model the role of information in games based on Epistemic Utility Theory.

Constraint (6) says that if the pipeline is defended, then it is invulnerable ($\psi_{ij}^{D} = 1$), otherwise, the attacker can create damages. Constraint (7) is applicable to nodes. If the node defended ($\phi_i^{D} = 1$), then the attacker cannot interrupt the production or pump station nodes, otherwise, the attacker can stop those nodes. Constraint (8) limits the total adversary resources.

The operator problem evaluates the operation cost based on the defender and the attacker strategies. Constraint (9) is the flow conservation, with the right-hand side accounting for the production at each source $S_{ip}$, total sink demand $D_{ip}$, and the shortage $U_{ip}$. On the left hand side, the network's adjacency matrix handles the flow dispatch within the network, where the binary parameter $h_{jip}$ stands for the existence of the pipeline ($i$, $j$) between nodes $i$ and $j$ that passes the product type $p$, where the model can handle any type of products and in this study it stands for (crude oil or NGL). Constraint (10) bound the total flow passing through a node to be less than the node capacity. Constraints (11)–(13) are to limit the pipeline flow $x_{ijp}$, source production $S_{ip}$, and the shortage $U_{ip}$ from each pipeline and source respectively. The defender and attacker strategies are reflected in Constraints (9)–(12) by multiplying the defender and attacker decision variables to the flow, node capacity, pipeline flow capacity, and source production capacity, respectively. The variables in the parenthesis in front of Constraints (9)–(13) are the dual variables associated with each constraint.

## 3. Solution Strategy

The decomposition approach, along with the column-and-constraint generation (C&CG) method [15], is employed here to solve the proposed tri-level defender-attacker–operator problem. Rahmaniani et al. [16] showed that the Benders Decomposition algorithm has also been applied to

bi-level optimization problems that cannot be transformed via the Karush–Kuhn–Tucker optimality conditions into single-level problems. Snydermaria et al. [17] followed such a procedure for a supply-chain problem and proposed a tri-level model, which is transformed into a bi-level model. To this end, the next subsection describes the formation of the so-called master problem and the sub-problem.

### 3.1. Master Problem

In this section, applying the shared cognition concept on top of hardening strategies against the adversary is considered. In this part, the attacker could spend multiple resources to elicit that information from the defender to inflict the most damage. Meanwhile, the defender is trying to distribute false information that can deflect the attacker from his intended target, resulting in depleting the adversary's limited resources. At the same time, the defender needs to spend some budget on his fortification strategy too. The model demonstrates the shared cognition concept within the first and second-level of the tri-level problem, namely the leader and attacker levels. The model formulates the distribution of false information about the network, including a posturing attack on unprotected nodes and pipelines and misleads the adversary into attacking protected components. This development of the shared cognitions concept in the model is illustrated in the master problem and by the defender–operator interactions as shown in Constraints (14)–(23) and the attacker–operator interactions as shown in Constraints (24)–(37).

The master problem's aim is to generate the fortification plans for defending the network, minimizing the attacker damages, and help the operator to distribute the network flow wisely. The objective function in Equation (14) is to minimize the transportation cost and the shortage cost. The flow variable in the master problem $x_{ijp(v)}$ denotes flow on the arc $(i, j)$ for oil or natural gas extracted from production facilities $S_{ip}$, where it is identified as N1 Reservoir and N2 Reservoir, as shown in Figure 2. As explained before, the defender side has the fortification plans that are implemented by utilizing Constraints (15)–(18). These iterative strategies will handle the hardening and posturing for the entire network's asset in each iteration $(v)$. Constraint (15) demonstrates the hardening and posturing for each pipeline in iteration $(v)$. Constraint (16) is for creating the defense and posturing for production facilities in each iteration $(v)$ , accordingly. Constraints (17) and (18) are to control the leader's fortification and posturing resources through total defending resources $B^D$ and total deception resources $B^F$. Notice once again, these resource budgets refer to the number of trials in hardening a facility and the number of trials in posturing. As will be seen later, these budgets will be studies parametrically. Since the master problem is solved by a number of iterations $(v)$ to diminish the gap between the master-problem lower bound and the sub-problem upper bound, this translates to an increase in the number of the master-problem constraints [2]. Sitting at the top level, the master problem solution from each iteration will be exported to the sub-problem as defense and posturing parameters respectively, see parameters ($\hat{\phi}_i^{DF}$, $\hat{\psi}_{ij}^{DF}$). On the other hand, the master problem will import the attacker strategies as parameters as indicated in the master problem, see parameters ($\hat{\phi}_i^A$, $\hat{\psi}_{ji}^A$), Constraints (19)–(23), associated within the master problem. Constraint (19) is the conservation flow in each iteration $(v)$ associated with the imported adversary binary parameter on pipelines $(\hat{\psi}_{ij}^A)$ from the solution of the sub-problem. The same constraint has a right-hand side accounting for the production at the sources $S_{ip(v)}$, total sink demands $D_{ip(v)}$, and the shortage $U_{ip(v)}$, for each iteration $(v)$, where this constraint will indicate how active the leader is in preventing damages.

$$\min_{\Gamma^M} \left( \sum_{(i,j),p,v} C_{ijp}^T x_{ijp(v)} + \sum_{i,p,v} C_{ijp}^{Sh} U_{ip(v)} \right) \tag{14}$$

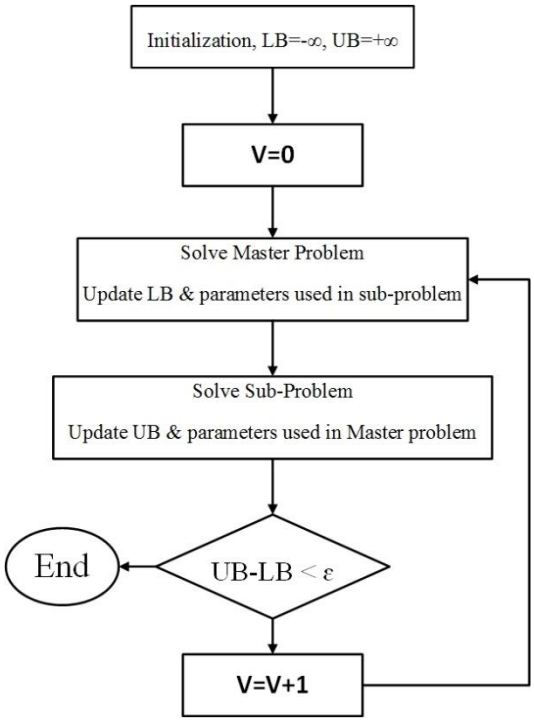


**Figure 2.** Solution procedure flow chart.

Subject to

$$\psi_{ij(v)}^{DF} = \left(\psi_{ij(v)}^{D} + \psi_{ij(v)}^{F}\right) - 2\psi_{ij(v)}^{D}\psi_{ij(v)}^{F} \; ; \; \forall (i,j), v \tag{15}$$

$$\phi_{i(v)}^{DF} = \left(\phi_{i(v)}^{D} + \phi_{i(v)}^{F}\right) - 2\phi_{i(v)}^{D}\phi_{i(v)}^{F} \; ; \; \forall i, v \tag{16}$$

$$\sum_{(i,j)} \psi_{ij(v)}^{D} + \sum_{i} \phi_{i(v)}^{D} \le B^{D} \tag{17}$$

$$\sum_{(i,j)} \psi_{ij(v)}^{F} + \sum_{i} \phi_{i(v)}^{F} \le B^{F} \tag{18}$$

$$\sum_{j\in(i,j)} x_{ijp}\left(1 - \hat{\psi}_{ij}^{A}\left(1 - \psi_{ij(v)}^{DF}\right)\right) - \sum_{j\in(j,i)} x_{jip(v)}\left(1 - \hat{\psi}_{ji}^{A}\left(1 - \psi_{ji(v)}^{DF}\right)\right) = S_{ip(v)} - D_{ip(v)} + U_{ip(v)} \; ; \; \forall i, p, v \tag{19}$$

$$\sum_{j\in(i,j)} x_{ijp(v)} \le v_{ip}\left(1 - \hat{\phi}_{i}^{A}\left(1 - \phi_{i(v)}^{DF}\right)\right); \; \forall i, p, v \tag{20}$$

$$0 \le x_{ijp(v)} \le \overline{x_{ijp}}\left(1 - \hat{\psi}_{ij}^{A}\left(1 - \psi_{ji(v)}^{DF}\right)\right)\left(1 - \hat{\phi}_{i}^{A}\left(1 - \phi_{i(v)}^{DF}\right)\right)\left(1 - \hat{\phi}_{j}^{A}\left(1 - \phi_{j(v)}^{DF}\right)\right); \; \forall (i,j), p, v \tag{21}$$

$$0 \le S_{ip(v)} \le \overline{S_{ip}}\left(1 - \hat{\phi}_{i}^{A}\left(1 - \phi_{i(v)}^{DF}\right)\right); \; \forall i, p, v \tag{22}$$

$$0 \le U_{ip(v)} \le \overline{U_{ip}} \; ; \; \forall i, p, v \tag{23}$$

where

$$\Gamma^{M} = \left\{\psi_{ij(v)}^{DF}, \psi_{ij(v)}^{D}, \psi_{ij(v)}^{F}, \phi_{i(v)}^{DF}, \phi_{i(v)}^{D}, \phi_{i(v)}^{F}, x_{ijp(v)}, U_{ip(v)}, S_{ip(v)}\right\}$$

Constraint (20) illustrates the condition under which flow occurs through the attacked nodes or pump stations for each iteration $(v)$. Constraint (21) is to control the flow capacity that can pass through each pipeline $x_{ijp(v)}$ in each iteration $(v)$ associated with pipelines adversary parameter

$\left(\hat{\psi}_{ij}^{A}\right)$. This constraint has upper bound $\overline{x_{ijp}}$ and lower bound of 0. Equation (22) is to bound the source production $S_{ip(v)}$ in each iteration $(v)$. The upper bound $\overline{S_{ip}}$ is associated with nodes adversary parameter $(\hat{\phi}_{i}^{A})$. Constraint (23) is to limit the amount of shortage $U_{ip(v)}$ exogenously between its upper bound $\overline{U_{ip}}$ and 0 irrespective of the presence or absence of successful attacks.

### 3.2. Sub-Problem

In this section, the sub-problem or attacker–operator interactions are simulated to generate the operator's objective of minimizing and the attacker's objective of maximizing flow and damage cost. The operator's dual problem, and the attacker problem representing the model's sub-problem. As explained, the sub-problem consists of two problems, the dual problem that represents the maximization of the operator problem presented in Equations (24)–(27), and the common attacker problem constraints presented in Equations (28)–(30), where the attacker seeks to maximize the demand shortage and the oil/gas delivery cost. The dual problem is sensitive to the cost of transportation, as shown in Equation (26), and it is growing up to its maximum rate, when there is a shortage in a specific production facility or any pipeline, as shown in Equation (27). The sub-problem will import the defender strategies $(\hat{\phi}_{i}^{DF},\ \hat{\psi}_{ij}^{DF})$ parameters from the master problem as illustrated in Equation (29); the pipelines defending parameter $\hat{\psi}_{ij}^{DF}$ and the production facilities defending parameter $\hat{\phi}_{i}^{DF}$, respectively.

$$\min_{\Gamma^{S}} -\left(\sum_{i,p}\left[\lambda_{ip}D_{ip} + \mu_{ip}^{s}\overline{S_{ip}}\left(1-\phi_{i}^{A}\right) + \mu_{ip}^{sh}\,\overline{U_{ip}} - \mu_{ip}^{n}v_{ip}\left(1-\phi_{i}^{A}\right)\right] - \sum_{i,j,p}\left[\mu_{ip}^{a}\overline{x_{ijp}}\left(1-\psi_{ij}^{A}\right)\right]\right) \tag{24}$$

Subject to

$$\lambda_{ip} + \mu_{ip}^{s} = 0\ ;\ \forall i,p \tag{25}$$

$$C_{ijp}^{T} - \lambda_{ip}h_{ijp} + \lambda_{jp}h_{jip} + \mu_{ip}^{n} + \mu_{ip}^{a} = 0\ ;\ \forall ij,p \tag{26}$$

$$C_{ip}^{Sh} - \lambda_{ip} + \mu_{ip}^{sh} = 0;\ \forall i,p \tag{27}$$

$$\psi_{ij}^{A} \le 1 - \hat{\psi}_{ij}^{DF};\ \forall ij \tag{28}$$

$$\phi_{i}^{A} \le\ 1 - \hat{\phi}_{i}^{DF};\ \forall i \tag{29}$$

$$\sum_{ij}\psi_{ij}^{A} + \sum_{i}\phi_{i}^{A} \le B^{A} \tag{30}$$

where

$$\Gamma^{S} = \left\{\psi_{ij}^{A}, \phi_{i}^{A}, \mu_{ip}^{s}, \mu_{ip}^{n}, \mu_{ip}^{a}, \mu_{ip}^{sh}\right\}$$

Equation (24) applies the Lagrangian formed from the dual variables $(\lambda)$ and $(\mu)$. The method is utilized to maximize the cost of all oil and gas operations within the network in the dual problem, where the first summation is to dual representation on the demand associated with the dual variable $\lambda_{ip}D_{ip}$, the production level associated with the dual variable and attacker strategy $\mu_{ip}^{s}\overline{S_{ip}}\left(1-\phi_{i}^{A}\right)$, the maximum lost and dual variable $\mu_{ip}^{sh}\,\overline{U_{ip}}$, and the upper limit of the production level, dual variable, and attacker strategy of production sources $\mu_{ip}^{n}v_{ip}\left(1-\phi_{i}^{A}\right)$. The second part is the pipeline upper bound, dual variable and attacker strategy on pipelines $\mu_{ip}^{a}\overline{x_{ijp}}\left(1-\psi_{ij}^{A}\right)$. Constraint (25), it is used to calculate the cost of optimal levels of production at the production sources. Constraint (26) is used to calculate the cost of optimal transportation flow in the pipelines. Equation (27), is to calculate the cost of the levels of shortage in the dual problem. Constraint (28), represents the beginning of the attacker problem, which states that if the pipeline is defended ($\hat{\psi}_{ij}^{DF}$=1), it is invulnerable, as the attacker variable $\left(\psi_{ij}^{A}=0\right)$. Constraint (29) is to implement the attack and defend plans for the production

sources, if the source defending strategy parameter ($\hat{\phi}_i^{DF} = 1$), means that this sources is safe and the attacker's source variable would be ($\phi_i^A = 0$). Equation (30) is used to control the total attacker resources for interruptions.

### *3.3. Solution Procedure*

The details of the solution procedure algorithm are provided in the following steps: **Step 1**: Set Lower Bound (LB) and Upper Bound (UB) equal to $-\infty$ and $+\infty$, respectively. **Step 2**: Set the iteration counter $v = 0$. **Step 3**: Solve Master problem $(\min_{\Gamma^M})$ subject to Constraints (14)–(23) to obtain the optimal solution of the defender–operator decision variables. **Step 4**: Update the LB by using the equation at each iteration $LB = \eta^*$. **Step 5**: Solve the Dual of Sub-problem $(\min_{\Gamma^S})$ subject to Equations (25)–(30) and obtain the decision variables for the Attacker–Operator problem by considering the decision parameters obtained from **Step 3**. **Step 6**: Update the UB, respectively. **Step 7**: If the term (UB–LB) becomes smaller than a predefined tolerance value $\epsilon$, the algorithm will terminate. The optimal solution is obtained from the defender and attacker decision variables. If not, then proceed to the following steps. **Step 8**: Update the iteration counter, $v \leftarrow v + \mathbf{1}$, and update the subproblem parameters used in the master problem obtained from **Step 5**. **Step 9**: Continue with **Step 3**.

The above steps mimic the interplay between the aggressor and the defender. The defender starts by trying different fortification and deception schemes to prevent attacks to the most important production sources and pipelines. The model helps to select the critical facilities according to their production rates, capacities, the exposure length of the pipeline, and the demands. On the other side, the attacker tries to damage the network by targeting selected production facilities. These models show the interactions between defender and attacker under different circumstances. The model is based on the related hard and soft sciences on the relationship between game theory and information value theory. Through the execution of the above algorithm, we will show that proper quantification of the utility function, the reward structure, is key to operational success. For example, we are able to quantify the benefit of implementing the deception strategies when the defender decided to utilize it.

## 4. Results and Discussion

We derived our model to a real operational petroleum network stated in Iraq (Figure 3) and used the relative data as input to study the behavior of the model. The notation on each node representing the facility's capacity in producing (demand) crude oil and NGL if it is a source (sink) node, respectively, and pump station's capacity if it is an intermediate node. The notations on the arcs representing the distance between facilities. The computational results show the objective function, when the defender experimented with 0 up to 21 hardening trials. Each trial can be considered as a resource that is expended to protect an additional facility. When the defender utilized few numbers of hardening resources ($B^D = 1$ or 2) in Equation (17), the model simply select facilities that will deliver oil and gas that are least expensive way, without considering the cost of shortage at demand facilities, which translates into ignoring the connectivity between production sources and the demand points. Starting with utilizing three hardening resource, the model would protect a source and a demand point and a pipeline that connect this origin and destination pair. This enables the operator to deliver petroleum from source to sink. If the defender applies more hardening resources, as presented in Figure 4, the model will seek the next most important facilities to protect, trying to minimize the operation cost and the shortage cost in the delivery network (see Figure 4).

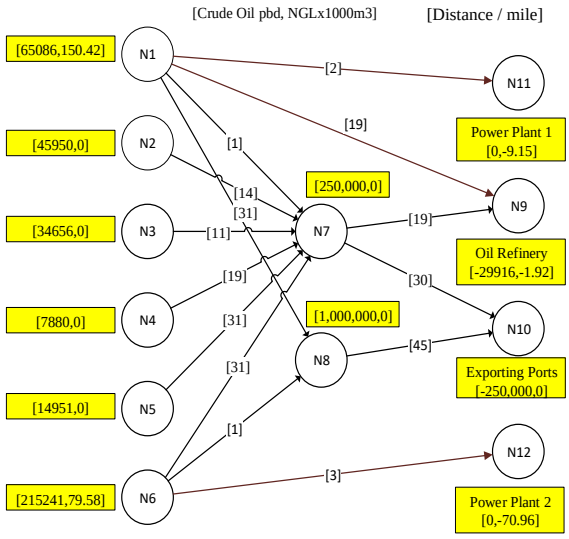


**Figure 3.** Network Representation.

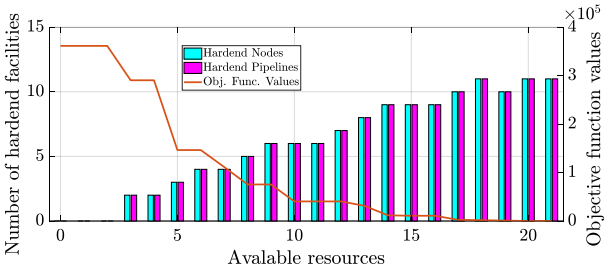


**Figure 4.** Model results verification: defender–attacker strategies without deception.

The model was successful in selecting the right pipelines and sources (sink) facilities based on the production rate, capacity, amount of pipeline flow, and the requested demands. It is clear that the curve drops most sharply with the investment of up to five hardened sources (sinks) and pipelines, particularly when the additional fifth hardening resource is expended.

From thereon, the objective function starts to level off, until it reaches its minimum of 0 by implementing a total of 17 hardening pipelines and sources (sinks) facilities, beyond which there are no additional benefits in expending more resources.

Moreover, a significant contribution of this paper is to implement the deception strategies within the protection plan on top of the hardening strategies.

From the deception strategy, the aggressor will see one protection plan without distinguishing between the facilities that are genuinely hardened and those that are faked. A deception strategy needs realistic posturing that makes the intruder believes that those facilities are truly protected. This speaks to the role of epistemic knowledge, which is defined as knowledge supporting a belief, truth, or hypothesis. The epistemic utility is a measure of the value of this knowledge in supporting a hypothesis, i.e., a measure of the importance of the information about the other game players relative to the belief that the other players are going to adopt a certain strategy [18]. At the same time, the empirical model component explores what kind of game information participants seek and receive and how participants react to such information exchange as they play the participatory game [18,19]. Among other soft factors, we investigated how epistemic knowledge, or side information, of the participants is used to support a game participant's beliefs or hypotheses during the conduct of the face-to-face game. Unlike operational utility, epistemic utility functions are an emerging branch of knowledge that is still under development [20,21]. When executed iteratively, the two model components will address both "hard" and "soft" factors in competition. Most importantly,

this experiment will help a better understanding and further development of epistemic utility theory and other emerging science on this subject.

Figure 5 is the best illustration of adopting five deception resources ($B^F = 5$), where the defender tries to protect three nodes and two pipelines with five deception resources and zero real hardening resource. This plan allowed the defender to save lots of operational costs and minimize the model's objective function.

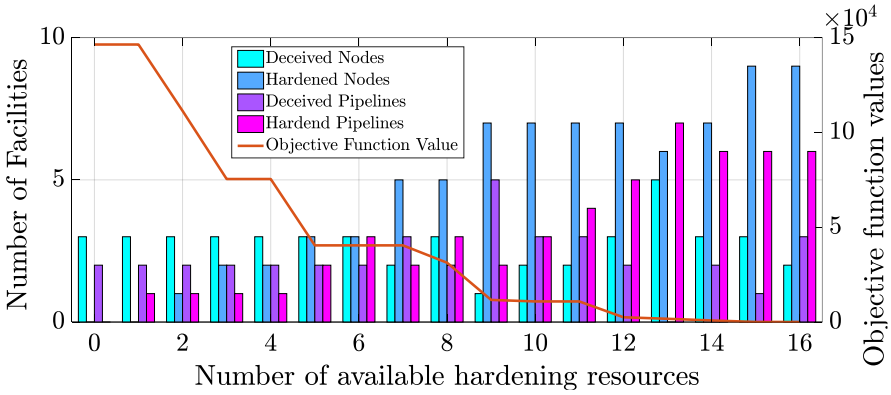


**Figure 5.** Model results verification: defender–attacker strategies with deception.

When the attacker thinks that it sees five protected facilities, it will not risk attacking, and accordingly, he would target other facilities that appear to be unprotected. When the defender employed five real hardening resources and five deception resources, the aggressor may see that the defender has protected 10 facilities, not being able to distinguish between three deception sources (sinks) facilities, three hardened sources (sinks) facilities, two deception pipelines, and three hardened pipelines. As a result, the aggressor will focus on the less critical facilities that were left unprotected due to limited available resources. The reader can see that the objective function would drop faster than the exclusively hardened case in Figure 4.

The model monitored different scenarios for fortification and deception to face the adversaries. The deception strategy was able to trick the attacker from targeting the most essential facilities with only five deception resources. What if the defender increases his deception resources? What if 10 deception resources are considered in the defender fortification plan? Does the objection function behave better than adopting five deception plans?

Figure 6 illustrates the judicious use of deception strategy; the fact that a limited amount of deception is better than excessive use of deception. Figure 6 is to monitor a comparison between three different scenarios, when no deception is involved, when five resources are utilized, and when 10 resources used in the fortification strategies.

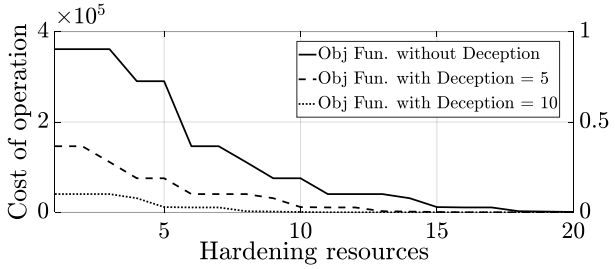


**Figure 6.** Objective function cost reduction with and without deception strategy.

From the illustration, the objective function behavior with five deception resources is better than utilizing 10 deception resources. Compared with the case of no deception, this figure shows a saving of $214,957.3 per day by applying just five deceptive resources. As observed from the same figure, it is

interesting to see that the cost reduction with an additional five deception resources (making a total of 10) is less than the cost saving of applying only five deception resources. Implementing the deception concept judiciously will help the leader to allocate his resources wisely. For example, the defender will spend only one deception resource for a node that serves both oil-and-gas. Without deception, the defender needs to spend two hardening resources for that production source as shown in Figure 7. Identifying the source and sinks in the oil-and-gas network can be considered as another high-level contribution of this paper.

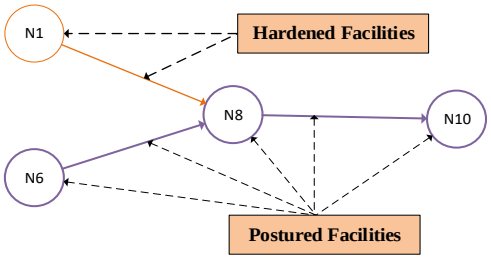


**Figure 7.** The model validated to include the most important facilities in the investment plan.

Figure 8 is an illustration of another case study that verifies the bi-level model works as intended when the defender used resources to protect the network from hardening and deception strategies or a combination of the two. By so doing, the attacker has prevented from targeting the critical facilities that will result in shortages in the demand sites, where the deception resources are $B^F = 10$, defending resources are $B^D = 10$, and attacker resources are $B^A = 10$. The defender was able to protect Source No. 3 and the connected pipeline, where the false information was used to posture the attacker from attacking it. These results based on the last iteration, where the defender tried to optimize his strategies to find the best solution for the network. From these results, we can see that the defender and attacker resources can play a major regulation in constructing fortifications and disruptions strategies. Allocating the limited defense resources were implemented in a good way to maximize security for the purpose of protecting the network as possible. The model can find the primary facilities to defend them, and if there is no risk for them, his plan will change and release false information about them. This strategy can be seen in Source No. 3 and pipelines N3–N7, where, in some iterations, the defender postured the attacker, then defended them, and finally, the defender decided to posture them, while the defending resources went to other critical facilities or pipelines within the network.

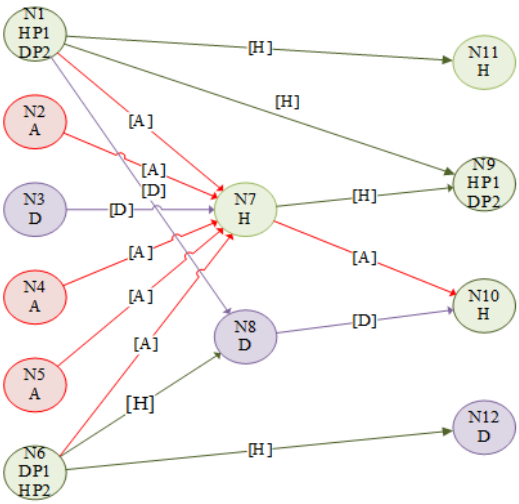


**Figure 8.** Network representation defender strategy (hardening and deception) as well as for successful attacks. H—hardening, D—deception, A—attack, P1—crude oil, P2—NGL.

Case number (1) shown in Table 2 is describing the deception, when the defender used five deception resources ($B^F = 5$), one defending resources ($B^D = 1$), and the attacker used ten attacks resources ($B^A = 10$). Also, Table 3, shows an example of the upper and lower levels behaviors and the model run time.

**Table 2.** Model behavior for different scenarios when the defender tried to use five deception resources and increases the protection budget.

| $B^F = 5$. | | | | |
|---|---|---|---|---|
| $B^D$ | $\phi_i^D$ | $\phi_i^F$ | $\psi_{ij}^D$ | $\psi_{ij}^F$ |
| 0 | - | $N6_{P1}$, N8, N10 | - | N6–N8, N8–N10 |
| 1 | - | $N6_{P1}$, N8, N10 | N6–N8 | N7–N10, N8–N10 |
| 2 | $N1_{P1}$ | $N6_{P1}$, N8, N10 | N1–N8 | N6–N8, N8–N10 |
| 3 | N6, N12 | $N6_{P1}$, N8, N10 | N6–N12 | N6–N8, N8–N10 |
| 4 | $N6_{P2}$, N12 | $N6_{P1}$, N8, N10 | N6–N12 | N6–N8, N8–N10 |
| 5 | N8, N10, N12 | $N1_1$, $N6_{P1,2}$ | N1–N8, N6–N8 | N6–N12, N8–N10 |

**Table 3.** Upper bound (UB), lower bound (LB) behavior, and the model run time.

| Iteration | UB Level | LB Level | Run Time |
|---|---|---|---|
| 1 | 361,372.000 | 297,602.392 | |
| 2 | 361,372.000 | 290,412.284 | 1.2 (s) |
| 3 | 361,372.000 | 297,602.392 | |

The model was able to solve the problem after a few iterations for all case studies. This can be claimed to the size of the selected network. The optimality gap is the difference between the upper bound and lower bound.

## 5. Conclusions and Recommendations

In this research, a real-world problem was investigated, formulated, and solved for preventing a petroleum and gas network from malicious attacks. The strategies of the defender, attacker, and operator were formulated in a tri-level mixed-integer nonlinear program. The strong duality theorem was used to merge the Attacker and Operator problems into a single-level one, resulting in a mixed-integer bi-level model. The defender in the master problem is an active defender, meaning that he will take the first move, to which the attacker will react, and the interaction between the defender and attacker continues iteratively.

The unique feature of this research is that the players participate in a communications game, well beyond a regular game. Information value has so far been discussed in terms of the utility derived from the information being communicated. There is, however, additional information that is deliberately or inadvertently generated in competitive communication environments, ranging from "blowing smoke" to "posturing". This type of information is the game information; it is responsible for the style of play and the performance of the game being considered. Players' actions, including deception, will generate and affect this information. This often leads toward counterintuitive results, perhaps due to such side information.

In our case study, a combination of defensive hardening of facilities and posturing is proposed. The model identifies the optimal defense strategies in the defender–operator in the first level and exports them as parameters to the attacker–operator in the second level; henceforth, an attack response strategy is formulated between the attacker and operator based on the imported parameters. This is followed again by the defender–operator actions that respond to the attacker with its best way to keep the oil-and-gas flowing. Solving this bi-level problem iteratively, the algorithm converges toward the final optimal solution in a very reasonable execution time of less than one minute. Our extensive computational experiments show many interesting results. For example, without any posturing,

the defender cannot take any action till after a minimum of three fortification attempts. Even with a commensurate amount of fortification, however, using an excessive amount of deception would not benefit as much as utilizing only a judicious amount.

Another significant finding is from the stockholder's vision. The network is an oil-and-gas one in Iraq. This network produced 383,764 barrels (PBD) of petroleum and 230 million standard cubic feet (MMSFD) of natural gas per day. Since Iraq is a member of (Organization of the Petroleum Exporting Countries) OPEC, the oil prices are standards for all OPEC members. The average price of a crude barrel of Iraqi crude oil in 2016 was \$40.00. Iraq does not export any natural gas; it is strictly for internal consumption and whatever is not consumed is burned. In the absence of earning global reserve currency, gas price is irrelevant and has been evaluated to be around \$1 per cubic feet by default according to [22]. Based on this background, the gross revenue per day, counting only oil sales to international markets, amounts to: \$40.00 × 383,764 = \$15,350,560. The net revenue per day is then \$15,350,560 − 12.5 × 383,764 = \$10,553,510. As shown in Figure 9, when stockholders decide on expending two hardening defender resources together with five deception resources, such posturing resulted in a cost saving of \$249,962.70. This represents \$249,962.70/10,553,510 = 2.37% of their daily net revenue.

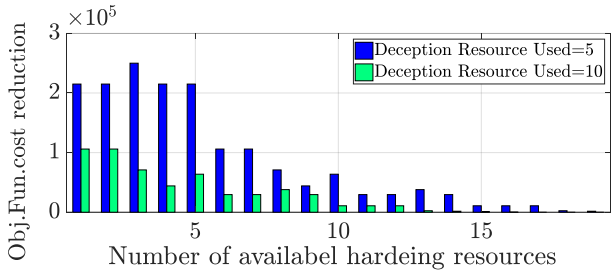


**Figure 9.** Value of deception verification.

Due to the proprietary nature of Iraqi state-owned industries, the amount of resources devoted to the protection of the network is unknown, particularly under the scenario of "rock bottom" oil prices in 2016. However, the above estimate suggests that the network operations can obtain \$249,962.70 worth of daily protection (or the equivalent of 2.37% of their daily revenue) by simply exercising five posturing attempts and by spending a small amount to harden merely two facilities.

For future extension, we plan on improving the methods for solving bi-level problems, developing the decomposition algorithm to make it more efficient than what is reported here. The first step is to place the solution algorithm in the general decomposition framework, following some ideas from [23]. Another promising piece of future work is to broaden the epistemic knowledge concept to include a larger role for shared cognition. Cooperative and non-cooperative games can be played, where the defender can spy on the non-cooperative group as well as sharing the obtained information within the cooperative partners following some of the ideas from [7]. Most critically, until the emerging science of information value theory is understood, using purely analytical gaming models will likely fall short of our model validation goal. We hope that this initial step in our research maps into a blueprint for a series of research projects that would ultimately help obtain a truly significant understanding of the subject.

**Author Contributions:** Conceptualization, Y.C., M.A., and H.D.; methodology, M.A. and H.D.; software, M.A. and H.D.; validation, Y.C.; formal analysis, M.A. and H.D.; investigation, M.A.; writing—original draft preparation, M.A.; writing—review and editing, Y.C., M.A., and H.D.; visualization, M.A.; supervision, Y.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Acknowledgments:** We would like to thank Nitin Agarwal (University of Arkansas at Little Rock) for supervision, comments, and expert advice on the manuscript. The authors gratefully acknowledge the financial support from Gas Pos Inc., North Little Rock, AR, USA, 72114.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A

| | |
|---|---|
| **Indexes** | |
| $D$ | Defender |
| $A$ | Attacker |
| $O$ | Operator |
| $i$ | Source nodes |
| $j$ | Destination node |
| $p$ | Produced product (crude oil, natural gas) |
| $v$ | Iterations in master problem |
| **Binary Variables** | |
| $\psi_{ij}^{A}$ | Attack on pipelines |
| $\phi_{i}^{A}$ | Attack on nodes |
| $\psi_{ij}^{D}$ | Defend on pipelines |
| $\phi_{i}^{D}$ | Defend on nodes |
| $\psi_{ij}^{F}$ | Posturing on pipelines |
| $\phi_{i}^{F}$ | Posturing on nodes |
| $\psi_{ij}^{DF}$ | Defend Strategy on pipelines |
| $\phi_{i}^{DF}$ | Defend Strategy on nodes |
| $\dot{x}$ | Binary variable |
| **Variables** | |
| $x_{ijp}$ | The amount of flow produced in node $i$ and transported to node $j$ for product type $p$. |
| $U_{ip}$ | The amount of shortage |
| $S_{ip}$ | Production source |
| $\lambda_{ip}$ | $\Gamma^{O}$ dual variables Equation (9) |
| $\mu_{ip}^{n}$ | $\Gamma^{O}$ dual variables Equation (10) |
| $\mu_{ip}^{a}$ | $\Gamma^{O}$ dual variables Equation (11) |
| $\mu_{ip}^{s}$ | $\Gamma^{O}$ dual variables Equation (12) |
| $\mu_{ip}^{sh}$ | $\Gamma^{O}$ dual variables Equation (13) |
| $\dot{A}$ | Linearization variable |
| **Parameters** | |
| $C_{ijp}^{T}$ | Cost transportation |
| $C_{ijp}^{Sh}$ | Cost shortage (big number) |
| $B^{D}$ | Total defending resources |
| $B^{F}$ | Total deception resources |
| $B^{A}$ | Total attacker resources |
| $D_{ip}$ | Sinks demands |
| $v_{ip}$ | Nodes capacity |
| $\overline{x_{ijp}}$ | Flow upper bound |
| $\overline{S_{ip}}$ | Source upper bound |
| $\overline{U_{ip}}$ | Shortage upper bound |
| $\hat{\psi}_{ij}^{DF}$ | Defend strategy on pipelines |
| $\hat{\phi}_{i}^{DF}$ | Defend strategy on nodes |
| $\hat{\psi}_{ij}^{A}$ | Attack strategy on pipelines |
| $\hat{\phi}_{i}^{A}$ | Attack Strategy on nodes |
| $h_{ijp}$ | Network adjacency matrix |
| $M$ | Very big number |
| $\overline{A}$ | Upper bound for $\dot{A}$, a big number |
| $z$ | Linearization parameter |

## Appendix B Linearization Methods

### *Appendix B.1. Linearizing the Product of Two Binary Variables*

Presume the constraint has the product $= \dot{x} \times \dot{y}$, where $(\dot{x}, \dot{y})$ variables are binary. The easiest way for linearizing above product is as displayed below:

$$z \leq \dot{x}$$

$$z \leq \dot{y}$$

$$z \geq \dot{x} + \dot{y} - 1$$

If the $\dot{x}$ or $y$ are set to 0, then by using the first two inequalities, we make sure that $z$ is equal to zero. If both $\dot{x}$ and $\dot{y}$ are fixed to 1, then the third inequality would make sure to mark $z$ equal to 1.

### *Appendix B.2. Linearizing the Product of a Binary Variable and a Continuous Variable*

This assumption is when the equation $z = \dot{A} \times \dot{x}$, where $\dot{A}$ is a continuous variable and $\dot{x}$ is set to be a binary variable. Since $\dot{A}$ is a continuous variable and if it is bounded by lower bound equal to zero and upper bound equal to $\overline{A}$ (or any big $M$), then the linearization is quite simple:

$$z \leq \overline{A} \times \dot{x}$$

$$z \leq \dot{A}$$

$$z \geq \dot{A} - (1 - x)\overline{A}$$

$$z \geq 0$$

If the binary variable $\dot{x}$ is set to zero, then the first inequality ensure that z will be zero. If $\dot{x}$ is set to be 1, then the former inequality makes sure that $\dot{x}$ is less than the Big $M$, which is more constricted by the following inequality. The third inequality states that $z$ has to be bigger that or equivalent to $\dot{A}$.

## References


1. Wood, R.K. Bilevel network interdiction models: Formulations and solutions. In *Wiley Encyclopedia of Operations Research and Management Science*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2011; pp. 1–11.
2. Anifowose, B.; Lawler, D.; van der Horst, D.; Chapman, L. Evaluating interdiction of oil pipelines at river crossings using environmental impact assessments. *Area* **2014**, *46*, 4–17. [CrossRef]
3. Murray, A.T. An overview of network vulnerability modeling approaches. *Spec. Sect. Geogr. Asp. Vulnerability* **2013**, *78*, 209–221. [CrossRef]
4. Leiniger, W. Games and Informaition, Fourth edition, An Introduction to Game Theory. *Int. J. Ind. Organ.* **1991**, *9*, 474–476. [CrossRef]
5. Cannon-Bowers, J.A.; Salas, E. Reflections on shared cognition. *J. Organ. Behav.* **2001**, *22*, 195–202. [CrossRef]
6. Zeng, B.; Zhao, L. Solving two-stage robust optimization problems using a column-and-constraint generation method. *Oper. Res. Lett.* **2013**, *41*, 457–461.
7. Chan, Y.; McCarthy, J. Game-Theoretic Paradigms in Collaborative Researchpar: Part 1—Theorical background. *Int. J. Soc. Syst. Sci.* **2014**, *6*, 331–347. [CrossRef]
8. International Energy Agency. *Iraq Energy Outlook*; IEA: Paris, France, 2012.
9. Wu, X.; Conejo, A.J. An Efficient Tri-level Optimization Model for Electric Grid Defense Planning. *IEEE Trans. Power Syst.* **2017**, *32*, 2984–2994. [CrossRef]
10. Conejo, A.J.; Baringo, L. *Investment in Electricity Generation and Transmission*; Springer: Cham, Switzerland, 2016.
11. Ramirez-Marquez, J.E.; Levitin, G. Optimal protection of general source-sink networks via evolutionary techniques. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1676–1684. [CrossRef]

12. Rahmaniani, R.; Gabriel, T.; Gendreau, M.; Rei, W. The Benders decomposition algorithm: A literature review. *Eur. J. Oper. Res.* **2017**, *259*, 801–817. [CrossRef]
13. Snyder, L.V.; Scaparra, M.P.; Daskin, M.S.; Church, R.L. Planning for Disruptions in Supply Chain Networks. *Tutor. Oper. Res.* **2006**, 234–257. [CrossRef]
14. Chan, Y.; Chan, Y. Network Throughput and Reliability: Preventing Hazards and Attacks through Gaming—Part 2: A Research Agenda. In *Game Theoretic Analysis of Congestion, Safety and Security*; Springer: Berlin, Germany, 2015; pp. 141–172.
15. Snyder, L.V.; Daskin, M.S. Models for reliable supply chain network design. In *Critical Infrastructure: Reliability and Vulnerability*; Advances in Spatial Science; Murray, A.T., Grubesic, T., Eds.; Springer: Cham, Switzerland, 2007; pp. 257–290.
16. Levine, T.R.; Mccornack, S.A. An Introduction to Advances in Deception Theory. *Lang. Soc. Psychol.* **2014**, *33*, 345–347. [CrossRef]
17. Levine, T.R. Truth-Default Theory (TDT): A Theory of Human Deception and Deception Detection. *Lang. Soc. Psychol.* **2014**, *33*, 378–392. [CrossRef]
18. Devi, T.; Sambandan, D. Towards Deception Detection in Concurrent Engineering. In Proceedings of the 2014 International Conference on Intelligent Computing Applications (ICICA'14), Coimbatore, India, 6–7 March 2014; pp. 358–366.
19. Tsikerdekis, M. Real-Time Identity Deception Detection Techniques for Social Media: Optimizations and Challenges. *IEEE Internet Comput.* **2017**, *22*, 35–45. [CrossRef]
20. Chan, Y.; McCarthy, J. Game-Theoretic Paradigms in Collaborative Research: Part 2-experimental design. *Int. J. Soc. Syst. Sci.* **2014**, *6*, 348–364. [CrossRef]
21. Pettigrew, R. Epistemic Utility Theory. 2010. Available online: http://philsci-archive.pitt.edu/5225/1/eputtheory3.pdf (accessed on 3 March 2020).
22. Pettigrew, R. A new epistemic utility argument for the principal principle. *Episteme* **2013**, *10*, 19–35. [CrossRef]
23. Ralphs, T.K.; Galati, M.V. Decomposition in Integer Linear Programming. In *Integer Programing*; CRC Press: Boca Raton, FL, USA, 2005; pp. 73–126.


© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).