Annals of Operations Research
https://doi.org/10.1007/s10479-023-05792-7

ORIGINAL RESEARCH

Game theory approach for secured supply chain management in effective trade management

Wei Chu[1] · Yanzhao Shi[2] · Xue Jiang[3] · Tiziana Ciano[4] · Bin Zhao[1]

Received: 15 August 2023 / Accepted: 11 December 2023

Abstract
In the current digital era, trade management faces complexities and challenges due to the expansive network of partners and traders in the e-commerce platform. Ensuring security, integrity, and trust has become crucial in this environment. The Industrial Internet of Things (IIoT) has revolutionised industries, offering enhanced productivity and service delivery. However, IIoT systems are susceptible to cybersecurity threats, jeopardising sensitive information, industrial controls, and product integrity. Applying supply chain technology has emerged as a viable solution to these challenges. It guarantees privacy and material provenance and facilitates machine-led maintenance. In this study, we propose a supply chain architecture explicitly designed for multi-factory environments, leveraging an Evolutionary Game Theory (EGT) approach. Our proposed approach introduces a fairness concept by including a subsystem that imposes taxes on supply chain nodes, promoting ethical conduct and discipline. Inspired by the ultimatum game, our solution employs a game mechanism that progressively penalises malicious actors, discourages fraudulent activities, enhances compensation systems, and reduces collusion. By adopting a game-theoretic model, we foster a sense of fairness and accountability among the participants. By leveraging the incentive structure of the supply chain, our proposed tool aims to establish a secure and trustworthy environment for industrial collaboration, addressing the critical need for increased trust among partners in industrial applications. Using the EGT approach, our supply chain architecture fosters a sustainable ecosystem wherein partners can engage in secure and reliable transactions, ensuring the integrity and trustworthiness of the entire network.

Keywords Game theory · Industrial IIoT · E-commerce · Logistics · Supply chain · Security · Networking · Secure trading

✉ Bin Zhao
zhaobin@bbc.edu.cn

1 School of Economics and Management, Bengbu University, Bengbu 233030, Anhui, China

2 Anhui Vocational College of Electronics And Information Technology, Bengbu 233030, Anhui, China

3 Semyung University Graduate School, Jecheon, Chungcheongbuk-do 27136, Korea

4 Department of Economics and Political Sciences, University of Aosta Valley, Aosta, Italy

Published online: 22 January 2024

1 Introduction

Trade management has become increasingly complex and challenging in the rapidly advancing era of digital technology and online transactions (Praveena et al., 2022; Bai et al., 2021; Vasnani et al., 2019). The widespread use of e-commerce platforms has resulted in a vast network of partners and traders, necessitating a heightened focus on security, integrity, and trust. As businesses engage in transactions across digital platforms, they face cyber threats that can compromise sensitive information and disrupt trade processes. It is crucial to address these challenges to ensure trade management systems' smooth and secure functioning (Khan et al., 2018; Kozhaya et al., 2021; Chen et al., 2023). This paper highlights the significance of trade management in the digital era and sets the stage for discussing the importance of privacy in secured supply chain management.

Privacy plays a vital role in ensuring the effectiveness of secured supply chain management. In interconnected global trade networks, it is imperative to safeguard sensitive information and prevent unauthorised access to maintain the integrity of the supply chain (Qian et al., 2021; Kilincer et al., 2021; Woods et al., 2022). Protecting the privacy of transactional data, customer details, and intellectual property is crucial for businesses to maintain their competitive advantage and safeguard their interests. However, the digital landscape presents unique challenges to privacy due to the inherent vulnerabilities of data during online transfers and the ever-present risk of data breaches. The increasing reliance on digital platforms for trade management introduces complexities and risks that must be addressed (Paul et al., 2019; Sivaraman et al., 2020; Avrachenkov et al., 2019; Ruan et al., 2016). The potential exposure of sensitive information during online transfers raises concerns about unauthorised access, data leaks, and misuse. The threat of data breaches further emphasises the importance of implementing robust privacy measures in supply chain management. Understanding the significance of privacy sets the foundation for highlighting the limitations of existing methods in adequately addressing this challenge(Cheng et al., 2016; Dai et al., 2023; Gao et al., 2021).

Existing methods often need help to keep pace with the dynamic nature of digital trade. These methods may rely on outdated or manual processes that need more agility and responsiveness in the digital era. Additionally, traditional approaches may need built-in mechanisms to ensure privacy and data security throughout the supply chain process(Guo et al., 2023). This limitation poses significant risks to trade management systems, as the potential for data leaks or breaches can lead to financial losses, reputational damage, and legal consequences. By profoundly analyzing these challenges, this article proposes a new novel approach called Game Theory Based Secured Supply Chain Architecture (GBSSCA) which involves Evolutionary Game Theory (ECT) as a solution to address these limitations (Bouhaddi et al., 2018; Jin et al., 2020; Wang et al., 2022a, 2022b).

The proposed GBSSCA approach presents a promising solution for addressing the challenges of secured supply chain management within the digital landscape. Utilising game theory principles, this approach introduces a fresh perspective of fairness and accountability to the supply chain architecture. One key aspect of the EGT approach is the implementation of a subsystem that imposes taxes on supply chain nodes. This system encourages ethical conduct and discipline among participants by incentivising them to act in the best interests of the entire supply chain ecosystem. The approach discourages malicious actors and promotes responsible behaviour by imposing taxes. Inspired by the ultimatum game, the game-theoretic model employed in the EGT approach progressively penalizes those engaging in malicious activities, thereby discouraging fraud and enhancing compensation systems

(Adami et al., 2016; Xing et al., 2020; Zheng et al., 2023; Wang et al., 2022a, 2022b). This model also reduces collusion, motivating participants to maintain a fair and transparent supply chain environment. Overall, the proposed EGT approach provides a comprehensive framework that addresses the challenges faced in secured supply chain management and establishes a system of fairness, accountability, and trust among participants (Ren et al., 2020; Douha et al., 2023). By leveraging game theory principles and introducing innovative mechanisms, this approach aims to enhance the integrity and reliability of supply chain processes in the digital landscape.

The main contributions of the paper are as follows.

- We propose a novel approach called the Game theory-based Secure Supply Chain Architecture (GBSSCA) for enhancing secured supply chain management in effective trade management.
- The proposed GBSSCA incorporates the Evolutionary Game Theory (EGT) approach to address security limitations and ensure privacy in the supply chain management process.
- The effectiveness of the proposed approach is demonstrated through rigorous experiments, validating its efficacy and efficiency.

The paper is structured as follows: Sect. 2 provides a comprehensive literature review, highlighting relevant research and studies in the field. Section 3 delves into the Proposed Evolutionary Game Theory (EGT) approach, explaining its key concepts and mechanisms. Section 4 presents the results of the experiments conducted to assess the effectiveness of the proposed approach. Finally, Sect. 5 concludes the paper by summarising the key findings, discussing their implications, and suggesting potential avenues for future research.

2 Literature Review

RLM-QRD Algorithm (Liu et al., 2021a, 2021b), the concept of Nash Equilibrium (Li et al., 2015), the Dataset of MIT (Peng et al., 2019), and the China National Vulnerability Database of Information Security (CNNVD), which are discussed briefly in Sect. 3. The paper (Zhu et al., 2021) addresses the challenges related to the selfishness of parking vehicles (PVs) and the potential threats from trustless or malicious PVs. The proposed solution introduces a reputation-based cooperative content delivery mechanism, utilising a two-layer auction game to optimise content delivery and rewards for mobile vehicles (MVs), PVs, and roadside units (RSUs). The paper (Xu et al., 2020) aims to overcome the limitations of traditional deterministic game models in accurately capturing the dynamic nature of network attack and defense strategies and external factors. It constructs a stochastic evolutionary game model using stochastic differential equations with Markov property, finding evolutionary equilibrium solutions and proving model stability.

A method (Zhang et al., 2021) presents the Pareto optimal decision vectors and solutions for the finite horizon indefinite mean-field stochastic cooperative linear-quadratic (LQ) difference game. The article establishes the equivalence between the solvability of coupled generalised difference Riccati equations (GDREs) and the solvability of the multi-objective optimisation problem. The motive of this study (Liu et al., 2021a, 2021b) is to address the limitations of conventional game models that assume ideal systems with unlimited computational resources for decision-making. The study aims to develop a new mathematical model of extensive games that incorporates bounded computational resources, allowing players only to foresee a portion of available alternatives in the future (Nasrin et al., 2022; Liu et al., 2022; Liu et al., 2023).

The article (Tian et al., 2019; Jiang et al., 2023; Jiang et al., 2022) proposes applying evolutionary game theory to model the evolution process of malicious users' attacking strategies and discusses the methodology for conducting evaluation simulations. The study (Mengibaev et al., 2020; Li et al., 2020) introduces a heterogeneous interaction mode where players can adopt different strategies for opponents. The impact of heterogeneous interaction dependency strength on privacy protection is explored through computer simulations, revealing that heterogeneous decision behavior can promote privacy protection. The study (Liu et al., 2020; Li et al., 2023; Luo et al., 2023) introduces an improved learning mechanism based on the network topology, establishes a learning object set based on the players' learning range, and incorporates the Fermi function to calculate the transition probability between learning object strategies (Shukla et al., 2022; Mo et al., 2023; Meng et al., 2020).

The paper (Shi et al., 2021; Tutar et al., 2023) introduces dynamic honeypots that adjust defense strategies based on hacker attacks, treating the confrontation between defenders and attackers as a strategic game. The goal is to improve the security of array honeypot systems by deriving evolutionarily stable strategies from the game model and analyzing the stability of strategy evolution based on the number of servers. The paper (Wang et al., 2021) aims to explore the dynamics of social payoffs and average social investments using evolutionary game theory.

The aim (Hu et al., 2020) of this research is to address the issue of overlooking strategy in cyber security defense. While various techniques exist, decision-making and optimal strategies play a significant role in the outcome of cyber-attack defense. The research utilizes a stochastic evolutionary game model with the Logit Quantal Response Dynamics (LQRD) equation, incorporating the parameter λ to quantify cognitive differences among real-world players. This study's objective (Guo et al., 2021) is to propose a dynamic defense strategy against dynamic load-altering attacks (D-LAAs) in the power grid. The study focuses on the interplay between the attacker and the defender in a multistage game, employing minimax-q learning to determine optimal strategies. The paper (Jie et al., 2019) focuses on modeling man-in-the-middle (MITM) attacks using a defender vs. multi-attacker Stackelberg game. The paper proposes an approach to compute the optimal defender strategy using a multi-double oracle algorithm.

3 Methodology

3.1 Proposed game model

3.1.1 Strategies initialization

Let us utilize the concept of (Douha et al., 2023) E-commerce trade management architecture encompasses three populations: e-commerce platform users (Population 1), manufacturers (Population 2), and attackers (Population 3). Figure 1 illustrates the structure of our E-commerce system. Population 1 comprises e-commerce platform users who engage in trade management activities for buying and selling goods and services. Population 2 represents the manufacturers who produce and supply various products to be traded on the e-commerce platform. Lastly, population 3 consists of attackers who threaten the security and integrity of the supply chain and trade management processes.

In secured supply chain management and effective trade management in the e-commerce platform, population 1 relies on the products supplied by Population 2. These products

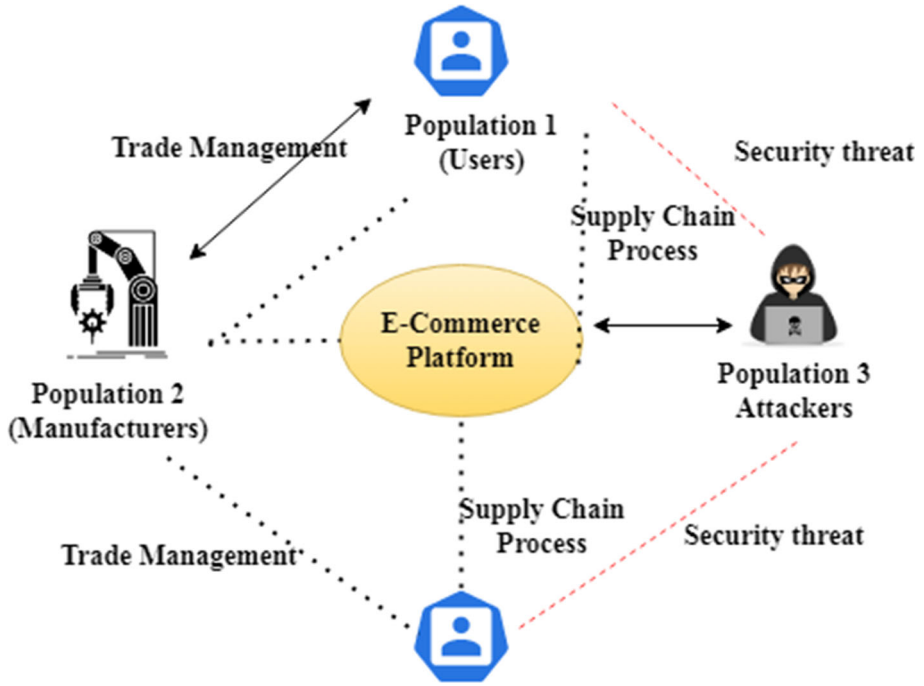

Fig. 1 E-commerce supply chain architecture

may include various items such as electronics, clothing, or consumables. However, the rise of cyberattacks and fraudulent activities in the e-commerce space necessitates a focus on ensuring the security and trustworthiness of the supply chain. To address these challenges, population 1 may invest in cybersecurity measures and adopt best practices to protect themselves and their customers from potential threats. This may involve implementing secure payment gateways, encrypting sensitive data, and enforcing stringent verification processes. By proactively enhancing cybersecurity measures, population 1 can mitigate risks and build trust among e-commerce platform users. In this proposed model, population 2 is critical as the manufacturers responsible for producing and supplying the products traded on the e-commerce platform. They need to prioritize security and integrity in their manufacturing processes, ensuring that their products are authentic, reliable, and free from vulnerabilities. By adhering to strict quality control and implementing secure supply chain practices, population 2 can contribute to a more secure and trustworthy e-commerce ecosystem. Meanwhile, population 3, the attackers, constantly threaten the secured supply chain management and effective trade management in the e-commerce platform. They may attempt malicious activities such as counterfeit product distribution, data breaches, or identity theft. Therefore, Population 1 and Population 2 must collaborate and implement robust security measures to detect and mitigate potential attacks from Population 3. By employing a system model that emphasizes secured supply chain management, the e-commerce platform can create a more secure and trustworthy environment for trade management. Through adopting advanced cybersecurity measures, stringent supply chain practices, and collaborative efforts, populations 1 and 2 can collectively minimize risks, enhance trust among users, and promote effective trade management in the e-commerce platform.

3.1.2 Proposed game model based on RLM-QRD Framework

In this section, we utilize the multistage evolutionary game model (MEGM) based on (Douha et al. 2023). MEGM is a framework in game theory that considers how multiple populations or players interact strategically across multiple stages or periods. Each population's decisions and strategies are influenced by the actions of other populations and the outcomes of previous stages. In the context of the E-commerce architecture depicted in Fig. 1, which involves e-commerce platform users (Population 1), manufacturers (Population 2), and attackers (Population 3), a multistage evolutionary game model can effectively capture the dynamic interactions and changes between these populations over time. The model enables an analysis of how the strategies and behaviors of each population evolve and affect the security and integrity of the e-commerce platform's supply chain and trade management processes.

By studying the system dynamics and assessing the effects of different strategies adopted by each population, the MEGM helps to identify optimal defense strategies, evaluate the system's vulnerability to attacks, and explore methods to enhance the security and effectiveness of supply chain management and trade practices. Considering multiple stages or periods allows for considering the populations' adaptability and facilitates the exploration of strategies that yield long-term benefits (Alipour & Bastani, 2023). Furthermore, the model captures the interdependencies between populations and their decision-making processes, which is crucial for understanding the complex dynamics of the system (Fig. 2).

Here, our proposed game model consists of Q-learning, Replication Dynamic Equations (QRD), and Reinforcement Learning Model (RLM).

The evolutionary game model based on QRD involves two main components: payoff quantification and QRD calculations (Yang et al., 2023; Xia et al., 2023). Payoff quantification

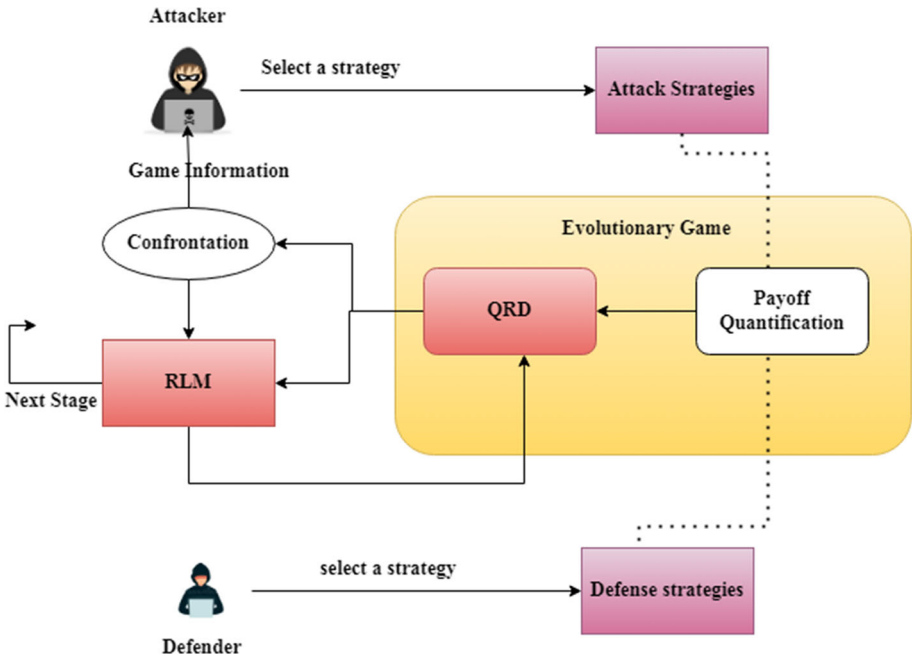

Fig. 2 Proposed EGT based on RLM-QRD

utilizes the information from the initial stage of the game to compute the revenue generated by both the attack and defense strategies in that stage. By considering the strategy revenues at the current stage, QRD calculations are performed to determine the optimal defense strategy through mathematical calculations. The RLM serves the purpose of connecting all stages of the game. It plays a crucial role in maintaining continuity and facilitating the evolution of strategies over time. The RLM utilizes the known game information to adjust the incentives or punishments associated with the attack and defense revenues in the subsequent stage. This adaptation is based on the observed outcomes and dynamics of the game. By influencing the behavior of the populations, the RLM promotes adopting strategies that yield better defense outcomes in the post stages.

3.1.3 Q-Learning

Q-Learning is a reinforcement learning method that functions as an asynchronous dynamic programming approach. It adapts the state-action values $Q_t(S', A')$ to estimate the state-action values $Q_{t+1}(S, A)$ at the next time step $(t + 1)$. The state-action value $Q_t(S, A)$ represents the expected revenue after taking action A in state S at time t.

$$Q_{t+1}(S, A) \leftarrow (1 - \delta) Q_t(S, A) + \delta(r + \gamma \max_{a'} Q_t\big(S', A'\big)) \tag{1}$$

Q-Learning updates the state-action values based on a formula using step size δ, immediate reinforcement r, and discount factor γ. Its principle is to iteratively select actions in discrete states, improving the evaluation of action quality to maximize profit and achieve the game's goal.

3.1.4 Replication dynamic equation

The replication dynamic equation for attackers and defenders in network attack and defense can be represented as.

For attackers

$$X_i'(t) = \frac{DX_i}{DT} = X_i\big[Q_{AS_i} - \bar{Q}_{AS_i}\big] \tag{2}$$

For defenders

$$Y_j'(t) = \frac{DY_j}{DT} = Y_j\big[Q_{DS_j} - \bar{Q}_{DS_j}\big] \tag{3}$$

Here, $X_i'(t)$ and $Y_j'(t)$ represent the probabilities of the attacker and defender selecting strategies AS_i and DS_j, respectively, at a given time t. Q_{AS_i} and Q_{DS_j} represent the expected revenues of the attacker's and defender's strategies, respectively. $\bar{Q}_{AS_i}$ and $\bar{Q}_{DS_j}$ represent the average revenues of the attack and defense strategy sets. The equations describe how the probabilities of strategy adoption change over time based on the differences between individual strategy revenues and average strategy revenues. The replication dynamic equation ensures the gradual adoption of strategies with better revenue, leading to the most beneficial strategy and the evolutionary stable strategy as the Nash equilibrium.

3.1.5 Payoff quantification of attack and defense strategy

Payoff quantification is crucial for analyzing the effectiveness of attack and defense strategies in achieving optimal network security defense. The attack payoff matrix AM represents the

attacker's revenue A_{ij} generated by a combination of attack AS_i and defense DS_j strategies, considering attack revenue AR and cost AC.

$$A_{ij} = Q_A(AS_i, DS_j) = AR - AC \tag{4}$$

The defense payoff matrix DM represents the defender's revenue value D_{ij} generated by the same strategy combination (AS_i, DS_j), considering defense revenue DR and cost DC. Both matrices capture the strategic outcomes for each stage, providing essential information for evaluating and selecting defense strategies.

$$D_{ij} = Q_D(AS_i, DS_j) = DR - DC \tag{5}$$

The attack payoff matrix in stage k

$$AM^k = \begin{bmatrix} A_{11}^k & A_{12}^k & \dots & A_{1m}^k \\ A_{21}^k & A_{22}^k & \dots & A_{2m}^k \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1}^k & A_{n2}^k & \dots & A_{nm}^k \end{bmatrix} \tag{6}$$

and defense payoff matrix in stage K

$$DM^k = \begin{bmatrix} D_{11}^k & D_{12}^k & \dots & D_{1m}^k \\ D_{21}^k & D_{22}^k & \dots & D_{2m}^k \\ \vdots & \vdots & \ddots & \vdots \\ D_{n1}^k & D_{n2}^k & \dots & D_{nm}^k \end{bmatrix} \tag{7}$$

are constructed similarly, incorporating the respective revenues and costs specific to that stage. These matrices enable a comprehensive analysis of the revenues generated by different attack and defense strategies, allowing for strategic decision-making in each stage of the game.

3.1.6 Q-learning replication dynamic equation

Based on the work of (Douha et al., 2023) and (Liu et al., 2021a, 2021b), the formula for the Q-Learning replicated dynamic equation was derived using Eqs. (2) and (3). This equation incorporates the Boltzmann probability distribution to represent attack and defense strategies. The Q-Learning algorithm is then introduced into the replicated dynamic equation, resulting in the QRD equation mentioned as

$$X'(t) = \frac{DX_i}{DT} = \frac{X_i\left[Q_{AS_i} - \bar{Q}_{AS}\right]}{RD} + \frac{\frac{1}{\tau}X_i \sum_{k=1}^{n} X_k ln(X_k/X_i)}{ME} \tag{8}$$

$$Y'(t) = \frac{DY_i}{DT} = \frac{Y_j\left[Q_{DS_j} - \bar{Q}_{DS}\right]}{RD} + \frac{\frac{1}{\tau}Y_j \sum_{l=1}^{m} Y_l ln(Y_l/Y_j)}{ME} \tag{9}$$

QRD strategy includes two equations: replication dynamic equation (RD) and mutation equation (ME). RD chooses the best strategy based on current information, while ME explores new strategies in unknown attack and defense scenarios, learning from errors and adjusting strategies. This approach captures the diversity and uncertainty of network attacks and defences (Douha et al., 2023). In the context of evolutionary equilibrium,

$$X'(t) = 0 \; and \; Y'(t) = 0 \tag{10}$$

when the strategies of players reach this state, it means that the rates of change of X and Y with respect to time (denoted as $X'(t)$ and $Y'(t)$ are not greater than zero. This implies that the strategies of the players have stabilized and are not changing significantly over time. In other words, they have reached a state of balance where further changes are minimal. In Eq. (10), the solution (X^*, Y^*) represents an evolutionary stable equilibrium point. This means that the strategies of the players have reached a stable state where neither player has an incentive to deviate from their current strategy. In order to achieve this stability, the τ value in the equation needs to be sufficiently large. This ensures that the selection probability of each strategy is influenced enough to maintain the equilibrium and prevent players from shifting to different strategies.

3.1.7 Reward value learning algorithm

In RLM, the incentive and punishment factors are calculated based on the reward variable Rv and the proportion of a An certain type of attack strategy Sn used in the previous stage. These factors determine the adjustment to the reward value in order to influence the attack and defense strategies in the next stage. The calculation of these factors takes into account α the defense result R from the last stage. Depending on whether the defense was successful or not, RLM modifies the reward value associated with the corresponding attack and defense strategies. This modification aims to enhance or diminish the reward value for these strategies in order to encourage or discourage their usage in the subsequent stage. By dynamically adjusting the reward values based on past performance and strategy proportions, RLM aims to optimize the selection of attack and defense strategies in future stages, ultimately improving the overall performance and effectiveness of the system.

Algorithm 1 .

Input: Revenue of strategy combination in the last stage (AM^{k01}, DM^{k01}), current stage k attack and defense strategy in the last stage (AS_i^{k01}, DS_j^{k01}), defense result if the last stage R.

Output: revenue value of each strategy combination in the current stage (AM^k, DM^k)

Step 1: Initialize Sn, An, Rv

Step 2: if $k = 1$ then

Step 3: Calculate α from the incentive and punishment factor of the reward value $\alpha = \frac{1}{2} \times Rv$

Step 4: else if $k > 1$ then

Step 5: Calculate α from the incentive and punishment factor of the reward value $\alpha = \frac{An}{Sn} \times Rv$

Step 6: end if

Step 7: if $R = 0$//The result of the last stage of defense was failure then

Step 8: $A_{ij}^k = A_{ij}^{k-1} + \alpha \; and \; D_{ij}^k = D_{ij}^{k-1} - \alpha$

Step 9: else

Step 10: $A_{ij}^k = A_{ij}^{k-1} - \alpha \; and \; D_{ij}^k = D_{ij}^{k-1} + \alpha$

Step 11: end if

Step 12: return (AM^k, DM^k)

The Algorithm 1 starts by initializing the variables Sn, An, Rv. It then calculates the value of α, which represents the adjustment factor for the strategies, based on the incentive and punishment factors of the reward value. If it is the first stage, α is set as half of the reward value Rv. For subsequent stages, α is calculated as the ratio of An to Sn multiplied by the reward value Rv. Next, the algorithm checks the defense result from the last stage R. If it is 0, indicating a failure in defense, the algorithm updates the attack and defense strategies for the current stage by adding α to the previous values of the strategies $A_{ij}^k = A_{ij}^{k-1} + \alpha$ and $D_{ij}^k = D_{ij}^{k-1} - \alpha$. On the other hand, if the defense result is non-zero, the algorithm updates the strategies by subtracting α from the previous values $A_{ij}^k = A_{ij}^{k-1} - \alpha$ and $D_{ij}^k = D_{ij}^{k-1} + \alpha$. Finally, the algorithm returns the updated revenue values of the strategy combinations for the current stage, represented as (AM^k, DM^k). This iterative process allows for the adjustment of strategies based on the previous outcomes and aims to optimize the revenue in each stage of the algorithm.

3.1.8 Optimal defense strategy selection based on RLM-QRD

In this paper, the focus is on finding the Nash equilibrium solution for a multistage evolutionary game. The authors consider the Nash equilibrium solution as a set of equilibrium solutions for each stage of the game. To achieve this, each stage of the game learns from the known game information using a reward value learning mechanism. This mechanism allows the players to update and modify the reward value associated with their defense strategy in the current stage. By incorporating the reward value learning mechanism, the players

can adapt and improve their strategies over time based on the feedback they receive. Based on the optimal defense strategy determined for each stage using the reward value learning mechanism, the paper proposes constructing a multistage optimal defense strategy set. This set comprises the collection of the optimal defense strategies identified at each stage of the game.

Algorithm 2 .

Input: Evolutionary game model based on RLM-QRD

Output: Probability set of optimal defense strategy in k-th stage Pr_D^k

Step 1: Initialize $Rg = (n, k, s, \theta, Q, \tau, \alpha)$

Step 2: for $i \leftarrow 1$ to n do

Step 3: for $j \leftarrow 1$ to m do

Calculate AM^k, DM^k from (6) and (7)

Step 4: end for

Step 5: for $k \leftarrow 1$ to t do

Step 6: for $j \leftarrow 1$ to m do

Step 7: Construct $Y^{'}(t)$ from (9)

Step 8: end for

Step 9: for $i \leftarrow 1$ to n do

Step 10: Construct $X^{'}(t)$ from (8)

Step 11: end for

Step 12: Calculate τ and Pr_D^k from (10)

Step 13: Calculate (AM^{k+1}, DM^{k+1}) from algorithm 1 (Reward value)

Step 14: output $Pr_D^k = (Y_1^k, Y_2^k \ldots . Y_m^k)$

Step 15: end for

The goal of the algorithm is to determine the probability set of the optimal defense strategy in each stage (denoted as Pr_D^k). At the beginning, the algorithm initializes the parameters including the number of players n, the current stage k a variable s, a parameter θ, and several variables Q, τ, α. Next, the algorithm enters a loop where it calculates the values of AM^k and DM^k for each player and strategy combination using Eqs. (6) and (7). This step helps to determine the players' actions and their corresponding defenses. Then, the algorithm proceeds to another loop for each stage $k$and strategy j. Within this loop, it constructs $Y'(t)$ based on an Eq. (9), which likely involves updating variables related to the players' actions. Similarly, the algorithm constructs $X'(t)$ within the stage loop for each player, based on Eq. (8). This step likely involves updating variables related to the players' defenses. After that it calculates the value of τ and the probability set of the optimal defense strategy Pr_D^k using an Eq. (10). This calculation likely takes into account the updated variables and determines

the players' optimal defense strategies. Furthermore, the algorithm calculates the values of AM^{k+1} and DM^{k+1} using Algorithm 1. Finally, the algorithm outputs the probability set of the optimal defense strategy in the kth stage Pr_D^k, which is a set of values denoted as $(Y_1^k, Y_2^k \ldots . Y_m^k)$.

4 Results and experiments

4.1 Experimental setup

In evaluating the effectiveness of the proposed GBSSCA, we leverage the attack and defense behavior databases sourced from MIT and the China National Vulnerability Database of Information Security (CNNVD) (Peng et al., 2019). The objective of this evaluation is to analyze the attack and defense atomic strategy within the context of the proposed GBSSCA. This experimental analysis centers around understanding the behaviors associated with cyber attacks and the corresponding defense mechanisms. The attack behavior database from MIT and the defense behavior database from CNNVD offer a comprehensive collection of documented attack and defense strategies, respectively. By utilizing these databases, we aim to assess the effectiveness of the GBSSCA in mitigating the identified attack strategies. Specifically, we analyze how the proposed system aligns with the observed attack behaviors and evaluate the robustness of its defense mechanisms in countering these attacks. This evaluation enables us to gauge the efficiency and reliability of the GBSSCA in securing the supply chain within the trade management system. By examining the alignment between the proposed approach and the documented attack and defense strategies, we can assess the extent to which the GBSSCA enhances the overall security and resilience of the supply chain in the face of cyber threats.

4.2 Evaluation metrics used

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall \frac{TP}{TP + FN}$$

$$F1 - score = 2 * ((Precision * Recall)/(Precision + Recall))$$

Also we evaluate the proposed GBSSCA based on the existing base line models such as Bayesian game model, EGT based on Attack and defense and QRD based EGT.

4.3 Dataset preparation and integration of attack and defense behavior databases

In this section, we discuss the crucial step of preparing the dataset for evaluation by combining the attack behavior database from MIT and the defense behavior database from CNNVD. By merging these two databases, we create a unified dataset that enables us to analyze the effectiveness of the proposed GBSSCA which is shown in Fig. 3. Each record within the dataset represents a specific behavior observed in cyber attacks and defense mechanisms.

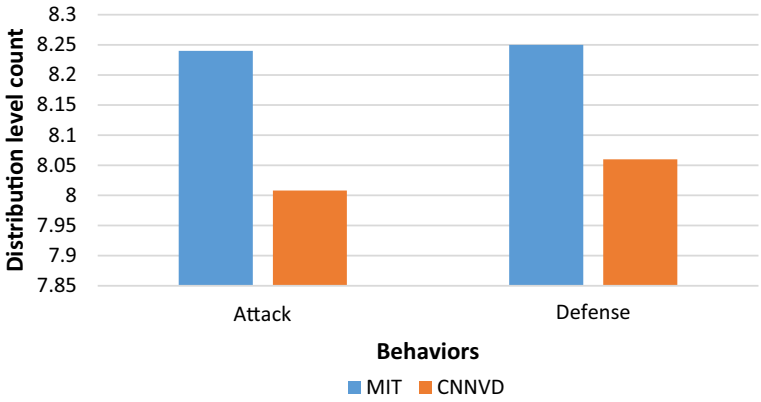

Fig. 3 Distribution of attack and defense behavior databases

This integration allows us to assess the alignment between the proposed approach and the documented attack and defense strategies, ultimately evaluating the GBSSCA's ability to enhance the overall security and resilience of the supply chain in the face of cyber threats.

4.4 Revenue values for different attack and defense strategies

The revenue outcomes associated with attack and defense strategies, denoted as AMK (Attack Strategy Revenues) and DMK (Defense Strategy Revenues), are crucial in understanding the financial prospects of various strategy pairs in our game model. By delving into these revenue figures, we obtain a nuanced picture of how profitable different combinations of attack and defense maneuvers could be. Take, for instance, a scenario where the defender opts for Defense Strategy 1 (DS1) and the attacker goes for Attack Strategy 1 (AS1); this pairing is predicted to bring in a revenue of 2. In a different combination, where Defense Strategy 2 (DS2) is employed by the defender against Attack Strategy 2 (AS2) from the attacker, the anticipated revenue remains at 2. However, a more lucrative outcome is observed when Defense Strategy 3 (DS3) and Attack Strategy 3 (AS3) are chosen by the defender and attacker, respectively, leading to an increased expected revenue of 4. Such insights into revenue values are vital for decision-makers, as they provide a financial lens to assess the effectiveness of various attack and defense strategies. This analysis not only helps in recognizing which strategy pairs are most financially beneficial but also aids in strategizing for maximum revenue generation. This information is crucial for selecting optimal defense strategies that align with network security objectives. By considering the revenue values, decision-makers can make informed choices and improve the effectiveness of their defense strategies to mitigate potential risks and achieve desired financial outcomes (Fig. 4).

4.5 Baseline comparison

The proposed GBSSCA model exhibits superior efficiency when compared to the other models. It achieves the highest accuracy of 0.89, surpassing the Bayesian model (accuracy: 0.8), the EGT-Attack and Defense model (accuracy: 0.84), and the QRD-EGT model (accuracy: 0.86). Furthermore, the precision of the proposed GBSSCA model is 0.91, outperforming the

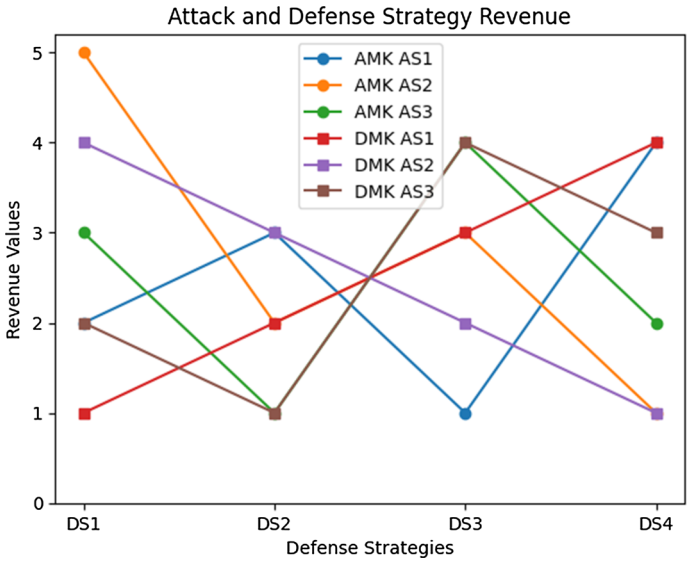

Fig. 4 Revenue values for different attack and defense strategies

Bayesian model (0.82), the EGT-Attack and Defense model (0.86), and the QRD-EGT model (0.88). This implies that the proposed GBSSCA model has a higher proportion of correctly predicted positive samples compared to the other models. Moreover, the recall of the proposed GBSSCA model is 0.96, outshining the Bayesian model (0.86), the EGT-Attack and Defense model (0.89), and the QRD-EGT model (0.91). This indicates a higher proportion of correctly predicted positive samples out of all actual positive samples for the proposed GBSSCA model. Overall, the proposed GBSSCA model demonstrates its superior efficiency by achieving higher accuracy, precision, and recall values, thus effectively identifying both attack and defense classes (Fig. 5).

4.6 Mean squared error rate (MSE)

When comparing the performance of the proposed GBSSCA model with the other models based on the Mean Squared Error (MSE) rate, the proposed GBSSCA model outperforms the other models. Its lower MSE rate indicates a smaller average squared difference between its predicted values and the actual values. This suggests that the proposed GBSSCA model provides more accurate predictions and has a better fit to the data compared to the Bayesian, EGT-Attack and Defense, and QRD based EGT models (Fig. 6).

4.7 Efficiency of proposed GBSSCA

Figure 7 illustrates the effectiveness of the proposed GBSSCA through the evaluation of revenue improvement, defense effectiveness, and stability analysis.

The revenue improvement achieved by the proposed architecture compared to baseline or existing approaches. The lines representing “Baseline Revenue” and “Proposed Revenue” show the revenue values obtained from traditional supply chain models or game theory

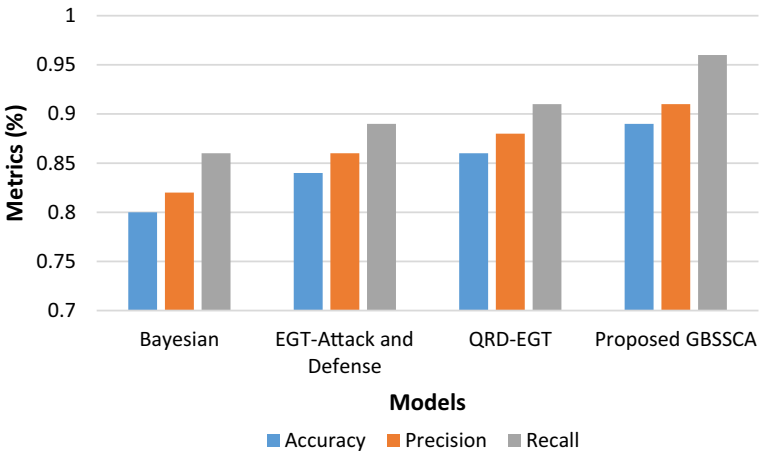

Fig. 5 Overall percentage achieved by the models

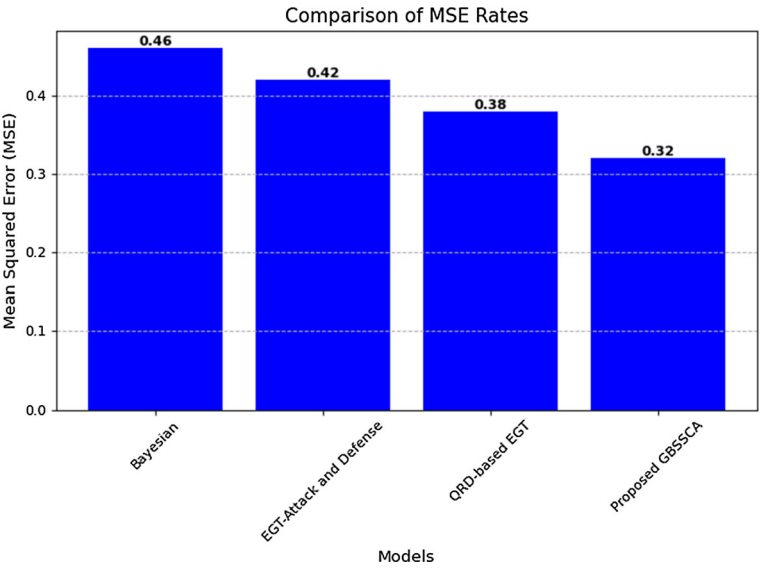

Fig. 6 Reducing error rate

approaches and the proposed GBSSCA, respectively. If the line representing "Proposed Revenue" consistently stays above the line representing "Baseline Revenue," it indicates that the proposed GBSSCA leads to higher revenue generation, indicating its effectiveness in improving the financial outcomes of the supply chain system.

Effectiveness of the defense strategies selected by the Reinforcement Learning Model (RLM) and QRD calculations. The lines labeled "Reduction in Attack Revenue" and "Increase in Defense Revenue" represent the reduction in attack revenue and the increase in defense revenue, respectively, achieved by the defense strategies employed in the proposed GBSSCA. If these lines consistently show a decreasing trend for attack revenue and an

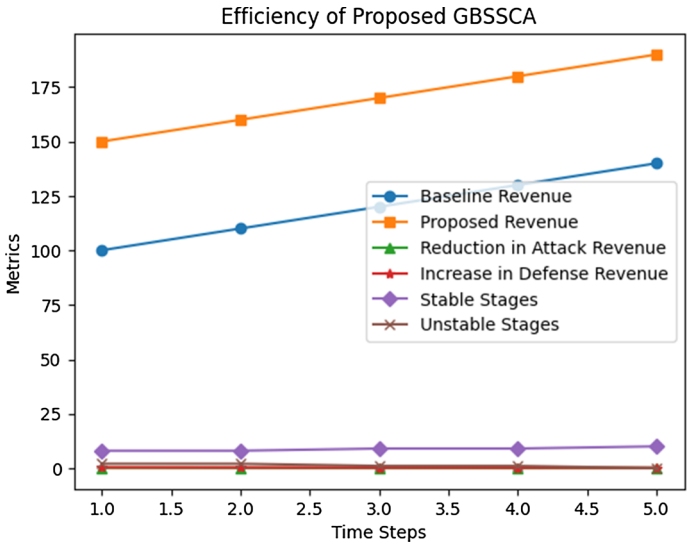

Fig. 7 Efficiency of proposed GBSSCA in terms of revenue improvement, defense effectiveness and stability analysis

increasing trend for defense revenue, it indicates that the proposed GBSSCA effectively reduces the financial losses caused by attacks and enhances the defensive capabilities of the supply chain system.

The stability of the system through the lines labeled "Stable Stages" and "Unstable Stages." These lines represent the number of stages in which the strategies reach a stable state (Nash equilibrium) (Li et al., 2015) and the number of stages in which the strategies are still unstable and undergoing significant changes. If the line for "Stable Stages" consistently shows higher values and the line for "Unstable Stages" remains close to zero, it indicates that the proposed GBSSCA is effective in maintaining a stable and equilibrium state, minimizing disruptive changes and promoting consistent performance throughout the supply chain system.

5 Conclusion

The paper explores the challenges of trade management in the digital era, focusing on the intricate networks of partners and traders in the e-commerce platform. It emphasizes the significance of security, integrity, and trust in this environment, acknowledging the vulnerability of Industrial Internet of Things (IIoT) systems to cybersecurity threats that compromise sensitive information, industrial controls, and product integrity. To tackle these challenges, the paper proposes a GBSSCA specifically tailored for multi-factory environments, leveraging an Evolutionary Game Theory (EGT) approach. The architecture aims to ensure privacy, material provenance, and enable machine-led maintenance. A key component is the introduction of a fairness concept through a subsystem that imposes taxes on supply chain nodes, fostering ethical conduct and discipline among participants. Drawing inspiration from the ultimatum game, the proposed solution employs a game mechanism to progressively penalize malicious actors, discourage fraudulent activities, enhance compensation systems, and

reduce collusion. By integrating a game-theoretic model, the paper strives to cultivate fairness and accountability among supply chain participants. The proposed tool capitalizes on the incentive structure of the supply chain to establish a secure and trustworthy environment for industrial collaboration, addressing the pressing need for increased trust among partners in industrial applications.

Author contributions WC: Conceptualization, Methodology, Formal analysis, Supervision, Writing—original draft, Writing—review & editing. YS: Writing—original draft, Writing—review & editing. XJ: Investigation, Data Curation, Validation, Resources, Writing—review & editing. TC: Project administration, Investigation, Writing—review & editing. BZ: Software, Visualization, Writing—original draft.

Funding This research was financially supported by the following agencies: 1. Support plan of excellent young talents from colleges and universities (gxyq2021029) 2. Project of Jianghuai Craftsmen E-commerce Talents Training (WJ-RCPY- 021) 3. Anhui Provincial Quality Engineering Project: "Mr. Shi Yanzhao Skills Master Studio"(2022jnds003) 4. Anhui provincial quality engineering project of "University and Enterprise Cooperation Practice Education Base between Bengbu University and Bengbu Aote Carton Machinery Co., Ltd. (2023xqhz035).

Data availability The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare that they have no competing interests.

Ethical approval Not applicable.

Consent for publication Not applicable.

References

Adami, C., Schossau, J., & Hintze, A. (2016). Evolutionary game theory using agent-based methods. *Physics of Life Reviews, 19*, 1–26.

Alipour, P., & Bastani, A. F. (2023). Value-at-Risk-Based Portfolio Insurance: Performance Evaluation and Benchmarking Against CPPI in a Markov-Modulated Regime-Switching Market. arXiv preprint https://arxiv.org/abs/2305.12539.

Avrachenkov, K., Huang, L., Marden, R. J., Coupechoux, M., & Giovanidis, A. (2019). Game theory for networks. In *Proceedings of the 8th International EAI Conference, GameNets 2019* (Vol. 277).

Bai, Y., Fan, K., Zhang, K., Cheng, X., Li, H., & Yang, Y. (2021). Blockchain-based trust management for agricultural green supply: A game theoretic approach. *Journal of Cleaner Production, 310*, 127407.

Bouhaddi, M., Radjef, M. S., & Adi, K. (2018). An efficient intrusion detection in resource-constrained mobile ad-hoc networks. *Computers & Security*, *76*, 156–177.

Chen, W., Wang, B., Chen, Y., Zhang, J., & Xiao, Y. (2023). New exploration of creativity: Cross-validation analysis of the factors influencing multiteam digital creativity in the transition phase. *Frontiers in Psychology, 14*, 1102085.

Cheng, B., Zhu, D., Zhao, S., & Chen, J. (2016). Situation-Aware IoT service coordination using the event-driven SOA paradigm. *IEEE Transactions on Network and Service Management, 13*(2), 349–361.

Dai, X., Xiao, Z., Jiang, H., Alazab, M., Lui, J. C. S., Dustdar, S., & Liu, J. (2023). Task co-offloading for D2D-assisted mobile edge computing in industrial internet of things. *IEEE Transactions on Industrial Informatics, 19*(1), 480–490.

Douha, N. G. Y. R., Sasabe, M., Taenaka, Y., & Kadobayashi, Y. (2023). An evolutionary game theoretic analysis of cybersecurity investment strategies for smart-home users against cyberattacks. *Applied Sciences, 13*(7), 4645.

Gao, H., Shi, D., & Zhao, B. (2021). Does good luck make people overconfident? Evidence from a natural experiment in the stock market. *Journal of corporate finance (Amsterdam, Netherlands), 68*, 101933.

Guo, Y., Wang, L., Liu, Z., & Shen, Y. (2021). Reinforcement-learning-based dynamic defense strategy of multistage game against dynamic load altering Attack. *International Journal of Electrical Power & Energy Systems*, *131*, 107113.

Guo, Y., Zhang, C., Wang, C., & Jia, X. (2023). Towards public verifiable and forward-privacy encrypted search by using blockchain. *IEEE Transactions on Dependable and Secure Computing, 20*(3), 2111–2126.

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.

Jiang, Z., & Xu, C. (2023). Disrupting the Technology Innovation Efficiency of Manufacturing Enterprises through Digital Technology Promotion: An evidence of 5G technology construction in China. *IEEE Transactions on Engineering Management*.

Jiang, H., Xiao, Z., Li, Z., Xu, J., Zeng, F., & Wang, D. (2022). An energy-efficient Framework for internet of things underlaying heterogeneous small cell networks. *IEEE Transactions on Mobile Computing*, *21*(1), 31–43.

Jie, Y., Choo, K. K. R., Li, M., Chen, L., & Guo, C. (2019). Tradeoff gain and loss optimization against man-in-the-middle Attacks based on game theoretic model. *Future Generation Computer Systems*, *101*, 169–179.

Jin, H., Zhang, H., Zhang, C., & Hu, H. (2020). Research on active defense decision-making method based on qrd in complex network. *Netinfo Security*, *20*(5), 72–82.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks, 188*, 107840.

Kozhaya, D., Decouchant, J., Rahli, V., & Esteves-Verissimo, P. (2021). Pistis: An event-triggered real-time byzantine-resilient protocol suite. *IEEE Transactions on Parallel and Distributed Systems*, *32*(9), 2277–2290.

Li, J., Kendall, G., & John, R. (2015). Computing nash equilibria and evolutionarily stable states of evolutionary games. *IEEE Transactions on Evolutionary Computation, 20*(3), 460–469.

Li, Q., Lin, H., Tan, X., & Du, S. (2020). Consensus for multiagent-based supply chain systems under switching topology and uncertain demands. *IEEE Transactions on Systems Man and Cybernetics: Systems, 50*(12), 4905–4918.

Li, J., Yang, X., Shi, V., & Cai, G. G. (2023). Partial centralization in a durable-good supply chain. *Production and Operations Management*, *32*(9), 2775–2787.

Liu, X., Zhang, H., Zhang, Y., & Shao, L. (2020). Optimal network defense strategy selection method based on evolutionary network game. *Security Communication Networks*. https://doi.org/10.1155/2020/5381495

Liu, Y., Chen, H., Zhang, H., & Liu, X. (2021). Defense strategy selection model based on multistage evolutionary game theory. *Security and Communication Networks, 2021*, 1–15.

Liu, C., Zhu, E., Zhang, Q., & Wei, X. (2021b). Exploring the effects of computational costs in extensive games via modeling and simulation. *International Journal of Intelligent Systems*, *36*(8), 4065–4087.

Liu, C., Wu, T., Li, Z., Ma, T., & Huang, J. (2022). Robust online Tensor Completion for IoT Streaming Data Recovery. *IEEE Transactions on Neural Networks and Learning Systems., 34*(12), 10178–10192.

Liu, X., Wang, S., Lu, S., Yin, Z., Li, X., Yin, L., & Zheng, W. (2023). Adapting feature selection algorithms for the classification of Chinese texts. *Systems*, *11*(9), 483.

Luo, J., Zhuo, W., & Xu, B. (2023). *The bigger, the better? Optimal NGO size of human resources and governance quality of entrepreneurship in circular economy*. Management Decision.

Meng, Y. (2020). The development trend of labor standards and China's participation into the reconstruction of labor standards in international trade agreements. *Journal of Chinese Human Resources Management, 11*(2), 30–36.

Mengibaev, U., Jia, X., & Ma, Y. (2020). The impact of interactive dependence on privacy protection behavior based on evolutionary game. *Applied Mathematics and Computation, 379*, 125231.

Mo, J., & Yang, H. (2023). Sampled value attack detection for busbar differential protection based on a negative selection immune system. *Journal of Modern Power Systems and Clean Energy, 11*(2), 421–433.

Nasrin, S., Shylendra, A., Darabi, N., Tulabandhula, T., Gomes, W., Chakrabarty, A., & Trivedi, A. R. (2022). Enos: Energy-aware network operator search in deep neural networks. *Ieee Access : Practical Innovations, Open Solutions*, *10*, 81447–81457.

Paul, J. A., & Wang, X. J. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, *122*, 113069.

Peng, J., Guo, M., & Quan, J. (2019). Software vulnerability and application security risk. *Information Resources Management Journal (IRMJ)*, *32*(1), 48–57.

Praveena, S., & Devi, S. P. (2022). A survey on fuzzy based game theory approaches for supply chain uncertainties in E-Commerce applications. *Materials Today: Proceedings, 62*, 4862–4868.
Qian, W., Lai, H., Zhu, Q., & Chang, K. C. (2021). Overview of network security situation awareness based on big data. In *Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2021* (pp. 875–883). Springer International Publishing.
Ren, H., Huang, H., Li, Q., Wu, Q., & Yang, Y. (2020). Operation optimization of multi-participants in a regional energy system based on evolutionary game theory. *Energy Reports*, *6*, 1041–1045.
Ruan, N., Gao, L., Zhu, H., Jia, W., Li, X., & Hu, Q. (2016). Toward optimal dos-resistant authentication in crowdsensing networks via evolutionary game. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)* (pp. 364–373). IEEE.
Shi, L., Wang, X., & Hou, H. (2021). Research on optimization of array honeypot defense strategies based on evolutionary game theory. *Mathematics, 9*(8), 805.
Shukla, P., Nasrin, S., Darabi, N., Gomes, W., & Trivedi, A. R. (2022). MC-CIM: Compute-in-memory with monte-carlo dropouts for bayesian edge intelligence. *IEEE Transactions on Circuits and Systems I: Regular Papers, 70*(2), 884–896.
Sivaraman, V., & Sikdar, B. (2020). A game-theoretic approach for enhancing data privacy in sdn-based smart grids. *IEEE Internet of Things Journal*, *8*(13), 10583–10595.
Tian, Z., Gao, X., Su, S., Qiu, J., Du, X., & Guizani, M. (2019). Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory. *IEEE Transactions on Vehicular Technology*, *68*(6), 5971–5980.
Tutar, H., Nam, S., & GüLer, S. (2023). Development of sustainable human resources in the period 2000–2021: A bibliometric review. *Journal of Chinese Human Resources Management, 14*(1), 117–139.
Vasnani, N. N., Chua, F. L. S., Ocampo, L. A., & Pacio, L. B. M. (2019). Game theory in supply chain management: Current trends and applications. *International Journal of Applied Decision Sciences*, *12*(1), 56–97.
Wang, Z., Li, C., Jin, X., Ding, H., Cui, G., & Yu, L. (2021). Evolutionary dynamics of the interdependent security games on complex network. *Applied Mathematics and Computation, 399*, 126051.
Wang, G., Chao, Y., Cao, Y., Jiang, T., Han, W., & Chen, Z. (2022). A comprehensive review of research works based on evolutionary game theory for sustainable energy development. *Energy Reports*, *8*, 114–136.
Wang, G., Chao, Y., Cao, Y., Jiang, T., Han, W., & Chen, Z. (2022b). A comprehensive review of research works based on evolutionary game theory for sustainable energy development. *Energy Reports*, *8*, 114–136.
Woods, D., Abdallah, M., Bagchi, S., Sundaram, S., & Cason, T. (2022). Network defense and behavioral biases: An experimental study. *Experimental Economics*, *25*(1), 254–286.
Xia, Y., Ding, L., & Tang, Z. (2023). Interaction effects of multiple input parameters on the integrity of safety instrumented systems with the k-out-of-n redundancy arrangement under uncertainties. *Quality and Reliability Engineering International*, *39*(6), 2515–2536.
Xing, X. H., Hu, Z. H., Wang, S. W., & Luo, W. P. (2020). An evolutionary game model to study manufacturers and logistics companies' behavior strategies for information transparency in cold chains. *Mathematical Problems in Engineering*. https://doi.org/10.1155/2020/7989386
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*, pp.1–15.
Xu, Y., Chen, H., Wang, Z., Yin, J., Shen, Q., Wang, D., & Hu, X. (2023). Multi-Factor Sequential Re-Ranking with Perception-Aware Diversification. Paper presented at the KDD '23, New York, NY.
Yang, H., Chen, C., Ni, J., & Karekal, S. (2023). A hyperspectral evaluation approach for quantifying salt-induced weathering of sandstone. *Science of The Total Environment, 885*, 163886.
Zhang, W., & Peng, C. (2021). Indefinite mean-field stochastic cooperative linear-quadratic dynamic difference game with its application to the network security model. *IEEE Transactions on Cybernetics, 52*(11), 11805–11818.
Zheng, Y., Xu, Y., & Qiu, Z. (2023). Blockchain traceability adoption in agricultural supply chain coordination: An evolutionary game analysis. *Agriculture, 131*(1), 184.
Zhu, Z., Xu, Y., & Su, Z. (2021). A reputation-based cooperative content delivery with parking vehicles in vehicular ad-hoc networks. *Peer-to-Peer Networking and Applications, 14*, 1531–1547.