HOW DOES THE INTERNAL STRUCTURE OF A COMPLEX SYSTEM INFLUENCE ITS OVERALL RISK? RISK MINIMIZATION FOR TREES

A. A. Shiroky* and A. O. Kalashnikov**

*,**Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

*✉ shiroky@ipu.ru, **✉ aokalash@ipu.ru

Abstract. The Defender–Attacker problem is often employed as a mathematical framework in risk management. In this problem, the above players with opposite goals allocate limited resources to system elements to minimize or maximize a risk function. It has been well-studied under the assumption of independent system elements. However, in complex systems, elements interact, causing significant differences between the measured and predicted risks. Although models with the interdependence of system elements are regularly considered in the literature, no comprehensive understanding has been formed of how the structure of a complex system influences its overall risk. We address this issue in a series of papers by investigating system structures of increasing complexity. Chains and stars have been analyzed previously; in this paper, the findings are extended to arbitrary trees. We optimize the placement of elements within a tree to minimize risk; derive upper bounds for the relative error of an approximate algorithmic solution of this problem for trees with a few branches and leaves; and explore the dynamics of these bounds when increasing the number of leaves and branches. As demonstrated, the resulting upper bounds do not exceed their counterparts for stars from the previous works.

Keywords: complex systems, risk, system structure, risk management, risk minimization algorithms, the problem of optimal element placement.

INTRODUCTION

The complexity of risk management is primarily connected with its multidisciplinarity. For example, the authors of the book [1] identified 15 *dimensions of* risk management, which include both relatively narrow fields (risk management in supply chains, financial risk management) and global ones (e.g., ethics in risk management). The second part of the book considered six cross-disciplines that partially overlap all fields, namely, *risk culture*, *risk-based decision making*, *risk leadership in complexity*, *resilience*, *communication uncertainty*, and *organizational change management and risk*. This classification is neither complete nor the only possible one. It illustrates that risk management can be discussed in relation to the specifics of a particular controlled system and with application to processes and properties characteristic of whole classes of systems. In this case, the models and methods, terminology, and even the definition of risk used will differ.

Without an accepted universal risk management model, the unifying role is played by basic principles valid for any controlled system. It is reflected in the ISO standard [2], offering a fairly general definition of risk due to uncertainty influencing goal achievement. As noted, the consequence of this influence should be understood as a deviation from the expected result or event (positive and (or) negative). To use such a definition in practice, one has to *measure* goals, uncertainty, and the deviations caused by it. Hence, it is necessary to investigate quantitative relationships for risk management using an appropriate mathematical apparatus.

Based on the character of risk management intended to minimize deviations, the mathematical problem of risk management should belong to the class of optimization problems. (In the case of players with strategic behavior in the system, the problem can be game-theoretic; for example, see [3–5].) However, an attempt to find studies devoted to mathematical models of risk management not related to a particular ob-

ject, class, or field is likely to fail. The reason is that if a research work deals with mathematical models of optimization applied to risk management, it will belong to the corresponding branch of mathematics, not to risk management. If the matter concerns risk management, the controlled object will be described explicitly, which binds the research work to its specifics.

Nevertheless, one may suppose the existence of models universal enough to consider in quantitative terms the general principles of risk management without binding to particular controlled objects, systems, or their classes. As it seems, this criterion is best met by the model of a protected system in the form of a weighted directed graph: the vertices are system elements (arbitrary objects), and the arcs with assigned weights characterize the direction and strength of connections between these elements that are important for risk management.

Note that such a graph is a complex network of arbitrary topology. The control object modeled (a protected system) can be a social network [6], a network of organizations [7], a computer network [8], or even belong to another class. In this paper, we consider a purely mathematical problem statement. In other words, the structure of a protected system does not necessarily reflect exactly the physical or organizational structure of the object modeled. At the same time, the arcs of a corresponding digraph show the mutual influence of elements. For example, when reducing the risks of aviation accidents in a region, the model will reflect rather the structure of causal relations between the types of accidents, their preconditions, and influence factors than the connections between the elements of the air traffic control infrastructure. If all system elements are independent from the viewpoint of risk transfer to each other, an adequate model will be a special case of an edgeless graph.

The general problem of risk management in complex networks can be formulated as follows.

Consider a protected system consisting of a finite set of elements (arbitrary objects): $S = \{s_1,..., s_i,..., s_n\}$, $i \in N = \{1,..., n\}$, $n \in \mathbb{N}$. Suppose the existence of two actors (also arbitrary for the time being), which will be called players *A* and *D* (the *Attacker* and *Defender*, respectively). They have opposite interests regarding the state of system *S*.

Let player *D* possess some resource amount $X \geq 0$ to be allocated, in an arbitrary way, among the elements of system *S*: $x = (x_1,\ldots, x_n)$, $x_i \geq 0$, $i \in N$, $\sum_{i=1}^{n} x_i \leq X$. Similarly, player *A* also has some resource amount $Y \geq 0$ to be arbitrarily allocated among the elements of system *S*: $y = (y_1,\ldots, y_n)$, $y_i \geq 0$, $i \in N$, $\sum_{i=1}^{n} y_i \leq Y$.

The model under consideration involves any measurable and arbitrarily divisible resource that can be represented by a nonnegative real number. Depending on the context, the resource can be capital, labor, time, production capacity, etc. (e.g., costs).

Suppose that the risk transfer influence is described by a weighted digraph $G(S, W)$, $W \subseteq S \times S$, $w_{ij} = (s_i, s_j) \in W$, $i, j \in N$. Let functions

$$\rho : s \to \mathbb{R}^0_+,\ \sigma : W \to \mathbb{R}^0_+,$$

be defined on $G(S,W)$, where ρ_i, $i \in N$, is the weight of vertices (the current value of local risk) and σ_{ij}, $i, j \in N$, is the weight of arcs (the intensity of risk transfer between system elements). The matrix $\Sigma = \|\sigma_{ij}\|$ represents the degree (or strength) of influence of the *i*th element of *S* on the *j*th one. The initial value of the functions ρ_i at $t = 0$, $\rho_i = \rho_i(x, y, t) = \rho_i(x, y, t = 0)$, is determined by the resource allocations x and y. The subsequent values of the weights ρ_i (for $t > 0$) depend only on the time-preceding values of these functions. Due to the mutual influence of system elements, their weights vary as follows:

$$\rho_i(t+1) = \rho_i(t) + \sum_{k=1}^{n} \sigma_{ik} (\rho_i(t) - \rho_i(t-1)),$$
$$t = 0, 1,\ldots;\ \rho_i(t = 0) = \tilde{\rho}_i. \qquad (1)$$

The arguments x and y in the above formula are omitted for the sake of compactness.

Let $\mathcal{X}(X)$ and $\mathcal{Y}(Y)$ denote the sets of admissible allocations of the resource amounts *X* and *Y*, respectively, among the elements of system *S* by players *D* and *A*:

$$\mathcal{X}(X) = \left\{(x_1,..., x_n) \in \mathbb{R}^n_+ : x_i \geq 0,\ i \in N,\ \sum_{i=1}^{n} x_i \leq X\right\},$$

$$\mathcal{Y}(Y) = \left\{(y_1,..., y_n) \in \mathbb{R}^n_+ : y_i \geq 0,\ i \in N,\ \sum_{i=1}^{n} y_i \leq Y\right\}.$$

Then, the problem of player *D* (the Defender's problem) is to find a resource allocation $x^* \in X$ minimizing the overall risk (i.e., the risk characterizing the

vulnerability of the entire system). It can be formally written as

$$x^* = \operatorname*{Argmin}_{x\in X} \lim_{t\to\infty} \rho(x,\, y,\, t) = \operatorname*{argmin}_{x\in X} \sum_{i=1}^{n} \lim_{t\to\infty} \rho_i(x,\, y,\, t). \quad (2)$$

This problem with constraints imposed on the eigenvalues of the mutual influence matrix of elements was solved in the paper [8]. For the problem statement under consideration, it is required to identify, with sufficient accuracy, the current values of local risks and the functional dependencies $\rho(x, y, \cdot)$ and, moreover, to quantitatively characterize the mutual influence of local risks. These tasks can be extremely labor-intensive and even impossible for real systems. Therefore, a topical problem is to find general risk management principles for a complex network system in order to achieve risk reduction even under incomplete information. The paper is devoted to solving this problem for trees.

The remainder of this paper is organized as follows. Section 1 briefly reviews mathematical models of failure propagation in complex networks. Next, Section 2 provides a general statement of the risk management problem in a complex system with a tree structure. A suboptimal solution of this problem is proposed in Section 3. The prospects of further research are discussed in the Conclusions.

1. MATHEMATICAL MODELS OF FAILURE PROPAGATION IN COMPLEX NETWORKS: A BRIEF REVIEW

In the most general case, the structure of a complex system can be considered a complex network of arbitrary topology. A successful attack on some element of a system (in other words, its failure) will be comprehended as the occurrence of an event under which this element ceases functioning. For the sake of simplicity, we analyze only the binary case in this paper: an element can be completely functional or nonfunctional. Many models have been developed to investigate various destructive effects (including targeted attacks on vertices and edges) in such networks, and new ones are proposed regularly. Risk assessment models of failure propagation are widely used when studying various complex systems, such as cyber-physical [9–17], computational [18–19], and social-medical [20–22].

Early models described the development of failures caused by non-targeted (e.g., random) influences. Among them, the best-known ones are the error resilience model [23–25], the forest fire model [26–28] and its derivatives, cellular automata-based models [29–32], and percolation models with random attacks [33]. The latter have several modifications in which destructive influences on network vertices and edges are targeted. These include percolations with targeted attacks [34–36], percolations with localized attacks [37–40], and *k*-core percolations [41–43].

The above failure propagation models combine well with the classical models of risk management in complex Defender–Attacker networks [44–46]. Recall that such models describe a conflict between two players (the Defender and Attacker) with opposite goals concerning the system under consideration. The Attacker spends available resources from some limited pool to disable the system. In turn, the Defender attempts to counteract the Attacker. In classical formulations, the Defender optimally allocates the resources among system elements to minimize its overall risk. However, this player can alternatively modify the system structure to achieve the same goal. Other models are required to describe such a scenario.

For example, the models of cascading error propagation [47, 48] cover structural changes, but such changes are not supposed targeted. The possibility of an intentional structure change is envisioned in models modified to the case of two interconnected networks [49–51]; meanwhile, this possibility applies only to the edges connecting the networks to each other.

Thus, the existing modeling apparatus is insufficient to manage the structure of a complex system, including minimization of its overall risk. In this paper and several previous studies, we focus on calculating the influence of the structure on risk, without regard to the resources allocated.

For this purpose, the basic problem (2) has been reformulated: the search for an optimal resource allocation to the elements of a fixed-structure system has been replaced by the search for an optimal placement of elements in some given structure and comparison of the structures. Dealing with this problem head-on seems impractical due to its high computational complexity, so we find approximate solutions for various structures in ascending order of their complexity, namely:

1) simple chain (see the analytical solution in [52]),

2) star (see an approximate solution with a guaranteed error in [53]),

3) tree (considered here),

4) an arbitrary structure (the solution will be constructed by generalizing the results established for simpler structures).

Note that the general efficient management problem of a complex system under uncertainty is equiva-

lent to the problem of risk minimization, where risk is understood as a measurable deviation from the maximum effective (target) mode of functioning of this system [2]. The mathematical equivalence of the problems was shown, e.g., in the paper [54]. No doubt, the problem of synthesizing or improving the structure of a controlled system (in particular, an organizational system) does not come to resource allocation, and risk is only one of the key performance indicators of its functioning. Nevertheless, when achieving the goals of a control system, risk should be considered the most significant indicator.

2. RISK CONTROL IN A COMPLEX SYSTEM WITH A TREE STRUCTURE: PROBLEM STATEMENT

Suppose that a protected system includes n elements $s_1,..., s_n \in S$, $n \in \mathbb{N}$. Let two numbers be assigned to each element: $p_i^0 \in (0, 1]$, denoting the eigen probability of a successful attack on the ith element, and $u_i > 0, u \in \mathbb{R}^+$, denoting the damage amount inflicted in case of a successful attack on the ith element.

Definition 1. The eigen risk of the ith element is the value $\rho_{s_i}^0 = u_i p_i^0$. ♦

We define a structure $W_m = \langle G(V, E), T\rangle, T \subseteq V$, where $G(V, E)$ is a directed graph with a vertex set V and an arc set E, and T is a subset of V (further called the *perimeter*). This paper considers structures with a perimeter consisting of exactly one vertex.

Definition 2. A vector sequence

$$B = \left\{\left(b_{01},..., b_{0q_0}\right), \left(b_{11},..., b_{1q_1}\right),..., \left(b_{l1},..., b_{lq_l}\right),..., \left(b_{L1},..., b_{Lq_L}\right)\right\},$$
$$b, L, q_l \in \mathbb{N}, l \in \mathbb{N} \cup \{0\},$$

is said to define a directed tree with m leaves if:

- The number $b_{li}, i \in \{1,..., q_l\}$, indicates the number of outgoing arcs for the corresponding vertex.
- The number L is the length of the maximum path.
- The number $q_l, l \le L$, determines the number of vertices at layer l (the path from the tree root to such vertices has length l);
- $q_0 = 1; q_l = \sum_{i=1}^{q_{l-1}} b_{(l-1)i} \ \forall l > 0; q_L = m$;
- $b_{L1} = b_{L2} = ... = b_{Lq_L} = 0$. ♦

Definition 3. The system structure generated by a sequence B is a tree with m leaves, denoted by $W_m = \langle G(V, E), T\rangle$, if

$$V = \left\{\{v_0\} \cup \bigcup_{j=1}^{b_{01}} \{v_{0j}\} \cup \bigcup_{i=1}^{q_1}\bigcup_{j=1}^{b_{1i}} \{v_{0ij}\} \cup ... \cup ... \cup \bigcup_{i=1}^{q_{L-1}}\bigcup_{j=1}^{b_{(L-1)i}} \{v_{0...ij}\}\right\};$$

$$E = \left\{\bigcup_{j=1}^{b_{01}} \{(v_0, v_{0j})\} \cup \bigcup_{i=1}^{q_1}\bigcup_{j=1}^{b_{1i}} \{(v_{0i}, v_{0ij})\} \cup ... \cup ... \cup \bigcup_{i=1}^{q_{L-1}}\bigcup_{j=1}^{b_{(L-1)i}} \{(v_{0...i}, v_{0...ij})\}\right\}; \ T = \{v_0\}. \blacklozenge$$

Figure 1 shows a tree with four leaves at the third layer as one example. Note that a special case of a tree with $b_{li} = 1, q_l = m \ \forall l < L, l \ne 0$, is a star with m rays. The corresponding types of structures have been considered previously in [53].

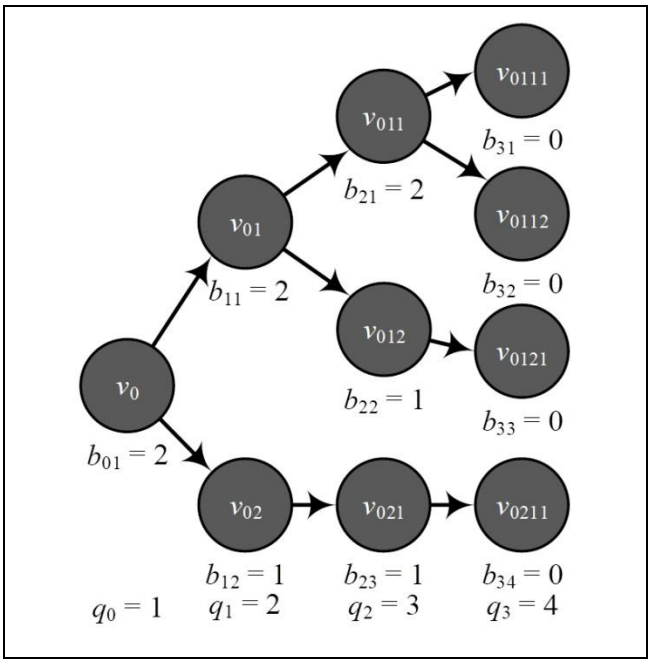

Fig. 1. A tree with m = 4 and L = 3. Vertex numbers are unique and reflect a simple path to the perimeter: it includes all vertices with numbers representing the subrows of the vertex number under consideration.

Definition 4. A bijective mapping $M^{-1}: S \to V$ is called a placement of elements of S in a tree W_m. The corresponding inverse mapping $M: V \to S$ is called the projection of the tree W_m into the set of elements S. ♦

Note that such a mapping exists only if the number of vertices in the graph $G(V, E)$ is equal to the number of elements in the protected system. In the case of an infinite number of vertices, the sets V and S must be countable.

Definition 5. The overall risk of a system with a set of elements S, placed in a tree W_m via a bijective mapping $M^{-1}: S \to V$, is the value

$$\rho\left(S, W_m, M^{-1}\right) = \rho_{M(v_o)} + \sum_{j=1}^{b_{01}} \rho_{M(v_{0j})} + \\ + \sum_{i=1}^{q_1} \sum_{j=1}^{b_{1i}} \rho_{M(v_{0ij})} + \ldots + \sum_{i=1}^{q_{L-1}} \sum_{j=1}^{b_{(L-1)i}} \rho_{M(v_{0\ldots ij})}. \blacklozenge \quad (3)$$

Let the protected system include a set of elements $S = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbb{N}$, with the corresponding eigen probabilities of successful attack, $P = \left\{p^0_{s_1}, p^0_{s_2}, p^0_{s_n}\right\}$, and damage amounts $U = \left\{u_{s_1}, u_{s_2}, \ldots, u_{s_n}\right\}$. Suppose also that possible attack paths are given by a tree $W_m = \langle G(V, E), T\rangle$, where $\sum_{l=1}^{L} q_l = n$. Then the overall risk minimization problem of the protected system is to find a placement M^{-1} of elements of S in the structure W_m such that

$$\rho(S, W_m, M^{-1}) \to \min. \quad (4)$$

For the special case $m = 1$, the exact solution has been described in [52]. For the case $q_1 = m \ \forall l < L, l \neq 0$, a suboptimal solution with an a priori bound of the relative error has been obtained in [53]. In this paper, we similarly derive such a bound for trees.

3. THE OPTIMAL PLACEMENT OF ELEMENTS IN A TREE STRUCTURE: AN APPROXIMATE SOLUTION

Suppose that for all system elements, the damage amounts in case of a successful attack are equally estimated: $u_{s_i} = u \ \forall i \in \{1, \ldots, n\}$. Then problem (4) takes the form

$$\rho\left(S, W_m, M^{-1}\right) = u\left(p_{M(v_0)} + \sum_{k=0}^{L-1} \sum_{i=1}^{q_k} \sum_{j=1}^{b_{ki}} \left(p_{M(v_{0\ldots ij})} \cdot \right.\right. \\ \left.\left. \cdot p_{M(v_{0\ldots i})} \cdot \ldots \cdot p_{M(v_0)} \right)\right) \to \min. \quad (5)$$

In addition, we require that the expression

$$p_{M(v_0)} + \sum_{k=0}^{L-1} \sum_{i=1}^{q_k} \sum_{j=1}^{b_{ki}} \left(p_{M(v_{0\ldots ij})} p_{M(v_{0\ldots i})} \cdot \ldots \cdot p_{M(v_0)} \right)$$

is finite for any values of L and $m = q_L$. For this purpose, let the eigen risks of all system elements be bounded above by a value called the marginal eigen risk; see the definition below and [53].

Definition 6. The marginal eigen risk of an element of a protected system placed in a structure $W_m = \langle G(V, E), T\rangle$ is the value

$$\rho^0_{\max} = \frac{u}{1 + \sqrt{m}}. \blacklozenge$$

Note that under the constraint $p_i \le \frac{1}{1+\sqrt{m}} = p^0_{\max}$, we have the inequality

$$\rho\left(S, W_m, M^{-1}\right) \le \\ \le u\left(p^0_{\max} + \sum_{k=0}^{L-1} \sum_{i=1}^{q_k} \sum_{j=1}^{b_{ki}} \left(p^0_{\max}\right)^{k+1} \right) \le u. \quad (6)$$

In formula (6), equality is achieved at $L = \infty$ for any finite m. Due to the construction of (6), the upper bounds on the increment of the overall risk for a star [53, *Table 2*] when moving away from the perimeter will remain true for trees as well. This fact is important: as expected, the upper bounds of the relative deviation from the optimal solution in the case of an arbitrary placement of elements in the structure at a fixed distance from the perimeter (given in [53]) can be used for trees.

To confirm this, we carry out a series of numerical experiments by analogy with [53]. Let us impose the following constraints:

$$\begin{cases} u = 1 \\ 0 < p^0_{M(v_{0\ldots i})} \le p^0_{M(v_{0\ldots ij})} \\ \quad \forall i \in \{1, \ldots, q_k\}, j \in \{1, \ldots, b_{ki}\}, k \in \{0, \ldots, L-1\} \\ p^0_{M(v_{0\ldots ij})} \le \frac{u}{1+\sqrt{m}} \\ \quad \forall i \in \{1, \ldots, q_k\}, j \in \{1, \ldots, b_{ki}\}, k \in \{0, \ldots, L-2\} \\ p^0_{M(v_{0\ldots ij})} \le \sum_{l=L}^{\infty} \left(\frac{u}{1+\sqrt{m}} \right)^{l+1} \\ \quad \forall i \in \{1, \ldots, q_{L-1}\}, j \in \{1, \ldots, b_{(L-1)i}\}. \end{cases}$$

We generate the expressions (3) for all placements obtained by permuting elements at a fixed distance k from the perimeter, starting from $k = 1$ (the first and farther layers). For each k, it is necessary to consider the cases $q_k = 2, \ldots, m$ corresponding to trees with q_k vertices of the kth layer. Then we analyze all possible absolute values for the difference of these expressions and find a global maximum for each of them. Dividing the resulting value by the minimum of the difference

of these two expressions yields the relative deviation. The maximum of such deviations is an upper bound on the relative error of the solution of problem (5).

The table represents the resulting values of the relative error for small trees.

Figure 2 shows the behavior of the relative error values at layers 1–4 depending on the number of outgoing arcs at the current layer and the number of leaves in the tree. These are the subsets $\{v_{0j}\}_{j=1}^{b_{01}}$ (Fig. 2a), $\left\{\{v_{0ij}\}_{j=1}^{b_{1i}}\right\}_{i=1}^{q_1}$ (Fig. 2b), $\left\{\{v_{0...ij}\}_{j=1}^{b_{2i}}\right\}_{i=1}^{q_2}$ (Fig. 2c), and $\left\{\{v_{0...ij}\}_{j=1}^{b_{3i}}\right\}_{i=1}^{q_3}$ (Fig. 2d). Note that it is similar to the behavior demonstrated by the values of the maximum risk increase under a given value of the marginal eigen risk. (For details, see Table 2 of the paper [53].) Namely, at the first layer the error grows with the number of leaves in the tree. At the second and farther layers, when the number of leaves is $m \geq 5$, the error decreases monotonically. Monotonicity is violated for a small number of leaves. This phenomenon was briefly described in [53]. We will not investigate this issue in more detail: the main objective is to develop risk management methods for complex network structures with thousands of vertices and edges.

Note that the experimental values of the relative deviation decrease monotonically with the distance to the perimeter. Therefore, to construct a system with an overall risk not exceeding the minimum possible one by more than 6.07% (the upper bound in Fig. 2b), it suffices to select, in an optimal way, an element for placing in the perimeter vertex and elements for placing in the first layer's vertices. Under the above condition $u_{s_i} = u \ \forall i \in \{1,...,n\}$, these are the vertices with the smallest eigen risks. Such an error is acceptable for a wide class of systems. When a higher level of protection is required, one should select q_2 additional elements from the unplaced ones with the smallest eigen risks and place arbitrarily the remaining elements in the vertices $V \setminus \left\{\{v_0\} \cup \bigcup_{j=1}^{b_{01}} \{v_{0j}\} \cup \bigcup_{i=1}^{q_1} \bigcup_{j=1}^{b_{1i}} \{v_{0ij}\}\right\}$. Then one should find the optimal placement of the selected elements in the vertices $\bigcup_{i=1}^{q_1} \bigcup_{j=1}^{b_{1i}} \{v_{0ij}\}$, e.g., by calculating $q_3!$ values of the overall risk for all possible permutations of elements at the second layer. In this case, the error of the resulting solution will be below 1.32%.

The estimated relative error of solving the problem of optimal element placement in vertex subsets of a tree structure. The values are rounded up to the fourth decimal.

The number of vertices in the subset	Vertex subset			
	$\{v_{0j}\}_{j=1}^{b_{01}}$	$\left\{\{v_{0ij}\}_{j=1}^{b_{1i}}\right\}_{i=1}^{q_1}$	$\left\{\{v_{0...ij}\}_{j=1}^{b_{2i}}\right\}_{i=1}^{q_2}$	$\left\{\{v_{0...ij}\}_{j=1}^{b_{3i}}\right\}_{i=1}^{q_3}$
Three leaves (m = 3)				
2	0.3095	0.0585	0.0119	0.0030
3	0.1548	0.0434	0.0088	0.0022
Four leaves (m = 4)				
2	0.3750	0.0571	0.0107	0.0025
3	0.2500	0.0461	0.0086	0.0020
4	0.2000	0.0607	0.0107	0.0024
Five leaves (m = 5)				
2	0.4223	0.0553	0.0097	0.0021
3	0.3168	0.0468	0.0082	0.0018
4	0.2563	0.0591	0.0098	0.0021
5	0.1709	0.0515	0.0085	0.0018
Six leaves (m = 6)				
2	0.4588	0.0535	0.0089	0.0018
3	0.3671	0.0466	0.0077	0.0016
4	0.2997	0.0574	0.0090	0.0018
5	0.2248	0.0512	0.0080	0.0016
6	0.1899	0.0607	0.0091	0.0018

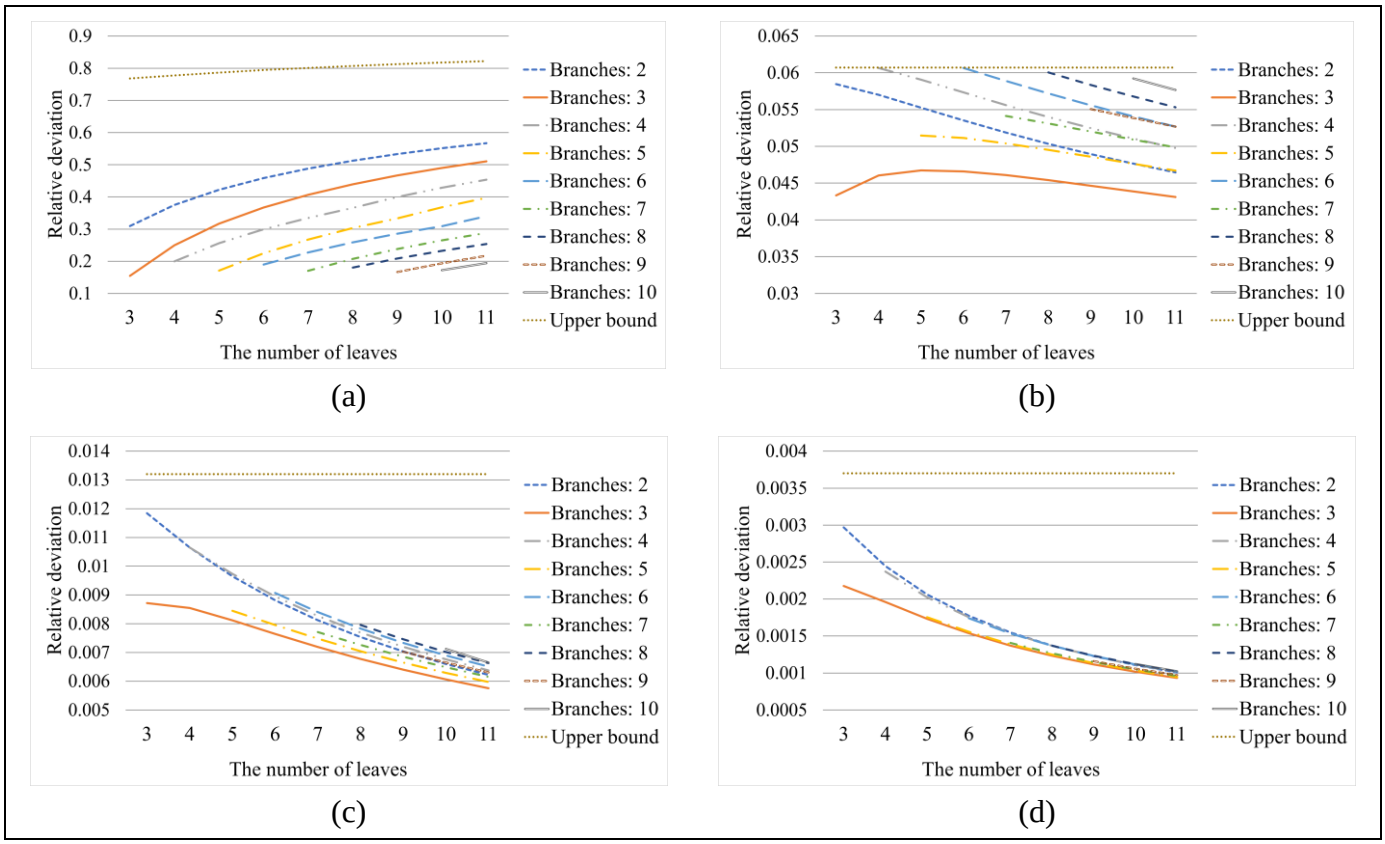

Fig. 2. The estimated relative deviation from the optimal element placement in subsets of a tree structure depending on the number of its leaves: the upper bounds in the vertex subset of the first layer (Fig. 2a) correspond to the maximum risk increment in the star structure (i.e., when the number of branches and leaves coincide); the upper bounds for the vertex subsets of layers 2–4 (Figs. 2b–2d) are the values obtained in [53] for a star structure with four rays (Fig. 2b) and two rays (Figs. 2c and 2d).

CONCLUSIONS

This paper continues a series of research works devoted to the influence of the internal structure of a complex system on its overall risk. To achieve the objective of the study, the problem of optimally placing protected system's elements in a given structure has been formulated. This problem statement allows considering the influence of the system structure on its risk regardless of the resources allocated (as in the classical Attacker–Defender problem). A direct method to solve this problem seems ambiguous, and we have decided to analyze different structures sequentially in ascending order of their complexity.

Chains have been considered in [52]. The general solution presented therein is a preference criterion to select a system element for placing in the vertex of a simple chain depending on its position to the perimeter. A star structure (one perimeter vertex and an arbitrary finite number of simple outgoing chains, particularly of infinite length) has been investigated in [53]. Upper bounds have been derived for the relative error of the problem solution under an arbitrary placement of elements starting from some distance to the perimeter.

In this paper, the upper bounds for star structures have been generalized to arbitrary trees. For this purpose, we have introduced a vertex designation system to indicate explicitly the path to the current vertex from the perimeter; have formulated the problem of optimal placement of system elements in the tree structure; and have calculated upper bounds for the relative error of the problem solution for trees with a small number of branches and leaves. Also, the behavior of these bounds has been analyzed when increasing the number of leaves and branches. According to the conclusions, the solution errors do not exceed the upper bounds obtained previously for star structures.

The results of this paper can be applied, e.g., in risk management for computer networks with variable topology, such as fog computers [55] or wireless mesh networks [56], in security system design [57], and many other fields. The approach proposed allows assessing to what extent rearranging the topology of a computer network (in another example, the structure of a security system) influences its overall protection;

the upper bounds derived allow estimating the overall risk of the system.

The next stage of research works will deal with arbitrary-topology structures with a single-vertex perimeter.

REFERENCES

1. *The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk*, Hillson, D., Ed., London: Kogan Page Publishers, 2023.
2. ISO 31000: Risk Management – Principles and Guidelines. Geneva, Switzerland: International Organization for Standardization, 2018.
3. Rass, S., On Game-Theoretic Risk Management (Part One) – Towards a Theory of Games with Payoffs that are Probability-Distributions, *arXiv:1506.07368*, 2015. DOI: https://doi.org/10.48550/arXiv.1506.07368
4. Rass, S., On Game–Theoretic Risk Management (Part Two) – Algorithms to Compute Nash-Equilibria in Games with Distributions as Payoffs, *arXiv:1511.08591*, 2015. DOI: https://doi.org/10.48550/arXiv.1511.08591
5. Rass, S., On Game–Theoretic Risk Management (Part Three) – Modeling and Applications, *arXiv:1711.00708*, 2017. DOI: https://doi.org/10.48550/arXiv.1711.00708
6. Ostapenko, A.G., Parinov, A.V., Kalashnikov, A.O., et al., *Sotsial'nye seti i destruktivnyi kontent* (Social Networks and Destructive Content), Novikov, D.A., Ed., Moscow: Goryachaya Liniya – Telekom, 2017. (In Russian.)
7. Kalashnikov, A.O., *Modeli i metody organizatsionnogo upravleniya informatsionnymi riskami korporatsii* (Models and Methods for the Organizational Management of Corporate Information Risks), Moscow: Trapeznikov Institute of Control Sciences RAS, 2011. (In Russian.)
8. Kalashnikov, A.O. and Anikina, E.V., Management of Information Risks for Complex System Using the "Cognitive Game" Mechanism, *Cybersecurity Issues*, 2020, vol. 38, no 4, pp. 2–10. (In Russian.)
9. Deng, S., Zhang, J., Wu, D., et al., A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack, *IEEE Transactions on Industrial Informatics*, 2023, vol. 19, no. 3, pp. 2899–2908.
10. Hu, B., Zhou, C., Tian, Y.–C., et al., Attack Intention Oriented Dynamic Risk Propagation of Cyberattacks on Cyber-Physical Power Systems, *IEEE Transactions on Industrial Informatics*, 2023, vol. 19, no. 3, pp. 2453–2462.
11. Xiaoxiao, G., Tan, Y., and Wang, F., Modeling and Fault Propagation Analysis of Cyber-Physical Power System, *Energies*, 2020, vol. 13, no. 3, art. no. e539.
12. Gao, X., Peng, M., Tse, C.K., and Zhang, H., A Stochastic Model of Cascading Failure Dynamics in Cyber-Physical Power Systems, *IEEE Systems Journal*, 2020, vol. 14, no. 3, pp. 4626–4637.
13. Marashi, K., Sarvestani, S.S., and Hurson, A.R., Identification of Interdependencies and Prediction of Fault Propagation for Cyber-Physical Systems, *Reliability Engineering & System Safety*, 2021, vol. 215, art. no. e107787.
14. Yan, K., Liu, X., Lu, Y., and Qin, F., A Cyber-Physical Power System Risk Assessment Model Against Cyberattacks, *IEEE Systems Journal*, 2023, vol. 17, no. 2, pp. 2018–2028.
15. Pelissero, N., Laso, P.M., and Puentes, J., Impact Assessment of Anomaly Propagation in a Naval Water Distribution Cyber–Physical System, *Proceedings of 2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, 2021, pp. 518–523.
16. Islam, M.Z., Lin, Y., Vokkarane, V.M., and Venkataramanan, V., Cyber–Physical Cascading Failure and Resilience of Power Grid: A Comprehensive Review, *Frontiers in Energy Research*, 2023, vol. 11, art. no. e1095303.
17. Zhang, C., Xu, X., and Dui, H., Analysis of Network Cascading Failure Based on the Cluster Aggregation in Cyber-Physical Systems, *Reliability Engineering & System Safety*, 2020, vol. 202, art. no. e106963.
18. Xing, L., Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience, *IEEE Internet of Things Journal*, 2021, vol. 8, no. 1, pp. 44–64.
19. Wang, Q., Jia, G., Jia, Y, and Song, W., A New Approach for Risk Assessment of Failure Modes Considering Risk Interaction and Propagation Effects, *Reliability Engineering & System Safety*, 2021, vol. 216, art. no. e108044.
20. Khoshakhlagh, A., Moradi Hanifi, S., Laal, F., et al., A Model to Analyze Human and Organizational Factors Contributing to Pandemic Risk Assessment in Manufacturing Industries: FBN–HFACS Modelling, *Theoretical Issues in Ergonomics Science*, 2023, vol. 25, no. 4, pp. 369–390.
21. Moore, S. and Rogers, T., Predicting the Speed of Epidemics Spreading in Networks, *Physical Review Letters*, 2020, vol. 124, no. 6, art. no. e068301.
22. Nasution, H., Jusuf, H., Ramadhani, E., and Husein, I., Model of Spread of Infectious Diseases, *Systematic Reviews in Pharmacy*, 2020, vol. 11, no. 2, pp. 685–689.
23. Albert, R., Jeong, H., and Barabasi, A.-L., Error and Attack Tolerance of Complex Networks, *Nature*, 2000, vol. 406, pp. 378–382.
24. Artime, O., Grassia, M., De Domenico, M., et al., Robustness and Resilience of Complex Networks, *Nature Reviews Physics*, 2024, vol. 6, no. 2, pp. 114–131.
25. Ming, L., Run-Ran, L., Linyuan, L., et al., Percolation on Complex Networks: Theory and Application, *Physics Reports*, 2021, vol. 907, pp. 1–68.
26. Bak, P., Chen, K., and Tang, C., A Forest-Fire Model and Some Thoughts on Turbulence, *Physics Letters A*, 1990, vol. 147, no. 5–6, pp. 297–300.
27. Palmieri, L. and Jensen, H.J., The Forest Fire Model: The Subtleties of Criticality and Scale Invariance, *Frontiers in Physics*, 2020, vol. 8, art. no. e00257.
28. Rybski, D., Butsic, V., and Kantelhardt, J.W., Self-organized Multistability in the Forest Fire Mode, *Physical Review E*, 2021, vol. 104, no. 1, art. no. eL012201.
29. Newman, D.E., Nkei, B., Carreras, B.A., et al., Risk Assessment in Complex Interacting Infrastructure Systems, *Proceedings of 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*, Big Island, HI, 2005. DOI: 10.1109/HICSS.2005.524
30. Li, X., Ji, L., Zhu, H., et al., Cellular Automata–Based Simulation of Cross-space Transmission of Energy Local Area Network Risks: A Case Study of a Power Supply Station in Beijing, *Sustainable Energy, Grids and Networks*, 2021, vol. 27, art. no. e100521.
31. Torres, M.A., Chávez-Cifuentes, J.F., and Reinoso, E., A Conceptual Flood Model Based on Cellular Automata for Probabilistic Risk Applications, *Environmental Modelling & Software*, 2022, vol. 157, art. no. e105530.
32. Sequeira, J.G.N., Nobre, T., Duarte, S., et al., Proof–of–Principle That Cellular Automata Can Be Used to Predict Infestation Risk by Reticulitermes grassei (Blattodea: Isoptera), *Forests*, 2022, vol. 13, no. 2, art. no. e237.

33.Gallos, L.K., Cohen, R., Argyrakis, P., et al., Stability and Topology of Scale-Free Networks under Attack and Defense Strategies, *Physical Review Letters*, 2005, vol. 94, no. 18, art. no. e188701.
34.Gallos, L.K., Cohen, R., Argyrakis, P., et al., Network Robustness and Fragility: Percolation on Random Graphs, *Physical Review Letters*, 2000, vol. 85, no. 25, art. no. e5468.
35.Wang, F., Dong, G., Tian, L., and Stanley, H.E., Percolation Behaviors of Finite Components on Complex Networks, *New Journal of Physics*, 2022, vol. 24, no. 4, art. no. e043027.
36.Dong, G., Luo, Y., Liu, Y., et al., Percolation Behaviors of a Network of Networks under Intentional Attack with Limited Information, *Chaos, Solitons & Fractals*, 2022, vol. 159, art. no. e112147.
37.Shao, S., Huang, X., Stanley, H.E., and Havlin, S., Percolation of Localized Attack on Complex Networks, *New Journal of Physics*, 2015, vol. 17, no. 2, art. no. e023049.
38.Dong, G., Xiao, H., Wang, F., et al., Localized Attack on Networks with Clustering, *New Journal of Physics*, 2019, vol. 21, no. 1, art. no. e013014.
39.Shang, Y., Percolation of Attack with Tunable Limited Knowledge, *Physical Review E*, 2021, vol. 103, no. 4, art. no. e042316.
40.Qing, T., Dong, G., Wang, F., et al., Phase Transition Behavior of Finite Clusters under Localized Attack, *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2022, vol. 32, no. 2, art. no. e023105.
41.Goltsev, A.V., Dorogovtsev, S.N., and Mendes, J.F.F., K-Core (Bootstrap) Percolation on Complex Networks: Critical Phenomena and Nonlocal Effects, *Physical Review E*, 2006, vol. 73, no. 5, art. no. e056101.
42.Burleson-Lesser, K., Morone, F., Tomassone, M.S., and Makse, H.A., K-core Robustness in Ecological and Financial Networks, *Scientific Reports*, 2020, vol. 10, no. 1, art. no. 3357.
43.Shang, Y., Generalized K-cores of Networks under Attack with Limited Knowledge, *Chaos, Solitons & Fractals*, 2021, vol. 152, art. no. e111305.
44.Al Mannai, W.I. and Lewis, T.G., A General Defender-Attacker Risk Model for Networks, *The Journal of Risk Finance*, 2008, vol. 9, no. 3, pp. 244–261.
45.Peng, R., Wu, D., Sun, M., and Wu, S., An Attack-Defense Game on Interdependent Networks, *Journal of the Operational Research Society*, 2021, vol. 72, no. 10, pp. 2331–2341.
46.Ren, J., Liu, J., Dong, Y., et al., An Attacker-Defender Game Model with Constrained Strategies, *Entropy*, 2024, vol. 26, no. 8, art. no. e26080624.
47.He, S., Zhou, Y., Yang, Y., et al., Cascading Failure in Cyber-Physical Systems: A Review on Failure Modeling and Vulnerability Analysis, *IEEE Transactions on Cybernetics*, 2024, pp. 1–19. DOI: 10.1109/TCYB.2024.3411868
48.Zhou, F., Xu X., Trajcevski, G., and Zhang, K., A Survey of Information Cascade Analysis: Models, Predictions, and Recent Advances, *ACM Computing Surveys (CSUR)*, 2021, vol. 54, no. 2, pp. 1–36.
49.Cui, P., Zhu, P., Wang, K., et al., Enhancing Robustness of Interdependent Network by Adding Connectivity and Dependence Links, *Physica A*, 2018, vol. 497, pp. 185–197.
50.Xu, X. and Fu, X., Analysis on Cascading Failures of Directed-Undirected Interdependent Networks with Different Coupling Patterns, *Entropy*, 2023, vol. 25, no. 3, art. no. e471.
51.Yang, X.H., Feng, W.H., Xia, Y., et al., Improving Robustness of Interdependent Networks by Reducing Key Unbalanced Dependency Links, *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2020, vol. 67, no. 12, pp. 3187–3191.
52.Shiroky, A. and Kalashnikov, A., Mathematical Problems of Managing the Risks of Complex Systems under Targeted Attacks with Known Structures, *Mathematics*, 2021, vol. 9, no. 19, art. no. e2468.
53.Shiroky, A. and Kalashnikov, A., Influence of the Internal Structure on the Integral Risk of a Complex System on the Example of the Risk Minimization Problem in a "Star" Type Structure, *Mathematics*, 2023, vol. 11, no. 4, art. no. e998.
54.Shiroky, A.A. and Kalashnikov, A.O., Natural Computing with Application to Risk Management in Complex Systems, *Control Sciences*, 2021, no. 4, pp. 2–17. ~~(In Russian.)~~
55.Shiroky, A.A., A Method for Rapid Risk Assessment of a Fog Computing System with a Star–Shaped Topology, *Proceedings of 17th International Conference Management of Large–Scale System Development (MLSD)*, Moscow, Russia, 2024, pp. 1–5.
56.Shiroky, A., Risk Management in the Design of Computer Network Topology, in *Lecture Notes in Computer Science*, vol. 14123, Vishnevskiy, V.M., Samouylov, K.E., and Kozyrev, D.V., Eds., Cham: Springer, 2024. https://doi.org/10.1007/978-3-031-50482-2_29. (Proceedings of the 26th International Conference on Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN 2023), Moscow, Russia, 2023.)
57.Shiroky, A.A., Risk Management in the Design of Security Systems with Nested Security Zones, *Proceedings of the 16th International Conference Management of Large-Scale System Development (MLSD)*, Moscow, Russia, 2023, pp. 1–4.

This paper was recommended for publication by V.N. Burkov, a member of the Editorial Board.

Received November 6, 2024, and revised March 21, 2025.
Accepted March 21, 2025.

Author information

Shiroky, Aleksandr Aleksandrovich. Cand. Sci. (Phys.–Math.), Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ shiroky@ipu.ru
ORCID ID: https://orcid.org/0000–0002–9130–5541

Kalashnikov, Andrei Olegovich. Dr. Sci. (Eng.), Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ aokalash@ipu.ru
ORCID ID: https://orcid.org/0000–0001–5204–1398

Cite this paper

Shiroky, A.A., Kalashnikov, A.O., How Does the Internal Structure of a Complex System Influence Its Overall Risk? Risk Minimization for Trees. *Control Sciences* **2,** 22–30 (2025).

Original Russian Text © Shiroky, A.A., Kalashnikov, A.O., 2025, published in *Problemy Upravleniya*, 2025, no. 2, pp. 27–37.

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com