A Bi-Level Stochastic Model with Averse Risk and Hidden Information for Cyber-Network Interdiction

MingChu Li, Wanyu Dong, Xiao Zheng, Anil Carie, and Yuan Tian

Abstract This paper proposes a method to enable a risk-averse and resource-constrained network defender to deploy security countermeasures in an optimal way to prevent multiple potential attackers with uncertain budgets. To solve the problem of information asymmetry between the attacker and the defender, a fake countermeasure (FC) is placed on the arc, and the situation of multiple attackers is also taken into consideration. This method is based on the risk aversion bi-level stochastic network interdiction model on the attack graph, which can easily map the path of attackers. Meanwhile, our method can minimize the weighted sum of all losses and minimize the risk of the defender's key nodes being destroyed. At the same time, in order to prevent the key node of the defender from being destroyed, the risk condition value measurement is taken into account in the stochastic programming model. We design a SA-CPLEX algorithm to provide a high-quality approximate optimal solution. And computational results suggest that our method provides better network interdiction decisions than traditional deterministic and risk-neutral models.

Keywords Stackelberg game · Averse risk · Hidden information · Bi-level programming · Cyber-security

M. Li · W. Dong (✉)
School of Software, Dalian University of Technology, Dalian, China
e-mail: dongwanyu@mail.dlut.edu.cn

M. Li
e-mail: mingchul@dlut.edu.cn

X. Zheng
School of Computer Science and Technology, Shandong University of Technology, Zibo, China
e-mail: xiao_zheng0910@163.com

A. Carie
School of Computer Science, VIT-AP, Amaravati, India

Y. Tian
School of Economics and Management, Dalian University of Technology, Dalian, China
e-mail: ytian@mail.dlut.edu.cn

A. K. Bashir et al. (eds.), *Proceedings of International Conference on Computing and Communication Networks*, Lecture Notes in Networks and Systems 394,
https://doi.org/10.1007/978-981-19-0604-6_49

1 Introduction

With the rapid development of information technology, people can browse a large number of websites through the Internet. The application scenarios of computer equipment have also expanded and penetrated into the public's access network technology and work [1–3]. However, while the computer brings more convenience, it also has certain security risks, causing some key information to be leaked and bringing certain economic losses. This paper studies the problem of a network defender to minimize worst-case damage by setting countermeasures against uncertain attacks. We propose a Stackelberg game between defenders and attackers, in which the defender not only can deploy true countermeasures (TCs) but also fake countermeasures (FCs). The deployment of FCs can be used to mislead the attacker's actions.

The goal of this research is to help the defender makes better use of the limited budget to protect the network from uncertain attacks. Therefore, it is necessary to establish a new interdiction model to formulate the risk aversion of the network defender under the uncertainty of the attackers' ability [4]. This paper establishes a defender-attacker stochastic Stackelberg game [5] model including risk aversion based on attack graph. Our stochastic network interdiction model can interdict multiple potential attackers with uncertain budgets. Compared with a model that considers a constant budget and a unique attacker, this modeling method is more representative of a realistic scenario. However, the traditional risk model stochastic programming usually takes the minimization of losses as their goal and does not take into account the risk of maximum loss scenarios. The risk aversion stochastic programming model minimizes the defender's expected loss and minimizing the risk of huge losses when the attackers' initial budget is uncertain.

We introduce a novel risk-averse bi-level stochastic network interdiction model based on attack graphs and use conditional risk value as risk measurement and customized accurate algorithm to solve the bi-level random network counter-measures model for risk aversion. This problem is defined as a bi-level stochastic network interdiction problem with risk aversion, the upper-level is the problem of the defender, and the lower-level is the problem of the attacker. In the upper-level model, the defender makes decisions without knowing the attacker's budget. While in the lower-level model, the attacker plans an attack route based on a known budget and a known interdiction strategy of the defender. And a simulated annealing algorithm based on the commercial solver CPLEX, namely, SA-CPLEX, is customized for our model to solve this NP-hard problem.

The contributions of this paper are as follows.

(1) We propose a risk-averse defender-attacker stochastic Stackelberg game model that merges fake countermeasures and multiple attackers with uncertain budgets.
(2) Conditional value-at-risk (CVaR) is involved in our model to measure the defender's risk performance with respect to the attackers' uncertain budgets.
(3) An effective algorithm is proposed to solve the resulting bi-level problem, which can provide an efficient solution for our model.

The remainder of this paper will be described in the following structure. In Sect. 2, we review the related works. The problem definition and formulation are presented in Sect. 3. In Sect. 4, we propose a heuristic algorithm and perform theoretical analysis on the proposed algorithm. We present the experimental results and analysis of the results in Sect. 5. Finally,we summarize our conclusions in Sect. 6.

2 Related Work

Attack graphs with different changes are widely used as a tool for network analysis, such as defensive tree [6], attack countermeasure tree [7], vulnerability dependency graph [8], etc. The way of network interdiction based on attack graphs to protect target nodes (key assets) is to remove a set of arcs or nodes from the attack graph. In the previous literature, attack graph network interdiction enhances network security by generating cut sets [9]. Khouzani et al. [10] studied the cyber-security defense problem using attack graphs to model a multi-stage attack. In addition to the mathematical model of attack graphs, some studies have proposed the use of traditional mathematical models to reduce the risk of network attacks. For example, Zheng et al. [11] allocated limited mitigation resources to increase the robustness of supply chain infrastructure information technology in cyber-attacks. A recent paper, Bhuiyan et al. [12] modeled multiple potential attackers, in which the attacker's actions are assumed to be absolutely unsuccessful if the defender deploys interdiction measures on the arc. But in real life, even if the defender installs defensive countermeasures, the attacker still has a certain chance to pass the arc. There are also studies that consider uncertainty in the bi-level network interdiction model, including the uncertainty of protection facilities to minimize the worst-case [13]. We have found that taking uncertainty into consideration has a positive direction for the completeness of the entire model.

In order to maximize the attackers' cost of the shortest path, Pay et al. [14] established a random shortest path network interdiction model. But in their network interdiction model, the huge risk posed by the attacker was not considered. In [15], the risk measure, i.e., conditional value-at-risk (CVaR), is incorporated into the location and protection problem. Furthermore, Lei et al. [16] studied stochastic flow interdiction problems using a risk-averse approach. As proved by Lei et al. [16], the model considering risk preferences can provide more robust solutions in comparison to the risk-neutral counterpart. In this regard, our paper also incorporates a risk measure to hedge against the huge risk.

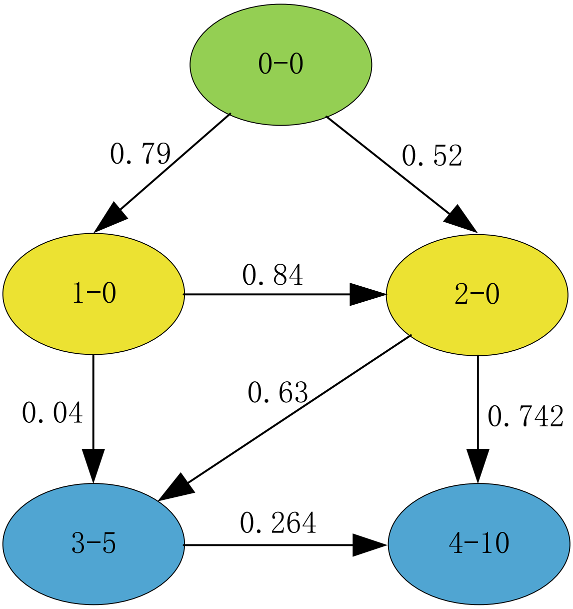
3 Problem Definition and Formulation

This paper studies the stochastic Stackelberg game interaction between the defender and two or more attackers in the risk aversion network using the attack graph. As shown in Fig. 1, the node represents the attack state,and its set is N. Each node is represented in the form of N-D, where N is the value of each node, and D is the defender's loss when the head node is destroyed. The green node is the initial safety condition, the blue node is the key node, and the yellow is the transition node. The attacker's attack path consists of an arc from the initial node to the key node. In the case of NCs in Fig. 1, the attacker's optimal plan is to destroy the key node through the attack path $0 \rightarrow 2 \rightarrow 4$. The attacker destroys any node in the attack graph, and the defender has a certain loss. The attackers start from the green initial node, and their goal is to destroy the blue node to maximize the defender's loss. Once the target node is successfully attacked, it will be completely destroyed.

The arc between the two nodes represents the action of the attacker. Set of arcs with the tail pointing to node $A_t(i)$, which indicates the prerequisite for the attacker's action, and it is a necessary security condition that the attacker should break during the action. Set of arcs with the head pointing to node $A_h(i)$, which represents the post-condition of the attacker's action, which is the security condition that the attacker breaks after the action is successful. The value V of the arc between two nodes indicates the probability of a successful attack through this arc. We can calculate the loss when a node is destroyed as $V \times d$. Taking the attack path $0 \rightarrow 2 \rightarrow 4$ as an example, the expected maximum loss to the defender is $3.8584 (= 0.79 \times 0.04 \times 5)$. Finding the optimal path by calculating and comparing the losses caused by different paths.

In our research, the defender-attacker stochastic Stackelberg game on the attack graph is modeled as a bi-level stochastic network interdiction problem with risk

Fig. 1 An example of attack graph



aversion. The upper-level indicates the problem of defender, and the lower-level represents the problem of attacker. Within the game, the defender first finds the arc where the attacker is most likely to attack without knowing the attackers' budget and spends a certain cost to install countermeasures (including TCs and FCs) on this arc within the deployment budget. The attacker's budget will only be obtained by the defender after they have completed the plan. b_d and $\bar{b}_d$ represent the defender's budget of deploying TCs and FCs, respectively. In order to optimize the defender model, some FCs will be placed in the path to mislead the attacker. It should be noted that there are also some paths in the graph that have no countermeasures (NCs). Minimizing expected losses is an important task for defenders while minimizing the huge risks caused by the loss of key assets.

In terms of the behavior of the defender, each attacker develops an attack plan based on their budget and destroys the key assets aiming to maximize the loss of the defender. Each attacker has an attack cost c_{ij}^{attack} when attacking through the arc, and their total cost should not exceed the budget. Intuitively, the FCs can be exposed or detected by the attacker, thus let o_{ij} be the exposure probability of FCs deployed on arc (i, j). If the attacker detects the FCs, the arc (i, j) equipped with FCs is the same as the one with NCs. Thus, according to both FCs and NCs, the attacker has the same probability to pass the arc, which is denoted by $\bar{p}_{ij}$. Also, let p_{ij} be the probability of passing the arc equipped with TCs.

In order to maximize the defender's loss, the attackers use a limited budget b_a to select the optimal attack plan in a given set of truncated arcs. The attackers start the attack from the vulnerable node and continue to penetrate the network through the transition node until the key asset (target node) is destroyed. If an attacker can break through one of the target nodes, the network defender will suffer losses. The attack path includes an arc from the initially vulnerable node N_I to the target node N_T. An attack plan consists of a combination of one or more attack arcs. Even if this arc can break through multiple target nodes in an attack strategy, the attacker only needs to successfully attack this arc once. In this way, the problem is transformed into a discrete optimization problem. In addition, once the target node is attacked, then it will be completely destroyed.

Decisions are made sequentially in bi-level stochastic programming [17]. The upper-level is to make decisions before the uncertainty is realized, and the lower-level is to make additional decisions after the uncertain parameters of each scenario are concretely realized. In the upper-level of our bi-level random programming model, the defender must make a decision to interdict even when the attacker's budget is not clear. In each case of the lower-level, each attacker specifies an attack plan with a known budget and knows the interdiction decision of the network defender. We use conditional risk value (CVaR) [18] as a risk indicator to measure risk aversion.

Our model will have to take into account the multiple attackers with uncertain budgets, where each attacker has a specific budget. The budgets of the defender and the attackers must be within their given limits. It is not certain which attacker the network defender will encounter, nor does it know the attacker's budget. However, according to the probability distribution of known parameter values, the defender can estimate the attacker's budget [19]. In order to simulate the uncertainty in the budget of multiple potential attackers, we consider a set of the limited number of scenarios S in the stochastic optimization problem. Each scenario represents an attacker with a specific budget. In the case of a limited budget, the defender chooses the best subset of arcs for deploying countermeasures to minimize the maximum loss in all scenarios (Table 1).

Table 1 Notation

Notation	Description
Sets	
N	Set of nodes
N_I	Set of initially nodes
N_T	Set of key nodes
A	Set of arcs
$A_t(i)$	Set of arcs with the tail pointing to node i
$A_h(i)$	Set of arcs with the head pointing to node i
S	Set of scenarios index by s
Parameters	
l_t	Loss resulting from breaching a key node $t \in N_T$
o_{ij}	Exposure probability of FCs deployed on arc (i, j)
p_{ij}	Probability of successful attack through the arc (i, j)
	equipped with TCs
$\bar{p}_{ij}$	Probability of successful attack through the arc (i, j)
	Equipped with FCs or NCs
p^s	Probability of scenario s
λ	The coefficient of risk
α	Confidence level
b_a	Attacker's budget
b_d	Defender's budget for deploying TCs
$\bar{b}_d$	Defender's budget for deploying NCs
c_{ij}^{attack}	Attack cost through arc (i, j)
c_{ij}^d	Cost of TCs on arc (i, j)
$\bar{c}_{ij}^d$	Cost of FCs on arc (i, j)
Decision variables	
x_{ij}	1 if TCs are deployed on arc (i, j), 0 otherwise
$\bar{x}_{ij}$	1 if FCs are deployed on arc (i, j), 0 otherwise
f_{ij}	1 if arc (i, j) is used for one or more attacks, 0 otherwise
z_i	Probability of node i being destroyed
y_{ij}	Product of z_i and f_{ij}
η	Upper-level variable (represents the value-at-risk, VaR)
v^s	Excess loss variable in scenario $s \in S$

3.1 Minimize the Disutility of Defender

The upper-level model is to minimize the disutility of defenders. The objective function (1) consists of two parts, where the first part calculates the expected minimum disutility of defenders in all scenarios. And the expected maximum loss in all scenarios is equal to the probability p^s of scenario s multiplied by the maximum total loss Q^s caused by the attackers to the defender in scenario s. The second part simulates the CVaR metric of huge loss risk. Constraints (2) and (3) limit the budget for deploying TCs and FCs, respectively. Constraints (4) prevent the TCs and FCs from being deployed at the same arc. Constraint (5) calculates the additional loss in all attack scenarios, and the excess loss variable in scenario s is greater than or equal to the maximum total loss minus the variables at the upper-level. Constraints (6) are binary requirements.

$$H = \min \sum_{s \in S} p^s Q^s(x, \bar{x}) + \lambda(\eta + \frac{1}{1-\alpha} \sum_{s \in S} p^s v^s) \tag{1}$$

$$\text{s.t.} \sum_{(i,j) \in A} c_{ij}^d x_{ij} \le b_d \tag{2}$$

$$\sum_{(i,j) \in A} \bar{c}_{ij}^d \bar{x}_{ij} \le \bar{b}_d \tag{3}$$

$$x_{ij} + \bar{x}_{ij} \le 1 \quad \forall (i,j) \in A \tag{4}$$

$$Q^s(x, \bar{x}) - \eta \le v^s \tag{5}$$

$$x_{ij}, \bar{x}_{ij} \in \{0, 1\} \quad \forall (i,j) \in A \tag{6}$$

$$\eta \in R \tag{7}$$

$$v^s \ge 0 \quad \forall s \in S \tag{8}$$

3.2 Maximize the Utility of Attacker

The lower-level model is to maximize the utility of the attacker. That is, the objective function (9) maximizes the loss caused by interdicting the target node multiplied by the probability of the target node t being destroyed. Constraint (10) limits that the total expenditure of the attack must be within their budget. Constraint (11) indicates that whether the attacker attacks the arc ij has a decisive influence on its success probability. If the attacker takes action, the probability of success is the product of the true attack probability, the fake attack probability, and the non-attack probability. Constraints (12) ensure that there is a higher probability that an attacker successfully destroyed node through an arc (i, j), and the probability of node j being attacked is less than or equal to the probability of successfully attacking through arc

ij.Constraints (13) indicate that only one attack is required on an arc ij.Constraints (14) indicate that if an arc is attacked one or more times, it will be 1, and if there is no attack, it will be zero.

$$Q^S(x, \bar{x}) = \max \sum_{t \in N_T} l_t z_t \tag{9}$$

$$s.t. \sum_{(i,j)\in A} c_{ij}^{\text{attack}} f_{ij} \le b_a \tag{10}$$

$$\beta_{ij} = f_{ij} \cdot p_{ij}^{x_{ij}} \cdot \bar{p}_{ij}^{(1-o_{ij})\bar{x}_{ij}} \cdot \bar{p}_{ij}^{1-(x_{ij}+\bar{x}_{ij})} \tag{11}$$

$$z_j \le \sum_{(i,j)\in A_e(j)} z_i \beta_{ij} \quad \forall j \in N/N_I \tag{12}$$

$$\sum_{i,j\in A_e(j)} f_{ij} \le 1 \quad \forall j \in N/N_I \tag{13}$$

$$f_{ij} \in 0, 1 \quad \forall (i, j) \in A \tag{14}$$

$$0 \le z_j \le 1 \quad \forall j \in N \tag{15}$$

Constraints (12) are nonlinear; however, the only nonlinear terms are $z_i f_{ij}$. In this regard, we define the auxiliary variables w_{ij} to replace them. For each $(i, j) \in A$ and $i \in N/N_I$, a set of new constraints is added to the formulation to line $w_{ij} = z_i f_{ij}$.

$$w_{ij} \le z_i \tag{16}$$

$$w_{ij} \le f_{ij} \tag{17}$$

$$w_{ij} \ge 0 \tag{18}$$

$$w_{ij} \ge f_{ij} + z_i - 1 \tag{19}$$

4 Solution Approach

It is difficult to solve the bi-level linear problem using existing algorithms directly. Because the model is more complicated, and it is an NP-hard problem [20]. In the past few years, many studies have proposed the use of precise algorithms or hybrid heuristics to solve the bi-level optimization problem. For example, Shamekhi Amiri et al. [21] invented a global iterative search method, inferring the potential behavior of followers as a new constraint for each iteration in the leader problem. In this paper, we propose a heuristic solution algorithm, namely SA-CPLEX, where the SA algorithm is used to solve the defender problem in the upper-level, and the CPLEX solver is used to obtain the optimal attacker's strategy in the lower-level.

In the heuristic algorithm, one of the crucial parts is the representation of the solution [22]. The heuristic algorithm also acts alternately on the coding space and the solution space [23]. It is a way to find the best solution within an acceptable time. The generation of the neighborhood and the fast calculation of the objective function are the goals of this algorithm. In addition, it must ensure that it has access to the entire solution space. The value of the initial solution will have some impact on the performance of the heuristic algorithm. In order to give an initial solution to the defender problem, we use a randomly sized subset as the central node [24]. And we define and use a single operator to generate adjacent solutions. This operator is called "Swap" and is used to change the solution representation to an arc in the array. Four parameters, T_0, T_f, δ and $I_{\max}$ are used in the algorithm. Among them, T_0 represents the initial temperature, and T_f is the final temperature at which the SA process is stopped [25]. δ is used as the cooling rate parameter of the upper-level problem. $I_{\max}$ is the number of solutions generated by the algorithm at each temperature.

The detailed algorithm is given in Algorithm 1. As shown in Algorithm 1, the algorithm first generates the initial solution of the defender and then improves this initial solution through subsequent iterations. According to the given defender's strategy $(x, \bar{x})$, the attacker's objective value $Q(x, \bar{x})$ can be calculated according to (9). We fix the initial temperature as T_0 and use it as the initial parameter of the algorithm. $(x, \bar{x})_{\text{best}}$ represents the optimal solution found so far, and f_{best} represents its relative objective function value. For each temperature, we define $\triangle E$ as the difference between the newly obtained solution and the target of the existing solution, that is, $\triangle E = H(Q((x, \bar{x})')) - H(Q(x, \bar{x}))$. We repeat this cycle at most once at each temperature and use the optimal solution obtained so far. Then the temperature decrease to $T \leftarrow \delta \times T$ after each iteration. Repeat the training until the current temperature T is lower than the pre-specified final temperature T_f, the algorithm ends.

5 Experiments

All experiments were performed on a personal computer with a 2.90 GHz Core (TM) i7-10700 CPU AND 16GB RAM. We implement our proposed algorithm in Matlab 2020a and ILOG CPLEX 12.10 is applied to solve the attacker's problems optimally. We have conducted a lot of experiments so that the average result will not change too much (Table 2).

5.1 *Parameter Setup*

We use an attack graph with a node size of $|N|$ (=50) for numerical experiments, and the arc size is about $2.15 \times |N|$. Breach loss of the goal nodes is uniformly from (500, 150), while the budget of this random attacker is Weibull distribution (100, 200). The probability of attack success is uniformly from (0, 1). The probability of a successful attack through the arc (i, j) equipped with TCs and FCs is between 0 and 1. Moreover, three different level of confidence are also tested for the experiments,

Algorithm 1 SA-CPLEX (T_0, T_f, δ, $I_{\max}$)

```
Generate a random initial solution $(x, \bar{x})$
$\forall s \in S$,Calculate $Q^S(x, \bar{x})$ using CPLEX
$Q(x, \bar{x}) = \sum_s Q^s(x, \bar{x})$
$T \leftarrow T_0$, $H_{\text{best}} \leftarrow H(Q(x, \bar{x}))$, $(x, \bar{x})_{\text{best}} \leftarrow (x, \bar{x})$, $I \leftarrow 0$
while $T > T_f$ do
    for $I < I_{\max}$ do
        Generate a new solution $(x, \bar{x})'$ based on $(x, \bar{x})$ using "Swap" operator
        $\forall s \in S$,Calculate $Q^S(x, \bar{x})'$ using CPLEX
        $Q((x, \bar{x})') = \sum_s Q^s((x, \bar{x})')$
        $\triangle E \leftarrow H(Q((x, \bar{x})')) - H(Q(x, \bar{x}))$
        if $\triangle E < 0$ then
            $(x, \bar{x}) \leftarrow (x, \bar{x})'$
            $H(Q(x, \bar{x})) \leftarrow H(Q((x, \bar{x})'))$
        else
            $\rho \leftarrow rand(0, 1)$
            if $\rho > e^{-|\triangle E|/T}$ then
                $(x, \bar{x}) \leftarrow (x, \bar{x})'$
                $H(Q(x, \bar{x})) \leftarrow H(Q((x, \bar{x})'))$
            end if
        end if
        if $H(Q(x, \bar{x})) < H_{\text{best}}(Q(x, \bar{x}))$ then
            $(x, \bar{x})_{\text{best}} \leftarrow (x, \bar{x})$, $H_{\text{best}} \leftarrow H(Q(x, \bar{x}))$
        end if
        $(x, \bar{x}) \leftarrow (x, \bar{x})_{\text{best}}$
        $I \leftarrow I + 1$
    end for
    $I \leftarrow 0$
    $T \leftarrow \delta \times T$
end while
return $(x, \bar{x})_{\text{best}}$, $H_{\text{best}}$
```

Table 2 Parameters and default values

Parameters	Values
Network size (nodes, $\|N\|$)	50
Arcs, $\|A\|$	$\approx 2.15 \times \|N\|$
Breach loss of the goal nodes	∼uniform (500, 1500)
Defender's budget, b_d	150
Level of confidence, α	0.2, 0.5, 0.8
Risk coefficient, λ	2, 4, 8, 10
Random attacker budget, b	∼weibull (50, 500)

i.e., $\alpha \in \{0.2, 0.5, 0.8\}$. We set the exposure probability of FCs deployed on arc (i, j) is in the range (0, 1). And Four different values of risk factors are also tested for the experiments, i.e., $\lambda \in \{2, 4, 8, 10\}$. Physical attacks or cyber-attacks on important infrastructure systems are also within the range that our attack graph can simulate [26].

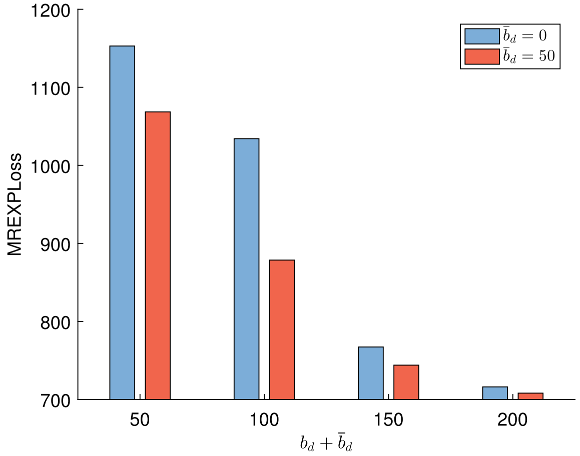
5.2 Effects of Involving FCs

Figure 2 shows variation of mean-risk expected maximum loss (MREXPLoss) with and without FC budget. For maps of different sizes, we have different defender's budgets. The eventual experimental results showed that when the total budget remains the same, the more budget spent on FCs, the smaller the MREXPLoss. And as the total budget value increases, MREXPLoss becomes smaller. As the budget increases, the defender has sufficient budget to place countermeasures in more attack paths. As a result, the combination of various defensive countermeasures has increased, making it more difficult for attackers to attack. At the same time, it can be seen from the experiment that when there is a lot of total budgets, the defender can protect more attack paths. In other words, the defender can have more combinations of different attack paths.

5.3 Effects of the Probability of Exposure

Figure 3 shows the variation of MREXPLoss under different exposure probabilities of FCs. We can see from the experimental results that the greater the probability of FCs being exposed through the arc (i, j), the smaller the value of MREXPLoss. In other words, when the probability of FCs being exposed is very small, the FC can be well hidden. This will cause more interference to the attacker, which will cause the attacker to make more wrong decisions. Therefore, the defender can better interdict the attack and reduce some losses.

Fig. 2 Variation of b_d and $\bar{b}_d$ with number of total budgets. Other parameters are: $|N| = 50$, $p_{ij} = 0.5$, $\bar{p}_{ij} = 0.5$, $o = 0.75$, λ=0



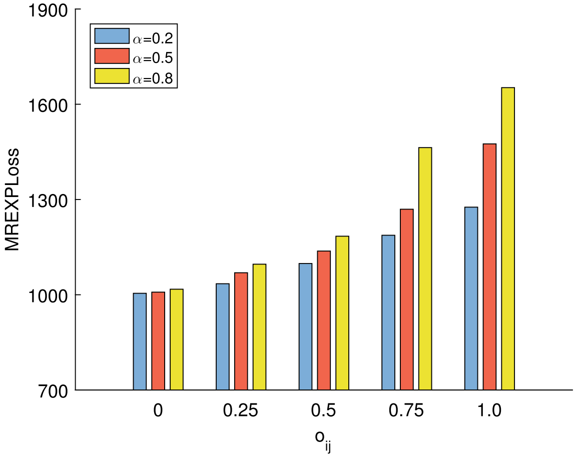


Fig. 3 Variation of α with possibility of o_{ij}. Other parameters are: $|N| = 50$, $p_{ij} = 0.5$, $\bar{p}_{ij} = 0.5$, $\lambda = 0$

5.4 *Effects of the Probability of Successful Attack*

Figures 4 and 5 show the variation of MREXPLoss in the probability of successful attack through the arc (i, j) with TCs and FCs, respectively. It can be concluded from the experimental results that when the attacker's success probability to TCs increases, the defender is more vulnerable to attack. Similarly, when the attacker's probability of success in FCs increases, the attacker will be more likely to destroy these TCs. As the probability of being successfully attacked in TCs or FCs is higher, their loss is greater.

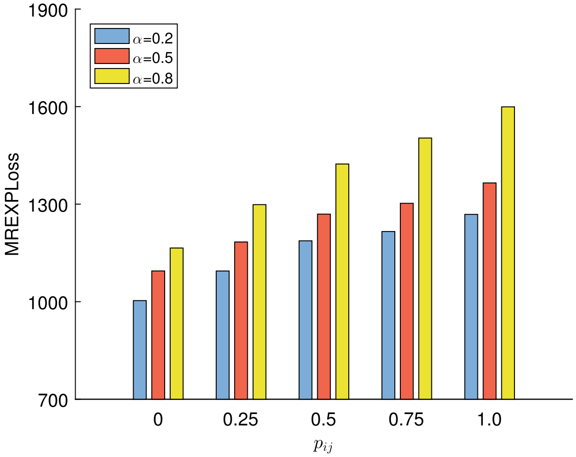
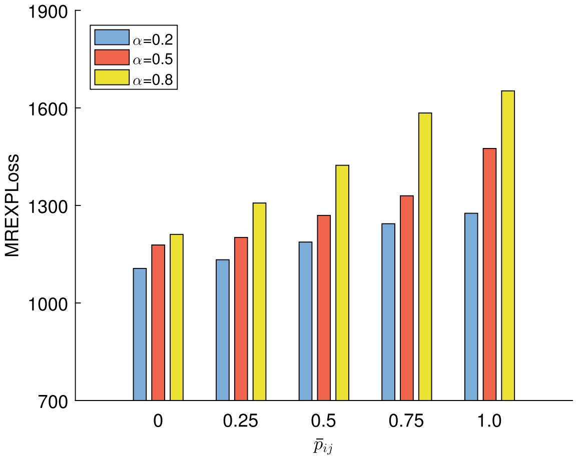


Fig. 4 Variation of α with possibility of p_{ij}. Other parameters are: $|N| = 50$, $\bar{p}_{ij} = 0.5$, $o = 0.75$, $\lambda = 0$

Fig. 5 Variation of α with possibility of $\bar{p}_{ij}$. Other parameters are:$|N| = 50$, $p_{ij} = 0.5$, $o = 0.75$, $\lambda = 0$



5.5 *Effects of the Budget of TCs and FCs*

Figure 6 shows the gap between the budget of TCs and FCs when the total budget remains the same. It can be seen from the experimental results that when the total budget value becomes larger, the constant real budget MREXPLoss is decreasing. As the total budget increases, MREXPLoss decreases at a higher rate. The defender can mislead the attacker by adjusting the ratio of the FCs budget to the TCs budget, thereby achieve a better protective effect.

Fig. 6 Variation of $b_d = 0$ and $\bar{b}_d$ with possibility of total budgets. Other parameters are: $|N| = 50$, $p_{ij} = 0.5$, $\bar{p}_{ij} = 0.5$, $o = 0.75$, $\lambda = 0$

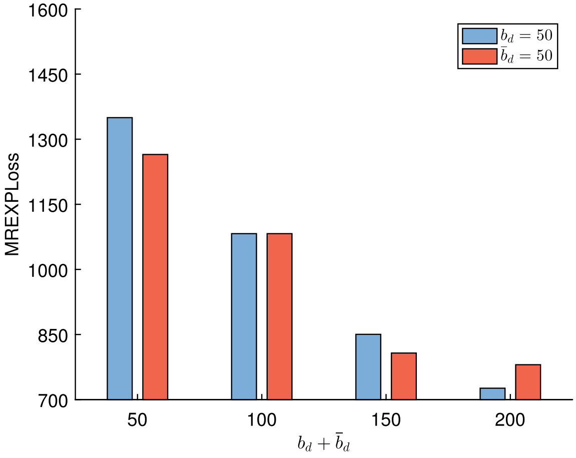
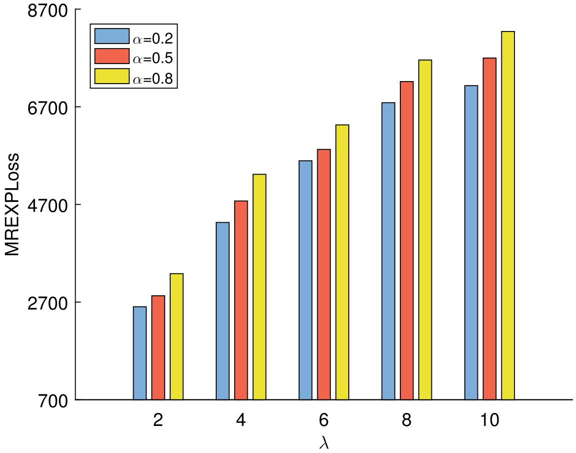


Fig. 7 Variation of α with possibility of λ. Other parameters are: $|N| = 50$, $p_{ij} = 0.5$, $\bar{p}_{ij} = 0.5$, $o = 0.75$



5.6 *Effects of Confidence Level and Risk Coefficient*

In our proposed model, two risk parameters, confidence level (α) and risk coefficient (λ) are our important parameter members. Figure 7 shows the variation of MREXPLoss with respect to λ under three different levels of α. As shown in the experimental results, we can clearly see the result of using risk metrics (CVaR) to minimize the losses caused by random attackers' budget cyber-attacks. The larger the value of α, the more concerned about the situation of major losses, and the more conservative the decision-making. To a certain extent, the goal of minimizing the expected value of the main loss scenario is also considered here. In other words, minimizing huge losses is not the only goal of our model. Because in this case, the optimal interdiction decision under risk-neutral preference also partially considers the minimization of large losses.

6 Conclusions

This article studies the problem of the best interdicting strategy from the perspective of the defender, where the defenders seek to minimize the risk of major losses. In addition, the budget uncertainty of multiple potential attackers and the fake countermeasures deployed by the defender are considered. Based on the extension of the traditional attack graph, we establish a risk aversion bi-level stochastic network interdiction model to formulate this problem. In our risk aversion model, our risk measure is CVaR. In response to this model, we developed a customized binary bi-level programming problem algorithm that combines randomness and risk aversion. Our model is closer to reality and considers more comprehensively for the defender. The experimental results show that the interdiction decision provided by our model is more robust than the traditional model. Successfully achieved the minimization of the huge loss risk caused by network attacks by avoiding risks. In the future, this paper can be easily applied to the security of the underwater wireless sensor networks [27], the gird monitoring systems [28] and the critical infrastructure systems [29].

Acknowledgements This work was support from the National Science Foundation of China (Grant No. 61877007), Fundamental Research Funds for the Central Universities (Grant No. DUT20GJ205), and the Shandong National Science Foundation of China (Grant No. ZR202103040468).

References

1. S. Noel, S. Jajodia, Optimal ids sensor placement and alert prioritization using attack graphs. J. Netw. Syst. Manage. **16**(3), 259–275 (2008)
2. S.B.H. Shah, F. Yin, I.U. Khan, Z. Chen, M. Zakarya, Collating and analysing state-of-the-art hierarchical routing protocols in WSN to increase network lifetime and conserve energy, in *Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS 2017*, Cambridge, United Kingdom, July 19–20, 2017, ed. by M. Hammoudeh, R.M. Newman, ACM, 2017, pp. 42:1–42:10. [Online]. Available: https://doi.org/10.1145/3102304.3102346
3. S.B. Shah, C. Zhe, F. Yin, I.U. Khan, S. Begum, M. Faheem, F.A. Khan, 3d weighted centroid algorithm & rssi ranging model strategy for node localization in wsn based on smart devices. Sustain. Cities Soc. **39**, 298–308 (2018)
4. R. Zhang, Q. Zhu, Y. Hayel, A bi-level game approach to attack-aware cyber insurance of computer networks. IEEE J. Select. Areas Commun. **35**(3), 779–794 (2017)
5. S.A. Zonouz, H. Khurana, W.H. Sanders, T.M. Yardley, Rre: a game-theoretic intrusion response and recovery engine. IEEE Trans. Parallel Distrib. Syst. **25**(2), 395–406 (2014)
6. S. Bistarelli, F. Fioravanti, P. Peretti, Defense trees for economic evaluation of security investments, in *Proceedings of the The First International Conference on Availability, Reliability and Security, ARES 2006, The International Dependability Conference—Bridging Theory and Practice, April 20–22 2006, Vienna University of Technology, Austria*. IEEE Computer Society (2006), pp. 416–423 [Online]. Available: https://doi.org/10.1109/ARES.2006.46
7. S.D. Roy, S. Kundu, Performance of an adaptive power based cdma cognitive radio networks, in *IEEE Symposium on Industrial Electronics and Applications (ISIEA)*, pp. 28–33 (2010)
8. E. Serra, S. Jajodia, A. Pugliese, A. Rullo, V.S. Subrahmanian, Pareto-optimal adversarial defense of enterprise systems. ACM Trans. Inf. Syst. Secur. **17**(3), 11:1–11:39 (2015). Available: https://doi.org/10.1145/2699907
9. M. Alhomidi, M. Reed, Finding the minimum cut set in attack graphs using genetic algorithms, in *International Conference on Computer Applications Technology (ICCAT)*, pp. 1–6 (2013)
10. M.H.R. Khouzani, Z. Liu, P. Malacaria, Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. Eur. J. Oper. Res. **278**(3), 894–903 (2019)
11. K. Zheng, L.A. Albert, J.R. Luedtke, E. Towle, A budgeted maximum multiple coverage model for cybersecurity planning and management. IISE Trans. **51**(12), 1303–1317 (2019)
12. T.H. Bhuiyan, H.R. Medal, A.K. Nandi, M. Halappanavar, Risk-averse bi-level stochastic network interdiction model for cyber-security risk management. Int. J. Crit. Infrastructure Prot. **32**, 100408 (2021). https://doi.org/10.1016/j.ijcip.2021.100408
13. G. Oliva, R. Setola, M. Tesei, A stackelberg game-theoretical approach to maritime counter-piracy. IEEE Syst. J. **13**(1), 982–993 (2018)
14. B.S. Pay, J.R.W. Merrick, Y. Song, Stochastic network interdiction with incomplete preference. Networks **73**(1), 3–22 (2019). https://doi.org/10.1002/net.21831

15. S. Jalali, M. Seifbarghy, S.T.A. Niaki, A risk-averse location-protection problem under intentional facility disruptions: a modified hybrid decomposition algorithm. Transp. Res. Part E-logist. Transp. Review **114**, 196–219 (2018)
16. X. Lei, S. Shen, Y. Song, Stochastic maximum flow interdiction problems under heterogeneous risk preferences. Comput. Oper. Res. **90**, 97–109 (2018)
17. A.M.F. Fard, M. Hajiaghaei-Keshteli, A bi-objective partial interdiction problem considering different defensive systems with capacity expansion of facilities under imminent attacks. Appl. Soft Comput. **68**, 343–359 (2018)
18. G. Yu, J. Zhang, Multi-dual decomposition solution for risk-averse facility location problem. Transp. Res. Part E: Logist. Transp. Rev. **116**, 70–89 (2018)
19. A.K. Nandi, H.R. Medal, S. Vadlamani, Interdicting attack graphs to protect organizations from cyber attacks: a bi-level defender-attacker model. Comput. Oper. Res. **75**, 118–131 (2016)
20. Q. Li, M. Li, J. Gan, C. Guo, A game-theoretic approach for the location of terror response facilities with both disruption risk and hidden information. Int. Trans. Oper. Res. **28**(4), 1864–1889 (2021). https://doi.org/10.1111/itor.12900
21. A. Shamekhi Amiri, S.A. Torabi, R. Ghodsi, An iterative approach for a bi-level competitive supply chain network design problem under foresight competition and variable coverage. Transp. Res. Part E: Logist. Transp. Rev. **109**, 99–114 (2018). Available: https://www.sciencedirect.com/science/article/pii/S1366554517305483
22. N. Aliakbarian, F. Dehghanian, M. Salari, A bi-level programming model for protection of hierarchical facilities under imminent attacks. Comput. Oper. Res. **64**, 210–224 (2015)
23. R. Khanduzi, A.K. Sangaiah, A fast genetic algorithm for a critical protection problem in biomedical supply chain networks. Appl. Soft Comput. **75**, 162–179 (2019)
24. N. Ghaffarinasab, A. Motallebzadeh, Hub interdiction problem variants: models and metaheuristic solution algorithms. Eur. J. Oper. Res. **267**(2), 496–512 (2018)
25. S.-W. Lin, J.N. Gupta, K.-C. Ying, Z.-J. Lee, Using simulated annealing to schedule a flowshop manufacturing cell with sequence-dependent family setup times. Int. J. Prod. Res. **47**(12), 3205–3217 (2009)
26. P.J. Hawrylak, M. Haney, M. Papa, J. Hale, Using hybrid attack graphs to model cyber-physical attacks in the smart grid, in *2012 5th International Symposium on Resilient Control Systems* (2012), pp. 161–164
27. S.B.H. Shah, Z. Chen, S.H. Ahmed, F. Yin, M. Faheem, S. Begum, Depth based routing protocol using smart clustered sensor nodes in underwater WSN, in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, June 26–27, 2018*, ed. by A. Abuarqoub, B. Adebisi, M. Hammoudeh, S. Murad, M. Arioua. ACM (2018), pp. 53:1–53:7. Available: https://doi.org/10.1145/3231053.3231119
28. S.B.H. Shah, L. Wang, M.E. Haque, M.J. Islam, A. Carie, N. Kumar, Lifetime improvements of smart sensors maintenance protocol in prospect of iot-based rampal power plant, in *2020 16th International Conference on Mobility, Sensing and Networking (MSN)* (2020), pp. 260–267
29. Q. Li, M. Li, R. Zhang, J. Gan, A stochastic bilevel model for facility location-protection problem with the most likely interdiction strategy, in *Reliability Engineering & System Safety* (2021), pp. 1–50. Available: https://doi.org/10.1016/j.ress.2021.108005