Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 2061769, 9 pages
https://doi.org/10.1155/2022/2061769

*Research Article*

# Using Advanced Analytic Techniques to Optimize Cyber-Physical Defensive Plans in Sports Infrastructures and Facilities

**Rui Wang**

*Zhengzhou Preschool Education College, Zhengzhou, Henan 450000, China*

Correspondence should be addressed to Rui Wang; wangrui_197910@163.com

Received 5 May 2022; Revised 18 May 2022; Accepted 24 May 2022; Published 11 June 2022

Academic Editor: Konstantinos Demertzis

The technical projects for securing a network of infrastructures and processes are designed, financed, carried out, maintained, and operated within a general infrastructure system, which can gather activities and funds of the private or public sector. The importance of such projects for modern society is enormous, and there is a positive correlation between the size of infrastructure projects and the strength of the national economy. At the same time, it falls within the critical infrastructure sector most of the time. This work, taking into account the massive importance of investments made in the field of sports and the corresponding significance of the design and implementation of robust cybersecurity systems, presents an innovative optimization system for the design, performance, and adaptation of safeguards of technical projects, which require a high level of security standards. A realistic optimization system of low computational complexity is proposed and tested, dividing the problem into a series of subproblems of one-step optimization, which can be solved with great ease and without requirements on computational resources. The great innovation of the proposed system is that the separation is done so that the solution results from the optimal individual solutions of the subproblems without affecting the final result.

## 1. Introduction

The primary objective of programs to construct sports infrastructure is to be of service to, further advance, and generally better society. These activities include conceiving of, designing, constructing, and operating facilities necessary for contemporary sports culture and organizing and staging the relevant sporting events. These projects are an essential component of a nation's infrastructure and have significant repercussions on social and economic fronts [1]. They require significant capital investment, provide public services, and, in most cases, are considered to fall within the area of responsibility of the public sector. The necessity and feasibility of most of these projects are usually assessed by general methods of determining their economic characteristics (costs and benefits) [2, 3].

Professionals involved in sports infrastructure projects recognize the interdisciplinary nature of their design. In addition to the operational effectiveness of these projects and their impact on public cohesion, health, and security, planners are called upon to consider their beneficial and adverse environmental, social, and economic effects. They must also consider other factors (e.g., institutional, aesthetic, legal, and financial) to determine whether a particular project is safe and successfully implemented. Designers today are staffed with employees specialized in scientific fields, such as engineering, computer science, economics, and law, who, in addition to technical specialization, have a basic understanding of other sciences and the ability to work with other professionals because the implementation of these projects requires a high degree of interdisciplinarity, especially in the field of ensuring the infrastructure grid they cover [4].

In conclusion, the natural, environmental, social, and most importantly the security framework within which the design takes place varies from that of a patchwork of space-time and topographic elements. Therefore, while trying to adopt a broad strategy and comprehensive techniques, planners need to note that any unique athletic project provides a range of features and constraints. This is something that must be taken into consideration. Techniques that have been effectively implemented in the design process in the past for specific sports projects of varying sorts might serve as a reference for developing similar projects in the future. On the other hand, individuals in charge of the majority of the projects will probably be required to make modifications in response to the changing circumstances and the general security considerations that have to be taken into account.

This work presents an innovative optimization system for designing, performing, and adapting safeguards for technical projects requiring high-security standards. Taking into account the enormous importance of investments made in the field of sports and the corresponding significance of the design and implementation of robust cybersecurity systems, this work presents an innovative optimization system for the design, performance, and adaptation of safeguards. In particular, a cutting-edge and extremely realistic optimization system is proposed to be used to develop, implement, and maintain technical projects that call for a high level of security standards. The problem is broken down into a series of individual one-step optimization subproblems when using an analytical optimization system. These subproblems are much simpler and easier to solve than the original problem.

*1.1. Related Literature Review.* This section introduces the essential academic searches related to a practical approach to defending a cyber-physical system on technical and policy levels.

Mehrdad et al. [5] reviewed the publications on industrial cyber-physical security. They aimed to tackle the power transmission systems' protection strengths and vulnerabilities in the face of malicious assaults. They stated that to obtain a greater sense of protection for energy systems. When tackling energy network security issues, researchers should take a systematic approach and examine all phases of the holistic resilience cycle. To enhance the cyber-physical integrity of electrical power networks [6, 7], the idea of the Holistic Resilience Cycle was presented. This is a structured method to power system security that is defined by four steps (prevention and planning, detection, mitigation and reaction, and system recovery) as being inextricably linked and comprehensible only in context.

The study of Cai et al. [8] is characterized by attack modeling, security assessment, attack identification, and mitigation. Existing approaches were evaluated to ascertain the true nature of the cyber-physical power system security issue. Based on these technologies' features and evolution tendencies, the limits of the present research were identified, and solutions were proposed to further this field's study [9]. According to their security study, the future focal areas can be stated as follows: the field of theory to the offensive penetration method of systems should be examined in conjunction with the actual communication infrastructure and security prevention mechanisms. With the cyber and physical worlds inextricably linked, the power system cascade failure induced by cyberattacks was investigated, and a fusion analysis and quantitative risk assessment approach has been provided. Finally, attack modeling and defensive detection were accomplished using a cyber-physical fusion model. Then, following attack route prediction, a qualitative distinction of common defects and intense assaults, real-time assessment of protection stability, and digital aid decision-making could be accomplished.

Lai et al. [6] introduced a trilevel optimization model for constructing a coordinated assault scenario and determining the ideal defense strategy, which is novel in resource management to resist an attack. Additionally, considerable reductions in unsaved energy were seen when the suggested optimization technique was used to distribute defense resources. The numerical findings indicate that assault and defense methods vary according to offensive budgets, defense budgets, and restoration periods. Intruders are likely to conduct assaults that result in compounding failures, and the ideal defense approach would prevent such failures. Additionally, the formulation might be enhanced by factoring in the uncertainty associated with the attacker and restoration processes, dynamic difficulties, and grid storage incorporation.

He and Yan [2] conducted a thorough and systematic evaluation of significant smart grid attack risks and security measures. They began their assessment by providing an overview of smart grid security from a cyber-physical viewpoint before focusing on attack strategies that substantially influence the functioning of the power grid and the accompanying response measures. They then examined the potential problems associated with smart grid security after an in-depth examination of the threats and responses. They concentrated on assaults and defenses in the smart grid by conducting a complete and systematic analysis of the state-of-the-art in the sector, including everything from protection frameworks to attack methods and defensive techniques and a variety of possibilities and problems. They believed that their publication would inform people of attack dangers and mitigation techniques in complex cyber-infrastructure facilities such as the smart grid and would motivate researchers to work on developing secure and resilient networks.

Hao et al. [10] developed a strategy for effectively computing an execution plan that optimizes the number of engineered code iterations to achieve maximum protection impact while ensuring the guarded task system's real-time controllability through a novel reaction time analysis. They demonstrated how to incorporate protection mechanisms into practical cases. The suggested approach can determine a suboptimal plan for executing a designed operating security inspection code for shielded tasks or programs to obtain the maximum protection impact while ensuring the system's stimulability. Both simulation-based testing and an application of the suggested approach on a prototype self-driving vehicle demonstrate that the proposed method may be utilized to secure real-time systems.

Hasan et al. [11] provided a technique for prioritizing cyber risk remediation plans in cyber systems that are both efficient and cost-effective (safety implications). These researchers developed a framework for estimating how cyberattacks and random system failures could affect their security and cause catastrophic harm. We undertook an operational impact assessment to determine the magnitude of the damage caused by CPS threats. They advised constructing a model based on a data-driven attack and fault graph. In the end, they suggested building a strategic response decision capacity that comprises mitigation measures and policies that balance functional robustness and risk. The exploratory study in a real-world testbed showed that allocating resources based on node importance significantly decreased system-level risk. In the future, they were intending to expand the system and include all accessible system-level remediation measures, patch management, and system resilience.

*1.2. Modeling the Cyber-Physical Defensive Plan.* In modern reality, the complexity of systems and the evolution of technology require integrated defense security planning through an optimal economic approach [12, 13]. Existing experience shows that the anticipated benefits of such design are significant, especially in developing countries, in terms of the quality of the final result, the economy achieved, and the speed of implementation. This is the case even though the degree to which such methodologies are used varies depending on the type of project being undertaken. However, the rigorous application of the systemic concept in manufacturing technical works is a challenging endeavor. This is because it necessitates the detailed characteristics of the system, several technical-economic studies, the application of behavior calculation models, sensitivity analysis, and the formulation of optimal strategies regarding the objectives that have been established. Even though rigorous systematic studies could be beneficial, the abovementioned requirements render their implementation in small-scale projects impractical and prohibitive. However, decision-making is a necessary and ongoing process [6]. The development of systematic analysis techniques with simplified requirements, which most scholars accept and able to improve the effectiveness of promoted measures, is of great practical importance.

It should be noted that the mathematical models of the system in the method of systematic analysis play a central role in the modeling of the systems in question, as it is an essential tool in the modern design and management of projects and strategies [14, 15]. In general, such a model consists of one or more statements, expressed in mathematical terms, that describe relationships between dependent and independent variables, as shown in Figure 1.

The cyber-physical defensive plan is described with a mathematical model. This model is comprised of equations, logical assertions, and other instructions for processing the data that is currently available, as well as for creating and analyzing data that has been artificially generated [16]. The relationships that describe the system, correlating the input and output variables, are expressed by parameters, which are typically required to be determined by observations and measurements of the output variables and which can be constant or variable in a predetermined manner. In general, the parameters must be determined by the observations and measurements of the variables that are output from the system. Exogenous variables are those that the person experimenting does not have any influence over, and probability functions are used to characterize them. On the other hand, variables whose values can be entirely or partially determined are referred to as choice variables. These are the variables that are discussed further below. Restrictions or prohibitions that are applied to the model can include physical, economic, or any number of other factors that mathematical models can express [17, 18].

The analysis of mathematical models includes tables, graphs, mathematical equations, logical statements, and verbal descriptions, which are means of describing system boundaries, system input, and output elements and their relationships, and any feedback between output and input variables to achieve the desired result of the relevant modeling [19]. Specifically, the different types of mathematical models of the system depending on the types of mathematical functions used in this modeling are presented below [20, 21]:

(1) Algebraic equation: It can be obtained by adjusting a curve in empirical measurements; for example,

$$y = f(x) = a_0 + a_1 x + a_2 x^2. \tag{1}$$

(2) Equation of differences: They can describe time-varying systems with delay, memory, multiple variables, and so on; for example,

$$\frac{y_{k+1} = a_k y_k + b_k x_k}{z_{k+1} = \gamma_1 y_{k+1}^{\gamma_2}}. \tag{2}$$

(3) Normal differential equation: It can be obtained from processes of reduction or increase of the examined variable state; for example,

$$\frac{\mathrm{d}y}{\mathrm{d}t} = a y(t) + b x(t), \tag{3}$$

where $a, b$ are the system parameters.

(4) Integral equation (an equation in which an unknown function appears under an integral sign): Known relationships that can be captured in the form of integral; for example,

$$y(t) = \int_{t_0}^{t} g(t, \tau) x(\tau) \mathrm{d}\tau. \tag{4}$$

(5) Differential equation with some derivatives; for example,

$$S \frac{\partial h}{\partial t} + \nabla (T \nabla h) = R - P, \tag{5}$$

where $S, t, h, R, P$ are the system parameters.

This particular equation is a differential equation, which means that it establishes a connection between one or more unknown functions and the derivatives of those functions. The function stands in for the system quantities; the results stand in for the rates of change those quantities are subject to, and the differential equation defines the connection between the two. To put it another way, the status variables

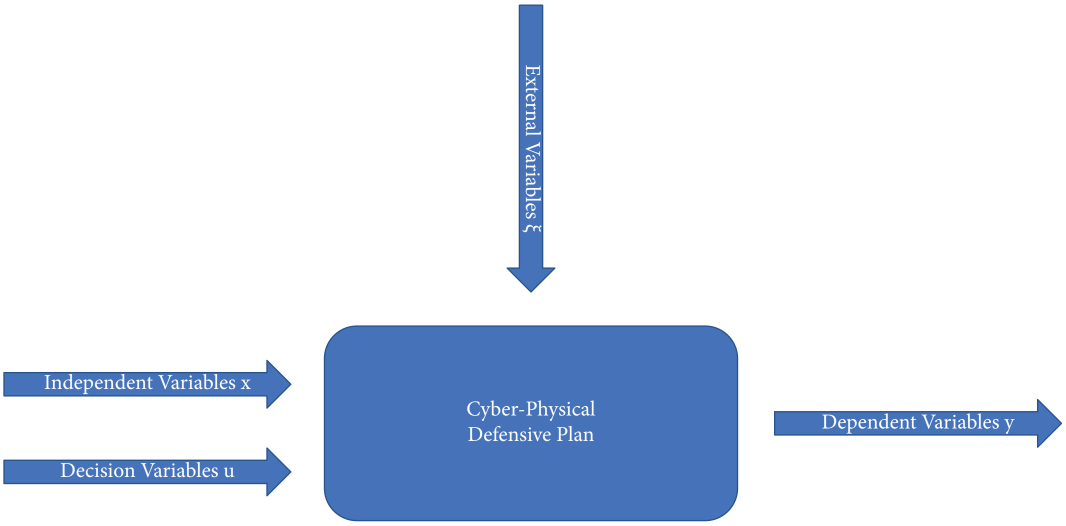

Figure 1: Schematic description of the mathematical model.

represent the bare minimum of variables needed to describe the conditions of the system at any given time or location. Each possible configuration of the decision variables gives rise to a distinct policy or group of decisions. It is possible to implement a method if doing so does not violate any restrictions, and the area of viable approaches is the set of all possible policies taken together.

The objective function is an all-encompassing way of expressing various concepts related to optimality or the most desirable outcome. In a broader sense, the objective function is a performance indicator that we can use to evaluate the implications or derivatives produced by the system. For instance, the goal function can be utilized to calculate the cost of various amounts of resources generated or used in the context of the sports projects that are the topic of this conversation.

Summarizing the above, the methodology proposed for modeling the cyber-physical defensive plan requires [2, 11]:

(1) Model of the system in the general form (as described in Figure 1):

$$\underline{y} = fn\left(\underline{x}, \underline{u}, \underline{\xi}\right), \tag{6}$$

with

$$\begin{aligned} \underline{y} &= \left[y_1, y_2, \ldots y_n\right]^T, \\ \underline{x} &= \left[x_1, x_2, \ldots x_n\right]^T, \\ \underline{u} &= \left[u_1, u_2, \ldots u_n\right]^T, \\ \underline{\xi} &= \left[\xi_1, \xi_2, \ldots \xi_n\right]^T. \end{aligned} \tag{7}$$

(2) Performance indicator (objective function) related to the outcome of a specific policy applied to the problem:

$$\min J = J\left(\underline{y}, \underline{u}\right). \tag{8}$$

(3) Set of restrictions:

$$\frac{F\left(y, \underline{\mathrm{u}}\right) = 0}{G\left(y, \underline{\mathrm{u}}\right) \geq 0}. \tag{9}$$

It should also be emphasized that the system in question is thought of as a model of distributed parameters. This means that it takes into account the behavioral deviations from point to point throughout the system. This contributes to the system's overall complexity and the very realistic modeling that is followed. In addition, the primary modeling techniques can be broken down into four categories: statistical methods, research simulation using sampling techniques, probabilistic models and techniques, and modeling techniques based on probabilities.

*1.3. Analytic Technique to Optimize Cyber-Physical Defensive Plan.* After the cyber-physical defensive plan parametric system has been modeled, the general optimization problem is formulated as follows: we want to determine the values of the decision variables $u$ that minimize the objective function $J$ with known $J, F, G$ functions under a set of constraints [22].

Specifically,

$$\begin{gathered} \min J = J\left(\underline{y}, \underline{u}\right), \\ F\left(\underline{y}, \underline{u}\right) = 0, G\left(\underline{y}, \underline{u}\right) \geq 0. \end{gathered} \tag{10}$$

Decision theory is divided into two broad categories, based on whether the decision-maker is a single body or multiple bodies. So far, similar problems have been encountered in the first category of methods, which can be divided into static or single-stage and serial or multistage, where time can be discrete or continuous. The static problem concerns minimizing the cost function, which is a function of the decision variables vector. In the serial problem, the vector of system state variables evolves in time or space according to a method of equations in which decision variables are also involved. The cost function is the sum of the transition costs at each stage and ultimately depends on the (known) initial situation and values of the decision variables at each stage [14, 23]. The solution to the above problem for optimal control is developed using classical optimization methods where the functions are continuous and derivable without restrictions.

The proposed method is an advanced method that separates the multistage optimization problem into a series of single-stage optimization problems [24]. Even multistage systems of increased complexity, such as the one under consideration, can be solved with particular ease. The great innovation of the proposed solution is that the separation is done in such a way that the optimal solution of the initial problem results from the optimal solutions of the individual issues so that the method of solving does not affect the final result.

To be more specific, the following policy holds [25–27]:

$$\pi = \{\mu_0, \ldots, \mu_{N-1}\}, \tag{11}$$

which is a set of functions that determines the values of the decision variables $\underline{u}_k$ from the values of the state variables $\underline{x}_k$; that is,

$$\underline{u}_k = \mu_k (\underline{x}_k). \tag{12}$$

The problem is to minimize costs for all possible policies $\pi$ so that

$$\min_{\pi} J_{\pi} (\underline{X}_0) = J^* (\underline{X}_0). \tag{13}$$

Let $S_k$ be the set of all possible states at time $k$ so that

$$(S_k \subset R^n). \tag{14}$$

And let $C_k$ be the set of all possible decisions at time $k$ so that

$$(C_k \subset R^m). \tag{15}$$

For every

$$\underline{x}_k \in S_k \Longleftrightarrow \underline{u}_k = \mu_k (\underline{X}_k) \in C_k. \tag{16}$$

Then, $U_k (\underline{X}_k)$ is the sum of all possible decisions at time $k$, if the state is $\underline{x}_k$ (i.e., takes into account the constraints of the problem):

$$U_k (\underline{X}_k) \subset C_k). \tag{17}$$

So, there is an acceptable policy:

$$\pi = \{\mu_0, \ldots, \mu_{N-1}\}, \tag{18}$$

which is a set of functions that have a value field of the set:

$$U_k (\underline{x}_k) or \mu_k \colon S_k \longrightarrow C_k. \tag{19}$$

such that

$$\mu_k (\underline{X}_k) \in U_k (\underline{X}_k) \forall \underline{X}_k \in S_k. \tag{20}$$

So, the intermediate cost depends only on the current situation at time $k$ and takes the form

$$J_k (x_k) = g_k (x_k, u_k) + J_{k+1} (f_k (x_k, u_k)). \tag{21}$$

In this equation, the problem of the existence of higher derivatives of the proposed function exists, where the sum of all possible decisions at time $k$ is a function of the actual decision. An acceptable policy is a self-adjoint operator $\pi$, and $U$ is a bounded self-adjoint operator. The proposed approach gives a new direction without multiple operator integrals to improve earlier results. It is a method that uses only unitary operators. This fact is proved as follows:

$$\begin{aligned}
J_N &= g_N (x_N) = J_N (x_N), \\
J_{N-1} &= g_N (x_N) + g_{N-1} (x_{N-1}, u_{N-1}) = g_{N-1} (x_{N-1}, u_{N-1}) + J_N (x_N) \\
&= g_{N-1} (x_{N-1}, \mu_{N-1} (x_{N-1})) + J_N (f_N (x_{N-1}, \mu_{N-1} (x_{N-1})) = J_{N-1} (x_{N-1}), \\
J_{N-2} &= g_N (x_N) + g_{N-1} (x_{N-1}, u_{N-1}) + g_{N-2} (x_{N-2}, u_{N-2}) = g_{N-2} (x_{N-2}, u_{N-2}) + J_{N-1} (x_{N-1}) \\
&= g_{N-2} (x_{N-2}, \mu_{N-2} (x_{N-2})) + J_{N-1} (f_{N-1} (x_{N-2}, \mu_{N-2} (x_{N-2}))) = J_{N-2} (x_{N-2}).
\end{aligned} \tag{22}$$

And the problem of minimization at each stage is expressed as follows:

$$\begin{gathered} J_N^*(x_N) = g_N(x_N), \\ J_k^*(x_k) = \min_{u_k\in U_k(x_k)}\left[g_k(x_k,u_k) + J_{k+1}^*(f_k(x_k,u_k))\right], \\ k = N-1, N-2, \ldots, 0, \end{gathered} \tag{23}$$

where $J_k^*(X_k) = J^*(X_k)$ is the optimal cost for the problem starting from the state $x_k$ at time $k$ and thus $J_0^*(X_0) = J^*(x_0)$ is the minimum cost of transition from $x_0$ to $x_{\mathrm{N}}$:

Consequently, if

$$\exists\pi^* = \{\mu_0^*, \ldots, \mu_{N-1}^*\}, \tag{24}$$

such that

$$\mu_k^*(X_k), \tag{25}$$

achieves the minimum for each $X_k$; then, $\mu^*$ is the optimal policy because

$$J_N^*(x_N) = g_N(x_N), \tag{26}$$

which is calculated from

$$J_k(x_k) = g_k(x_k,u_k) + J_{k+1}^*(x_{k+1}). \tag{27}$$

So, based on the principle of optimality, if $\{\mu_0^*, \ldots, \mu_{N-1}^*\}$ is optimal for the initial problem, then $\{\mu_k^*, \ldots, \mu_{N-1}^*\}$ is optimal for the problem starting at time $k$.

Finding the most effective approach to solving many important practical problems requires one to investigate many approaches. In many cases, this requires determining either the highest or lowest value that can be returned by a function. The majority of these issues can be resolved by first locating the right function and then applying the principles of calculus in order to ascertain whether the needed maximum or minimum value should be found. In this problem, this means that the best policy will yield the minimum cost of moving to the final state from any intermediate stage $k$. The proof of this is based on the following two propositions [28]:

$$\min_{x,y}\left[h_1(x) + h_2(x,y)\right] = \min_x\left[h_1(x) + \min_y h_2(x,y)\right]. \tag{28}$$

$$\min_\mu\left[h(x,\mu(x)\right] = \min_\mu\left[h(x,u)\right]. \tag{29}$$

As for $i+1$,

$$j_{i+1}^*(x_{i+1}) = j^*(x_{i+1}) = \min_{\{\mu_{i+1},\ldots,\mu_{N-1}\}}\left[g_N(x_N) + \sum_{k=i+1}^{N-1} g_k(x_k,\mu_k(x_k))\right]. \tag{30}$$

Then, for $i$, we have

$$J^*(x_i) = \min_{\{\mu_i,\ldots,\mu_{N-1}\}}\left[g_N(x_N) + \sum_{k=i}^{N-1} g_k(x_k,\mu_k(x_k))\right]. \tag{31}$$

So,

$$\begin{aligned} &= \min_{\mu_i} g_i(x_i,\mu_i(x_i)) + \min_{\{\mu_{+1},\ldots,\mu_{k+1}\}}\left[g_N(x_N) + \sum_{k=i+1}^{N-1} g_k(x_k,\mu_k(x_k))\right] \\ &= \min_{\mu_i} g_i(x_i,\mu_i(x_i)) + J^*(x_{i+1}) \\ &= \min_{\mu_i} g_i(x_i,\mu_i(x_i)) + J^*(x_{i+1}). \end{aligned} \tag{32}$$

And so,

$$= \min_{u_i\in U_i(x_i)} g_i(x_i,u_i) + J_{i+1}^*(f_i(x_i,u_i)) = J_i^*(x_i). \tag{33}$$

This fact verifies the request and solves the initial optimization problem.

Finally, although the computational load can be huge for a large number of decision variables and many stages, the proposed algorithm $|C| \times |S| \times N$ is much faster than the simple solutions. As shown above, no exhaustive calculation is applied for each $k$, provided that

$$S_k \longrightarrow C_k|Cl^{|S|}. \tag{34}$$

Since for $N$ stages, the policy $\pi = \{\mu_0, \ldots, \mu_{N-1}\}$ is optimized based on

$$\left\{|C|^{|S|}\right\}^N = |Cl|^{|S|N}. \tag{35}$$

Lattice models are a method that can be utilized in the valuation of economic derivatives. In a lattice model, the shortest route is searched to make the best conclusion on finding the most inexpensive bid in the search for CCTV equipment for the physical perimeter security of the sports project under consideration. It is necessary to use a discrete-time model to model the potential correlation aspects of complicated issues. The preceding technique is shown using a concrete case described in detail [29–31]. Due to the dependence on multiple paths, the Monte Carlo methods fail to make optimal decisions. The Monte Carlo methods are a comprehensive class of computer algorithms based on the concept of repeatedly taking a sample from a random pool to acquire numerical results. The fundamental idea is to use a chance to find solutions to problems that, in theory, might be solved using deterministic methods. When the issue in question involves a large number of variables that are each constrained uniquely, these methods are computationally inefficient. This indicates that approximating a solution using these methods consumes a significant amount of both time and computational effort. In addition, the model will

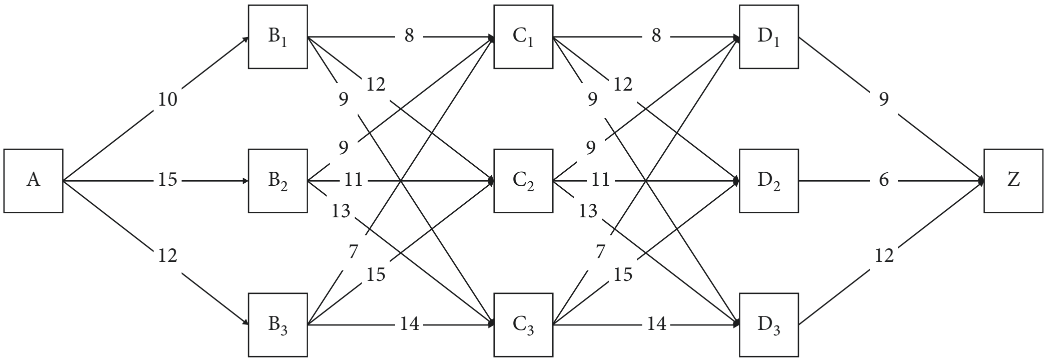

FIGURE 2: Financial lattice model.

produce unsatisfactory outputs if the parameters and constraints that are fed into it are of low quality. In this example, the solution with the minimum cost is requested within the A–Z, where the transition costs are as shown in Figure 2.

As shown in the figure, no loop has a negative cost. If the connection $ij$ does not exist we set $c_{\mathrm{ij}}$ = infinity, while $c_{ii}$ is taken as 0. Also, $x_{\mathrm{k}}$ is taken as the state where the node is in $k$ stage (stage is the transition between nodes, and control is the decision of the next situation). $X_{k+1} = u_k$ is taken as a dynamic equation, and $g_k(X_k, u_k) = c_{X_k}u_k = c_{ij}$ as a cost function.

So based on the proposed algorithm, we have

$$J_N(x_N) = g_N(x_N) = \begin{cases} \infty if\ x_N = A \\ 0 if\ x_N = Z \end{cases}. \tag{36}$$

The optimal cost to get to node $j$ starting from $i$ is calculated as follows:

$$J_k(x_k) = \min_{u_k}\left[c_{x_k u_k} + J_{k+1}(u_k)\right]\eta J_k(i) = \min_j\left[c_{ij} + J_{k+1}(j)\right]. \tag{37}$$

Implementing the corresponding table of statements, without using exhaustive calculation, the statements are calculated as follows [32–34]:

$$3^3 = n^{N-1}\text{where } N \geq 3, \tag{38}$$

where $N$ is the number of stages and $n$ is the number of nodes in each intermediate stage.

The solution will occur in 3 stages, wherein each stage a decision will be made for an offer. The benefits are

$$a_j\left(1 - e^{-b_j x_j}\right). \tag{39}$$

The costs are

$$c_j x_j^{d_j}. \tag{40}$$

The state equation is

$$S_{j+1} = S_j - X_j. \tag{41}$$

The objective function is

$$g_j\left(x_j\right) = a_j\left(1 - e^{-b_j x_j}\right) - c_j x_j^{d_j}. \tag{42}$$

So,

$$\frac{J_N^*(S_N) = g_N(S_N) = 0}{J_j^*\left(X_j\right) = \max_{x_j}\left[g_j\left(x_j\right) + J_{j+1}^*\left(S_j - X_j\right)\right] j = N-1, N-2, \ldots, 0}. \tag{43}$$

Therefore, the best policy is

$$\frac{A[10] \longrightarrow B_1[8] \longrightarrow C_1[8] \longrightarrow D_1[9] \longrightarrow Zf^* = 35}{A[10] \longrightarrow B_1[9] \longrightarrow C_3[7] \longrightarrow D_1[9] \longrightarrow Zf^* = 35}. \tag{44}$$

## 2. Conclusions

In this work, we proposed an innovative optimization system for designing, implementing, and updating technical security projects, which require a high level of security standards. It is an analytical way of optimizing that divides the multistage optimization problem into a series of one-step optimization problems. Even multistage systems of increased complexity can be solved with particular ease. The great innovation of the proposed solution is that the separation is done in such a way that the optimal solution of the initial problem results from the optimal solutions of the individual issues so that the method of solving does not affect the result.

A clear example of the proposed procedure was presented descriptively. Specifically, the shortest route was sought in a lattice model to find the best decision on finding the most economical bid in the search for CCTV equipment for the physical perimeter security of the sports project in question. The solution with the minimum cost was achieved based on the proposed approach.

The extensive comparison with probabilistic methodologies that represent parts of stochastic systems through appropriate statistical parameters is an essential aspect that they should expand upon in the next stage of this research project. Additionally, queuing methods and inventory theory may give models for more extensive optimization and perhaps more efficient local decision-making systems.

## Data Availability

The data used in this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

## References

[1] M. PatéCornell, M. Kuypers, M. Smith, and P. Keller, "Cyber risk management for critical infrastructure: a risk analysis model and three case studies," *Risk Analysis*, vol. 38, no. 2, pp. 226–241, 2018.

[2] H. He and J. Yan, "Cyberphysical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[3] D. L. Marino, C. S. Wickramasinghe, K. Amarasinghe et al., "Cyber and physical anomaly detection in smart-grids," in *Proceedings of the 2019 Resilience Week (RWS)*, pp. 187–193, San Antonio, TX, USA, November 2019.

[4] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. Tubino, and S. E. Quincozes, "Towards a Distributed Approach for Detection and Mitigation of Denial of Service Attacks within Industrial Internet of Things," *IEEE Internet Things Journal*, vol. 8, no. 6, pp. 4569–4578, 2021.

[5] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-physical resilience of electrical power systems against malicious attacks: a review," *Current Sustainable/Renewable Energy Reports*, vol. 5, no. 1, pp. 14–22, 2018.

[6] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Applied Energy*, vol. 235, pp. 204–218, 2019.

[7] P. Akubathini, S. Chouksey, and H. S. Satheesh, "Evaluation of Machine Learning approaches for resource constrained IIoT devices," in *Proceedings of the 2021 13th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 74–79, Chiang Mai, Thailand, October 2021.

[8] X. Cai, Q. Wang, Y. Tang, and L. Zhu, "Review of cyber-attacks and defense research on cyber physical power system," in *Proceedings of the2019 IEEE Sustainable Power and Energy Conference (iSPEC)*, pp. 487–492, Beijing, China, November 2019.

[9] P. Boström-Rost, "On Informative Path Planning for Tracking and Surveillance," 2019, http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-157026.

[10] X. Hao, M. Lv, J. Zheng, Z. Zhang, and W. Yi, "Integrating cyber-attack defense techniques into real-time cyber-physical systems," in *Proceedings of the 2019 IEEE 37th International Conference on Computer Design (ICCD)*, pp. 237–245, Abu Dhabi, UAE, November 2019.

[11] K. Hasan, S. Shetty, A. Hassanzadeh, and S. Ullah, "Towards Optimal Cyber Defense Remediation in Cyber Physical Systems by Balancing Operational Resilience and Strategic Risk," in *Proceedings of the MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, pp. 1–8, Norfolk, VA, USA, November 2019.

[12] L. Alzubaidi, J. Zhang, A. J. Humaidi et al., "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *Journal of Big Data*, vol. 8, no. 1, p. 53, 2021.

[13] M. T. Amron, R. Ibrahim, and S. Chuprat, "A review on cloud computing acceptance factors," *Procedia Computer Science*, vol. 124, pp. 639–646, 2017.

[14] S. Roy, S. U. Kadir, Y. Vorobeychik, and A. Laszka, "Strategic remote attestation: testbed for internet-of-things devices and stackelberg security game for optimal strategies," in *Decision and Game Theory for Security*, pp. 271–290, Springer, Berlin, Germany, 2021.

[15] S. Varshney, D. Munjal, O. Bhattacharya, S. Saboo, and N. Aggarwal, "Big data privacy breach prevention strategies," in *Proceedings of the 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, pp. 1–6, Gunupur Odisha, India, December 2020.

[16] R. Cavazos-Cadena and R. Montes-de-Oca, "The value iteration algorithm in risk-sensitive average markov decision chains with finite state space," *Mathematics of Operations Research*, vol. 28, no. 4, pp. 752–776, 2003.

[17] J. Qian, J. P. Lu, S. L. Hui, Y. J. Ma, and D. Y. Li, "Dynamic analysis and CFD numerical simulation on backpressure filling system," *Mathematical Problems in Engineering*, vol. 2015, Article ID e160641, 8 pages, 2015.

[18] B. Bordel, R. Alcarria, and T. Robles, "Recognizing human activities in Industry 4.0 scenarios through an analysis-modeling- recognition algorithm and context labels," *Integrated Computer-Aided Engineering*, vol. 29, no. 1, pp. 83–103, 2021.

[19] M. P. Deisenroth, T. Ohtsuka, F. Weissel, D. Brunn, and U. D. Hanebeck, "Finite-horizon optimal state-feedback control of nonlinear stochastic systems based on a minimum principle," in *Proceedings of the IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, pp. 371–376, Heidelberg, Germany, September 2006.

[20] K. Jin, T. Yin, C. A. Kamhoua, and M. Liu, "Network Games with Strategic Machine Learning," in *Lecture Notes in Computer Science, Decision and Game Theory for Security*, pp. 118–137, Springer, Berlin, Germany, 2021.

[21] C. Sangüesa, "Error bounds in approximations of random sums using gamma-type operators," *Insurance: Mathematics and Economics*, vol. 42, no. 2, pp. 484–491, 2008.

[22] O. Sundström, L. Guzzella, and P. Soltic, "Optimal hybridization in two parallel hybrid electric vehicles using dynamic programming," *IFAC Proceedings Volumes*, vol. 41, no. 2, pp. 4642–4647, 2008.

[23] A. R. Butler, T. H. Nguyen, and A. Sinha, "Countering attacker data manipulation in security games," in *Decision and Game Theory for Security*, pp. 59–79, Springer, Berlin, Germany, 2021.

[24] X. Wang, Y. Ji, J. Wang, Y. Wang, and L. Qi, "Optimal energy management of microgrid based on multi-parameter dynamic programming," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, Article ID 155014772093714, 2020.

[25] A. R. Horowitz, "Loss functions and public policy," *Journal of Macroeconomics*, vol. 9, no. 4, pp. 489–504, 1987.

[26] C. Segovia and K. Smith-Miles, "Integrating Game Theory and Data Mining for Dynamic Distribution of Police to Combat Crime," in *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, pp. 780–783, Santiago, Chile, September 2018.

[27] M. Bellare and O. Goldreich, *On probabilistic versus deterministic provers in the definition of proofs of knowledge Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, pp. 114–123, Springer, Berlin, Germany, 2011.

[28] S. Gupta, S. Al-Obaidi, and L. Ferrara, "Meta-analysis and machine learning models to optimize the efficiency of self-healing capacity of cementitious," *Material," Materials*, vol. 14, no. 16, 2021.

[29] A. Grabowski and T. Pfau, "A lattice of magneto-optical and magnetic traps for cold atoms," in *Proceedings of the 2003 European Quantum Electronics Conference. EQEC 2003 (IEEE Cat No.03TH8665)*, p. 274, June 2003.

[30] T. Reisz, "A power counting theorem for Feynman integrals on the lattice," *Communications in Mathematical Physics*, vol. 116, no. 1, pp. 81–126, 1988.

[31] Y. Zhang, Y. Wang, and J. Yang, "Lattice LSTM for Chinese sentence representation," *IEEE Transactions on Audio Speech and Language Processing*, vol. 28, pp. 1506–1519, 2020.

[32] J. Xie, X. Bai, D. Feng, and D. Gan, "Peaking cost compensation in northwest China power system," *European Transactions on Electrical Power*, vol. 19, no. 7, pp. 1016–1032, 2009.

[33] Y. Azan Basallo, V. Estrada Senti, and N. Martinez Sanchez, "Artificial intelligence techniques for information security risk assessment," *IEEE Latin America Transactions*, vol. 16, no. 3, pp. 897–901, 2018.

[34] X. Liang, T. Qi, Z. Jin, S. Qin, and P. Chen, "Risk assessment system based on fuzzy composite evaluation and a back-propagation neural network for a shield tunnel crossing under a river," *Advances in Civil Engineering*, vol. 2020, Article ID 8840200, 14 pages, 2020.