Research Article

Applications of Game Theory and Advanced Machine Learning Methods for Adaptive Cyberdefense Strategies in the Digital Music Industry

Jing Jing

Music Teaching Department, Zhengzhou Preschool Education College, Zhengzhou 450000, China

Correspondence should be addressed to Jing Jing; jing_jing26e@126.com

Received 3 May 2022; Revised 17 May 2022; Accepted 24 May 2022; Published 17 June 2022

1. Introduction

As the cyberspace landscape evolves rapidly, a dynamic framework emerges in which very delicate balances are observed to make optimal decisions. The asset, information, and data values that modern organizations must manage constantly increase. New cyber-attack techniques are continually developing while existing technological defense systems age, making active defense strategies resilient. Furthermore, economic changes, institutional reorganizations, consumer trends, and legal and regulatory compliance requirements all impact decision-making and the overall development of sound defense strategies for an organization or company. To maintain its competitive advantage, the organization in question will need to continuously improve its defense strategies, which will be based on ongoing knowledge and utilization of the cyber threat landscape [1]. An accurate inventory of all assets classified by their value to the organization is critical in assessing the severity of the risks they face and, as a result, the decisions that must be made about them.

Game theory [2] can be used in cybersecurity to create tangible solutions that will allow the maximum utilization of existing strategies and optimize them to create a robust and long-term security environment at the organization level [3–5]. Using game theory principles, cyber security professionals can implement a network of controls that specialize and, as a result, reduce the risk to their valuable assets. They can also apply areas with a low level of risk, maximizing their return on investment. As a result, using specialized scenarios based on game theory, it is possible to predict the attackers’ strategy at each stage of the attack cycle, assisting in developing intelligent models to improve cyber security and the development of new intelligent systems to deter attackers.

This study presents applications of game theory and advanced machine learning methods for adaptive cyber defense strategies in the digital music industry. An
innovative application of a repetitive game methodology for cyber-attack analysis is proposed; using Bayesian inference [6], the next steps in the game can be predicted so that the best cyber defense strategies can be implemented to shield an organization from cyber-attacks.

2. Literature Review

The literature on game theory for adaptive cyber defense approaches is extensive, whether at the network level, where we must deal with massive amounts of raw data or at the strategy level.

In 2015, Laszka et al. [7] developed a strategy for reducing spear-phishing assaults by targeted per-user filtering criteria. They framed the task of screening harmful e-mails, both targeted and untargeted, as a security game. These defined optimum filtering techniques and demonstrated how they might be computed in practice. They put their theoretical hypotheses to the test by comparing them to two datasets taken from the actual world. Using two different sets of real data, they demonstrated that the recommended baselines result in less harm than the nonstrategic restrictions. In addition, they found that the improvement over nonstrategic criteria was more substantial for the comprehensive information. This improvement was unaffected by an increase in the number of targeted customers. This indicated that their technique scaled effectively, both analytically and in terms of how well it performed.

Schlenker et al. [8] explored the critical issue of allocating cyber alarms to a restricted number of professionals in cyber security activities. They proposed the cyber-alert allocation game to investigate this issue and demonstrated how to compute the defender’s best options. They offered a unique technique for addressing implement ability concerns in determining the defender’s best marginal tactic to resolve this game. Finally, they presented heuristics for solving big games like the one described and an objective assessment of the suggested framework and solution methods.

Nguyen et al. [9] conducted a study of deep reinforcement learning (DRL) techniques used in cyber protection. They discussed various critical topics, such as DRL-based security approaches for cyber-physical infrastructure, independent intrusion detection approaches, and multiagent DRL-based game theory simulations for cyber-attack defensive tactics. Additionally, extensive debates and potential study paths on cyber security focusing on DRLs are provided. They hoped that this exhaustive assessment would provide the groundwork for and support future research into the ability to develop DRL to address more sophisticated digital privacy concerns.

Alpcan and Basar [10], in 2010, in their book, about network security and game theoretic approaches, aimed to present a theoretical foundation for making resource allocation decisions that balance available capabilities and perceived security risks in a principled manner. They focused on analytical models based on game, information, communication, optimization, decision, and control theories applied to diverse security topics. At the same time, connections between theoretical models and real-world security problems are highlighted to establish the critical feedback loop between theory and practice.

Hemberg et al. [11] presented an architecture for adversarial AI called RIVALS that abstractly replicated the hostile, competing for a coevolutionary mechanism in security contexts. The purpose was to develop a system capable of pro-active cyber security against dynamic automated attackers. They reviewed its present uses and how it is used to develop defensive measures. Further work will involve expanding it to enable more cyber defense purposes, creating more effective or genuine reality methods, and applying other Nash equilibrium-finding algorithms to other cyber security challenges with established Nash equilibria [12] and analyzing efficiency.

3. Proposed Game Strategy

Many cyber-attacks follow a pattern built on repeating tactics or procedures over time. Infrastructure vulnerability control strategies, for example, can compete with current defensive systems and change their applications over time. In this sense, attackers and defenders engage regularly, and these interactions may be depicted using repetitive games, which are a type of dynamic game [13]. The concept described here is using a repeated game to evaluate cyber-attacks and simulating some cooperative behaviors without a clear endpoint. A repetitive game begins with a static game repeated infinitely or intermittently many times. A reward is given to each player who completes a specific action in this strategic stage game. The sum of each player’s gains throughout the game constitutes their final reward. In addition, Bayesian inference [14] can predict the next steps in the game to produce the appropriate countermeasures and implement the best cyber defense strategies that govern a complex system with high uncertainty [15].

The starting point for modeling the proposed system is a static game of the following format:

$$\Gamma = \{N, (X_i, u_i)_{i \in N}\},$$

(1)

where \(N = \{1, 2, \ldots, n\}\) is the set of players, \(X_i\) is the set of the player’s pure strategies, and \(u_i\) is its performance function. Assume that this stage game is repeated \(T\) times, where \(T\) is finite or infinite. Each repetition takes place over a period. A typical time (or stage) is denoted by \(i\), where \(i = 1, 2, \ldots, T\). The interaction evolves as follows [16, 17]:

(1) In period 1, players simultaneously select actions, which we symbolize as \(x^1 = (x^1_1, x^1_2, \ldots, x^1_n)\), where the pointer symbolizes the player and the exponent symbolizes the stage (time period). The action \(x^1_i\) belongs to the set \(X_i, i \in N\). Each player has been informed afterward of the choices of the other players. The performance of player \(i\) in this period is

$$u_i(x^1), \quad i \in N. \quad (2)$$

(2) In period 2, players choose at the same time actions \(x^2 = (x^2_1, x^2_2, \ldots, x^2_n)\). Each player has been informed
afterward of the choices of the other players. Player’s

\[ u_i(x^t), \quad i \in N. \quad (3) \]

(3) In period \( T \), players choose actions
\[ x^T = (x_1^T, x_2^T, \ldots, x_n^T). \] The player’s odds are
\[ u_i(x^T), \quad i \in N. \quad (4) \]

(4) If \( T \) is finite, the interaction is complete (at the end of period \( T \)). Otherwise, the game continues in perpetuity.

In the repetitive game, we suggest each player earns a sequence of payoffs (one payoff for each period). This yield sequence is assumed to be valued using the discounted sum of the sequence terms. The term discount expresses the individual [18]. The closer \( \delta \) is to 0, the less the individual values a future versus a present performance. In other words, the smaller the \( \delta \) is, the less the person is interested in the future or the more impatient he is. Conversely, the higher the \( \delta \) (the closer it is to 1) is, the more a person values a future performance or is more patient [19–21].

Let a finite terminal story \( h^f = (x^1, x^2, \ldots, x^T) \). If the discount rate of player \( i \) is given by the parameter \( \delta_i \in (0,1) \), then the discounted sum of the payoffs of player \( i \) is
\[
V_i \equiv u_i(x^1) + \delta_i u_i(x^2) + \delta_i^2 u_i(x^3) + \cdots + \delta_i^{T-1} u_i(x^T) = \sum_{t=1}^{T} \delta_i^{t-1} u_i(x^t). \quad (5)
\]

Let now an infinite terminal story \( h^\infty = (x^1, x^2, \ldots) \). In this case, the discounted sum of player’s payoffs is
\[
V_i \equiv u_i(x^1) + \delta_i u_i(x^2) + \delta_i^2 u_i(x^3) + \cdots + \sum_{t=1}^{\infty} \delta_i^{t-1} u_i(x^t). \quad (6)
\]

In the case of infinity \( T \), instead of the discounted sum of the odds, we use the discounted average of the player’s odds as a valuation function:
\[
u_i^t = u_i(x^t), \quad t = 1, 2, \ldots \quad (7)
\]

Based on the relation, player \( i \) obtains the sequence of odds \( (u_1^t, u_2^t, \ldots) \). We define a number \( c \) such that \( t \) is indifferent between the series of yields \( (u_1^t, u_2^t, \ldots) \) and the sequence \((c, c_1, \ldots, c_n)\). So, we take the following relation [22]:
\[
V_i = \sum_{t=1}^{\infty} \delta_i^{t-1} u_i^t = \sum_{t=1}^{\infty} \delta_i^{t-1} c. \quad (8)
\]

However, it is true that
\[
\sum_{t=1}^{\infty} \delta_i^{t-1} c = \frac{c}{1 - \delta_i}. \quad (9)
\]

Consequently, we have
\[
V_i = \sum_{t=1}^{\infty} \delta_i^{t-1} u_i^t = \frac{c}{1 - \delta_i} \quad (10)
\]

so that
\[
(1 - \delta_i)V_i = (1 - \delta_i) \sum_{t=1}^{\infty} \delta_i^{t-1} u_i^t = c. \quad (11)
\]

The term \((1 - \delta_i)V_i\) is the discounted average of the yield sequence \((u_1^t, u_2^t, \ldots)\). The functions \( V_i \) and \((1 - \delta_i)V_i\) express the same preferences since one is a positive monotonic transformation. Thus, the set of all terminal histories is the set of all sequences [3, 23]:
\[
h^\infty = (x^1, x^2, \ldots). \quad (12)
\]

So, player \( i \) evaluates the terminal history \( h^\infty \) based on the function:
\[
V_i = \sum_{t=1}^{\infty} \delta_i^{t-1} u_i(x^t), \quad (13)
\]

or it is equivalent:
\[
(1 - \delta_i)V_i = (1 - \delta_i) \sum_{t=1}^{\infty} \delta_i^{t-1} u_i(x^t). \quad (14)
\]

So, we have the repetitive game \( G^\infty(\delta) \).

A rule that dictates the player’s behavior in response to any and all scenarios is an example of a strategy. Consequently, a single-player strategy is a guideline for picking actions at each stage (repetition) of the stage game as a function of previous decisions when playing a game that features observable actions and is repetitive. To be more exact, the energy that the player will pick at each narrative stage is determined by the strategy used in a game with just one player and repeated steps. The action must be feasible; that is, it must belong to all the available options of the gaming stage [24, 25].

Odds pairs corresponding to the four pairs of clear strategies are feasible (in the sense that there are strategies that generate specific returns). It should also be noted that all convex combinations of two or more yield pairs of pure methods constitute achievable yields (using mixed strategies) [5, 26].

In general, the total possible odds of the stage game are given by the quadrilateral in Figure 1, which has as vertices the four pairs of payoffs corresponding to the clear strategies described by the set \{(5, 5), (0, 6), (6, 0), (1,1)}.
4. Application Testing

In order to model the proposed system, a specialized threat scenario was implemented with an application study in the music industry. This was done because the large number of visitors combined with the enormous amounts of music content spent on a daily basis creates a new landscape of threats, in which the clear strategies for cybersecurity need to be rearranged on an ongoing basis. According to this logic, they frequently employ advanced techniques, including zero-day attacks, to launch attacks on music streaming platforms that modern cybercriminals have targeted [24, 27, 28].

For the implementation of the proposed system, we consider a static game \( \Gamma = \{N, (X_i, u_i)_{i \in N}\} \), such that

1. \( (u^*_1, u^*_2, \ldots, u^*_n) \) is the payoff vector of a Nash equilibrium of \( \Gamma \) (the Nash equilibrium is a solution technique for non-cooperative games with two or more participants in game theory. We assume that each player is aware of the equilibrium strategies that the other players would employ and that no player stands to gain by simply changing his strategy [2] if each participant has decided on a strategy and no one has the option of modifying their strategy. On the contrary, the other players maintain their strategy constant; their set of plans and results are the Nash equilibrium.

2. \( (\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n) \) is a vector of possible returns of \( \Gamma \) such that \( \bar{v}_i > u^*_i \) for each \( i \).

3. The discount rate \( \delta \) is quite large.

Then, there is a perfect subgame balance for the game \( G^{\text{so}}(\delta) \) with average odds \( (\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n) \).

To prove the above scenario, we will assume that the vector \( (\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n) \) can be achieved through a vector of pure strategies \( \bar{x} = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) \). That is, \( u_i(\bar{x}) = \bar{u}_i, i \in N \). It should be noted that it is not necessary to assume clean strategies. If this is not the case, vector \( V \) is achieved through mixed strategies [5, 10].

Suppose that the equilibrium returns \( (u^*_1, u^*_2, \ldots, u^*_n) \) of \( \Gamma \) are derived from the strategy vector \( (x^*_1, x^*_2, \ldots, x^*_n) \).

We consider the following firing strategy:

1. Stage \( i = 1 \):
   (a) player \( i \) selects an action \( \bar{x}_i \)

2. Stage \( i > 1 \):
   (a) If the result in the previous stages 1, 2, ..., \( t-1 \) is \( \bar{x} \), player \( i \) selects an action \( \bar{x}_i \)
   (b) In all other cases, player \( i \) selects an action \( x^*_i \)

We will examine the players’ motivations for adopting or not the above strategy.

Let us look at player \( i \) if all other players adopt the firing strategy. We must determine the optimal response of \( i \) in each period where it has observed a result \( \bar{x} \) and its optimal response in each period where it has observed a result different from \( \bar{x} \).

It should be recorded the actions that \( i \) will take if it observes in a period \( t \) that in the previous period \( t-1 \) a result other than \( \bar{x} \) was outcome. Player \( i \) knows that, in period \( t \), the other players will choose the actions \( x^*_i \), and that this will be done in perpetuity (because they follow the firing strategy). Therefore, the optimal reaction of \( i \) is to choose \( x^*_i \) in perpetuity.

Let us now see what player \( i \) will do in those periods for which history contains only the result \( \bar{x} \). Suppose that, in some of them, \( i \) chooses to deviate from the energy \( \bar{x}_i \). The optimal deviation, which we denote by \( x^*_d, d \) is, what solves the problem.

In particular,

\[
\max_{\bar{x}_i} u_i(x_i, \bar{x}_{-i}).
\]

The yield of \( i \) during the deviation period is

\[
u^*_d \equiv u_i(x^*_d, \bar{x}_{-i}),
\]

where it is true that

\[
u^*_d \geq \bar{u}_i.
\]

From the next period, the other players will start choosing \( x^*_e \) after noticing the choice \( x^*_d \) of \( i \). The punishment period of \( i \) will therefore begin. Given this, the optimal response of \( i \) is to select the energy \( x^*_e \). Thus, from the period following the deviation to perpetuity, \( i \) will have a payoff of \( u^*_i \) per period. Its average discounted return from the breach is, therefore,

\[
(1 - \delta)(u^*_d + \delta u^*_e + \delta^2 u^*_e + \ldots) = (1 - \delta)u^*_d + \delta u^*_e.
\]

If, on the contrary, \( i \), after each story that contains only \( \bar{x} \), chooses the action \( \bar{x}_i \); its return will be \( \bar{u}_i \) because after such a story, the other players choose \( \bar{x}_{-i} \). For each of the following periods, the same result will be repeated, and \( i \) will continuously gain \( \bar{u}_i \) per period. The average payoff of \( i \) in this case is

\[
(1 - \delta)(\bar{u}_i + \delta \bar{u}_i + \delta^2 \bar{u}_i + \ldots) = (1 - \delta) \frac{1}{1 - \delta} \bar{u}_i = \bar{u}_i.
\]

Therefore, player \( i \) will select \( \bar{x}_i \) after each story that contains only \( \bar{x} \), if
\[ \tilde{u}_i \geq (1 - \delta)u_i^d + \delta u_i^* \iff \delta(u_i^d - u_i^*) \geq u_i^d - \tilde{u}_i. \]  

(20)

If the following inequality relations are valid,

\[ u_i^d \geq \tilde{u}_i > u_i^* , \]  

(21)

so it applies

\[ \delta \geq \frac{u_i^d - \tilde{u}_i}{u_i^d - u_i^*}. \]  

(22)

And so

\[ \frac{u_i^d - \tilde{u}_i}{u_i^d - u_i^*} \leq 1. \]  

(23)

The possible payoffs that exceed the Nash payoffs are shown in Figure 2.

Next, to determine which value can best estimate the random variable, we apply Bayesian inference to create a loss function, which will measure how wrong the estimate is, that is, how different the estimation of the parameter is from its actual price. This means that the goal is for the value of the estimate to minimize the loss function. For example, in the absolute error loss function, underestimation and overestimation of the parameter are punished in the same way, depending on the deviation of the estimate. In contrast to the preceding statement, the linear loss function penalizes underestimation with a different weight than overestimation.

The evaluation of the decision rules is done through the risk function, which is defined as the average value of the loss function. If \( L(\delta, \theta) \) is the loss function and \( \delta = \delta(x) \) is the decision rule, the hazard function of the decision rule \( \delta \) is mathematically expressed as

\[
R(\delta, \theta) = E_\theta L(\delta, \theta) = \int \theta L(\delta(x), \theta)f(x|\theta)d\theta.
\]  

(24)

In the Bayesian approach, it is possible to balance the risk function of each decision rule, based on ex-ante personal opinion, through \( u(\theta) \). So, the Bayesian risk is defined as [29–31]

\[
I(x) = \int \theta(\delta(x)^2 - 2\theta\delta(x) + \theta^2)p(\theta|x)d\theta
\]

\[ = \int \theta(\delta(x)^2 - 2\theta\delta(x) + \theta^2)P(\theta|x)d\theta + \int \theta^2 P(\theta|x)d\theta.
\]

(28)

Next, to determine which value can best estimate the random variable, we apply Bayesian inference to create a loss function, which will measure how wrong the estimate is, that is, how different the estimation of the parameter is from its actual price. This means that the goal is for the value of the estimate to minimize the loss function. For example, in the absolute error loss function, underestimation and overestimation of the parameter are punished in the same way, depending on the deviation of the estimate. In contrast to the preceding statement, the linear loss function penalizes underestimation with a different weight than overestimation.

The evaluation of the decision rules is done through the risk function, which is defined as the average value of the loss function. If \( L(\delta, \theta) \) is the loss function and \( \delta = \delta(x) \) is the decision rule, the hazard function of the decision rule \( \delta \) is mathematically expressed as

\[
R(\delta, \theta) = E_\theta L(\delta, \theta) = \int \theta L(\delta(x), \theta)f(x|\theta)d\theta.
\]  

(24)

In the Bayesian approach, it is possible to balance the risk function of each decision rule, based on ex-ante personal opinion, through \( u(\theta) \). So, the Bayesian risk is defined as [29–31]
The above function is minimized for \( \delta(x) \) when
\[
\delta(x) = \frac{\int_\Theta \theta p(\theta|x) d\theta}{\int_\Theta p(\theta|x) d\theta} \quad (29)
\]
\[\quad = E(\theta|x).\]

So, through a hypothesis check, we can determine the correctness of a hypothesis that concerns an action without dealing with estimating the possible values of the strategy. Based on this view, it is possible to predict the future prices of the process as, through the ex-post distribution, the forecasting process is immediate and accurate.

Assuming that, for a random sample of observations \( x = x_1, x_2, \ldots, x_n \), it is desirable to predict the future observation \( y \), and it is necessary to calculate the a posteriori distribution of prediction \( \pi(y|x) \). For the mathematical calculation of the ex-post distribution, the mathematical analysis of the ex-prediction distribution \( g(x) \) is required:
\[
g(x) = \int_\Theta f(x, \theta) d\theta = \int_\Theta f(x|\theta) u(\theta) d\theta. \tag{30}\]

Observing the equation, it is easy to see that the integral contains the product of the probability function \( f(x|\theta) \), with the ex-ante distribution \( u(\theta) \). Thus, based on the above procedure, the mathematical definition of the ex-post prediction distribution \( \pi(y|x) \) will be made:
\[
\pi(y|x) = \int_\Theta f(y, \theta|x) d\theta
= \int_\Theta f(y|\theta, x) p(\theta|x) d\theta
= \int_\Theta f(y|\theta) p(\theta|x) d\theta. \tag{31}\]

The probability function of the following observations is equal to the integral of the joint probability function \( f(y, \theta|x) \). It should be noted that this time the shared distribution function is bound to the observed data. Re-applying the Bayesian theorem, we conclude that the ex-post distribution of prediction is again equal to the product of probability \( f(y|\theta) \), but this time, with the ex-post distribution \( p(\theta|x) \), this is completed for the variable \( \theta \).

The effect of the ex-post information is therefore apparent. It should be noted that, from the probability function \( f(y, \theta|x) \), we came to the probability function if all a posteriori information originates from the parameter \( \theta \).

To prove the validity of the methodology described above, we will make the assumption that we will count the number of privilege escalation attacks made against a randomly chosen account on the music streaming platform that is the focus of the current example.

Suppose that the number of specific attacks over a period follows the “Poisson” distribution \( (\theta), \theta \in \Theta = (0, \infty) \), i.e.,
\[
f(x_i|\theta) = e^{-\theta^\gamma_i} x_i^! \]
\[\quad = 1, 2, \ldots, n. \tag{32}\]

For \( n \) observation time, the probability of the sample is
\[
L(\theta|x) = \prod_{i=1}^n f(x_i|\theta)
= \prod_{i=1}^n e^{-\theta^\gamma_i} x_i^!
= e^{-n\theta^\gamma} \prod x_i \quad \tag{33}\]

Suppose that the ex-ante distribution of \( \theta \) follows the Gamma distribution \( (a \beta) \), where \( a, \beta > 0 \); quantities are known as a function of probability density:
\[
u(\theta) = \frac{\theta^{a-1} e^{-(\theta/\beta)}}{\beta^a \Gamma(a)}. \tag{34}\]

Therefore, the distribution margin is
\[
g(x) = \int_0^\infty L(\theta|x) u(\theta) d\theta
= \int_0^\infty e^{-n\theta^\gamma} \prod x_i \left( \frac{\theta^{a-1} e^{-(\theta/\beta)}}{\beta^a \Gamma(a)} \right) d\theta
= \frac{1}{\beta^a \Gamma(a)} \prod x_i \int_0^\infty e^{-\theta^{\beta(-a/\beta)}/\beta} \sum x_i^{a-1} d\theta
= \frac{(\beta/n\beta + 1)\sum x_i^{a+1} \Gamma(\sum x_i + a)}{\beta^a \Gamma(a) \prod x_i} \int_0^\infty e^{-\theta^{\beta(-a/\beta)}/\beta} \sum x_i^{a-1} d\theta
= \frac{(\beta/n\beta + 1)\sum x_i^{a+1} \Gamma(\sum x_i + a)}{\beta^a \Gamma(a) \prod x_i} \int_0^\infty e^{-\theta^{\beta(-a/\beta)}/\beta} \sum x_i^{a-1} d\theta
= \frac{(\beta/n\beta + 1)\sum x_i^{a+1} \Gamma(\sum x_i + a)}{\beta^a \Gamma(a) \prod x_i}. \tag{35}\]

Therefore, the a posteriori distribution of \( \theta \) is
The ex-post distribution following the Gamma distribution was expected since the Gamma distribution family, where the ex-distribution belongs, is conjugated to the Poisson distribution.

The ex-post average value for the above Gamma distribution is \[30, 32, 33\]

\[
E(\theta|x) = \left( \sum_{i=1}^{n} x_i + \alpha \right) \left( \frac{\beta}{n\beta + 1} \right) = \frac{\beta \sum x_i + \alpha \beta}{n\beta + 1 + n\beta + 1} \tag{38}
\]

Let \( r \sim \text{Poisson}(\theta) \) be a new independent observation. The equation gives the forecast distribution:

\[
\pi(y|x) = \int_{\theta} f(y|\theta)p(\theta|x)d\theta, \tag{39}
\]

where for the specific statistical model it is \[34, 35\]

\[
\pi(y|x) = \int_{\theta} \left( e^{-\theta y} \right) \left( \frac{e^{-\theta(n\beta + 1)/\beta}}{(\beta/n\beta + 1)} \right)^{\theta y} \frac{1}{\Gamma(\sum x_i + \alpha + y)} \frac{\theta^\alpha}{\beta^\alpha \Gamma(\theta)} \Gamma \left( \sum x_i + \alpha + y \right) \left( \Gamma(y + t1) \right) \frac{\beta}{n\beta + 1 + n\beta + 1} \left( \frac{\beta}{n\beta + 1} \right) \tag{40}
\]

which is a negative binomial with parameters \[36–38\]:

\[
\left( \sum x_i + \alpha, \frac{\beta}{n\beta + \beta + 1} \right). \tag{41}
\]

5. Conclusions

This research offered an original and forward-thinking application of game theory and cutting-edge machine learning methods for adaptive cyber protection measures. It suggested a methodology based on game theory, which concerns the study of elements that characterize situations of competitive interdependence with an emphasis on the decision-making process of more than one decision maker. We make the assumption that every player is informed of the equilibrium tactics that the other players will use and that no player has anything to gain by merely altering the strategy that he uses. Therefore, in order to figure out which value can provide the most accurate estimation of the random variable, we use Bayesian inference to devise a loss function. This function will measure how inaccurate the estimate is, or more specifically, how far off the estimation of the parameter is from the actual price. This indicates that the objective is to have the value of the estimate be as low as possible concerning the loss function.

Specifically, the study of features that characterizes conditions of competitive interdependence includes the opponents. To be more specific, a methodology based on a repeated game is used to examine cyber-attacks and model behaviors and research how defenders and attackers make decisions in an environment where they compete. The unique approach developed can forecast the future moves in the game to generate the proper countermeasures and apply the most acceptable cyber defense tactics that govern a company. This ability is based on the use of Bayesian inference, which is a type of statistical inference. The suggested system was tested with great success in a particular application scenario in the digital music sector and how to cope
with upcoming cyber-attacks. The testing was successful on both fronts.

A crucial step in further developing the proposed model is the further investigation of how they can adapt the method parameters to processes of modern and asynchronous change of the initial parameters of the evaluators. This is one of the processes that will further the development of the proposed model. As a result, the expansion and empirical exploration of the characteristics of the method estimators in finite samples, which call for the use of Monte Carlo simulations, is also a vital component of the proposed system’s evolutionary parameter.

Data Availability

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

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] S. Musman and A. Turner, “A game theoretic approach to cyber security risk management,” The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 15, no. 2, pp. 127–146, 2018.

[2] L. Grønbæk, M. Lindroos, G. Munro, and P. Pintassilgo, “Basic concepts in game theory,” in Game Theory and Fisheries Management Game Theory and Fisheries Management: Theory and Applications, L. Grønbæk, M. Lindroos, G. Munro, and P. Pintassilgo, Eds., pp. 19–30, Springer International Publishing, Berlin, Germany, 2020.

[3] D. A. Akinwumi, G. B. Iwasokun, B. K. Alese, and S. A. Oluwadare, “A review of game theory approach to cyber security risk management,” Nigerian Journal of Technology, vol. 36, no. 4, p. 1271, 2018.

[4] T. Alpcan, Y. Vorobeychik, J. S. Baras, and G. Dán, “Decision and game theory for security,” in Proceedings of the 10th international conference, GameSec 2019, Stockholm, Sweden, November 2019.

[5] C. T. Do, N. H. Tran, C. Hong et al., “Game theory for cyber security and privacy,” ACM Computing Surveys, vol. 50, no. 2, pp. 1–37, 2018.

[6] I. M. del ´Aguila and J. del Sagrado, “Bayesian networks for enhancement of requirements engineering: a literature review,” Requirements Engineering, vol. 21, no. 4, pp. 461–480, 2016.

[7] A. Laszka, Y. Vorobeychik, and X. Koutsoukos, “Optimal personalized filtering against spear-phishing attacks,” in Proceedings of the AAAI Conference on Artificial Intelligence, Austin, TX, USA, February 2015.

[8] A. Schlenker, H. Xu, M. Guirguis et al., “Don’t bury your head in warnings: a game-theoretic approach for intelligent allocation of cyber-security alerts,” in Proceedings of the 26th International Joint Conference on Artificial Intelligence, pp. 381–387, Melbourne, Australia, August 2017.

[9] T. T. Nguyen and V. J. Reddi, “Deep reinforcement learning for cyber security,” IEEE Transactions on Neural Networks and Learning Systems, pp. 1–17, 2021.

[10] T. Alpcan and T. Basar, “Network security,” Cambridge University Press, Cambridge, NY, USA, 2010.

[11] E. Hemberg, L. Zhang, and U.-M. O’Reilly, “Exploring adversarial artificial intelligence for autonomous adaptive cyber defense,” in Adaptive Autonomic Secure Cyber Systems, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., pp. 41–61, Springer International Publishing, Berlin, Germany, 2020.

[12] S. Ganzfried, “Computing Nash equilibria in multiplayer DAG-structured stochastic games with persistent imperfect information,” in Decision and Game Theory for Security, pp. 3–16, Berlin, Germany, 2021.

[13] L. Huang and Q. Zhu, “Strategic learning for active, adaptive, and autonomous cyber defense,” in Adaptive Autonomic Secure Cyber Systems, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., Springer International Publishing, pp. 205–230, Berlin, Germany, 2020.

[14] P. Peng Xie, J. H. Li, X. Ximing Ou, P. Peng Liu, and R. Levy, “Using Bayesian networks for cyber security analysis,” in Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), pp. 211–220, Chicago, IL, USA, June 2010.

[15] Y. F. Dolgii and P. G. Surkow, “Asymptotics of regularized solutions of a linear nonautonomous system of advanced differential equations,” Differential Equations, vol. 46, no. 4, pp. 470–488, 2010.

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

[17] T. Halabi, M. Bellaiche, and A. Abusitta, “A cooperative game for online cloud federation formation based on security risk assessment,” in Proceedings of the 2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 83–88, Shanghai, China, June 2018.

[18] A. Schlenker, O. Thakoor, H. Xu, F. Fang, M. Tambe, and P. Vayanos, “Game theoretic cyber deception to foil adversarial network reconnaissance,” in Adaptive Autonomic Secure Cyber Systems Adaptive Autonomic Secure Cyber Systems, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., pp. 183–204, Springer International Publishing, Berlin, Germany, 2020.

[19] H. Worthington, R. S. McCrea, R. King, and R. A. Griffiths, “Estimation of population size when capture probability depends on individual states,” Journal of Agricultural, Biological, and Environmental Statistics, vol. 24, no. 1, pp. 154–172, 2019.

[20] Z. Ni, Q. Li, and G. Liu, “Game-model-based network security risk control,” Computer, vol. 51, no. 4, pp. 28–38, 2018.

[21] M. Redmayne, “Objective probability and the assessment of evidence,” Law, Probability and Risk, vol. 2, no. 4, pp. 275–294, 2003.

[22] M. N. Alsaeleh and E. Al-Shaer, “Automated cyber risk mitigation: making informed cost-effective decisions,” in Adaptive Autonomic Secure Cyber Systems, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., Springer International Publishing, pp. 131–157, Berlin, Germany, 2020.

[23] S. Venkatesan, S. Sugrim, J. A. Youzwak, C.-Y. J. Chiang, and R. Chadha, “A framework for studying autonomic computing models in cyber deception,” in Adaptive Autonomic Secure Cyber Systems, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., pp. 89–107, Springer International Publishing, Berlin, Germany, 2020.
[24] J. Jia and N. Z. Gong, “Defending against machine learning based inference attacks via adversarial examples: opportunities and challenges,” in *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., Springer International Publishing, pp. 118–307, Berlin, Germany, 2020.

[25] A. K. Guts, “Models of flood-attacks, mathematical catastrophe theory, theory of differential games and security strategies,” in *Proceedings of the 2020 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, pp. 1–5, Omsk, Russia, August 2020.

[26] Y. Urakawa, “Application of limited Pole-placement method to state feedback system,” in *Proceedings of the 2021 IEEE International Conference on Mechatronics (ICM)*, pp. 1–5, Kashiwa, Japan, March 2021.

[27] B. Nugraha, N. Kulkarni, and A. Gopikrishnan, “Detecting adversarial DDoS attacks in software-defined networking using deep learning techniques and adversarial training,” in *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 448–454, Rhodes, Greece, July 2021.

[28] M. Papastergiou, D. Kanaros, A. Papamichou, and N. Vernadakis, "Effects of a project based on mobile applications, exergames and a web 2.0 social learning platform on students' physical activity and nutritional criteria in the era of COVID 19," *Educational Media International*, vol. 58, no. 4, pp. 297–316, 2021.

[29] R. M. El-Sagheer, M. A. W. Mahmoud, and H. M. Hasaballah, "Bayesian estimations using MCMC approach under three-parameter burr-XII distribution based on unified hybrid censored scheme," *Journal of Statistical Theory and Practice*, vol. 13, no. 4, p. 65, 2019.

[30] A. J. M. Garrett, “Review: probability theory: the logic of science, by E. T. Jaynes,” *Law, Probability and Risk*, vol. 3, no. 3–4, pp. 243–246, 2004.

[31] S. Frey, A. Rashid, P. Anthonsamy, M. Pinto-Albuquerque, and S. A. Naqvi, "The good, the bad and the ugly," in *Proceedings of the 2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*, p. 496, Gothenburg, Sweden, February 2018.

[32] C. A. Coelho, "The generalized integer gamma distribution-A basis for distributions in multivariate statistics," *Journal of Multivariate Analysis*, vol. 64, no. 1, pp. 86–102, 1998.

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

[34] T. W. Anderson, *An Introduction To Multivariate Statistical Analysis*, Wiley, Hoboken, NJ, USA, 2003.

[35] J. O. Berger, "Bayesian analysis," in *Statistical Decision Theory and Bayesian Analysis*, J. O. Berger, Ed., Springer, pp. 118–307, New York, NY, USA, 1985.

[36] J. O. Berger, "Basic concepts," in *Statistical Decision Theory and Bayesian Analysis*, J. O. Berger, Ed., Springer, pp. 1–45, New York, NY, USA, 1985.

[37] E.-H. Choi, T. Fujiwara, and O. Mizuno, "Weighting for combinatorial testing by bayesian inference," in *Proceedings of the 2017 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 389–391, Tokyo, Japan, March 2017.

[38] Z. Yu, T. Huang, and J. K. Liu, "Implementation of bayesian inference in distributed neural networks," in *Proceedings of the 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pp. 666–673, Valladolid, Spain, March 2018.