[1.]S. P. ADISA, [2.] C. O. AKANBI, [1.] I. K. OGUNDOYIN

CLASSIFICATION AND ANALYSIS OF CYBER–ATTACK INTENSITIES: A GAME THEORETIC APPROACH

[1.] Information and Communication Technology Directorate, Federal Polytechnic Ede, Osun State, NIGERIA
[2.]Information and Communication Technology Department, Osun State University, Osun State, NIGERIA

Abstract: Computer networks are integral to modern life, yet face escalating security risks, necessitating innovative cyber security strategies. This study introduces a novel no cooperative game theory model to enhance cyber–attack prevention. The model, structured as a two–player game with attackers and defenders, aims to identify and mitigate cyber security risks through a three–level strategy approach. The model yields a Mixed Strategies Nash Equilibrium using non–zero–sum game theory and linear algebraic techniques. Simulations conducted in Python, using libraries such as numpy and nashpy and data scraped from three websites, evaluated residual energy, defence success rates, and defensive redundancy. The results show that the level–0 defence strategy completed 10,000 cycles with 100% residual energy. The developed model (Level–M) showed slightly lower performance with 80.21% residual energy, however, the level–2 defence strategy, which had the highest defence success rate, only achieved 39.9% residual energy. Additionally, Level–M exhibited superior performance with a defensive redundancy of 22.43%, compared to 67.74% for level–2, indicating that Level–M effectively allocates resources and avoids unnecessary defensive mechanisms when no attack occurs. This implies that a non–cooperative, non–zero–sum approach can improve the system's defence against cyber threats and produce an economical defence mechanism. Notably, these simulation metrics reveal the model's superior efficacy and efficiency in preventing dynamic cyber threats. Extensive simulations validate our model's efficacy, affirming its capacity to offer invaluable insights into proactive cyber defence mechanisms. The study's conclusions underscore the prospective utility of the formulated game theoretic model, which is poised to empower defenders with enhanced system protection and exploitation strategies.
Keywords: non–zero–sum, non–cooperative game theory, cyber–attack, attack, defence

1. INTRODUCTION

According to Perwej et al. (2021), a cyber–attack is an assault by cybercriminals on one or more computers or networks utilizing one or more computers. A cyber–attack can use a compromised computer to launch more assaults, steal data, or intentionally disable machines. Cybercriminals employ a range of techniques, such as password guessing. SQL injection, ransomware, phishing, malware, and denial of service to initiate cyber–attacks (Naik, 2023).

Introducing new threats and attack vectors means that the field of cyber security is constantly changing. One must practice proactive thinking and ongoing attention to get ahead of cybercriminals. According to Afifi (2021), it is imperative for organizations to do security audits, update and patch software regularly, and educate staff members about potential hazards. Proactive techniques, such as penetration testing and vulnerability assessments, are also included in the realm of cyber security to find system vulnerabilities before malevolent actors use them (Papatsaroucha et al., 2021). Moreover, using artificial intelligence and machine learning methodologies is vital in promptly identifying and addressing cyber risks (Zeadally et al., 2020).

While working on the problem of safeguarding computer and cyber resources, several researchers encountered an additional difficulty that has presented a challenge to other researchers. A system with few cyber–attacks is necessary, even though there may not be a perfect way to prevent them. Game theory has been successfully applied to cyber protection in the recent literature (Zhang & Malacaria, 2021; Abapour et al., 2020; Attiah et al., 2018; Bhuiyan, 2016) to simulate attacker/defender scenarios. This work will also provide results, particularly an alternative perspective on how game theory may be used to prevent cyber–attacks at the lowest possible cost. Game theory addresses strategic interactions among multiple decision makers, called players (and, in some contexts, agents) (Ho, 2022). It has uses in computer science, systems science, logic, and

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

all branches of social science. There are two traditional branches of the game: non–cooperative and cooperative (Azar, 2021). Cooperative game theory focuses on situations where players can make binding agreements. It examines how groups of players, called coalitions, can form and achieve outcomes that are beneficial to them. On the other hand, non–cooperative game theory addresses situations where binding agreements among players are not possible or not allowed. In non–cooperative games, players make decisions independently and pursue their own individual interests. Analyzing player interactions strategically and forecasting results based on each player's decisions and tactics are the key points of emphasis. The Nash equilibrium, in which no player has an incentive to unilaterally change his or her strategy, is a common idea in non–cooperative game theory. Both branches of game theory have their own distinct methods and models for analyzing strategic situations. They offer insightful information about cooperation, competitiveness, and decision–making in a variety of disciplines, such as political science, computer science, and economics.

Countless researchers have developed cyber security/prevention models but ignored dynamic threats in favor of a static, game–theoretic model with a particular security attack or defence. However, the few that concentrated on the dynamic model did not consider the intensities of the attacks nor the frequency with which the intensities are altered to get a better payoff. This has wasted the defender's resources and restricted some access that was not necessary. This research aims to develop a non–competitive, non–zero–sum game theory model using linear algebra techniques and simulate it with three different metrics that will showcase the contributions of the model.

2. RELATED WORKS

Several researchers have demonstrated studies on cyber–prevention using different techniques, including game theory, because of its demonstrated ability to produce a more effective cyber–prevention model. It was noted that the game theory promised to provide a better solution for cyber–attacks. The study conducted by Ho et al. (2022) investigated the application of game theory in the field of cyber security. This text provides a fundamental introduction to the notion of game theory, followed by a comprehensive survey of the research undertaken using game theory in the field of cyber security. Researchers are actively utilizing linear programming as one of their methodologies. The statement suggests that games can be created and examined to determine the most effective strategies for addressing cyber security by analyzing the optimal actions made by participants. In addition, they proposed a methodical resolution to the cyber security problem using game theory, which will include a credible mathematical solution.

(Attiah et al., 2018) conducted a study on the dynamic interaction between attackers and defenders, wherein both parties possess intelligence and adapt their assault or defence strategies in a dynamic manner. The equilibrium was established utilising the Nash equilibrium methodology, which is founded on a non–cooperative zero–sum game theory. The researchers showcased the applicability of the new game theory to various cyber security issues by employing three distinct types of network attacks. Based on the data, the suggested system demonstrates superior performance compared to two previous defence systems with predefined strategies. A comparison was made between the mean residual energy and the rate of success in defence. The highly protective mechanism was unveiled. However, in reality, the outcome is not a situation where one party's gain is equal to the other party's loss. The defender's loss may not necessarily result in a gain for the attacker, and vice versa, this negative the theory of zero sum game theory. The dynamic behaviour of the attacker is not accurately represented; the analysis of the node is not utilised.

Adisa et al. (2024) presented a paper on a framework for a game theoretic model for cyber threat prevention. Non–cooperative non–zero–sum was used, and two metrics such as success rate and residual energy were used to validate the model presented. The result showed that the model

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

performed better than the previous research that uses non–zero–sum and dynamically prevents, and it was proposed that more metrics can be used for future research.
Zarreh et al. (2019) developed a game theory model to tackle cyber security issues in advanced manufacturing systems, including extensive computer–controlled integration. The cost function of the game payout matrix was determined by considering the expenses associated with maintaining a defence mechanism, the financial losses incurred from an assault, and the costs involved in recovering from an attack. This approach accurately reflects the real–world dynamics of manufacturing systems. The proposed method can be extended to domains other than automated manufacturing systems by modifying the cost components in the utility function. Due to the incorrect assumption of zero sum, the researcher suggests using non–zero–sum in future studies to examine normal–form games (non–zero–sum) with imperfect information and irrational players in order to reach improved results.
Iqbal et al (2019) surveyed the literature on game theory modeling of networks/cyber security and identified numerous difficulties that must be solved in this field, such as the difficulty of calculating a game–theoretical equilibrium strategy, measuring security characteristics including risk, privacy, confidence and reliance, Selecting the optimal game model to address a certain security issue, Choosing a game can be done simply on intuition, which may or may not be supported by existing facts. Furthermore, it was proposed that a two–player game may serve as a framework for a security game including an assailant and a protector. Additionally, the dynamic form of this game could encompass multiple stages of attack and defence. The prevailing belief among researchers studying security game models is that participants possess boundless rationality. However, empirical evidence from real–life scenarios and experimental investigations indicates that players do not consistently exhibit rational behaviour.
Abapour (2020) introduced a model in which the defence aims to achieve the highest possible resource allocation to maximise its payoffs, while the attacker aims to minimise the risk of being traced and penalised. The min–max approach was utilised. A novel game idea that combines simulation and game–theoretic approaches is proposed to tackle the problem of unknown observability in the payoff matrix. It has been proposed that incorporating other methodologies into game theory might yield a more effective defence solution. This approach is applicable only in the presence of a saddle point.
Zhang and Malacaria Pasquale (2021) devised an efficient multistage cyber–defence strategy to counter multistep attacks. The mathematical framework incorporates preventive optimization to mitigate pre–existing security risks, as well as online optimization to combat ongoing threats. The optimization is formulated as a Bayesian Stackelberg game, where the defence possesses limited information about the attacker's present state. The optimization problem is solved by utilizing the characteristics of totally uni–modular matrices, strong duality, and mixed–integer linear programming. This solution effectively decreases the security risk of ongoing attacks compared to previous methods. Additionally, it offers cyber security experts a unified mathematical framework for both preventive investment and countermeasures against ongoing attacks. The study employed a dynamic attack/defence model, however without recording the intensities.
(Johnson & Tanmay, 2017) A mathematical model was proposed to analyse the Distributed Denial of Service (DDoS) attack and its correlation with factors like inter–arrival time or rate of arrival of the attacking clients accessing the server. Moreover, the model analyses the attack model in terms of the victim server's depletion of bandwidth and buffer space. The model utilised a self–organizing map, an unsupervised learning technique, to create clusters of similar features. The actions of the clusters are thereafter examined using mathematical correlation and a normal probability distribution in order to identify a DDoS attack. This analysis solely focuses on the DDoS assault paradigm and its specific impact on depleting server resources, including bandwidth and memory.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

The study revealed that the probability of resource exhaustion is contingent upon the frequency at which the attacking clients reach the victim server. Prioritising the augmentation of the target server's buffer size and the number of open channels has been identified as the initial defensive measure against a DDoS attack, preceding the detection of such an attack by Intrusion Discovery Systems/Intrusion Protection Systems (IDS/IPS).

3. METHODOLOGY

This section comprises many sections that detail the methodology adopted in this research.

Data Collection

For this study, web scrapping was employed for data collection from three (3) distinct websites. These websites have been carefully selected based on their relevance to the research topic and the availability of the required data. This method of data gathering was used based on the parameters (username, password, IP address, time of activities) needed to easily formulate the model proposed for this research, and gathering data from multiple sources will enhance a comprehensive and diverse dataset, enhancing the validity and reliability of the research findings. The selected websites provided valuable information that aligns with the objectives and scope of the study, enabling a thorough analysis and interpretation of the collected data. Web Scraping Algorithm (Figure 1) was used to acquire data from the selected websites with the following parameters.

Algorithm 1: Web Scraping Pseudocode for Data Collection

```
START
username ← get(username)
password ←get(password)
ipaddress ← getUserIP($ip2)
timeInserted ← CURRENT_TIMESTAMP
If (successStatus = TRUE):
successStatus ← 1
else:
successStatus ← 0
end if
function getUserIP($ip2):
if (!empty($_SERVER['HTTP_CF_CONNECTING_IP'])) :
return $_SERVER['HTTP_CF_CONNECTING_IP']
else
return $_SERVER['HTTP_X_REAL_IP']
end if
end function
database.call():
Insert result INTO table ($username, $password, $Ipaddress, $timeInserted, $successStatus)
STOP
```

Attackers Strategies Classification

The relevant information obtained from the data scrapped (using Algorithm 1) was subjected to a classification algorithm (Algorithm 2) to determine the intensity of the attack

Algorithm 2: Classification Algorithm for Attackers' Strategies

```
START
Initialize Variables
    intensity ← 0;  counter0 ← 0; counter1 ← 0; counter2 ← 0
Connect to the Database
        Establish a connection to the database
Fetch Records
        Execute SQL query to fetch records from the security table where records are not already recorded in the  attack Intensity table
Process Each Record
        For each record r in the fetched records:
        Extract fields from r:
```


ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

```
sn ⟵ r[sn]; username ⟵ r[username]; password ⟵ r[password]
ipaddress ⟵ r[ipaddress]; timest ⟵ r[timest]; ipaddress2 ⟵ r[ipaddress2]
sta ⟵ r[sta]
  If sta = 1 then:
intensity ⟵ 0; counter0 ⟵ counter0 + 1
  Else:
            Execute SQL query to check if there are more than 5 previous attacks on the same IP:
            If more than 5 previous attacks:
        intensity ⟵ 1
        counter1 ⟵ counter1 + 1; Increment k
        If k ≥ 5 and more than 5 attacks within the last 5 minutes:
            timeSTART ⟵ timest
            timeEND ⟵ timeSTART + 5 minutes
            Execute SQL query to check for attacks within the last 5 minutes on the same IP:
              If more than 3 attacks within the last 5 minutes:
                  intensity ⟵ 2
                  counter2 ⟵ counter2 + 1
               Else:
                   intensity ⟵ 1
                   counter1 ⟵ counter1 + 1
                  Else:
             intensity ⟵ 0; k ⟵ 0
             counter0 ⟵ counter0 + 1
      If sta is empty:
            sta ⟵ 0
      Insert record into the attack Intensity table with the calculated intensity and other details
6.  Display Summary
      Display summary of attack intensities
7.  END
```

A total of 100,000 were classified out of 275,700 records collected from the three websites for this research. The results obtained from this classification process are presented in Table 1. The table showcases the relevant findings and insights derived from the data, providing a structured overview of the research outcomes. The classified records serve as a valuable resource for this study, enabling the research team to draw meaningful conclusions and contribute to understanding the subject matter.

For modeling, the attacker's scenarios are categorized into three distinct forms: no attack (attack–0), low–intensity attack (attack–1), and high–intensity attack (attack–2). Similarly, the defender's scenarios are categorized as no defence (defend–0), low–intensity defence (defend–1), and high–intensity defence (defend–2). This simplifies and enhances the explanatory power of the model. Both players select their strategies concurrently without cooperation, operating under the assumption of common knowledge about the game and the potential gains or losses (represented by U).

Table 1: Strategy Classification

Attack Level	Attack Description	Number
0	No Attack	75,931
1	Low–Intensity Attack	23,404
2	High–Intensity Attack	665
Total		100,000

Password Guessing and SQL Injection Attacks Classifications

The password–guessing attack method involves a systematic and exhaustive trial of every conceivable combination of characters to uncover a user's password. It is a brute force attack aimed at illegally obtaining access to a system or account without proper authorization. Attack–1, also known as level–1 of attack, consists of low–intensity password–guessing attempts that do not require any specific expertise from the attacker. In this situation, the attacker mimics the behavior of a regular user by submitting login attempts individually. This type of password–guessing attack is characterized by its slow pace of password trials, which leads to a considerably longer duration

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

for the attacker to discover the correct password. Attack–2 consists of increased intensity in password guessing attempts, utilising advanced tactics such as implementing numerous virtual client schemes. This approach enables an attacker to create several virtual clients using just one computing unit.

SQL injection attacks can also be classified based on the intensity of the attacks: Low–intensity attacks, known as Level–1 attacks, are comparable to manual SQL injection attacks. These attacks involve human attackers who manually devise and execute SQL injection techniques. Unlike automated attacks, these manual attacks are often more targeted and sophisticated, although they can also be slower and more labor–intensive. Level–1 attacks reflect this lower intensity and require a higher degree of manual involvement from the attacker. High–intensity attacks, known as Level–2 attacks, are commonly referred to as automated SQL injection attacks. These attacks are conducted using automated scripts or tools that exploit database vulnerabilities. Level–2 attacks pose a significant threat to organizations, representing a heightened intensity of attack compared to Level–1, emphasizing the use of automated tools and the potential for widespread damage.

A tailored script was developed to categorize each trial conducted by the attacker, considering the frequency of trials launched within a specific time frame and the attacker's previous trial patterns. This script enables the classification and analysis of each attack attempt based on the number of trials made by the attacker and their historical trial behavior. Algorithm 2 shown the algorithm for this script.

Defender Strategies Classification

This section discussed the defence strategy classifications; the defender's strategy is divided into three levels: level–0 (No–defence), level–1 (low–intensity defence), and level–2 (high–intensity defence). In this research, level–2 is assumed to require more resources than level–1, while level–0 does not necessitate any resources. However, it is essential to note that if an attack occurs and the defender does not take any defensive measures, their primary protective resources are at risk. Therefore, it is not advisable for the defender to remain idle (level–0) and refrain from defending.

The defender's level–1 strategy aims to deny the attacker certain information or restrict their access to the system. This strategy involves incorporating minimal additional requirements, such as supplementary information during user or node registration. On the other hand, the level–2 strategy demands more technical signatures that may be more complex for machines to supply. The defender can adopt a proactive approach to safeguarding the system against potential attacks by implementing different defence strategies. Each level offers varying degrees of protection and imposes different requirements on the attacker, aiming to create multiple layers of defence and mitigate security risks.

Model Formulation

We assume the following for our three–level attack/defence strategies model:

- **Assumption 1:** The value of resources under protecting (α) is always more significant than the cost to defend ($C_{\gamma n}$) or attack ($C_{\beta n}$). Hence, the defender or attacker would not be incentivized to engage in defence or attack activities. In other words, $\alpha > C_{\beta n}, C_{\gamma n}, n \in \{0,1,2\}$.
- **Assumption 2:** The cost to incur for the attack strategy β1(Attack–1) is less than the cost for attack strategy β2 (Attack–2) for the attacker. Specifically, $C_{\beta 1} < C_{\beta 1}$. This assumption represents the idea that Attack–2 is a strategy of attack that is more aggressive as well as effective than Attack–1.
- **Assumption 3:** This assumption recognizes that defend–2 is a stronger and active defence strategy compared to Defend–1. Defend–2 entails higher defence costs, indicating that it requires more resources, advanced technologies, or sophisticated countermeasures to implement successfully.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

— **Lemma 1**: Let α = resources under protection, cost of defence – $C_{\gamma n}$, cost of attack $C_{\beta n}$, given that $\alpha > C_{\gamma n}$ and $\alpha > C_{\beta n}$ for $n \in \{0, 1, 2\}$

— **Implication:**

≡ For the defender: $C_{\gamma n} < \alpha$ → It is economically viable to defend

≡ For the attacker: $C_{\beta n} < \alpha$ → It is economically viable to attack

— **Proof**: Assume that both the attacker and defender are rational agents who participate in the game if and only if their actions yield positive net benefits. If $\alpha < C_{\gamma n}$, the defender's cost of defence $\alpha > C_{\gamma n}$ and $\alpha > C_{\beta n}$ for $n \in \{0, 1, 2\}$ exceeds the value of the asset, making it irrational to defend. Therefore, no defence strategy would be undertaken if the cost surpasses the asset's value. If $\alpha < C_{\beta n}$, the attacker's cost of attack exceeds the value of the asset, making it irrational to attack. Thus, no attack strategy would be undertaken if the cost exceeds the asset's value. Given these conditions, we ensure:

— **Lemma 2:** Let the cost of Attack–2= $C_{\beta 2}$, cost of attack–1 = $C_{\beta 1}$, Given that $C_{\beta 2} > C_{\beta 1}$

— **Proof**: Assume the attacker is a rational agent who chooses strategies based on cost–efficiency and potential impact. Attack–2 necessitates increased resources like advanced tools, multiple attack channels, higher technological expertise and more financial investment, higher power consumption, greater memory usage. Given $C_{\beta 1} < C_{\beta 2}$

— **Attack–1**: Lower cost, less complexity, simpler execution. Suitable for less critical or opportunistic attacks.

— **Attack–2**: Higher cost, more complex, higher potential impact. Suitable for targeted, high–value attacks.

The attacker evaluates strategies based on costs and benefits:

$$\text{choose} \begin{Bmatrix} \text{Attack} - 1 \text{ if: } C_{\beta 1} > C_{\beta 2} \text{ and desired impact is lower} \\ \text{Attack} - 2 \text{ if: } C_{\beta 2} > C_{\beta 1} \text{ but offers significantly higher impact} \end{Bmatrix}$$

— **Implication:** This analysis and the corresponding lemma reinforce that Attack–2's higher cost is justified by its greater potential impact and complexity. This supports the game model's exploration of the attacker's strategic choices and resource allocation in executing different attack strategies

— **Lemma 3:** Let the cost of defend–2= $C_{\gamma 2}$, cost of defend–1 = $C_{\gamma 1}$, Given that $C_{\gamma 2} > C_{\gamma 1}$

— **Proof**:

≡ Defend–1 ($C_{\gamma 1}$) and Defend–2 ($C_{\gamma 2}$) are the two strategies available to the defender. By assumption, $C_{\gamma 1} < C_{\gamma 2}$. Defend–1 utilizes fewer resources in terms of memory and power consumption. Defend–2 utilizes more resources, requiring advanced methodologies and tools.

≡ Since $C_{\gamma 1} < C_{\gamma 2}$, the cost associated with implementing Defend–2 surpasses that of Defend–1.

≡ A rational defender will compare the costs $C_{\gamma 1}$ and $C_{\gamma 2}$. Given $C_{\gamma 2} > C_{\gamma 1}$, the defender will only opt for Defend–2 if the expected payoff justifies the higher cost. Therefore, for a rational defender aiming to maximize utility, $C_{\gamma 2} > C_{\gamma 1}$ holds true, confirming the lemma.

— **Implication**: This analysis and the corresponding lemma reinforce that Defend–2's higher cost is justified by its greater potential effectiveness and complexity. This supports the game model's exploration of the defender's strategic choices and resource allocation in implementing different defence strategies.

— Furthermore, the game model necessitates that we specify the result of the attacker using a particular attack plan and the defender using a particular defence strategy. We assume the following results for the game:

— **Assumption 4:** Attack–k is successful against defence–n such that $k<n$ and $k \subset n$ and defence–n is successful against Attack–t such that $n > t$ and $t \subset n$ for $n \in \{0,1,2\}$

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

— Lemma 4: Let A_k represent the attack strategy and D_k represent the defence strategy for k∈{0,1,2}. Given that: A_{k-1} is successful against D_k , D_k is successful against both A_k and A_{k-1}

— Proof:

≡ A_{k-1} is successful against D_k : Success (A_{k-1}, D_k) =True

≡ D_k is successful against both A_k and A_{k-1}, Success (D_k, A_k)=True,Success (D_k, A_{k-1})=True

By considering these assumptions, the model delineates the conditions under which the attacker or defender can achieve success in the game. It establishes the relationships between different attack and defence strategies and their respective outcomes, thereby providing a framework for analyzing the strategic interactions and decision–making processes in the non–cooperative game model for cyber–attack prevention. A payout matrix was created to depict the non–cooperative, non–zero–sum game between the attacker and defence based on the mentioned assumptions. The payoffs linked to the different strategies that both players employed are shown in Table 2. The efficiency of the attack and defence plans, the related expenses, and the degree of security attained were some of the considerations that went into determining the precise values in the payout matrix. In order to determine the best tactics for both the attacker and the defender, taking into account the possible results and rewards connected with each move, the payoff matrix is a useful tool for game analysis.

Table 2: Attack–Defence Payoff Matrix

Attacker (β)	Defence (γ)			
	γ_0	γ_1	γ_2	Probability
β_0	0,α	0, $\alpha-c_{\gamma 1}$	0, $\alpha-c_{\gamma 2}$	p_0
β_1	$\alpha-c_{\beta 1}$, $-\alpha$	$-c_{\beta 1}$, $\alpha-c_{\gamma 1}$	$-c_{\beta 1}$, $\alpha-c_{\gamma 2}$	p_1
β_2	$\alpha-c_{\beta 2}$, $-\alpha$	$\alpha-c_{\beta 2}$, $-\alpha-c_{\gamma 1}$	$-c_{\beta 2}$, $\alpha-c_{\gamma 2}$	p_2
Probability		q_0	q_1	q_2

Based on the assumptions mentioned, the model that incorporates the attacker–defender game theory, considering the non–zero–sum relationship between the attacker and defender payoffs can be achieved in the following.

$G = \{I, A, U\}$ → Game

$I = \{\beta, \gamma\}$→Players (β = Attacker, γ = Defender/Administrator)

$A = \{\beta_k, \gamma_k \,|k \in \{0,1,2\}$→ Strategies ($\beta k$ = Attacker , γk = Defender)

$U = \{U_a, U_d\}$ →Payoff/Utility ($U\beta$ = Attacker , $U\gamma$ = Defender

Cost of Attack = $C\beta$, Cost of Defending = $C\gamma$, Resources Protecting = α

$$G = \{\{\beta, \gamma\}\{\beta_k, \gamma_k \,|k \in \{0,1,2\}, \{U_a, U_d\}\, \beta \rightarrow \beta\, \gamma \rightarrow \gamma\} \quad (1)$$

also let; Let p_0, p_1, p_2 be the propability that the attacker β choose strategy level 0, 1, 2 respectively and q_0, q_1, q_2 be the probability that the defender γ choose strategy level 0, 1, 2 respectively.

Where;

p_0 is the probability of attacker plays attack level 0 (ie. β_0), p_1 is the probability of attacker plays attack level 1 (ie. β_1), p_2 is the probability of attacker plays attack level 0 (ie. β_2) and q_0 is the probability of defender plays defend level 0 (ie. γ_0), q_1 is the probability of defender plays defend level 1 (ie. γ_1), $q_2$is the probability of defender plays defend level 0 (ie. γ_2)

In the payoff matrix in Table 2, there is no element of the matrix known as the saddle point of the matrix game that simultaneously resides at the minimum of the row in which it occurs and the maximum of the column in which it occurs. that is, there is not a single deterministic tactic that can be used by an attacker or defender. As a result, the model's Mixed Strategy Nash Equilibrium (MSNE) will be solved algebraically. A probability distribution $\widehat{P}$ over the set of pure strategies S for every participant in the security preventative game is such:

$$\widehat{P} = (p_1, p_1, p_2, p_3 \ldots p_r) \epsilon \mathbb{R}^R \geq 0, \text{ and } \sum_{i=0}^{R} p_t = 1 \quad (2)$$

$$eU(p_0) = eU(p_1) = eU(p_2) \quad (3)$$

$$eU(q_0) = eU(q_1) = eU(q_2) \quad (4)$$

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

$\mathbf{eU(p_0)}$ represents the expected utility for the attacker when playing strategy level–0, also known as attack–0. $\mathbf{eU(p_1)}$ represents the expected utility for the attacker when playing strategy level 1, also known as attack–1. $\mathbf{eU(p_2)}$ represents the expected utility for the attacker when playing strategy level 2, also known as attack–2.

The expected utility is a measure that considers the potential outcomes and their probabilities associated with a particular strategy. In the context of the game, $\mathbf{eU(p_n)}$ captures the anticipated benefits or gains that the attacker expects to achieve by employing attack–n. This expected utility value is influenced by factors such as the success rate, the payoff or reward associated with a successful attack, and the likelihood of encountering different defence strategies from the defender. By calculating and comparing the expected utilities of different strategies, the attacker can make informed decisions to maximize their potential gains in the game.

$\mathbf{eU(q_0)}$ represents the expected utility for the defender when playing strategy level–0, also known as defend–0. This utility is a measure that considers the potential outcomes and their probabilities associated with a particular strategy, $\mathbf{eU(q_1)}$ represents the expected utility for the defender when playing strategy level–1, also known as defend–1. This utility is a measure that considers the potential outcomes and their probabilities associated with a particular strategy, $\mathbf{eU(q_2)}$ represents the expected utility for the defender when playing strategy level–2, also known as defend–2. This utility is a measure that considers the potential outcomes and their probabilities associated with a particular strategy.

In the context of the game, $\mathbf{eU(q_n)}$ captures the anticipated benefits or gains that the defender expects to achieve by employing defend–n. This utility value is influenced by factors such as the effectiveness of defend–n in countering various attack strategies, the level of resource investment required, and the potential impact on the system's security. By calculating and comparing the expected utilities of different strategies, the defender can make informed decisions to maximize their potential gains and enhance the overall defence against cyber–attacks.

The various outcomes and their probabilities associated with any combination of attacker and defender tactics can be evaluated in order to determine the expected payout of attacker A for playing β_0, β_1, and β_2 when defender γ chooses methods γ_0, γ_1, and γ_2, respectively. The average payout that the attacker expects to receive across several game plays is represented by the expected payoff. We take into account the payoff matrix, which contains the profits or rewards for various combinations of attacker and defender methods, in order to calculate the predicted payout. We can determine the expected payout for each attacker tactic by multiplying the probability of each result by the corresponding payoffs and adding them together.

By evaluating the expected payoffs for all combinations of attacker and defender strategies, we can gain insights into the potential gains and risks associated with different choices, which can inform the decision–making process for both the attacker and defender in the game.

$$\mathbf{eU(p_0) = q_0(0) + q_1(0) + q_2(0)} \quad (5)$$

$$\mathbf{eU(p_1) = q_0(\alpha - c\beta_1) + q_1(-c\beta_1) + q_2(-c\beta_1)} \quad (6)$$

$$\mathbf{eU(p_2) = q_0(\alpha - c\beta_2) + q_1(\alpha - c\beta_2) + q_2(-c\beta_2)} \quad (7)$$

Substituting (5), (6), and (7) in (3), we have the probability distribution $\mathbf{q_0}$, $\mathbf{q_1}$and $\mathbf{q_2}$

By substituting equations (5), (6), and (7) into equation (3), we obtain the probability distribution $\mathbf{q_0}$, $\mathbf{q_1}$ and $\mathbf{q_2}$. The probability distribution represents the likelihood or probability of each defender strategy being selected. The probabilities $\mathbf{q_0}$, $\mathbf{q_1}$ and $\mathbf{q_2}$ are determined based on the expected utilities $\mathbf{eU(q_1)}$, $\mathbf{eU(q_1)}$, and $\mathbf{eU(q_2)}$for the defender's strategies, which capture the anticipated benefits or utilities for the defender when playing each strategy. Substituting these expected utilities into equation (3) allows us to calculate the probability distribution q_0, q_1, and q_2, which reflect the relative probabilities of the defender selecting each strategy. The probability distribution provides insights into the defender's decision–making process and the likelihood of them choosing

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

each strategy based on their anticipated benefits or utilities. By analyzing the probability distribution, we can understand the defender's strategic preferences and make predictions about their likely choices in the game.

$$q_0 = \frac{c\beta_1}{\alpha},\ q_1 = \frac{c\beta_2 - c\beta_1}{\alpha},\ q_2 = 1 - \frac{c\beta_2}{\alpha}, \tag{8}$$

Similarly, the expected payoff of defender γ for playing γ_0, γ_1, and γ_2 when attacker β selects strategies β_0, β_1 and β_2 respectively can be calculated. The expected payoff of the defender, denoted as $eU(q_0)$, $eU(q_1)$and $eU(q_2)$ represents the anticipated benefits or utilities for the defender when playing each strategy against the attacker's strategies. By substituting these expected utilities into the payoff equation, the expected payoffs can be calculated for the defender when facing each possible combination of attacker strategies. This allows us to determine the relative benefits or utilities of the defender's strategies based on the likely actions of the attacker. The expected payoffs provide insights into the defender's decision–making process and the potential outcomes of different strategy combinations in the game. They help the defender assess the potential gains or losses associated with their choices and make informed decisions on which strategy to employ. Analyzing the expected payoffs allows us to understand the defender's strategic preferences and evaluate the effectiveness of their strategies in different scenarios. It helps us gain insights into the possible outcomes of the game and can guide the defender in selecting the most advantageous strategy to maximize their expected payoff.

$$eU(q_0) = p_0(\alpha) + p_1(\alpha - c\gamma_1) + p_2(\alpha - c\gamma_2) \tag{9}$$

$$eU(q_1) = p_0(-\alpha - c\gamma_1) + p_1(\alpha - c\gamma_1) + p_2(\alpha - c\gamma_1) \tag{10}$$

$$eU(q_2) = p_0(-\alpha) + p_1(-\alpha - c\gamma_1) + p_2(\alpha - c\gamma_2) \tag{11}$$

By substituting the equation (9), (10), and (11) in equation (3), we have the probability distribution p_0, p_1, p_2.

$$p_0 = 1 + \frac{c\gamma_1 - c\gamma_2}{\alpha},\ p_1 = \frac{c\gamma_1}{2\alpha},\ p_2 = \frac{2c\gamma_2 - 3c\gamma_1}{2\alpha} \tag{12}$$

The probability distribution assists in predicting the possible outcomes of the game and aids the defender in formulating effective countermeasures. By understanding the probabilities of different attacker strategies, the defender can adapt their own strategies to mitigate risks and maximize their defensive capabilities. Overall, the probability distribution provides valuable information for strategic planning and decision–making in the game, enabling the defender to anticipate and respond effectively to the attacker's actions.

Simulation and Performance Evaluation

The simulation employed the Python programming language, along with the NumPy and Nashpy libraries. The developed model was employed to forecast potential strategies for the defender across various scenarios while the attacker operated randomly. Attack and defence strategies were generated for 10,000 cycles. This was generated based on the developed model, the algorithm for model simulation is shown in Algorithm 3. This result will be used for our performance evaluation. Three metrics were employed, Success Rate, Defensive Redundancy, and Residual Energy, to gain valuable insights into the performance, effectiveness, and energy efficiency of the developed model across different scenarios. These metrics contribute to the comprehensive evaluation and analysis of the model's capabilities, enabling us to draw meaningful conclusions and make informed decisions for further improvements or applications. In the given context where " α " represents the resources allocated to protection and considering different scenarios based on the relative values of α, Cost of Defence ($C\gamma_n$), and Cost of Attack (C_{an}), the following scenario can be made:

- When α is higher than the Cost of Defence ($C\gamma_n$) and Cost of Attack (i.e. $\alpha > C\gamma_n, c\beta_n$, n ∈ {0,1,2}, and the Cost of Defence is higher than the Cost of Attack (i.e. $C\gamma_n > c\beta_n$).
- When α is lower than the Cost of Defence ($C\gamma_n$) and Cost of Attack (i.e. $\alpha < C\gamma_n, c\beta_n$, n ∈ {0,1,2}, and the Cost of Defence is higher than the Cost of Attack (i.e. $C\gamma_n > c\beta_n$).

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

— When α is significantly higher than the Cost of Defence ($C\gamma_n$) and Cost of Attack (ie. $\alpha >> C\gamma_n$, $c\beta_n$, n ∈ {0,1,2}, and the Cost of Defence is higher than the Cost of Attack (i.e. $C\gamma_n > c\beta_n$).

Overall, the relative values of α, $C\gamma_n$, and $c\beta_n$ provide insights into the resource allocation and strategic considerations for defence and attack. These scenarios highlight different resource allocation strategies and the balance between defence and attack in relation to their respective costs.

Algorithm 3: Model Simulation Algorithm

1. START
2. Initialize:
   – num_players ⟵ 2
   – num_strategies ⟵ 3; – r ⟵ 50
   – ca ⟵ { ca_0 ⟵ 0, ca_1 ⟵ 10, ca_2 ⟵ 20 }
   – cd ⟵ { cd_0 ⟵ 0, cd_1 ⟵ 20, cd_2 ⟵ 40 }
3. SET payoff matrix values:
   – Attacker's payoff matrix A:
     – A_{11} ⟵ 0, A_{12} ⟵ 0, A_{13} ⟵ 0
     – A_{21} ⟵ r – ca_1, A_{22} ⟵ –ca_1, A_{23} ⟵ –ca_1
     – A_{31} ⟵ r – ca_2, A_{32} ⟵ r – ca_2, A_{33} ⟵ –ca_2
   – Defender's payoff matrix D:
     – D_{11} ⟵ r, D_{12} ⟵ r – cd_1, D_{13} ⟵ r – cd_2
     – D_{21} ⟵ –r, D_{22} ⟵ r – cd_1, D_{23} ⟵ r – cd_2
     – D_{31} ⟵ –r, D_{32} ⟵ –r – cd_1, D_{33} ⟵ r – cd_2
4. COMPUTE probability distribution of Defender (q_0, q_1, q_2):
   – q_0 ⟵ ca_1 / r
   – q_1 ⟵ (ca_2 – ca_1) / r
   – q_2 ⟵ 1 – (ca_2 / r)
5. COMPUTE probability distribution of Attacker (p_0, p_1, p_2):
   – p_0 ⟵ 1 + (cd_1 – cd_2) / r
   – p_1 ⟵ cd_1 / (2r)
   – p_2 ⟵ (2cd_2 – 3cd_1) / (2r)
6. Initialize data list
7. DEFINE Nash equilibrium probabilities as a 2D array:
   [[p_0, p_1, p_2], [q_0, q_1, q_2]]
8. Set num_simulations ⟵ 10000
9. Initialize chosen_strategiesk ⟵ 0
10. Initialize a DataFra(df) with columns 'Attacker' and 'Defender' with initial values [0]
11. Specify the path and filename for the Excel file as 'output_1.xlsx'
12. FOR each simulation in num_simulations DO
    – Initialize chosen_strategies as an empty list
    – FOR each player in num_players DO
      – Generate a random integer (random_num) between 0 and 2
      – Compute cumulative probabilities for the current player
      – SET chosen_strategy to the index of the first element in cumulative_probs that is greater than or equal to random_num
      – Append chosen_strategy to chosen_strategies
    – END FOR
    – PRINT 'Chosen Strategies:', chosen_strategies
    – Create a new record as a dictionary with 'Attacker' and 'Defender' values from chosen_strategies
    – Append the new record to the DataFrame (df)
    – WRITE the updated DataFrame to the Excel file (filename)
    – PRINT the updated DataFrame
13. PRINT 'Data successfully exported to Excel file:', filename
14. END

4. RESULTS AND DISCUSSIONS

In the simulation of the model, a dataset consisting of 10,000 records was generated for defence strategies and was played against the attackers' data. The simulation encompassed various

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

scenarios for the model. The outcomes derived from these simulations were documented, and performance evaluation was carried out based on the simulation results and presented as a result in the study. Specifically, the results based on the three scenarios for residual energy were presented in Figure 4(a), 5(a) and 6(a), respectively, defence success rate presented in Figure 4(b), 5(b) and 6(b) respectively and defensive redundancy presented in Figure 4(c), 5(c) and 6(c) respectively.

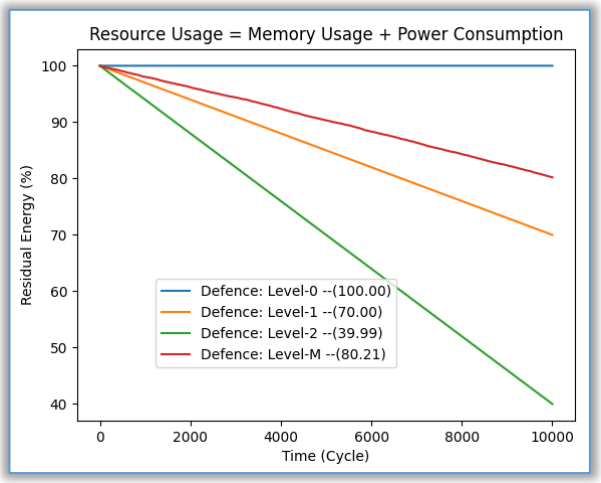

Figure 4(a): Residual Energy, when r >C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}

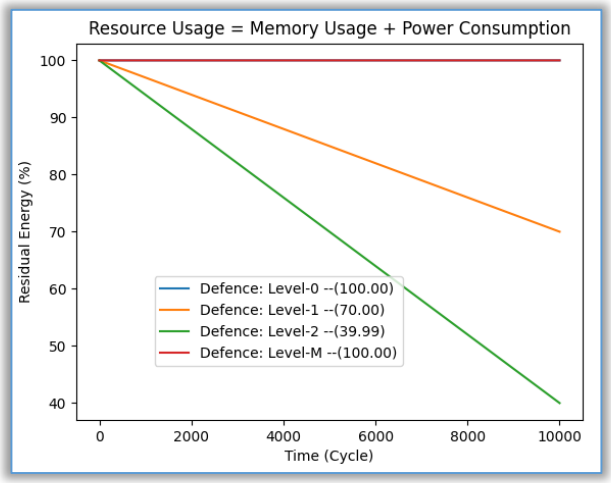

Figure 5(a): Residual Energy, when r <C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}

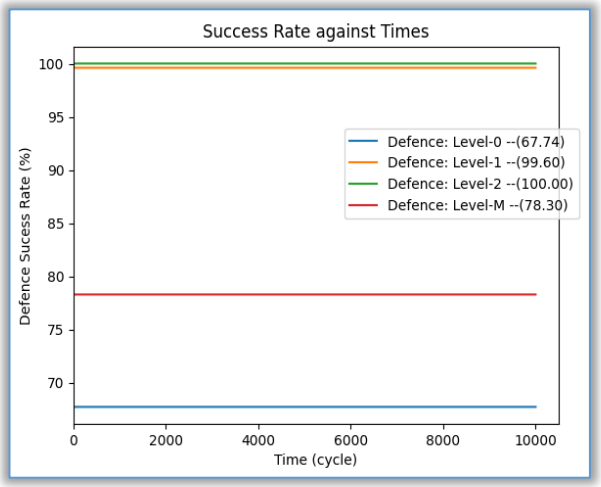

Figure 4(b): Defence Success Rate, when r >C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}

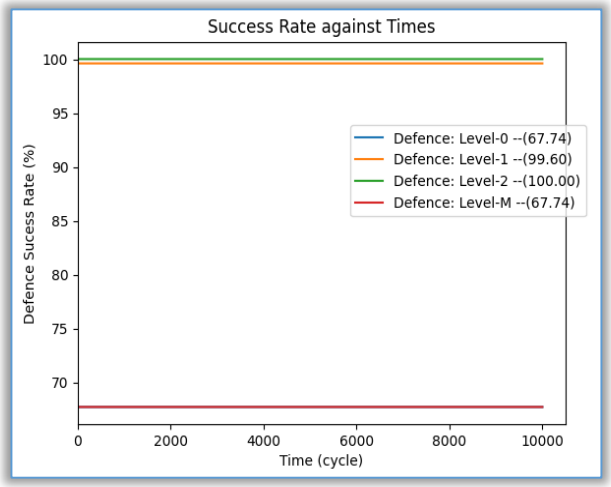

Figure 5(b): Defence Success Rate, when r <C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}

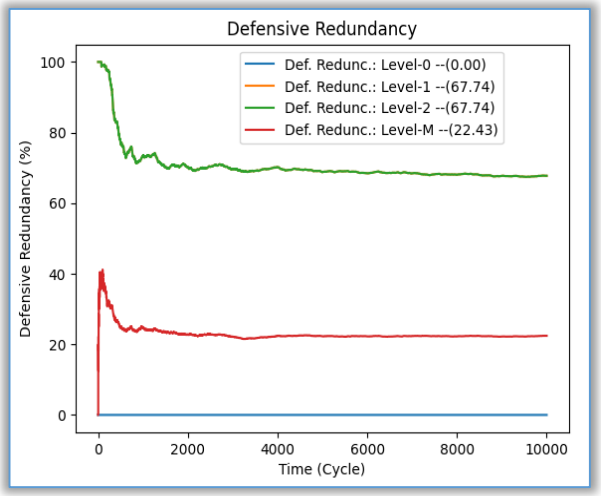

Figure 4(c): Defensive Redundancy when r >C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}.

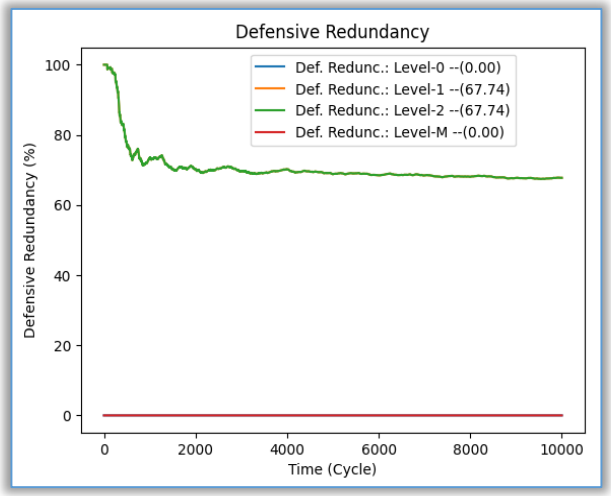

Figure 5(c): Defensive Redundancy when r <C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

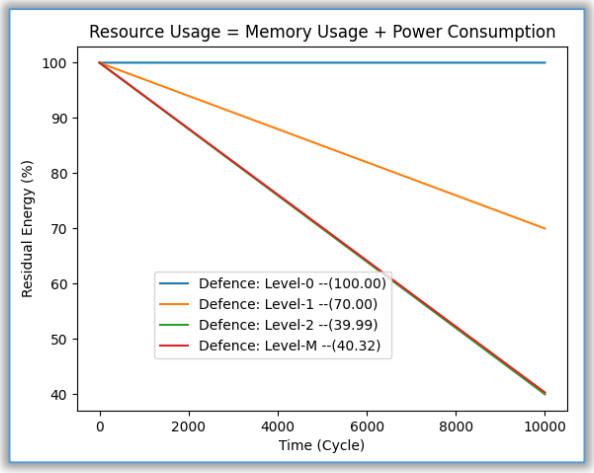

Figure 6 (a): Residual Energy, when r >>C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}.

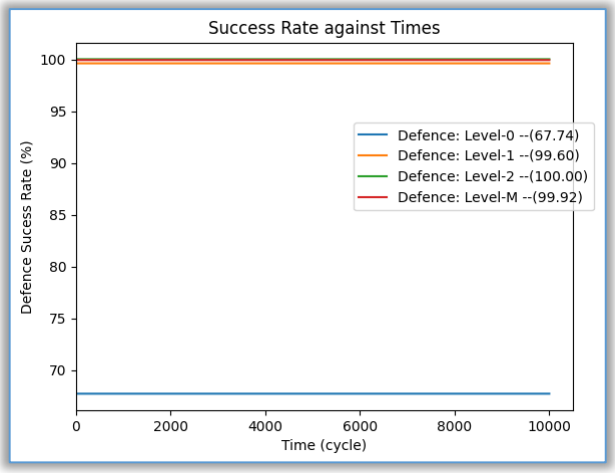

Figure 6(b): Defence Success Rate, when r >>C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}

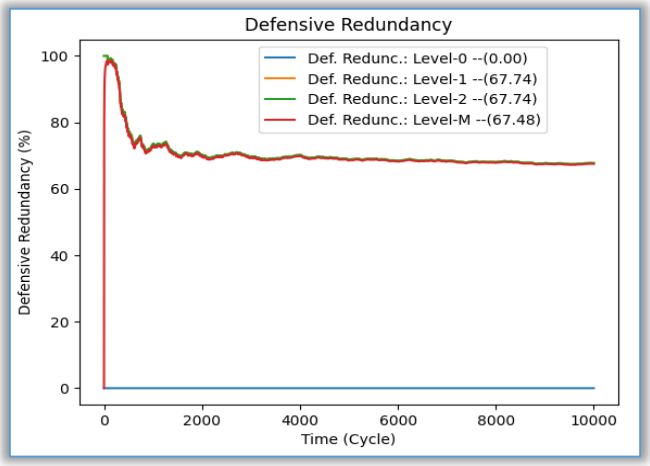

Figure 6(c): Defensive Redundancy, when r >>C_{dn}, C_{an}, n ∈ {0,1,2}, C_{dn}>C_{an}

The evaluation results show that the developed model performed excellently compared to the three static strategies, levels (0, 1, 2). In scenario 1, it was observed that the level–0 defence strategy completed the 10,000 cycles with 100% residual energy, and the level–M defence strategy, which is the model developed, exhibited a slightly lower performance with 80.21% residual energy. Surprisingly, level–2 defence strategy, which had the best defence success rate, achieved a residual energy of 39.9%. Level–M also exhibited superior performance compared to level–2, boasting a defensive redundancy of only 22.43% in contrast to level–2 that had 67.74%. This indicates that the new model (Level–M) effectively allocates resources, refraining from unnecessary defensive measures when no attack occurs. In scenario 2, Level M performed well by placing its residual energy at 100% and defensive redundancy at 0%; since resources under protection are less than the cost of defence, the new model (level–M) is sensitive to the cost implication. In scenario 3, the new model also performed well by putting a more defensive strategy in use since resources under protection are significantly greater than the cost of defence. This shows that the new model produced an economical defence mechanism.

5. CONCLUSION

The classification was done properly based on ideas emanated from experts referenced in this journal, it serves as an initial steppingstone for researchers and cyber security experts interested in crafting proactive defence strategies using game theory models. However, implementation of the model is essential to fine–tune and validate the framework's efficacy within real–world cyber security contexts.

The simulation results indicate that the formulated model (level M) in non–zero–sum approach holds promise in creating a best defence strategy model for cyber security prevention. It

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

demonstrates the potential to establish a powerful system based on the model developed within this work. Future researchers could expand this model by incorporating additional cyber–attack scenarios and constructing a practical system grounded in non–zero–sum, non–cooperative game theory.

References

[1] Abapour, S., Nazari–Heris, M., Mohammadi–Ivatloo, B., & Tarafdar Hagh, M. (2020). Game theory approaches for the solution of power system problems: A comprehensive review. Archives of computational methods in engineering, pp. 27, 81–103
[2] Adisa, S. P., Akanbi, C. O., & Ogundoyin, I. K. (2024). A framework for a game theoretic model for cyber threats prevention. FUOYE Journal of Engineering and Technology, 9(2), 195
[3] Afifi, M. A. (2020). Assessing information security vulnerabilities and threats to implementing security mechanism and security policy audit. Journal of Computer Science, 16(3), 321–329
[4] Attiah, A., Chatterjee, M., & Zou, C. C. (2018, May). A game theoretic approach to model cyber–attack and defence strategies. In 2018 IEEE International Conference on Communications (ICC) (pp. 1–7). IEEE.
[5] Azar, M. M., Monfared, M. A. S., & Monabbati, S. E. (2021). Non–cooperative two–player games and linear bi–objective optimization problems. Computers & Industrial Engineering, 162, 107665
[6] Bhuiyan, B. A. (2016). An overview of game theory and some applications. Philosophy and Progress, 111–128
[7] Ho, E., Rajagopalan, A., Skvortsov, A., Arulampalam, S., & Piraveenan, M. (2022). Game Theory in defence applications: A review. Sensors, 22(3), 1032
[8] Iqbal, A., Gunn, L. J., Guo, M., Babar, M. A., & Abbott, D. (2019). Game theoretical modelling of network/cyber security. IEEE Access, 7, 154167–154179.
[9] Naik, N. (2023). Implementation of techniques to avoid cyber–attacks. The Online Journal of Distance Education and e–Learning, 11(2).
[10] Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., Pallis, E., & Markakis, E. K. (2021). A survey on human and personality vulnerability assessment in cyber–security: Challenges, approaches, and open issues. arXiv preprint arXiv:2106.09986.
[11] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669–710
[12] Rawal, B. S., Manogaran, G., & Peter, A. (2023). Cyber security and Identity Access Management. Singapore: Springer.
[13] Zarreh, A., Wan, H. da, Lee, Y., Saygin, C., & al Janahi, R. (2019). Risk assessment for cyber security of manufacturing systems: A game theory approach. Procedia Manufacturing, 38, 605–612
[14] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cyber security. Ieee Access, 8, 23817–23837.
[15] Zhang, Y., & Malacaria, P. (2021). Bayesian Stackelberg games for cyber–security decision support. Decision Support Systems, 148, 113599

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665
copyright © University POLITEHNICA Timisoara, Faculty of Engineering Hunedoara,
5, Revolutiei, 331128, Hunedoara, ROMANIA
http://annals.fih.upt.ro