Journal of Future Sustainability 5 (2025) 179–194

Contents lists available at GrowingScience

Journal of Future Sustainability

homepage: www.GrowingScience.com/jfs

Optimizing cybersecurity in cyber-physical manufacturing systems: A game-theoretic approach and quantal response equilibrium study

Alireza Zarreh[a], Mobin Zarreh[b*], HungDa Wan[a] and Can Saygin[c]

[a]*Department of Mechanical Engineering, The University of Texas at San Antonio, San Antonio, TX, USA*
[b]*School of Computing and Augmented Intelligence, Arizona State University, Tempe, AZ 85287, USA*
[c]*Senior Vice President for Research Dean of the Graduate College, The University of Texas Rio Grande Valley, Grande Valley, TX, USA*

C H R O N I C L E

Article history:
Received: June 1, 2024
Received in revised format: July 29, 2024
Accepted: September 2, 2024
Available online: September 2, 2024

Keywords:
Game theory
Cybersecurity in manufacturing
Best strategy for defense
Quantal response equilibrium
Risk Analysis
Optimization

A B S T R A C T

In the era of Industry 4.0, advanced manufacturing systems are increasingly integrating cyber and physical components, making them susceptible to sophisticated cyber-attacks. Addressing these vulnerabilities is crucial for maintaining the integrity and efficiency of manufacturing processes. This study introduces a comprehensive game-theoretic model to tackle cybersecurity challenges in such systems. The interaction between cyber attackers and defenders is modeled as a strategic game, incorporating a cost function that includes production losses, recovery from attacks, and maintaining of defense strategies. Both deterministic and probabilistic approaches are employed: linear programming identifies optimal strategies, achieving Nash equilibrium under ideal conditions, while the Quantal Response Equilibrium (QRE) method captures player behavior under uncertainty. The optimization problem is solved using the CPLEX library in Python, ensuring robust and efficient computation of optimal mixed strategies. The methodology is demonstrated through a numerical example, highlighting the identification of potential vulnerabilities and optimal defense strategies. The analysis reveals that the defender's learning curve is longer and more complex than the attacker's, emphasizing the necessity for advanced and adaptive defense strategies. This comprehensive approach not only predicts attacker behavior but also suggests effective defense mechanisms tailored to specific threats. The findings underscore the importance of strategic decision-making in enhancing the cybersecurity resilience of cyber-physical manufacturing systems, offering valuable insights for mitigating cybersecurity risks effectively. The most significant result indicates the critical need for timely and adaptive defense mechanisms to counter sophisticated cyber threats, ensuring the sustained operation and security of modern manufacturing environments.

1. Introduction

The production of diverse products within highly adaptable systems that meet customer demands is being achieved through recent advancements in manufacturing, particularly by integrating cyber and network technologies into traditional physical manufacturing systems. These integrated systems, known as cyber-physical manufacturing systems (CPMS), provide manufacturers with the ability to control and manage complex operations with high reliability in real-time (Jakovljevic et al., 2017). Concepts such as Cloud Manufacturing, Software as a Service (SaaS), and Industry 4.0 are all encompassed within this domain (Adamson et al., 2017; Krishnaiyer et al., 2018; X. F. Liu et al., 2017). However, alongside these benefits come new challenges, as these advancements have introduced manufacturing systems to novel threats that previously posed little concern. Attackers now exploit networks and cyber systems as conduits to infiltrate and carry out malicious activities within the system (Knapp & Langill, 2014). Concurrently, these malicious activities have become increasingly covert and more challenging to detect, significantly raising the cost of defensive measures (J Bayuk et al., 2011). Recent studies indicate that manufacturing systems have become increasingly appealing to cyber attackers, emerging as one of the most targeted sectors in recent years (*2017 DBIR*, 2017). Despite technological advancements, a key factor contributing to this trend is the failure of manufacturing systems to implement adequate defense strategies against cyber-physical attacks (*Cyber Risk in Advanced*

* Corresponding author.
E-mail address: mobin.zarreh@asu.edu (M. Zarreh)

ISSN 2816-8151 (Online) - ISSN 2816-8143 (Print)

doi: 10.5267/j.jfs.2025.9.002

Manufacturing | Deloitte US, 2017). These systems are frequently connected to the internet without sufficient preventive defense mechanisms in place. As a result, the combination of these vulnerabilities and the absence of robust defense measures renders manufacturing systems particularly attractive targets for cyber attackers (Ani et al., 2017).

The consequence of cyber-physical threats could be devastating for a CPMS. Notable incidents include the 2014 German steel mill attack, where spear-phishing led to massive physical damage (Singh et al., 2020) and the 2015 Ukraine power grid attack that cut power to 230,000 people (Ferrari et al., 2020). 2017 Triton malware attack in Saudi Arabia aimed to disable safety systems in a petrochemical plant, risking catastrophic damage (Pearce et al., 2019). In 2020, Israel's water infrastructure faced an attack intending to alter chlorine levels, threatening public health, but it was thwarted in time (Cook et al., 2016). These examples underscore the critical need for robust cybersecurity in industrial and manufacturing systems.

It's important to recognize that the motivations and objectives behind attacks on manufacturing systems vary significantly. Attackers can range from industry competitors seeking a competitive edge to state-sponsored entities or organized crime groups (*Manufacturing - Cyber Executive Briefing | Deloitte | Analysis*, 2016). The likelihood of different types of attacks on a manufacturing system varies, requiring customized defense mechanisms to effectively counter the specific threats posed by each attacker. However, implementing all possible defense strategies can be prohibitively expensive. Therefore, it is crucial to assess the probability of specific attack types based on the unique characteristics of the manufacturing system to optimize defense efforts effectively.

To address cybersecurity vulnerabilities, two primary approaches can be utilized: the retrospective approach and the proactive approach. The retrospective approach involves analyzing past attacks to defend against current threats. As illustrated in Fig. 1, when a hacker successfully creates and implements a new approach against security systems, other attackers quickly adopt and disseminate it. In response, the security community eventually develops countermeasures, prompting attackers to devise new methods, thereby perpetuating the cycle. While this approach can be effective against inexperienced attackers, it falls short when dealing with advanced cyber weapons targeting manufacturing systems that lack a history of such threats.

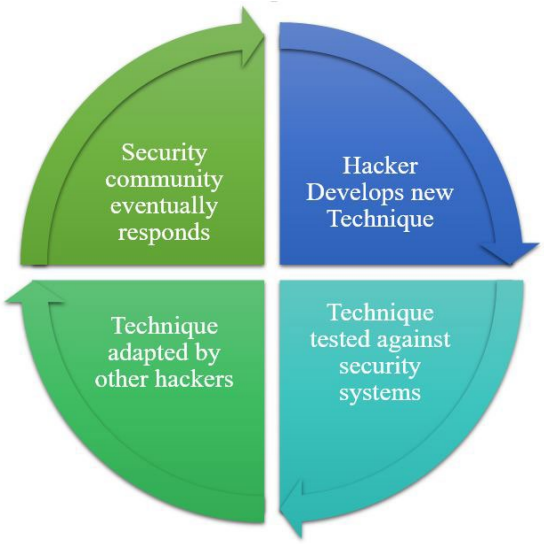

Fig. 1. Retrospective approach cycle

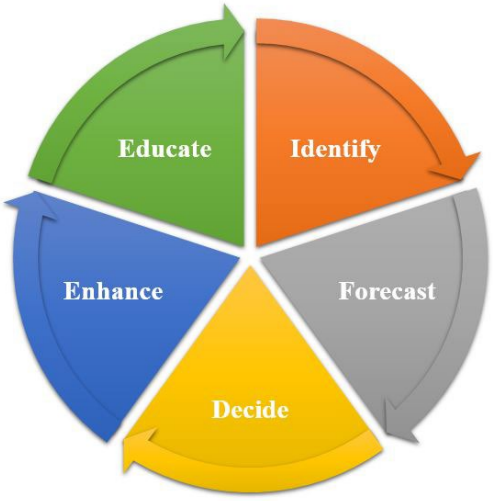

Fig. 2. Proactive approach

Conversely, the proactive approach seeks to anticipate cyber-attacks by predicting attackers' likely behaviors and assessing their capabilities, enabling the implementation of effective countermeasures. These countermeasures may include traditional IT responses, such as taking infected systems offline, reinstalling software, or conducting thorough system checks on likely targets. Additionally, they may involve more tailored strategies for manufacturing systems, such as rescheduling production or redesigning platforms to mitigate the impact of an attack (Miller, 2016). As illustrated in Fig. 2 this approach provides management with an estimation of potential threat consequences, aiding in the selection of appropriate defensive measures to bolster security. Generally, proactive risk mitigation strategies, such as optimizing decision-making through advanced predictive models, have been shown to significantly improve system resilience against potential threats (Tashakkori et al., 2024). Furthermore, recent advancements in protecting neural networks from adversarial attacks highlight the effectiveness of stochastic computing in strengthening cybersecurity efforts (Banitaba et al., 2024).

However, predicting cyber-attacks in manufacturing systems is a complex and challenging endeavor. Modeling the interactions between attackers and cyber systems within an analytical framework to forecast potential attacks presents substantial difficulties.

This research proposes a proactive approach to addressing security challenges in CPMS by assessing the likelihood and impact of various attacks and recommending optimal defense strategies. To achieve this, the CPMS is modeled with a focus on cybersecurity concerns, employing game theory to represent the interactions between the CPMS and attackers as two players in a strategic game. The utility function of the game is constructed by incorporating factors such as defense strategies, production losses, recovery efforts, and the effectiveness of defensive actions against different types of attacks. The model is first analyzed using linear optimization under the assumption of perfect conditions—rational players with complete information—allowing the identification of the optimal long-term strategy that minimizes damage. In this context, "long-term" refers to the point at which both players have identified their optimal strategies and remain consistent after numerous interactions. However, recognizing that real-world scenarios are rarely ideal, the analysis is extended using the Quantal Response Equilibrium (QRE) method. This approach captures the behavior of players when they lack complete information, enabling the system to respond more effectively to cyber threats. The proposed method is demonstrated through a numerical example, where potential cybersecurity vulnerabilities in a CPMS are identified, and optimal strategies are determined to mitigate damage both over time and in the long run.

The structure of this paper is as follows: Section 2 reviews the relevant literature on vulnerability assessment and examines commercial tools applicable to CPMS. Section 3 provides an overview of the theoretical framework used to model a cyber-physical manufacturing system. In Section 4, two approaches are presented for analyzing this model. Section 5 offers a numerical example to enhance understanding of the model and connects the findings from the previous section to the literature review. In conclusion, Section 6 provides a summary of the paper's main contributions and proposes potential directions for future research to improve the model's effectiveness and practical application.

2. Literature Review

Several literatures employ retrospective approach to mitigate cyber-physical threats in manufacturing systems and enhance their trustworthiness. These studies try to add an extra layer of defense specifically designed for manufacturing systems to improve traditional IT cybersecurity. (Bagheri et al., 2015) propose a cyber-physical architecture for self-aware machines in industry 4.0 manufacturing environment. (Wu et al., 2018) developed a testbed for cyber manufacturing systems, designed to facilitate simulation and data collection aimed at exploring cybersecurity within the manufacturing sector. (Riel et al., 2017) A method was proposed for the integrated design of cyber-physical systems, emphasizing the identification and assessment of functional safety and cybersecurity. This approach merges two established standards with the defense-in-depth concept, originally developed for military applications, to help electronics and software engineers effectively integrate safety and security considerations. (Vincent et al., 2015) advocated for a real-time product/process design approach to detect cyber-attacks, addressing the limitations of quality control systems in cyber-physical manufacturing environments. (Shafae et al., 2019) recommended using quality control (QC) tools as an additional physical detection layer to complement traditional IT security measures. (Wu et al., 2017) utilized a machine learning approach to detect cyber-physical attacks by developing a taxonomy specific to cyber manufacturing systems.

In contrast, much of the existing literature in this field adopts a qualitative proactive approach, focusing on identifying vulnerabilities, warning of the potential consequences of cyber-physical threats, and proposing general solutions and countermeasures for manufacturing systems. For instance, certain studies emphasize the danger of cyber-attacks leading to the production of faulty parts. (Wells et al., 2014) examine the unique features that set manufacturing systems apart from other cyber-physical systems and highlight the necessity for cybersecurity tools designed specifically for the manufacturing context. (Portilla et al., 2014) emphasize the security challenges and vulnerabilities associated with Supervisory Control and Data Acquisition (SCADA) systems in flexible manufacturing environments. Another study by (A. Zarreh et al., 2019a) stresses the importance of accounting for cybersecurity threats as potential sources of failure within total productive maintenance practices to ensure system reliability.

Several qualitative studies concentrate specifically on the cybersecurity challenges associated with additive manufacturing, which is one of the most popular and emerging production methods. (Sturm et al., 2017) examine the vulnerabilities of additive manufacturing (AM), particularly highlighting its susceptibility when using STL files during the production process. Another study by (Zeltmann et al., 2016) explores how cyber-attacks that alter the printing orientation can significantly affect the mechanical behavior of AM-produced specimens, even though the specimens may appear identical.

There are relatively few studies that adopt a quantitative proactive approach to addressing cybersecurity in manufacturing systems. (A. Zarreh et al., 2018b, 2018a) employ a simplified zero-sum game model to represent the interaction between attackers and manufacturing enterprises, aiming to evaluate the impact of cyber-physical threats and identify effective defense strategies. In another study, (A. Zarreh et al., 2019b) propose a risk management framework designed to address the limitations of ISO27k and FMEA in managing cyber-physical threats. Similarly, (DeSmit et al., 2018) apply game-theoretic principles to identify cyber vulnerabilities in manufacturing and enhance security measures.

Recent advancements in cybersecurity for electrical cyber-physical systems (CPS) have increasingly utilized game theory to devise optimal defense strategies. Game-theoretic approaches and finding mixed strategy Nash equilibrium, have proven effective in various domains beyond cybersecurity, such as resource management (Zarreh et al., 2024), economics (Fadavi, 2024) and etc. Yan et al. (Yan et al., 2021) propose a dynamic defense strategy based on zero-sum games of incomplete information, focusing on achieving Nash equilibrium. Similarly, (T. Peng et al., 2021) construct a game model to simulate dynamic interactions between attackers and defenders, selecting optimal strategies through dynamic technology deployment.

(Shao & Li, 2021) explore the allocation of defense resources in power systems, incorporating bounded rationality and QRE to determine the best defense approaches. (H. Hu et al., 2020) utilize a stochastic evolutionary game model to balance defense costs and benefits in dynamic adversarial interactions. (Xu et al., 2020) further this approach by providing a method to achieve optimal defense strategies under stochastic disturbances. (Yao et al., 2021) propose a game theory-based defensive method to minimize system performance deterioration in CPPSs under cyber-attacks, employing reinforcement learning to find Nash equilibrium. In another study, (Hu et al., 2020) extend the signaling game model to analyze optimal strategies for both attackers and defenders using a two-way signaling framework.

(Kalderemidis et al., 2022) combine game theory with the 0-1 Knapsack method to optimize cybersecurity investments and defense strategies, validated through practical use cases. (H. Zhang et al., 2022) integrate qualitative differential and evolutionary games in a dynamic model to assess cybersecurity threats and determine effective defense strategies. (M. Yang & Feng, 2023) enhance defense accuracy against complex network attacks using an improved evolutionary game model that considers heterogeneous groups and dynamic environments. (Zhu et al., 2022) develop a multiagent deep reinforcement learning (MADRL) method for defending against multiple advanced persistent threat (APT) attackers, emphasizing the benefits of shared defensive strategies. (Zhang et al., 2022) investigate attacker-defender interactions in APT scenarios, proposing strategies to minimize information leakage and optimize resource allocation.

(Gao et al., 2022) introduce a game-theoretic framework to analyze optimal injection attack strategies on CPS, utilizing Pontryagin's maximum principle. (Ait Temghart et al., 2023) apply a modified quantal response approach within the Stackelberg security game framework to optimize cybersecurity decisions in cloud computing, balancing effectiveness and costs. (Khalid et al., 2023) systematically review game-theory approaches for detecting and defending against APTs, highlighting their effectiveness across various sectors. (Wan et al., 2023) use hypergame theory to model interactions between multiple APT attackers and a single defender, proposing adaptive strategies to reduce false positives and negatives in network intrusion detection systems.

(Z. Liu et al., 2023) develop active defense technology using a Bayesian model, transforming attack-defense scenarios into a dynamic game and optimizing strategies through Bayesian subgames. (Banik et al., 2023) present an optimization-based approach for CPS defense, incorporating adversarial decision-making and Bayesian optimization. (Sun et al., 2023) combines adversarial machine learning, control theory, and game theory to enhance detection and mitigation of attacks on vehicle platooning systems. (Ge & Zhu, 2023) introduce a zero-trust authentication framework for 5G IoT networks, using game theory to prevent lateral attacker movements and improve network security.

(Y. Zhang et al., 2023) propose a resource-constrained attack model for man-in-the-middle attacks on state estimators, optimizing strategies to maximize estimation error while maintaining stealth. (Peng et al., 2023) introduce an epidemic-based model for analyzing malware propagation in multiplex networks, presenting static and dynamic control strategies to prevent spread.(Li et al., 2023) proposes an attack path prediction method using dual reinforcement learning for 5G industrial CPS, offering accurate identification of attack paths without relying on traditional assumptions. These studies collectively highlight the critical role of game theory in developing sophisticated and effective cybersecurity strategies for modern cyber-physical systems.

2.1. Research Gap

While numerous studies have employed both retrospective and qualitative proactive approaches to address cybersecurity threats in CPMS, there is a noticeable deficiency in quantitative proactive methodologies. Retrospective approaches, such as those proposed by Bagheri et al. and Wu et al., focus on creating architectures and testbeds to understand past cyber-physical threats and mitigate future ones. Qualitative proactive approaches highlight vulnerabilities and suggest general countermeasures without providing quantitative analysis or decision-making frameworks. Although a few studies, such as those by Zarreh et al. (2018a, 2018b), have explored game theory and simulation-based models to evaluate and manage cyber-physical threats in manufacturing systems, these efforts remain in their early stages and lack comprehensive application.

Furthermore, game theory has been extensively adopted in other domains to enhance cybersecurity, but its application in CPMS is still underexplored. The existing literature often treats manufacturing systems' cybersecurity with generic IT security measures, overlooking the unique challenges and requirements of CPMS. This paper aims to address this gap by presenting a game theory-based approach, incorporating long-term equilibrium and QRE analysis, to enhance cybersecurity

management in CPMS. By doing so, it provides a robust quantitative framework that not only evaluates the repercussions of cyber-physical threats but also optimizes defense strategies specifically tailored for the manufacturing sector. This approach promises to bridge the gap between qualitative warnings and quantitative decision-making, offering a more precise and effective method for managing cybersecurity in advanced manufacturing environments.

3. Modeling CPMS cyber-attacks

This section outlines how a game theory approach can be applied to model a manufacturing system in the context of cybersecurity challenges. To begin with, the fundamental principles of game theory are introduced to facilitate an understanding of the games, which will then be used to develop a model for predicting cyber-attacks. In essence, game theory represents the interactions among multiple decision-makers, each of whom can choose from various actions that lead to different outcomes. The players strive to choose the most effective actions that will maximize their rewards, all while predicting the behavior of other rational participants.

To represent any relationship or interaction as a game, three essential components need to be established: the players, the possible actions for each player, and a utility function (or payoff matrix) (Owen, 1995). A player is a central entity within the game, responsible for making decisions regarding which actions to take. A player is the primary entity in the game responsible for making decisions about actions. This could represent an individual, a machine, or a group of individuals within the game. An action refers to a specific move or choice made within the game. Lastly, the payoff is the positive or negative reward a player receives based on the combined actions of all players in the game (Roy et al., 2010). In modeling a cyber-physical manufacturing system as a game, these elements are defined as follows:

Players In this model, the game is structured as a two-player scenario, with the decision-makers being the attacker and the defender. The attacker may represent a group of individuals, governments, or organizations (Cardenas et al., 2009), that seek to benefit from compromising a manufacturing system. Conversely, the defender represents the system or organization responsible for implementing countermeasures to mitigate the damage caused by an attack.

Action sets: The next step in constructing the game is to define the action sets for each player. For the attacker, the action set includes all possible malicious activities that exploit system vulnerabilities, represented as $A = \{a_1, a_2, \dots, a_n\}$ where n denotes the number of actions available to the attacker. Similarly, the defender's action set comprises all potential defense mechanisms, actions, or countermeasures that can be employed to eliminate, prevent, or mitigate an attack. This is represented as $D = \{d_1, d_2, \dots, d_m\}$ where m indicates the number of actions available to the defender.

Utility function (payoff matrix): To represent the players' motivations, a reward and cost framework is employed, assigning a value (γ_{a_k,d_l}) o each combination of actions taken by the players. This function can be illustrated as an $n \times m$ matrix in the context of a two-player game. In this matrix, the rows correspond to the actions of one player, typically the attacker, while the columns correspond to the actions of the other player, typically the defender. In our model, the row player is the attacker, and the column player is the defender, as outlined below:

$$\Gamma = \begin{pmatrix} \gamma_{11} & K & \gamma_{1m} \\ M & \gamma_{a_k,d_l} & M \\ \gamma_{nm} & L & \gamma_{nm} \end{pmatrix}, \forall\, a_k, d_l \tag{1}$$

In the context of the game, "reward" and "cost" are broad concepts used to quantify the payoff of actions in either tangible terms, such as financial gains and losses, or intangible terms, such as social status, satisfaction, disrespect, or disappointment. For example, in the study (Lye & Wing, 2005), the reward for a successful attack is measured by the anticipated recovery effort required from the system administrator. Similarly, in the research by (P. Liu et al., 2005) the reward is defined by the extent of bandwidth consumed during a DDoS attack. Conversely (Sallhammar et al., 2006) introduce cost as an alternative outcome, highlighting that risk-averse attackers might avoid certain attack actions due to the potential consequences of being detected. This research frames the game model as a zero-sum game, meaning the attacker's gain is exactly equal to the defender's loss. In other words, the game is structured as a win-lose scenario, where if the attacker selects action a_k and the defender selects action d_l, the payoff γ_{a_k,d_l} represents the amount the attacker gains, which is the same amount the defender loses. To construct the utility function, the key characteristics of CPMS that are relevant to cybersecurity are considered, as outlined below:

$$\gamma_{a_k,d_l} = s_{d_l} - \left(s_{a_k} \times e_{a_k,d_l}\right) + T \times p_{a_k} \times \left(1 - e_{a_k,d_l}\right) + r_{a_k} \times \left(1 - e_{a_k,d_l}\right) \qquad ,\forall\, a_k, d_l \tag{2}$$

This utility function consists of three elements, first, maintaining the cost of a defense mechanism, second, cost of production loss, and finally, cost of recovery for the system to its good initial state from an attack. The first two components of the function, as described in Eq. (2), pertain to the cost of maintaining the defense mechanisms. Let $s = \{s_1, s_2, \dots, s_m\}$ represent the set that includes the costs associated with implementing and maintaining each defense mechanism. From a game theory perspective, if a defense mechanism is fully effective, its corresponding element in the function should not yield a positive value. Thus, for each element of the function, any ineffective costs represent a gain for the attacker.

It is important to recognize that not every defense mechanism is fully effective as a countermeasure against an attack. A defensive action may be fully or partially effective against one or more attack actions. The combined effectiveness of these defensive actions can be represented as a matrix, with each element ranging from zero to one, as shown in Eq. (3). If the element e_{a_k,d_l} equals 1, it indicates that the defense strategy d_l is sufficiently effective to prevent, eliminate, or recover from the attacker's action a_k. Conversely, if the element equals 0, it means that the defense action provides no benefit as a countermeasure against that specific attack. Therefore, the larger the value of each element, the more effective it is as a countermeasure for a particular type of attack.

$$E = \begin{matrix} \\ a_1 \\ \vdots \\ a_n \end{matrix} \begin{matrix} \begin{matrix} d_1 & L & d_m \end{matrix} \\ \begin{pmatrix} e_{11} & K & e_{1m} \\ M & e_{a_k,d_l} & M \\ e_{nm} & L & e_{nm} \end{pmatrix} \end{matrix}, \forall\, a_k, d_l \;\&\; 0 \le e_{a_k,d_l} \le 1 \tag{3}$$

The third component of the reward function addresses the monetary losses incurred by the system due to an attack. For a manufacturer, key attributes such as integrity, availability, and consistency of production are critical, making them primary targets for an attacker. If T represents the total production and p_{a_k} denotes the rate of production loss due to attack type a_k expressed as $p = \{p_1, p_2, \dots, p_n\}$, where $0 \le p \le 1$, then multiplying the total production by the rate of loss and the ineffectiveness of various defense mechanisms allows for the calculation of production losses considering all types of actions. The final component of the reward function is based on the recovery cost required to restore a manufacturing system to its original operational state after an attack. This aspect primarily focuses on how the mitigation techniques impact the utility function. Let's assume the recovery costs can be represented by a set $r = \{r_1, r_2, \dots, r_n\}$, where each element indicates the recovery cost associated with a specific type of attack. With all the elements of the game now defined, it is essential to clarify a few key terms that will be used later to analyze the game and optimize the outcomes.

Strategies: As previously discussed, the core challenge in a cybersecurity game lies in determining the likelihood of actions, primarily from the attacker, which is represented as the probability of each player's chosen actions. In a mixed strategy game, a player's strategy is defined as a set of probabilities. For the attacker, this set is represented as $\Pi = \{Pr(a_1), Pr(a_2), \dots, Pr(a_n)\}$, and for the defender, it is denoted as $\Phi = \{Pr(d_1), Pr(d_2), \dots, Pr(d_m)\}$. If both players consistently choose only one of their actions, meaning the probability of that action is 100%, the game is referred to as a pure strategy (a game with a saddle point). A player's strategy can also be understood in terms of what might occur over repeated plays or as representing the population dynamics in a single round of play. In this research, the attacker is viewed as a group of individuals, each with different motives and potentially employing a pure strategy. However, the overall strategy of the attacker group is characterized by the probability distribution of the actions chosen within the group.

$$\sum_{k=1}^{n} Pr(a_k) = 1, \qquad \sum_{l=1}^{m} Pr(d_l) = 1 \tag{4}$$

Global utility (game value): In mixed strategy games, global utility reflects the overall reliability of a system. It represents the expected long-term rewards or gains for the players. This value is calculated as the sum of the probabilities that the attacker and defender choose actions a_k and d_l respectively (i.e., the likelihood of their actions), multiplied by the corresponding element of the utility function.

$$Gu(\Pi, \Gamma, \Phi) = \sum_{a_k \in A} \sum_{d_l \in D} \Pr(a_k).\gamma_{a_k,d_l}.Pr(d_l) \tag{5}$$

By its nature, this game is a stochastic one, involving rational players with complete information. In this context, rationality implies that each player aims to maximize their accumulated payoff (global utility) by selecting actions that yield the best possible outcomes, while also taking into account the behavior of the other player. Complete information indicates that both players are fully aware of the consequences (rewards) associated with each action.

4. Analyzing the model

4.1. Using Linear Programming

In nature, the cybersecurity game is a loose-win game, and for this reason, the game is defined as a non-cooperative zero-sum game. Generally, in any game, players tend to increase their payoff by choosing the best strategy. In terms of the model, players are willing to maximize global utility by manipulating their strategy. However, since the model is defined as a zero-sum, the defender tends to minimize the global utility. It could be explained as the manufacturing system seeks to prevent or mitigate the consequence of the attack.

In order to solve and analyze the model, it is formulated as a general optimization problem with a multi-objective function in which on the first, the attacker tries to maximize the payoff while on the second the defender tends to mitigate and minimize the consequences of the attack.

The optimization problem can be defined as equation (6) in which the desired outcome is the strategy of attacker and defender that no player can deviate from in order to gain more benefits. These strategy profiles are called the mixed strategy Nash equilibrium.

$$Gu^* = Gu(\Pi^*, \Gamma, \Phi^*) = \min_{\Phi}\max_{\Pi} Gu\left(\Pr(a_k), \Pr(d_l), \gamma_{a_k,d_l}\right) \tag{6}$$

According to Nash's theorem, every finite game possesses an equilibrium, known as the Nash equilibrium (Nash, 1951), where each player cannot further improve their payoff. This state, denoted as U*, represents the optimal mixed strategy, where the game achieves its Nash equilibrium. To solve the game, a feasible constraint is applied, which can be expressed as follows:

$$Gu^* \geq Gu, \quad \forall\, Gu, \Pr(a_k), \Pr(d_l) \tag{7}$$

However, solving a two-player game becomes challenging when the size of the payoff matrix exceeds three for each player ($i.e., m \geq 3, n \geq 3$). (Von Neumann & Morgenstern, 1947) first discovered the connection of the game with linear programming, and later (Dutta, 1999) demonstrated that a mixed strategy solution must exist for two-player zero-sum games. The game is formulated as a linear program with two objective functions, providing a computationally efficient method to solve problems where each player has more than three possible actions. Each objective function reflects the efforts of the players: the attacker seeks to maximize their gain, while the defender aims to minimize the damage. In these problems, e is a vector of ones. In the first problem, the variables are w (a real number) and A (an n-dimensional vector). The first constraint ensures that each component of $\Pi\Gamma$ (of which there are m) is greater than or equal to w. The second and third constraints require that Π be a probability distribution for the attacker.

In the second problem, the variables are v and Φ (an m-dimensional vector). The first constraint ensures that each component of $\Phi\Gamma$ (there are n of them) is less than or equal to v. The second and third constraints require that Φ be a probability distribution for the defender. For a deeper understanding of how to solve two-player zero-sum games using linear programming, readers are referred to (Joel Sobel, n.d.; Y. M. Yang et al., 2011). The constraints are as follows:

$$\begin{aligned} &w^* = max\, w \\ &s.t. \begin{cases} \Pi\Gamma - we \geq 0 \\ \Pi.e = 1 \\ 0 \leq Pr(a_k) \leq 1 \end{cases} \end{aligned} \qquad \begin{aligned} &v^* = min\, v \\ &s.t. \begin{cases} \Phi\Gamma - ve \leq 0 \\ \Phi.e = 1 \\ 0 \leq Pr(d_l) \leq 1 \end{cases} \end{aligned} \tag{8}$$

Finally, with the tools and approach in place to determine the optimal strategy, various combinations of defense mechanisms need to be evaluated. The total number of possible combinations is $2^m - 1$, where m represents the number of available defense mechanisms. By comparing the global utility of the optimal mixed strategies for each combination with the associated maintenance costs, the most effective combination can be identified based on the target criteria of the optimal strategy. This process will be further detailed in the illustrative example section.

4.2. Using Quantal Response Equilibrium (QRE)

The optimal mixed strategy outlines the most effective moves for each player, yet certain assumptions may not be applicable in every scenario. In noncooperative games, three fundamental principles typically apply. First, a player's decisions are shaped by their expectations of how other players will act. Second, each player's choices are considered optimal based on these expectations. Third, the expectations regarding other players' actions are generally accurate in a probabilistic sense. These principles lead to a stable state known as Nash equilibrium, which the game typically reaches over time. This equilibrium assumes that both players are rational, consistently seeking to maximize their payoff, fully aware that their opponents are also rational, and have complete knowledge of the outcomes of each combined action. However, these conditions

are not always applicable in cybersecurity games. In reality, player behavior is frequently influenced by errors due to incomplete information. For example, an attacker might carry out random attacks on a system without fully understanding the potential rewards or repercussions. Moreover, empirical studies show that players do not always behave entirely rationally; they often make mistakes and fail to select the optimal action. Nevertheless, as players gain experience and learn from previous decisions, their behavior tends to become more rational over time. The QRE adjusts the second principle of the game by incorporating the effect of errors, enabling a more realistic representation of player behavior.

In the QRE method, errors arising from semi-rational players, incomplete information, or short-term behavior can be represented by the tuning parameter λ. When λ, is small, players exhibit less rational behavior, and as λ increases, their behavior becomes more rational. Essentially, as λ approaches zero, players' actions are almost entirely random, whereas as λ approaches infinity, players consistently choose the action with the highest expected payoff. This parameter λ can also be interpreted as a measure of responsiveness or precision in decision-making. Additionally, in most scenarios, as players gain experience and learn from previous decisions, their decision-making precision improves over time ($limt \to \infty \lambda t = \infty$). Therefore, λ can also be viewed as a time parameter, indicating that decision noise decreases over time. However, λ still depends on various factors such as the player's type, incomplete information, biases, emotions, and more.

Given these imperfect conditions, the goal for each player is not necessarily to find the best strategy, but rather to determine the best response to their opponent's behavior. In a logit QRE, which is the most common form of QRE, players choose their strategies based on a probability distribution, P_{r_i}. This distribution is determined by the expected utility for player i when choosing strategy j under the assumption that other players are following the probability distribution $P_{r_{-i}}$ (Goeree et al., 2016).

$$Pr_i^j = \frac{exp\left(\lambda U_i^j(Pr_{-i})\right)}{\sum_{j \in A|D} exp\left(\lambda U_i^j(Pr_{-i})\right)} \tag{9}$$

The expected utility function reflects player i's expectations about the actions of other players when they choose action j. As shown in Eq. (9), the expected utility is directly related to the probabilities of the other players' actions. In other words, if a player deviates from their best strategy or makes a mistake, it alters the expected utility of the other players. Therefore, the optimal response for a player involves taking into account the potential errors of others in the game. In summary, the probability distribution of each player is directly linked to the probability distributions of the other players, as illustrated below:

$$U_i^j(Pr_{-i}) = \sum_{k \in A|D} Pr_{-i}^k . \gamma_{ij,-ik} \tag{10}$$

To solve the game with P_{r_i}, and $P_{r_{-i}}$ as unknowns, one must address a system of non-linear equations, with a total of $n + m$ unknowns for each tuning parameter. To fully understand the spectrum of players' rationality and their learning processes, it is necessary to solve this system of equations across all possible values of the tuning parameters.

In practice, the parameter λ is initially set to zero, and the game is solved to determine the probabilities. At this stage, the probabilities should be equal across all actions, reflecting random choice behavior, which serves as the first sanity check of the calculation. Subsequently, the tuning parameter λ is incrementally increased, and the entire analysis is repeated for each new value. The calculation continues until the probabilities of all players' actions converge to specific values. These values typically represent the dominant Nash equilibrium of the game. As a second sanity check, the converged probabilities are compared to the optimal mixed strategy equilibrium derived in the previous section, and they should match.

5. Illustrative example

This section presents a numerical example to further demonstrate the approaches discussed in the previous section. First, a cyber-physical manufacturing system will be analyzed with respect to its cybersecurity concerns, identifying potential risks and vulnerabilities, as well as possible defensive policies to mitigate these issues. Second, the problem will be framed as a game, making it amenable to analysis using the methods previously introduced.

5.1. Problem definition

The CPMS considered in this example is a typical medium to large-scale manufacturing system with a continuous production line and a high degree of integration between cyber and physical systems, such as those found in automotive manufacturing. As previously discussed, the system's vulnerabilities are represented as the action set for the attacker. For this specific system, nine threats and vulnerabilities are identified which can be shown as a set of action for the attacker as $A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} =$ {Insider privilege misuse, Theft of intellectual properties, Disruption of production line, Infecting SCADA, Corruption of quality management system, Software Security Flaws and Threats, Disruption of supply chain, Access privilege of mobile device and wireless communication, Corruption of data and cloud} where a_k denotes an attack action.

Insider attack as one of the most frequent attacks in the industry today is when company employees with malicious intent may leak information to untrusted sources. According to the Data Breach Investigation Report by Verizon, out of 750 cyber incidents they monitored in the manufacturing sector in 2016, 10% were due to insider attacks (*2017 DBIR*, 2017). The theft of intellectual properties is another vulnerability in the system. Intellectual properties refer to high-value business information, including product design, business plans, financial strategies, asset information, and patents.

The ultimate goal of a CPMS is to stabilize production under cyber threats to satisfy customer demands, so disruption of the production line is the biggest concern. This problem could happen due to other vulnerabilities such as insider attack or infected SCADA in the system, though, from the defender's point of view, it is the primary concern and should be treated as separate vulnerability. SCADA systems, which are the most prevalent type of industrial control systems used for data collection, system monitoring, and machinery control, are also susceptible to vulnerabilities. Numerous studies in the literature have identified this as a critical vulnerability (Ali et al., 2018; Coffey et al., 2018; B. Zhu et al., 2011).

The next system vulnerability is software security, which includes two types of flaws: non-malicious operation, and malicious operations. Malicious flaws are intentionally designed to harm the system such as computer viruses, Trojan horses, and worms. Disruption of the supply chain is another threat to the system. In a recent incident, a virus attack to a supplier of Apple Co. delayed the shipment of the company's products.

Wireless network security as a vulnerability in CPMS is one of the most researched fields of cybersecurity. Various security concerns like weak passwords, lacking strong authentications, downloading content from unknown third-party platforms, and operating system updates in mobile devices are in this category (Henze et al., 2017). The last vulnerability is data, application, and cloud corruption. The cloud service has several benefits and most of the time is more secure than an enterprise. However, if there is a security breach in the cloud the consequences could be severe (Bouzary & Chen, 2018).

Having the attacker's action set defined, the actions for the CPMS as the defender is shown as a set of twelve defensive actions as follows:

$D = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9, d_{10}, d_{11}, d_{12}\}$ = {Resource allocation and Dynamic scheduling, Upgrading legacy systems, Preventive checkups, Information security system, Monitoring and Visualization, Network Security and Authentication, Security program for a SCADA systems, Supply Chain Security, Mobile Device Security and Wireless Communication, Data and Cloud Security, Intellectual Property Protection, Do noting} where d_l denotes a defender action. Answering a cybersecurity threat like any other risk is categorized to mitigate, avoid, transfer, or accept the risk. In this game, d_1 is a mitigation technique, $d_2, d_3, d_4, d_6, , d_8, d_9$ are avoiding policies, d_{10} is to transfer the risk, d_{12} is when accepting the risk and finally d_5, d_7, d_{11} could be categorized to either avoid or mitigate risk.

Resource allocation and dynamic scheduling as the first defensive action could be used to reduce the adverse effect of an attack in the system by rerouting and distributing the jobs to deferent resources (Bouzary & Chen, 2019).

Legacy systems are a significant issue in the manufacturing sector, and upgrading these systems and preventive checkups could help avoid the threat. Also, implementing an information security system such as firewalls, intrusion detection system, virus protection software, security auditing systems, vulnerability scanners, and packet filtering routers could avoid cyber threats. Moreover, network security and authentication such as enciphering or encryption, supply chain security to secure both supplier and retailer, mobile device security, and wireless communication like securing access point and implementing SSID will considerably avoid cybersecurity risks.

Furthermore, monitoring and visualization of networks, desktops, and storages; security program for SCADA systems; and intellectual property protection such as persistent encryption and watermarking could both avoid and/or mitigate risk in a cyber-physical manufacturing system. Lastly, the system could transfer the risk to a third party, such as utilizing a cloud for its data. As said above, this policy is subjected to vulnerability if the cloud provider gets breached. Also, if the consequence of risk is low or it is not very likely to happen, the system could accept the risk by doing nothing. In the following the matrix of the effectiveness of defensive action against attacks is provided. Based on the efficacy of each defense action for various attacks, the matrix of effectiveness is formed, as shown in Table 1. Each element of this matrix, as discussed above, demonstrates the effectiveness of a specific defense action in order to mitigate or avoid particular attack action. For example, resource allocation and dynamic scheduling (d_1) can mitigate 95% of supply chain disruption (a_7), while it is not effective at all in case of theft of intellectual properties (a_2). The maintaining cost of each defense action, the production loss rate, and cost of recovery in the total production of 1000 products are summarized in Table 2.

Table 1
Matrix of the effectiveness of defensive action vs. attacks.

		Mitigate	Avoid	Avoid	Avoid	Mitigate/ Avoid	Avoid	Mitigate/ Avoid	Avoid	Avoid	Transfer	Mitigate/Avoid	Accept risk
		d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}
		Resource allocation and Dynamic scheduling	Upgrading legacy systems	Preventive checkups	Information security system	Monitoring and Visualization	Network Security and Authentication	Security program for SCADA systems	Supply Chain Security	Mobile Device Security and Wireless Communication	Data and Cloud Security	Intellectual Property Protection	Do nothing
a_1	Insider privilege misuse	0.4	0.8	0.7	0.9	0.8	0.1	0.1	0	0.8	0.95	0.9	0
a_2	Theft of intellectual properties	0	0.9	0.1	0.95	0.4	0.1	0.1	0	0.6	0.8	0.9	0
a_3	Disruption of production line	0.8	0.4	0.6	0.2	0.6	0.1	0.1	0.1	0.3	0.2	0.1	0
a_4	Infecting SCADA	0.8	0.2	0.7	0.8	0.6	0.4	0.95	0.1	0.8	0.2	0.1	0
a_5	Corruption of quality management system	0.3	0.1	0.1	0.6	0.3	0.1	0	0.3	0	0.1	0.3	0
a_6	Software Security Flaws and Threats	0.2	0.95	0.2	0.95	0.5	0.1	0.1	0.1	0	0.2	0	0
a_7	Disruption of supply chain	0.95	0.3	0.3	0.3	0.6	0.1	0.4	0.9	0	0.5	0.2	0
a_8	Access privilege of mobile device and wireless communication	0.2	0.3	0.3	0.6	0.9	0.95	0.1	0	0.95	0.1	0.3	0
a_9	Corruption of data and cloud	0.1	0	0	0.3	0.8	0.8	0	0	0	0.95	0.3	0

Table 2
Summary of system details utilized in the illustrative example.

Type of game	Two players zero-sum game with incomplete information and semi-rational players
Maintaining cost of defense mechanism	$s = \{400, 600, 100, 100, 300, 300, 400, 700, 150, 300, 100, 0\}$ where s_l denotes maintaining cost for d_l
Production loss rate	$p = \{0.8, 0.1, 1, 0.8, 0.6, 0.3, 0.7, 0.2, 0.4\}$ where p_k refers to the production loss rate according to a_k
Total production	$T = 1000$
Cost of recovery	$r = \{400, 300, 200, 500, 50, 50, 200, 300, 100\}$ where r_k the cost of recovering from attack a_k to restore the system to its original state.

5.2 Linear Optimization Analysis

Having all the necessary element of utility function defined, the function could be calculated by equation (2) for each joint action form both players and can be shown as a 9×12 matrix below in which rows demonstrate the actions form attacker and columns represent actions form the system.

$$\Gamma = \begin{bmatrix} 960 & 360 & 390 & 130 & 300 & 1350 & 1440 & 1900 & 270 & 75 & 130 & 1200 \\ 800 & 100 & 450 & 25 & 420 & 630 & 720 & 1100 & 220 & 140 & 50 & 400 \\ 320 & 1080 & 520 & 1040 & 600 & 1350 & 1440 & 1710 & 945 & 1200 & 1170 & 1200 \\ 340 & 1520 & 420 & 280 & 640 & 960 & 85 & 1800 & 290 & 1280 & 1260 & 1300 \\ 735 & 1125 & 675 & 300 & 665 & 855 & 1050 & 945 & 800 & 855 & 525 & 650 \\ 600 & 47.5 & 360 & 22.5 & 325 & 585 & 675 & 945 & 500 & 520 & 450 & 350 \\ 65 & 1050 & 700 & 700 & 480 & 1080 & 780 & 160 & 1050 & 600 & 800 & 900 \\ 720 & 770 & 420 & 240 & 80 & 40 & 810 & 1200 & 32.5 & 720 & 420 & 500 \\ 810 & 1100 & 600 & 420 & 160 & 160 & 900 & 1200 & 650 & 40 & 420 & 500 \end{bmatrix}$$

The mixed strategy Nash equilibrium could be found by using linear programming optimization. This approach is effective for determining the best strategies for both attackers and defenders in cyber-physical systems. Mathematical modeling and optimization techniques, similar to those used in other complex problem domains such as logistical problems (Aghakhani et al., 2023), identified as one of the most common approaches for the optimization problems by Zarreh et al. (2024), thus demonstrate the potential for enhancing cybersecurity defenses.

To identify the optimal strategies for both attackers and defenders, the optimization problem is formulated as a two-player zero-sum game with the objective of minimizing potential damage from cyber-attacks while optimizing defense strategies under given constraints. This multi-objective function aims to maximize the attacker's payoff and minimize the defender's losses.

The optimization problem is solved using the CPLEX library in Python, a powerful tool for linear programming, mixed-integer programming, and quadratic programming problems. CPLEX is renowned for its efficiency and ability to handle large-scale optimization problems, making it an ideal choice for our complex game-theoretic model. In this implementation, decision variables represent the probabilities of choosing different strategies for both players. The objective functions are constructed based on utility functions, incorporating the costs of maintaining defense mechanisms, production losses, and recovery efforts. The CPLEX solver is used to find the optimal mixed strategy Nash equilibrium by setting up the optimization problem through CPLEX's API. This API provides comprehensive functions for defining variables, constraints, and the objective function. The solver uses advanced algorithms, such as branch-and-bound, cutting planes, and heuristics, to navigate through potential solutions efficiently. All combinations of defensive action should be considered, but if all actions are taken into account, it is shown that the game has no saddle point, meaning the players are going to alternate their choices to gain a better outcome. The global utility (game value) is 588.97, while the optimal strategies for players are as follows:
$\Pi = \{0.0722, 0, 0.3995, 0, 0.4814, 0, 0, 0\ 0.0469\}$ for attacker
$\varphi = \{0.512, 0, 0.0369, 0.3075, 0.1436, 0, 0, 0, 0, 0, 0, 0\}$ for defender

By definition, the optimal mixed strategy Nash equilibrium is when the global utility is minimum. That means the adverse effects of attacks on the system are minimized however if the maintaining cost of defense policies are considered that could be not the choice that an enterprise looks. A costly action could lead to a good result, but the main objective of the defender is to find the most reasonable strategy that leads to a relatively good outcome. It means system looks for a relatively low cost of a defense policy with minimum damage to the system. If all the defensive actions that are no probable to happen

(defense action with zero probability) are ignored to deploy, the maintaining cost of defense strategy will reduce, but it will change the whole game perspective since it is a perfect game, and the attacker knows all available actions for the defender. To overcome that dilemma, it is necessary to consider all the possible combinations of defense actions and find the optimal mixed strategy equilibrium for each of them and then compare them to recommend a policy that fits a system needs best regarding its cybersecurity. In this example, $4095 = (2^{12} - 1)$ possible combinations exist where each instance is solved and analyzed separately to find the optimal strategy and global utility.

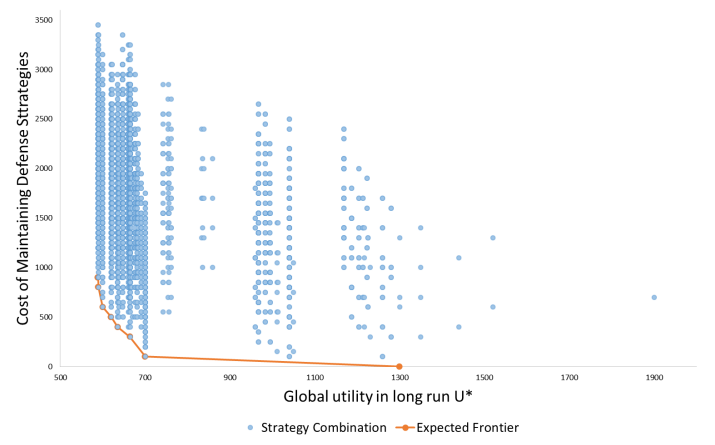

Fig. 3. The payoff from an attack in a long time vs. cost of maintaining strategies

Fig. 3 shows a scatter plot for each combination of defense actions, which is the defense policy for the system with its cost of maintaining and the optimal global utility that can be achieved through it. As can be seen, many policies lead to having reasonably low damage to the system but, the cost of maintaining these policies is the issue. The expected frontier line is drawn by connecting eight points where global utility is achieved at the lowest maintaining cost. Global utility and maintaining cost of these points are shown in Table 3.

This result suggests a significant implication to companies under cyber threat. Even though a company has a wide variety of defense policies, the best choice is limited to those on the expected frontier line illustrated in Fig. 3. It should also be noted that finding the best set of strategies is dependent on how much the company estimates the effectiveness of defenses over cyberattacks. For example, in a large company with a continuous production line, minimizing losses (resulting in lower global utility) over the long term could be a crucial factor in decision-making. In contrast, for a small or medium-sized company with batch production, maintaining the operation might be the primary consideration.

Table 3
Global utility and maintaining the cost for expected frontier policies

d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}	Global Utility	Maintaining Cost
1	0	1	1	1	0	0	0	0	0	0	0	589.0	900
1	0	0	1	1	0	0	0	0	0	0	0	589.6	800
1	0	1	1	0	0	0	0	0	0	0	0	600.3	600
0	0	1	1	1	0	0	0	0	0	0	0	620.1	500
0	0	0	1	1	0	0	0	0	0	0	0	635.5	400
0	0	0	0	1	0	0	0	0	0	0	1	664.4	300
0	0	1	0	0	0	0	0	0	0	0	1	700.0	100
0	0	0	0	0	0	0	0	0	0	0	1	1300.0	0

5.3 Analyzing with QRE method

In the previous section, the example was analyzed considering the assumption that players show entirely rational behavior, and the result addresses the amount that the system will lose in the long run. In this section, the same example will be analyzed with QRE method to understand the imperfect condition and see the behavior of players through the time that helps us find the best response to cybersecurity threats in short-run as well.

As was mentioned before, in QRE, the behavior of each player depends on the other player. Besides, since players' actions are subjected to errors due to incomplete information if one player makes mistakes in choosing the best strategy, another player should adjusts his strategy as well. Mathematically, this is modeled by utilizing equation (9) and (10) as a non-linear optimization. The problem is solved with different amount for tuning parameter, which is an implication of time from zero to the point that strategies converge into a certain amount.

Fig. 4 shows the behavior of the attacker with respect to tuning parameter. As can be seen, for near-zero tuning parameter, the attacker shows random behavior and probability of all choice of actions are equal. However, as time passed, he started to adopt choosing a few of the action more because of the past rewards. This behavior goes on until he learns everything about the game and the opponent and hence keeps up with a particular strategy over and over that earns him the best outcome. For this example, he chooses to utilize only four actions out of nine with a specific probability over time. The final probabilities of attacks are consistent with the optimal mixed strategy that was found in the previous section when all actions were considered.

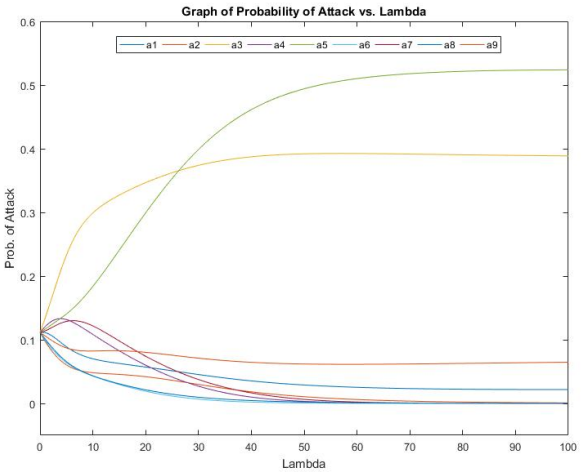

Fig 4. Attacker's behavior with respect to tuning parameter

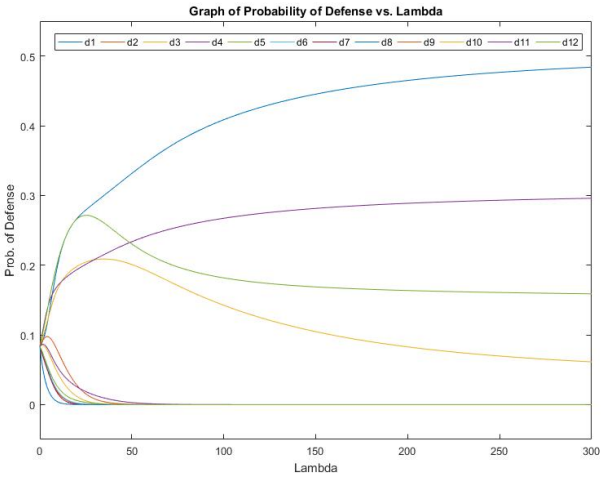

Fig 5. Defender's behavior with respect to tuning parameter

As Fig. 5 shows, the defender also demonstrates similar behavior in the sense that at the beginning, the system behaves randomly for choosing the strategy, but over the time it adopts a specific strategy to encounter the opponent. A point to remind here is that none of the players show the consistent interest of adopting specific action over time. For instance, defender, at the beginning gets interested in using d_5 over d_4, but after a period its behavior changes and finally, it stabilizes by using d_4 with the probability of over 30% and d_5 below 15%. A significant difference between the behaviors of players in this game is the amount of time and effort they need to adopt the optimal mixed strategy. The lambda for the attacker behavior to get converged is only around 100, while the lambda needed for the system is more than 1500. That implies that defender needs more time to find the optimal strategy. The reason is the complexity of the defender's actions. As the number of available choices for a player increases, it gets harder to find the best strategy exponentially. Fig. 6 illustrates the game from the global utility (game value) point of view with respect to lambda presuming both players are learning. In this case, the defender lowers the global utility by adjusting the strategy at the beginning (lambda less than 18). However, since the attacker's choice of actions are less complicated and hence his learning pace is higher in comparison with defender, the global utility starts to increase again (lambda 18 to 60) until both players reach to the point that is not able to enhance it further. This point is Nash equilibrium by definition.

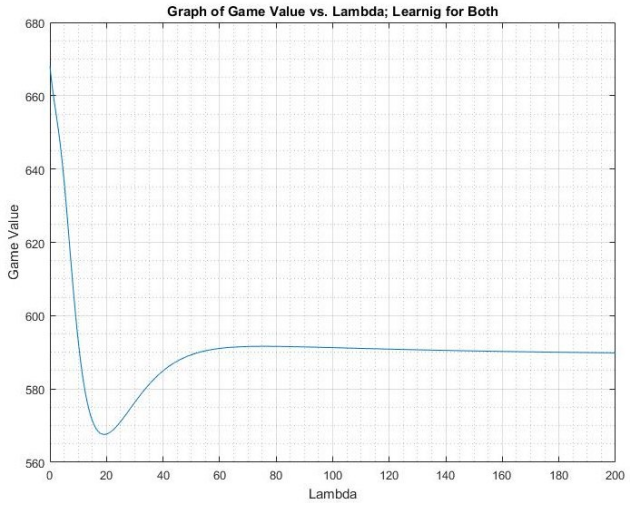

Fig 6. Global utility with respect to tuning parameter

Additionally, analyzing the one-to-one interaction of attacker and defender actions is essential. The minimum damage to the system (general utility) can only be achieved when the defender uses the proper response for the attacker's actions. Some examples of these responses are illustrated in Fig. 7. These graphs display the proper response from the defender when a type of attack is utilized with a certain probability to have the minimum damage on the system. The red diamond at one end of the graph demonstrates the optimal probability for both players when Nash equilibrium is reached.

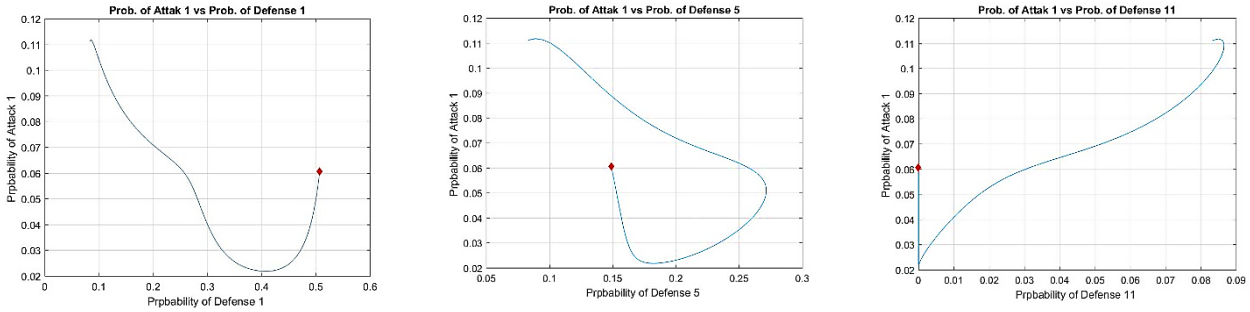

Fig 7. Probability of an attack vs. probability of a defense

The QRE is an effective method to understand the behavior of players in different circumstances, but there is a setback. This method needs a considerable amount of computation to reach the convergence point. This effort increases exponentially when the dimensions of the game increase. In reality, in a large size cyber-physical manufacturing system, there would be much more vulnerability to address, and also the defending policies available are more. Technically, some of the defensive actions that we considered for this example include several approaches that the defender can choose. In a comprehensive assessment, each of these little steps and actions should be considered separately for the defender to choose. Furthermore, every small vulnerability on the system could be seen as an opportunity for attackers to take advantage. However, this could take a long time to be solved by QRE method. On the contrary, since it is a single attempt assessment, the lengthy process could be ignored.

6. Conclusion and future works

This study demonstrates the effectiveness of applying game theory to the manufacturing domain, particularly in evaluating the trustworthiness of CPMS under cyber threats. By comparing different defense policies, game theory offers a strategic approach to managing cybersecurity, especially in environments with limited access to real-world data and where the maturity of cybersecurity measures is still developing. The proactive approach employed in this research effectively models the interaction between attackers and CPMSs, facilitating the decision-making process to identify optimal defense strategies. Three key characteristics of manufacturing systems—namely, the cost of maintaining defense mechanisms, the cost of production losses due to an attack, and the cost of recovery—were identified as fundamental elements in forming the utility function. These elements were crucial in evaluating the effectiveness of various defensive policies against cyber-attacks. The use of linear programming to calculate the optimal mixed strategy Nash equilibrium provided insights into how different defense strategies impact the overall security of the system. Although the minimum global utility indicates better security, it must be balanced against the cost of maintaining these defense strategies to ensure that the chosen approach is cost-effective for the enterprise.

The study also introduced the QRE method to predict attacker behavior, accounting for the varying levels of rationality displayed by players over time. This approach acknowledges that as attackers learn from their actions, they become more logical, requiring the defender to adapt their strategies to minimize damage effectively. The numerical case study further illustrated how the optimal strategy might differ from the one with the lowest global utility due to the influence of maintenance costs. The QRE method also highlighted the time-dependent nature of strategy optimization, showing that defenders need more time to develop effective strategies due to the complexity of their actions. The significance of the methods presented in this paper lies in their ability to provide manufacturing system managers with a reliable understanding of the potential consequences of cyber-physical threats. By enabling the evaluation of various defense strategies before any severe damage occurs, this approach enhances the resilience of manufacturing systems as they increasingly integrate cyber and physical components.

Future research should explore the implications of treating cybersecurity as a non-zero-sum game. While this study simplified the problem by assuming a zero-sum framework, the motivations of attackers and defenders are often different, and more realistic models could yield more accurate results. Additionally, since the defender's losses are not always equivalent to the attacker's gains, future studies should consider using separate utility functions for each player to provide a more nuanced analysis. Another avenue for future research is the integration of Hidden Markov Models to account for the hidden

states of the system under certain attacks. This approach could improve the model by allowing the analysis of interactions across multiple games, each representing different types of attackers. Modeling these interactions as separate but interrelated games could offer a more comprehensive understanding of the cybersecurity dynamics in CPMS.
These advancements would contribute to the development of more sophisticated and realistic cybersecurity models, ultimately enhancing the resilience of manufacturing systems against an increasingly complex threat landscape.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used OpenAI's tool Chat GPT in order to edit and write some parts of the paper. After using this service, the authors reviewed and edited the content as needed.

References

Adamson, G., Wang, L., Holm, M., & Moore, P. (2017). Cloud manufacturing–a critical review of recent development and future trends. *International Journal of Computer Integrated Manufacturing*, *30*(4–5), 347–380.

Aghakhani, S., Pourmand, P., & Zarreh, M. (2023). A Mathematical Optimization Model for the Pharmaceutical Waste Location-Routing Problem Using Genetic Algorithm and Particle Swarm Optimization. *Mathematical Problems in Engineering*, *2023*(1), 6165495.

Ait Temghart, A., Marwan, M., & Baslam, M. (2023). Stackelberg Security Game for Optimizing Cybersecurity Decisions in Cloud Computing. *Security and Communication Networks*, *2023*(1), 2811038.

Ali, S., Balushi, T. A., Nadir, Z., & Hussain, O. K. (2018). ICS/SCADA System Security for CPS. In *Cyber Security for Cyber Physical Systems* (pp. 89–113). Springer, Cham. https://doi.org/10.1007/978-3-319-75880-0_5

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74.

Bagheri, B., Yang, S., Kao, H.-A., & Lee, J. (2015). Cyber-physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment. *IFAC-PapersOnLine*, *48*(3), 1622–1627. https://doi.org/10.1016/j.ifacol.2015.06.318

Banik, S., Ramachandran, T., Bhattacharya, A., & Bopardikar, S. D. (2023). Automated Adversary-in-the-Loop Cyber-Physical Defense Planning. *ACM Transactions on Cyber-Physical Systems*, *7*(3), 1–25.

Banitaba, F. S., Aygun, S., & Najafi, M. H. (2024). Late Breaking Results: Fortifying Neural Networks: Safeguarding Against Adversarial Attacks with Stochastic Computing. *arXiv Preprint arXiv:2407.04861*.

Bouzary, H., & Chen, F. F. (2018). Service optimal selection and composition in cloud manufacturing: A comprehensive survey. *The International Journal of Advanced Manufacturing Technology*, 1–14.

Bouzary, H., & Chen, F. F. (2019). A hybrid grey wolf optimizer algorithm with evolutionary operators for optimal QoS-aware service composition and optimal selection in cloud manufacturing. *The International Journal of Advanced Manufacturing Technology*, *101*(9–12), 2771–2784.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). Challenges for securing cyber physical systems. *Workshop on Future Directions in Cyber-Physical Systems Security*, *5*. https://pdfs.semanticscholar.org/d514/97e5827cc00d9d00c26e27a769d42284cfba.pdf

Coffey, K., Maglaras, L. A., Smith, R., Janicke, H., Ferrag, M. A., Derhab, A., Mukherjee, M., Rallis, S., & Yousaf, A. (2018). Vulnerability Assessment of Cyber Security for SCADA Systems. In S. Parkinson, A. Crampton, & R. Hill (Eds.), *Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach* (pp. 59–80). Springer International Publishing. https://doi.org/10.1007/978-3-319-92624-7_3

Cook, A., Smith, R., Maglaras, L., & Janicke, H. (2016). *Measuring the risk of cyber attack in industrial control systems*.

Cyber risk in advanced manufacturing | Deloitte US. (2017). Deloitte United States. https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

DBIR: Understand Your Cybersecurity Threats. (2017). Verizon Enterprise Solutions. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

DeSmit, Z., Kulkarni, A. U., & Wernz, C. (2018). Enhancing cyber-physical security in manufacturing through game-theoretic analysis. *Cyber-Physical Systems*, *4*(4), 232–259.

Dutta, P. K. (1999). *Strategies and games: Theory and practice*. MIT press.

Fadavi, N. (2024). Dynamic Price Dispersion of Seasonal Goods in Bertrandâ€“Edgeworth Competition. *Applied Economics and Finance*, *11*(2), 14–33.

Ferrari, P., Sisinni, E., Bellagente, P., Rinaldi, S., Pasetti, M., de Sá, A. O., Machado, R. C., Carmo, L. F. da C., & Casimiro, A. (2020). Model-based stealth attack to networked control system based on real-time Ethernet. *IEEE Transactions on Industrial Electronics*, *68*(8), 7672–7683.

Gao, S., Zhang, H., Wang, Z., Huang, C., & Yan, H. (2022). Optimal injection attack strategy for cyber-physical systems under resource constraint: A game approach. *IEEE Transactions on Control of Network Systems*, *10*(2), 636–646.

Ge, Y., & Zhu, Q. (2023). Gazeta: Game-theoretic zero-trust authentication for defense against lateral movement in 5g iot networks. *IEEE Transactions on Information Forensics and Security*.

Goeree, J. K., Holt, C. A., & Palfrey, T. R. (2016). *Quantal Response Equilibrium: A Stochastic Theory of Games*. Princeton University Press.

Henze, M., Hiller, J., Hummen, R., Matzutt, R., Wehrle, K., & Ziegeldorf, J. H. (2017). Network Security and Privacy for Cyber-Physical Systems. *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, H. Song, GA Fink, and S. Jeschke (Eds.)*.

Hu, H., Liu, Y., Chen, C., Zhang, H., & Liu, Y. (2020). Optimal decision making approach for cyber security defense using evolutionary game. *IEEE Transactions on Network and Service Management*, *17*(3), 1683–1700.

Hu, Y., Zhang, H., Guo, Y., Li, T., & Ma, J. (2020). A Novel Attack-and-Defense Signaling Game for Optimal Deceptive Defense Strategy Choice. *Wireless Communications and Mobile Computing*, *2020*(1), 8850356.

J Bayuk, D Cavit, E Guerrino, J Mahony, B McDowell, & P. Staarfanger. (2011). *Malware risks and mitigation report* (BITS Financial Services Roundtable).

Jakovljevic, Z., Majstorovic, V., Stojadinovic, S., Zivkovic, S., Gligorijevic, N., & Pajic, M. (2017). Cyber-Physical Manufacturing Systems (CPMS). In V. Majstorovic & Z. Jakovljevic (Eds.), *Proceedings of 5th International Conference on Advanced Manufacturing Engineering and Technologies* (pp. 199–214). Springer International Publishing.

Joel Sobel. (n.d.). *Linear Programming Notes IX: Two-Person Zero-Sum Game Theory*. https://econweb.ucsd.edu/~jsobel/172aw02/notes9.pdf

Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022). *GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments*. 1–9.

Khalid, M. N. A., Al-Kadhimi, A. A., & Singh, M. M. (2023). Recent developments in game-theory approaches for the detection and defense against advanced persistent threats (APTs): A systematic review. *Mathematics*, *11*(6), 1353.

Knapp, E. D., & Langill, J. T. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Krishnaiyer, K., Chen, F. F., & Bouzary, H. (2018). Cloud Kanban Framework for Service Operations Management. *Procedia Manufacturing*, *17*, 531–538. https://doi.org/10.1016/j.promfg.2018.10.093

Li, X., Hu, X., & Jiang, T. (2023). Dual-Reinforcement-Learning-Based Attack Path Prediction for 5G Industrial Cyber–Physical Systems. *IEEE Internet of Things Journal*, *11*(1), 50–58.

Liu, P., Zang, W., & Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security (TISSEC)*, *8*(1), 78–118.

Liu, X. F., Shahriar, M. R., Al Sunny, S. M. N., Leu, M. C., & Hu, L. (2017). Cyber-physical manufacturing cloud: Architecture, virtualization, communication, and testbed. *Journal of Manufacturing Systems*, *43*, 352–364. https://doi.org/10.1016/j.jmsy.2017.04.004

Liu, Z., Ma, B., Xing, J., & Cao, W. (2023). Computer Security Active Defense Technology Based on Bayesian Model. *Applied Mathematics and Nonlinear Sciences*.

Lye, K., & Wing, J. M. (2005). Game strategies in network security. *International Journal of Information Security*, *4*(1–2), 71–86.

Manufacturing—Cyber Executive Briefing | Deloitte | Analysis. (2016). Deloitte Belgium. https://www2.deloitte.com/be/en/pages/risk/articles/Manufacturing.html

Miller, K. L. (2016). What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach. *FLA. BJ*, *90*, 23–23.

Nash, J. (1951). Non-cooperative games. *Annals of Mathematics*, 286–295.

Owen, G. (1995). *Game theory*. Academic Press.

Pearce, H., Pinisetty, S., Roop, P. S., Kuo, M. M., & Ukil, A. (2019). Smart I/O modules for mitigating cyber-physical attacks on industrial control systems. *IEEE Transactions on Industrial Informatics*, *16*(7), 4659–4669.

Peng, B., Liu, J., & Zeng, J. (2023). Dynamic analysis of multiplex networks with hybrid maintenance strategies. *IEEE Transactions on Information Forensics and Security*.

Peng, T., Lu, Y., Zuo, J., & Gan, J. (2021). *Research on Strategy Selection of Dynamic Defense Based on Game Theory*. 479–484.

Portilla, N. B., de Queiroz, M. H., & Cury, J. E. (2014). Integration of supervisory control with SCADA system for a flexible manufacturing cell. *Industrial Informatics (INDIN), 2014 12th IEEE International Conference On*, 261–266. http://ieeexplore.ieee.org/abstract/document/6945518/

Riel, A., Kreiner, C., Macher, G., & Messnarz, R. (2017). Integrated design for tackling safety and security challenges of smart products and digital manufacturing. *CIRP Annals*, *66*(1), 177–180. https://doi.org/10.1016/j.cirp.2017.04.037

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A survey of game theory as applied to network security. *System Sciences (HICSS), 2010 43rd Hawaii International Conference On*, 1–10. http://ieeexplore.ieee.org/abstract/document/5428673/

Sallhammar, K., Helvik, B. E., & Knapskog, S. J. (2006). Towards a stochastic model for integrated security and dependability evaluation. *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference On*, 8-pp. http://ieeexplore.ieee.org/abstract/document/1625306/

Shafae, M. S., Wells, L. J., & Purdy, G. T. (2019). Defending against product-oriented cyber-physical attacks on machining systems. *The International Journal of Advanced Manufacturing Technology*. https://doi.org/10.1007/s00170-019-03805-z

Shao, C.-W., & Li, Y.-F. (2021). Optimal defense resources allocation for power system based on bounded rationality game theory analysis. *IEEE Transactions on Power Systems*, *36*(5), 4223–4234.

Singh, S., Karimipour, H., HaddadPajouh, H., & Dehghantanha, A. (2020). Artificial Intelligence and Security of Industrial Control Systems. In K.-K. R. Choo & A. Dehghantanha (Eds.), *Handbook of Big Data Privacy* (pp. 121–164). Springer International Publishing. https://doi.org/10.1007/978-3-030-38557-6_7

Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., & Parker, R. (2017). Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects. *Journal of Manufacturing Systems*, *44*, 154–164.

Sun, G., Alpcan, T., Rubinstein, B. I., & Camtepe, S. (2023). To Act or Not To Act: An Adversarial Game for Securing Vehicle Platoons. *IEEE Transactions on Information Forensics and Security*.

Tashakkori, A., Erfanibehrouz, N., Mirshekari, S., Sodagartojgi, A., & Gupta, V. (2024). Enhancing stock market prediction accuracy with recurrent deep learning models: A case study on the CAC40 index. *World Journal of Advanced Research and Reviews*, *23*(1), 2309–2321.

Vincent, H., Wells, L., Tarazaga, P., & Camelio, J. (2015). Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. *Procedia Manufacturing*, *1*, 77–85.

Von Neumann, J., & Morgenstern, O. (1947). *Theory of games and economic behavior, 2nd rev*.

Wan, Z., Cho, J.-H., Zhu, M., Anwar, A. H., Kamhoua, C. A., & Singh, M. P. (2023). Resisting multiple advanced persistent threats via hypergame-theoretic defensive deception. *IEEE Transactions on Network and Service Management*, *20*(3), 3816–3830.

Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, *2*(2), 74–77.

Wu, M., Song, J., Lucas Lin, L. W., Aurelle, N., Liu, Y., Ding, B., Song, Z., & Moon, Y. B. (2018). Establishment of intrusion detection testbed for CyberManufacturing systems. *Procedia Manufacturing*, *26*, 1053–1064. https://doi.org/10.1016/j.promfg.2018.07.142

Wu, M., Song, Z., & Moon, Y. B. (2017). *Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods*. Journal of Intelligent Manufacturing. https://doi.org/10.1007/s10845-017-1315-5

Xu, X., Wang, G., Hu, J., & Lu, Y. (2020). Study on stochastic differential game model in network attack and defense. *Security and Communication Networks*, *2020*(1), 3417039.

Yan, B., Yao, P., Wang, J., Yang, T., Ruan, W., & Yang, Q. (2021). *Game theoretical dynamic cybersecurity defense strategy for electrical cyber physical systems*. 2392–2397.

Yang, M., & Feng, L. (2023). Optimal Defense Strategy for Data Security Based on Improving Evolutionary Game Model between Heterogeneous Groups. *Journal of Computers*, *34*(2), 141–160.

Yang, Y. M., Guo, Y., Feng, L. C., & Di, J. Y. (2011). Solving two-person zero-sum game by Matlab. *Applied Mechanics and Materials*, *50*, 262–265.

Yao, P., Hao, W., Yan, B., Yang, T., Wang, J., & Yang, Q. (2021). *Game-Theoretic Model for Optimal Cyber-Attack Defensive Decision-Making in Cyber-Physical Power Systems*. 2359–2364.

Zarreh, A., Saygin, C., Wan, H., Lee, Y., & Bracho, A. (2018a). A game theory based cybersecurity assessment model for advanced manufacturing systems. *Procedia Manufacturing*, *26*, 1255–1264.

Zarreh, A., Saygin, C., Wan, H., Lee, Y., & Bracho, A. (2018b). Cybersecurity Analysis of Smart Manufacturing System Using Game Theory Approach and Quantal Response Equilibrium. *Procedia Manufacturing*, *17*, 1001–1008.

Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Al Janahi, R. (2019a). Cyber-Security Concerns for Total Productive Maintenance in Smart Manufacturing Systems. *Procedia Manufacturing*, Accepted.

Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Al Janahi, R. (2019b). Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach. *Procedia Manufacturing*, Accepted.

Zarreh, M., Khandan, M., Goli, A., Aazami, A., & Kummer, S. (2024). Integrating Perishables into Closed-Loop Supply Chains: A Comprehensive Review. *Sustainability*, *16*(15), 6705.

Zarreh, M., Yaghoubi, S., & Bahrami, H. (2024). Pricing of drinking water under dynamic supply and demand based on government role: A game-theoretic approach. *Water Resources Management*, *38*(6), 2101–2133.

Zeltmann, S. E., Gupta, N., Tsoutsos, N. G., Maniatakos, M., Rajendran, J., & Karri, R. (2016). Manufacturing and security challenges in 3D printing. *Jom*, *68*(7), 1872–1881.

Zhang, H., Tan, J., Liu, X., Huang, S., Hu, H., & Zhang, Y. (2022). Cybersecurity threat assessment integrating qualitative differential and evolutionary games. *IEEE Transactions on Network and Service Management*, *19*(3), 3425–3437.

Zhang, L., Zhu, T., Hussain, F. K., Ye, D., & Zhou, W. (2022). A game-theoretic method for defending against advanced persistent threats in cyber systems. *IEEE Transactions on Information Forensics and Security*, *18*, 1349–1364.

Zhang, Y., Peng, Z., Wen, G., Wang, J., & Huang, T. (2023). Optimal Stealthy Linear Man-in-the-Middle Attacks With Resource Constraints on Remote State Estimation. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*.

Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. https://doi.org/10.1109/iThings/CPSCom.2011.34

Zhu, T., Ye, D., Cheng, Z., Zhou, W., & Philip, S. Y. (2022). Learning games for defending advanced persistent threats in cyber systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2410–2422.