A Framework for a Game Theoretic Model for Cyber Treats Prevention

[1]Solagbade P. Adisa., [2]Caleb O. Akanbi., [2]Ibrahim K. Ogundoyin.
[1]Information and Communication Tech. Directorate, Federal Polytechnic Ede, Osun State, Nigeria,
[2]Information and Communication Technology Department, Osun State University, Osun State, Nigeria,
adisasp@federalpolyede.edu.ng | akanbico@uniosun.edu.ng | ibraheem.ogundoyin@uniosun.edu.ng

Received: 20-MARCH-2024; Reviewed: 09-MAY-2024; Accepted: 10-MAY-2024
https://dx.doi.org/10.4314/fuoyejet.v9i2.7

ORIGINAL RESEARCH

Abstract - The dynamic nature of cyber treats presents formidable challenges in thwarting and managing cyberspace. Conventional security measures often lag-behind swiftly evolving tactics employed by cybercriminals, necessitating a more proactive approach. This paper introduces a framework that advocates for the integration of game theory models to introduce strategies for preventing cyber threats. The framework explores how attackers and defenders interact in cyber fields using ideas from noncooperative non-zero-sum game theory and linear algebra. By comprehensively analyzing and modeling the decision-making processes of both parties, it becomes possible to implement proactive measures that fortify cybersecurity defense. Two distinct performance metrics—residual energy and success rate—were used to assess the model's effectiveness. The results show that, under realistic assumptions, the developed model achieved an excellent success rate of 99.65% and better residual energy compared to three other fixed-strategy defense systems. This implies that a noncooperative non-zero-sum approach can used to improve the system's defense against cyber threats.

Keywords- attack, cyber-attack, defense, game theory, prevention

1. INTRODUCTION

In contemporary society, computer networks play an integral role in our daily activities. The increasing prevalence of security threats has prompted a consistent shift towards prioritizing security considerations (Krejci, 2011). Network security begins with the authorization procedure, which is often carried out through a username and password. The objectives of a cyber-attack may include intentional destruction of systems, data theft, or the exploitation of a compromised computer as a launch point for subsequent attacks. The escalating occurrences of cyber-attacks and identity theft contribute to a pervasive sense of apprehension about the Internet. Given the substantial reliance of economic and communication infrastructures on computer networks and information technology, cyber-attacks emerge as a significant and escalating threat to our societal fabric (Jang-Jaccard & Nepal, 2014).

Network security becomes a challenging topic since numerous new network attacks have appeared increasingly sophisticated and caused vast loss to network resources (Liang & Xiao, 2013). Many critical infrastructures such as airports, hospitals, and oil pipelines have become potentially vulnerable to intentional cyber-attacks (Sokri, 2018; Johnson & Martinez, 2022). Because of the advent of new threats and attack vectors, the field of cybersecurity is constantly evolving. To keep ahead of cybercriminals, regular awareness and aggressive steps are required. Organizations must update and patch software on a regular basis, conduct security audits, and provide employee training to raise knowledge about potential dangers and proactive measures, such as penetration testing and vulnerability assessments, can be used in cybersecurity to uncover holes in systems before bad actors exploit them (Thomas et al., 2023; Rathore et al., 2020). In carrying out all these activities, organizations incur additional operational cost and disruption of service.

Artificial Intelligence (AI) and Machine Learning (ML) are essential technologies that can identify and react to cyber-attacks in real-time (Ji et al., 2022; Abu-Rahmeh, 2021). Game theory offers solution concepts that address the problem of allocating payoffs. The core is one such concept, which represents a set of payoff allocations where no coalition can obtain a higher total payoff by deviating from the allocation. The Shapley value and the Nash bargaining solution are other prominent solution concepts that provide ways to distribute the benefits of cooperation based on principles of fairness and bargaining power (Myerson, 1991).

Game theory, a sub-field of AI, has been applied in addressing cyber threats. A non-cooperative game theory has been adopted by (Amadi et al., 2017; Iqbal et al., 2019; Attiah et al., 2018; Zhang & Malacaria, 2021) in modelling attacker and defender relationship but ignored dynamic threats in favour of a static, game-theoretic model with a particular security attack or defence. However, few authors that concentrated on the dynamic model did not consider the intensities of

*Corresponding Author

Section B- ELECTRICAL/COMPUTER ENGINEERING & COMPUTING SCIENCES

Can be cited as:

Adisa S. P.., Akanbi C. O., Ogundoyin I. K. (2024) A Framework for a Game Theoretic Model for Cyber Treats Prevention, FUOYE Journal of Engineering and Technology (FUOYE**JET**), **9(2)**, **195-202.** **http://.doi.org/10.46792/fuoyejet.v9i2.7**

the attacks, the cost of defence and attack as well as 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. Hence, this study proposes a non-cooporative non zero sum game theoretic model approach for a cyberattacks prevention.

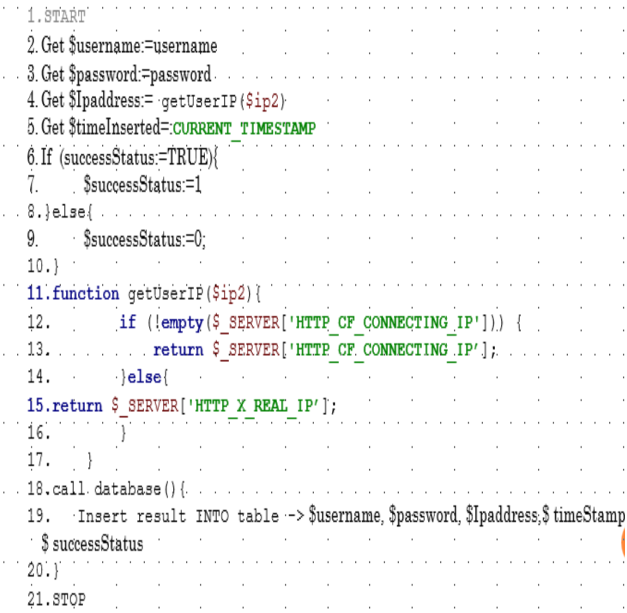
In this paper, a game-theoretic approach is employed to model the interaction between an attacker and a defender in a security context, mathematical models of strategic interaction among rational decision-makers (Myerson, 1991). The players, namely the attacker and defender, operate at three different levels of strategies: level-0, level-1, and level-2. For the attacker, level-0 represents no attack, level-1 indicates a low-intensity attack, and level-2 signifies a high-intensity attack. On the defender's side, level-0 implies no defense, level-1 denotes a low-intensity defense, and level-2 signifies a high-intensity defense. These strategy levels characterize the intensity of actions chosen for both attacking and defending. The objective is to find the optimal defense strategy based on an economic model, aiming to efficiently prevent the system from succumbing to attacks. The paper discusses the interplay between these strategies and how the game-theoretic framework aids in determining the most effective defense strategy against potential attacks. This approach allows for a nuanced understanding of security dynamics and aids in devising robust defense mechanisms.

A preventive optimization is included in the mathematical framework to reduce prior security risk, the optimization is modelled as a Bayesian Stackelberg game in which the defense has limited knowledge of the current attacker state. The proposed optimization is solved using the properties of totally unimodular matrices, strong duality, and MICP (MILP (Mixed-Integer linear programming), respectively.

Linear programming has been utilized in cyber-attack prevention, yet the capability to devise practical mathematical solutions to gaming problems remains a significant challenge within game theory (Amadi et al., 2017). Additionally, (Zarreh et al., 2019) tackled cybersecurity challenges in sophisticated manufacturing systems characterized by high-level computer-controlled integration. Their research proposed a method for constructing and addressing a game theory model, albeit with the simplification of employing zero-sum game theory, which may not reflect reality accurately.

(Sokri, 2020) presented a model where the attacker's objective is to minimize the risk of detection and punishment, while the defender aims to optimize resource allocation to maximize their payoffs. The methodology relies on a min-max approach, where the defender aims to minimize their maximum possible loss. However, the effectiveness of this method relies on the presence of a saddle point in the payoff matrix.

Figure 1: Web Scraping Algorithm for Data Collection



```
START
Get $username:=username
Get $password:=password
Get $Ipaddress:= getUserIP($ip2)
Get $timeInserted=:CURRENT_TIMESTAMP
If (successStatus:=TRUE){
      $successStatus:=1
}else{
      $successStatus:=0;
}
function getUserIP($ip2){
        if (!empty($_SERVER['HTTP_CF_CONNECTING_IP'])) {
            return $_SERVER['HTTP_CF_CONNECTING_IP'];
        }else{
return $_SERVER['HTTP_X_REAL_IP'];
        }
    }
call database(){
    Insert result INTO table -> $username, $password, $Ipaddress,$ timeStamp
 $ successStatus
}
STOP
```

Many researchers have adopted a non-cooperative game theory in modelling attacker and defender relationship but ignored dynamic threats in favour of a static, game-theoretic model with a particular security attack or defence (Afraa et al., 2018). However, few authors that concentrated on the dynamic model did not consider the intensities of the attacks, the cost of defence and attack as well as 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. Hence, this study proposes a non-corporative non zero sum game theoretic model approach for a cyberattacks prevention.

In summary, the investigation revealed that a game theory approach capable of accommodating dynamic scenarios and associated costs is yet to be introduced. Such an advancement is essential to develop a more effective and cost-efficient model for preventing cyber threats.

2. MATERIALS AND METHODS

Data was collected from three distinct websites, chosen carefully based on their relevance to the research and the availability of required data. Utilizing multiple sources ensured a comprehensive and diverse dataset, bolstering the validity and reliability of the research findings. The selected websites furnished valuable information aligned with the study's objectives and scope, facilitating a thorough analysis and interpretation of the gathered data. A Web Scraping Algorithm (see Figure 1) was employed to gather data from these websites, utilizing parameters such as Username, Password, IP Address, and Timestamp. For security purposes, usernames and passwords were encrypted. Analysis of timestamps enabled assessment of attack frequency and timing, thereby uncovering potential patterns or trends. The conceptual model diagram (Figure 2) provides a high-level overview of the theoretical framework or model being used. In this work, there are two players: attacker and defender.

The attacker or a normal node sends a message, the system performs login checks to authenticate the user.

The relevant information obtained from the login process is then sent to the database for storage and classification module for processing. Next, the information from the database is passed to the classifier module, which assists in the classification of the data. If there is no previous history available, a null value is sent. However, if there is a history, the classification module utilizes this information for classification purposes. The results from the classification module are then sent to the payoff determinant module. Simultaneously, the defender also sends their chosen strategy to the payoff determinant module. The payoff determinant module analyzes the strategies and determines the payoff or outcome of the game. The results and outcomes of the game are reported back to the database for future reference and analysis.

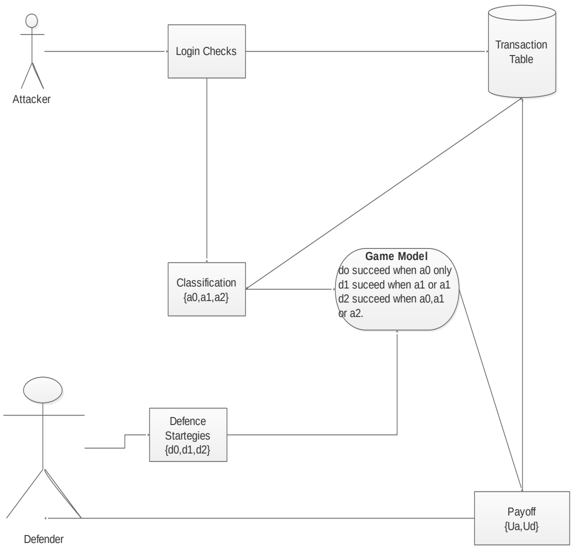
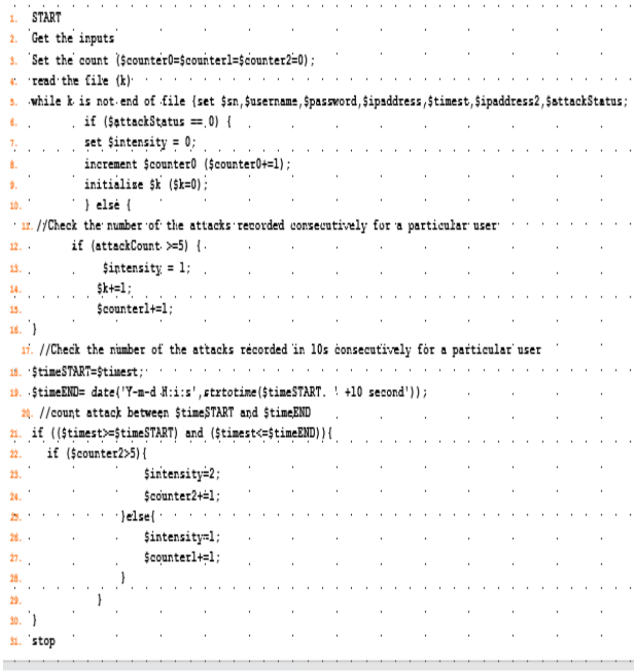


Figure 2: System Architecture of the proposed system

This allows for the collection and storage of valuable data related to the game outcomes, which can be used for further research, evaluation, and decision-making. By integrating the classification module, payoff determinant module, and database, the system enables the classification of messages, the selection of strategies, and the recording of game results. This comprehensive approach enhances the system's effectiveness in addressing security threats and facilitates the analysis of game outcomes for continuous improvement and decision support.

The parameters collected collectively contribute to the assessment of attack intensity (level 0, level 1, and level 2) through the utilization of a custom script (Figure 3) integrated into the login page of the three websites. This algorithm was developed from the rich idea gotten from experts' researchers and literatures relating to the research at hand. This custom script acts as a plugin and incorporates the analysis of parameters such as usernames, passwords, IP addresses, and timestamps. By leveraging this script, the research can evaluate the severity of the attacks based on the gathered data. The custom script serves as a valuable tool in categorizing and quantifying the intensity levels of the attacks, enabling a comprehensive analysis of the security threats faced by the websites under investigation.

A total of 255,000 records has been collected from the three websites for this research. After thorough analysis and classification, 125,728 records have been successfully classified. 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 further analysis and interpretation, enabling the research team to draw meaningful conclusions and contribute to the understanding of the subject matter.



```
START
Get the inputs
Set the count ($counter0=$counter1=$counter2=0);
read the file (k)
while k is not end of file {set $sn,$username,$password,$ipaddress,$timest,$ipaddress2,$attackStatus;
        if ($attackStatus == 0) {
        set $intensity = 0;
        increment $counter0 ($counter0+=1);
        initialize $k ($k=0);
        } else {
 //Check the number of the attacks recorded consecutively for a particular user
      if (attackCount >=5) {
           $intensity = 1;
          $k+=1;
          $counter1+=1;
}
 //Check the number of the attacks recorded in 10s consecutively for a particular user
$timeSTART=$timest;
$timeEND= date('Y-m-d H:i:s',strtotime($timeSTART. ' +10 second'));
 //count attack between $timeSTART and $timeEND
if (($timest>=$timeSTART) and ($timest<=$timeEND)){
  if ($counter2>5){
               $intensity=2;
               $counter2+=1;
             }else{
               $intensity=1;
               $counter1+=1;
             }
          }
}
stop
```

Figure 3: Classification Algorithm for Attackers' Strategies

https://dx.doi.org/10.4314/fuoyejet.v9i2.7

For modelling, the attacker's scenarios have been categorized into three distinct forms: no attack,

low-intensity attack, and high-intensity attack. Similarly, the defender's scenarios categorized as no defense, low-intensity defense, and high-intensity defense. This simplifies and enhances the explanatory power of the model. Both players select their strategies concurrently without any 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	87,931
1	Low Intensity Attack	37,132
2	High Intensity Attack	665
Total		**125,728**

The following assumption were made for the purpose of modelling a non-cooperative non-zero-sum game theory:

i. The value of resources under protecting (r) is always greater than the cost to defend (Cd_n) or attack (Ca_n) against them, as otherwise, the defender or attacker would not have any incentive to engage in defense or attack activities, respectively. In other words, ., $r > C_{an}, C_{dn}, n \in \{0,1, 2\}$.

ii. The cost to incur for the attack strategy a_1 (Attack-1) is less than the cost for attack strategy a_2 (Attack-2) for the attacker. Specifically, $ca_1 < ca_2$. By assuming that $ca_1 < ca_2$, we acknowledge that Attack-2 is a more potent and resource-intensive strategy for the attacker. In contrast, Attack-1 is characterized as a less resource-intensive strategy, implying that it may involve simpler methods, manual execution, or a lower scale of attack efforts. While Attack-1 may be less potent compared to Attack-2, it still poses a threat and can potentially compromise the security of the target system.

iii. This assumption recognizes that defend-2 is a stronger and active defense strategy compared to Defend-1. Defend-2 entails higher defense costs, indicating that it requires more resources, advanced technologies, or sophisticated countermeasures to implement successfully.

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:

i. In the following circumstances, the attack is successful:

   a. **Attack-1 vs. Defend-0**: The attacker's level 1 attack strategy is successful when the defender does not deploy any defense measures.

   b. **Attack-2 vs. Defend-1 or Defend-0**: The attacker's level 2 attack strategy is successful when the defender either uses the level 1 defense strategy or does not deploy any defense measures. These assumptions imply that the attacker's more advanced and aggressive attack strategy (Attack-2) has a higher likelihood of success compared to the less intensive attack strategy (Attack-1). Additionally, when the defender does not implement any defense measures, the attacker's success is almost guaranteed.

ii. The defense is successful under the following scenarios:

   a. **Defend-1 vs. Attack-1 or Attack-0:** The defender's level-1 defense strategy is successful in mitigating the attacker's level-1 attack or when no attack is launched.

   b. **Defend-2 vs. Attack-2 or Attack-1 or Attack-0:** The defender's level-2 defense strategy is successful in mitigating the attacker's level-2 attack, level-1 attack, or when no attack is launched. These assumptions recognize that the defender's more advanced and robust defense strategy (Defend-2) has a higher probability of success in countering both the advanced and less intensive attack strategies. The defender's level-1 defense strategy (Defend-1) is effective against the less intensive attack strategy (Attack-1) and when no attack is initiated.

iii. There is a gain 'r' for the defender when the attacker is unsuccessful, i.e., No-Attack vs. No-Defend. This assumption implies that when the attacker does not launch any attack and the defender does not deploy any defense measures, the defender gains a certain advantage or benefit represented by 'r'. This gain can be attributed to the defender's ability to maintain the system's security and protect valuable resources from potential attacks.

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 defense 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. 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-Defense Payoff Matrix

		Defense (D)			
		d_0	**d_1**	**d_2**	**Probability**
Attacker (A)	**a_0**	$0, r$	$0, r-c_{d1}$	$0, r-c_{d2}$	p_0
	a_1	$r-c_{a1}, -r$	$-c_{a1}, r-c_{d1}$	$-c_{a1}, r-c_{d2}$	p_1
	a_2	$r-c_{a2}, -r$	$r-c_{a2}, -r-c_{d1}$	$-c_{a2}, r-c_{d2}$	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.

$G = \{I, A, U\}$

$I = \{A, D\}$

$A = \{a_k, d_k \mid k \in \{0, 1, 2\}$

$U = \{U_a, U_d\}$

$$G = \{\{A, D\}, \{a_k, d_k \mid k \in \{0,1,2\}, \{U_a, U_d\} a \rightarrow A\ d \rightarrow D\} \quad (1)$$

Where;

$G = \text{Game}$, $I = \text{players(Attacker, Defender)}$,

$A = \text{Attacker}$, $S = \text{Strategies}$,

$D = \text{Defender/Administrator}$,

$ak = \text{Attacker Strategies}$,

$dk = \text{Defender Strategies}$,

$U = \text{Payoff/Utility}$,

$Ua = \text{Attacker Strategies}$,

$Ud = \text{Defender Strategies}$

also let; $\text{Cost of Attack} = Ca$,

$\text{Cost of Defendin} = Cd$,

$\text{Resources Protecting} = r$

Let p_0, p_1, p_2 be the propability that the attacker A choose strategy level 0, 1, 2 respectively and q_0, q_1, q_2 be the probability that the defender D choose strategy level 0, 1, 2 respectively.

Where;

p_0 is the probability of attacker plays attack level 0 (ie. a_0), p_1 is the probability of attacker plays attack level 1 (ie. a_1), p_2 is the probability of attacker plays attack level 0 (ie. a_2) and q_0 is the probability of defender plays defend level 0 (ie. d_0), q_1 is the probability of defender plays defend level 1 (ie. d_1), $q_2$is the probability of defender plays defend level 0 (ie. d_2)

The payoff matrix in Table 2 does not have a saddle point, also known as an equilibrium in game theory, where a value is the largest in its column and the smallest in its row. As a result, the model's Mixed Strategy Nash Equilibrium (MSNE) was solved algebraically. In this work, players adopt probability distributions over their strategies in such a way that their opponents are indifferent among their available strategies. In other words, each player is using a mixed strategy (a probability distribution over their available strategies) that makes their opponent indifferent to the choices they make. This equilibrium concept reflects a balance where neither player has an incentive to unilaterally deviate from their chosen strategy, given the mixed strategies chosen by the other player.

A probability distribution P over the set of pure strategies S for every participant in the security preventative game is such:

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

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

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

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

In the context of the game, $eU(p_n)$ 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 of attack-n, the payoff or reward associated with a successful attack, and the likelihood of encountering different defense 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. Likewise, $eU(q_0)$ represents the expected utility for the defender when playing strategy level-0, also known as defend-0. $eU(q_1)$ represents the expected utility for the defender when playing strategy level-1, also known as defend-1. $eU(q_2)$ represents the expected utility for the defender when playing strategy level-2, also known as defend-2.

In the context of the game, $eU(q_n)$ 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 defense against cyber attacks.

The various outcomes and their probabilities associated with any combination of attacker and defender tactics can be evaluated to determine the expected payout of attacker A for playing a0, a1, and a2 when defender D chooses methods d0, d1, and d2, respectively. The average payout that the attacker expects to receive across several game plays is represented by the expected payoff. We consider the payoff matrix, which contains the profits or rewards for various combinations of attacker and defender methods, 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, this equations can be obtained.

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

$$eU(p_1) = q_0(r - ca_1) + q_1(-ca_1) + q_2(-ca_1) \quad (6)$$

$$eU(p_2) = q_0(r - ca_2) + q_1(r - ca_2) + q_2(-ca_2) \quad (7)$$

By substituting equations (5), (6), and (7) into equation (3), we obtain the probability distribution q_0, q_1 and q_2. The probabilities q_0, q_1 and q_2 are determined based on the expected utilities $eU(q_1)$, $eU(q_1)$, and $eU(q_2)$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.

$$q_0 = \frac{ca_1}{r},\ q_1 = \frac{ca_2 - ca_1}{r},\ q_2 = 1 - \frac{ca_2}{r}, \quad (8)$$

Similarly, the expected payoff of defender D for playing d_0, d_1, and d_2 when attacker A selects strategies a_0, a_1 and a_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.

$$eU(q_0) = p_0(r) + p_1(r - cd_1) + p_2(r - cd_2) \quad (9)$$

$$eU(q_1) = p_0(-r - cd_1) + p_1(r - cd_1) + p_2(r - cd_1) \quad (10)$$

$$eU(q_2) = p_0(-r) + p_1(-r - cd_1) + p_2(r - cd_2) \quad (11)$$

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

$$p_0 = 1 + \frac{cd_1 - cd_2}{r},\ p_1 = \frac{cd_1}{2r},\ p_2 = \frac{2cd_2 - 3cd_1}{2r} \quad (12)$$

The simulation utilized the Python programming language environment, 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 in a randomized mode. Two metrics was employed, Success Rate 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 "r" represents the resources allocated to protection, and considering different scenarios based on the relative values of r, Cost of Defense (C_{dn}), and Cost of Attack (C_{an}), the following scenario was considered:

1. When r is higher than Cost of Defense (C_{dn}) and Cost of Attack (i.e. r >C_{dn}, C_{an}, n Є {0,1,2}, and the Cost of Defense is higher than Cost of Attack (i.e. C_{dn}>C_{an}).
2. When r is lower than Cost of Defense (C_{dn}) and Cost of Attack (i.e. r <C_{dn}, C_{an}, n Є {0,1,2}, and the Cost of Defense is higher than Cost of Attack (i.e. C_{dn}>C_{an}).

Overall, the relative values of "r", C_{dn}, and C_{an} provide insights into the resource allocation and strategic considerations for defense and attack. These scenarios highlight different resource allocation strategies and the balance between defense and attack in relation to their respective costs.

3. RESULTS AND DISCUSSIONS

In the conducted simulation, a dataset comprising 10,000 records was generated to evaluate defense strategies in various scenarios. The model was played against the collected data, and the outcomes were documented and presented as preliminary results in this paper. Specifically, the preliminary results for residual energy were illustrated in Figure 4(a), and success rates were depicted in Figure 4(b). The defender had the option to employ different strategies, labelled as level-0, level-1, level-2, and level-Real. Level-0 signified no defense, level-1 indicated low-intensity defense, level-2 denoted high-intensity defense, while level-Real represented the strategy derived from the developed model.

In Figure 5(a) and 5(b), the results for level-0 showed a 100% residual energy and a 93.7% success rate, indicating that no defense was utilized. For level-1, there was a 70% residual energy and a 100% success rate, suggesting that 30% of energy was expended, and level-1 attacks constituted the highest threat level by the attacker. This enabled the defender to achieve a 100% success rate at level-1 defense. Level-2 exhibited a 39.99% residual energy with a 100% success rate, indicating that 60.01% of energy was used. Level-Real showed a 46.66% residual energy and a 99.65% success

https://dx.doi.org/10.4314/fuoyejet.v9i2.7

rate, signifying that 53.04% of energy was utilized. These results aligned with the expected outcomes of the proposed defense strategy.

In the second scenario, residual energy and success rates were presented in Figure 5(a) and Figure 5(b), respectively. Level-Real exhibited a 100% residual energy, while level-2 showed 39.99%, indicating that the developed model is sensitive to economic factors, making it dynamic. When the resource under protection is valued lower than the cost of defense, defending becomes impractical, resulting in potential losses. The implication of these findings is that level-Real produced superior results compared to other defense strategies (levels).

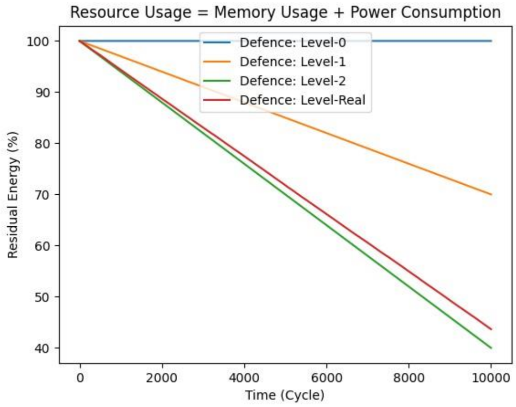


Figure 4(a): Residual Energy, when r >Cdn, Can, n ϵ {0,1,2}, Cdn>Can

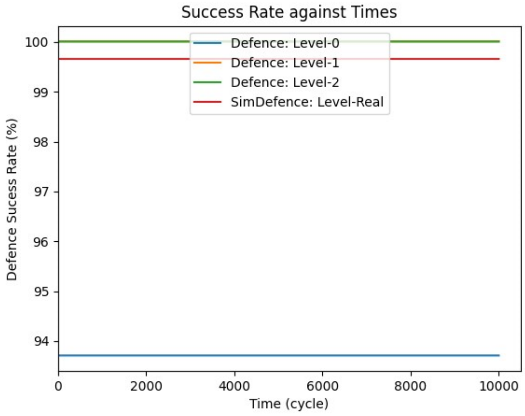


Figure 4(b): Success Rate, when r >Cdn, Can, n ϵ {0,1,2}, Cdn>Can

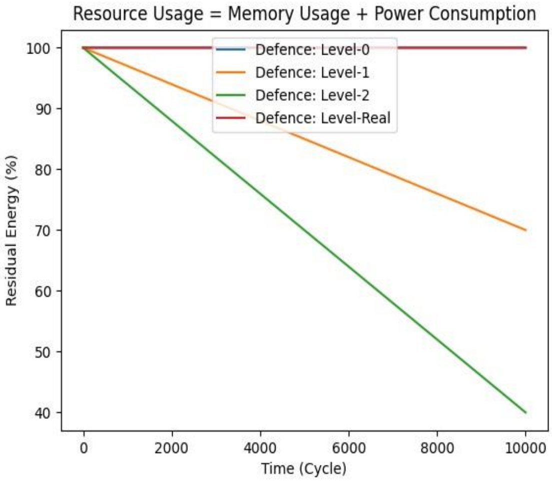


Figure 5(a): Residual Energy, when r <Cdn, Can, n ϵ {0,1,2}, Cdn>Can

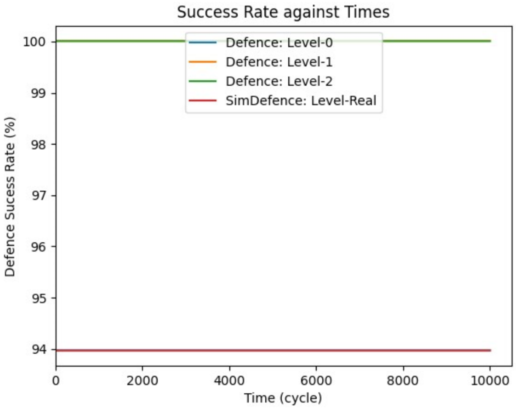


Figure 5(b): Success Rate, when r <Cdn, Can, n ϵ {0,1,2}, Cdn>Can

4. CONCLUSION

The framework introduced in this work serves as an initial stepping-stone for researchers and cybersecurity experts interested in crafting proactive defense strategies using game theory models especially using non-cooperative and non-zero-sum. The simulation results indicate that the non-zero-sum approach holds promise in creating a robust and economical model for cybersecurity prevention, which was not captured in the previous research. It demonstrates the potential to establish a powerful system based on the model developed within this framework. However, further research and collaboration are essential to fine-tune and validate the framework's efficacy within real-world cybersecurity contexts. Future researchers could expand this model by incorporating additional cyberattack scenarios and constructing a practical system grounded in non-zero-sum, non-cooperative game theory.

Declarations

Ethics approval and consent to Participate

Not applicable

Consent for Publication

Not applicable

Availability of data and materials

Data will not be shared. It was got from data scrapping of selected institutions and it a sensitive information.

Competing interests

The authors declare that no competing interests related to the research presented in this paper. There are no financial or non-financial conflicts of interest that could be perceived to influence the work.

Funding

Not applicable

Authors' contribution

Author 1 is responsible for most of the research activities, including manuscript preparation, data gathering, model development, simulations, and results discussion. Authors 2 and 3 are primarily involved in supervising the entire research process, providing technical guidance, and contributing their expertise. They also read and approved the final manuscript.

Acknowledgements

This work was supported by Engr Dr. Adebisi Adetunji and Engr. Abdulwakil Adekunle Kasali

REFERENCES

Abu-Rahmeh, A., Alsmadi, I., & Chaudhry, S. A. (2021). Detection and classification of malware using machine learning: A survey. IEEE Access, 9, 38406-38426.

Amadi Emmanuuel Chukwudi, Eze Udoka, & Ikerionwu Charles. (2017). Game Theory Basics and Its Application in Cyber Security. Advances in Wireless Communications and Networks, 3(4), 45. https://doi.org/10.11648/j.awcn.20170304.13

Attiah, A., Chatterjee, M., & Zou, C. C. (2018). A Game Theoretic Approach to Model Cyber Attack and Defense Strategies.

Iqbal, A., Gunn, L. J., Guo, M., Ali, B. M., & Abbott, D. (2019). Game theoretical modelling of network/cybersecurity. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.294835

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005.

Ji, Y., Yu, L., Li, S., & Zhang, X. (2022). Artificial Intelligence-Based Cybersecurity Defense Technologies: Advances, Challenges, and Opportunities. *IEEE Transactions on Big Data, 8*(3), 808-822.

Johnson, R., & Martinez, S. (2022). Cyber attacks targeting physical systems: A comprehensive analysis. Journal of Cybersecurity, 12(4), 345-362.

Krejci, R. (2011). Network Security Monitoring of Smart Home System. Czech Republic: Masaryk University.

Liang, X., & Xiao, Y. (2013). Game theory for network security. IEEE Communications Surveys and Tutorials, 15(1), 472–486. https://doi.org/10.1109/ SURV.2012. 062612. 00056

Myerson, R. B. (1991). *Game Theory*. Harvard University Press. Available: https://books.google.com.ng/books?id=1w5PAAAAMAAJ.

Rathore, S., Kim, D. H., & Baik, D. K. (2020). Cybersecurity Risks and Countermeasures in the Era of Industrial IoT. *IEEE Communications Surveys & Tutorials*.

Sokri, A. (2018). Optimal Resource Allocation in Cyber-Security: A Game Theoretic Approach. Procedia Computer Science, 134, 283–288. https://doi.org/10.1016/j.procs.2018.07.172

Sokri, A. (2020). Game theory and cyber defense. In International Series in Operations Research and Management Science, 280, 335–352. Springer New York LLC. https://doi.org/10.1007/978-3-030-19107-8_18.

Thomas, R., et al. (2023). Building a resilient cybersecurity framework: Best practices for organizations. Journal of Information Assurance and Security, 18(2), 91-108.

Zarreh, A., Wan, H. da, Lee, Y., Saygin, C., & al Janahi, R. (2019). Risk assessment for cybersecurity of manufacturing systems: A game theory approach. Procedia Manufacturing, 38, 605–612. https://doi.org/10.1016/j.promfg.2020.01.077.

Zhang, Y., & Malacaria, P. (2021). Bayesian Stackelberg games for cyber-security decision support. Decision Support Systems, 148. https://doi.org/10.1016/j.dss.2021.113599.