Application of Deception Technique for the Management of Zero-Day Exploit

Nyia Okechukwu C.[1*], Gilbert Aimufua.[1], Julius Adebowale M.[2], Victor Emmanuel Kulugh[3]

[1]Centre for Cyberspace; Nasarawa State University, Keffi (NSUK), Nigeria

[2]Department of Computer Science, Baze University Abuja

[3]Department of cybersecurity, Bingham University, Karu

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2025.100800002

Received: 18 July 2025; Accepted: 24 July 2025; Published: 27 August 2025

ABSTRACT

Zero-day exploit has remained one of the main challenges facing network administrators over the years; while several studies have been proposed to help solve this problem, the need for a deception model which is reliable remains a gap. The aim of this study is deception technique for zero–day exploit management. The methodology used is quantitative. The testbed under study is Ethnos cyber limited. The research method are modelling of the network facility, formulation of vulnerability problem, proposed behavioural analytical model using Stochastic Game Theory (SGT) technique, modelling of the decoy facility with honeypot techniques, modelling of the decoy vulnerability with honeypot techniques, then modelling of the new deception technique for zero-day attack management. To implement the new security solution on the testbed, python programming language was applied, while the data used for the coding was collected from the testbed. Simulation was applied for the testing of the new security model using data collected from the testbed. Metrics such as Attack Diversion Rate (ADR), Honeytoken Activation Rate (HAR), Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate (FPR), vulnerability conviction rate and exploitability rate were all applied to evaluate the model performance. The ADR reported as 91.56%, MTTD recorded as 5.96s, while the rate of honeypot activation was measured as 87.45%. The exploitability and conviction rate of the honeytoken reported 0.6 and 0.98 respectively. MTTR reported 10.04s, while the false positive rate reported an average of 3.07%.

Keywords: Zero-Day; Deception Technique; Exploit; Attack; Stochastic Game Theory; Honeypot

INTRODUCTION

Globally, one of the main challenges facing computer system networks is Zero-Day Attack (ZDA). Sarhan et al. (2022) defines ZDA as an unknown cybersecurity vulnerability, which hackers exploit to illegally penetrate and attack a network. The ZDA are made up of three components which are vulnerabilities, exploits and attacks. The vulnerabilities are inherent flaws or defects in the network hardware and software vulnerability exploitation components. This may result from human error, delayed patch and updates, legacy systems, technical glitches, insider attack, etc. (Reddy et al., 2024; Roumani, 2021). These vulnerabilities include weak passwords, outdated software, outdated network technologies, etc., and are classified based on their severity in the Common Vulnerabilities and Exposure (CVE) list, which is a catalogue of computer network vulnerabilities (SakthiMurugan et al., 2023). Zero-day exploits on the other hand refers to codes, software, tools or techniques used by cyber-attackers to identify and take advantages of the vulnerabilities within a

network, unknown to the administrators (Singh, 2019). In order words, the zero-day exploit is a process of identifying vulnerability within a network and then flagged as pathway for zero-day threat actors to gain unauthorized access and then inflict cyber-attack through the deployment of weaponized tools such as malware, wormholes, virus, etc. (Teymourlouei et al., 2023; Topcu et al., 2023).

Among these three components of zero-day, vulnerability is the most prioritized for cyber criminals. According to Zahoora et al., (2022) and Peppes et al. (2023), zero-day vulnerabilities are highly valuable in the underground market when auctioned by threat actors (groups of hackers who actively search for vulnerabilities in computer networks, software or hardware for exploitation), and are exploited for ZDA. For instance, in 2022, the Google project zero team reported 18 different ZDA (Schiaffino et al., 2023). Another example is the Microsoft CVE-2016-067 vulnerability threat on windows machine (Sharukh, 2020). Furthermore, Peppes et al. (2023) reported a major hit on different organizations such as Google, Yahoo, Morgan Stanley, etc. which affected millions of users due to its severity. These impacts of ZDA necessitate the need for Vulnerability Management (VM).

VM refers to the systematic process of identifying, classifying, prioritizing, and addressing security vulnerabilities in software and IT infrastructure. In traditional models, this involves patching known vulnerabilities and deploying security tools such as firewalls, intrusion detection systems, and antivirus systems to reduce the attack surface. However, the nature of zero-day vulnerabilities complicates this process since these flaws are unknown until actively exploited by attackers.

Deception technology is defense tactics which employ deceptive tools to divert attacker away from original network infrastructure to a decoy facility, and have been engages for ZDA detection, monitoring and mitigation (Tan et al., 2022; Sayed et al., 2023; Oluoha et al., 2021; Nandakumar et al., 2022). In Sivamohanet al. (2022), deception technique was identified as one of the most researched defence strategies in cyber security studies due to several advantages it provides, particularly decoy and threat intelligence.

Popular deception methods include Honey-X, camouflaging, mimicking, etc. (Oluoha et al., 2021). Among the deception methods, Honey-X (Niakanlahajiet al., 2020) has been widely used by researchers (Perkins and Howell, 2021; Sivamohanet al., 2022; Morozov et al., 2023) for ZDA management. This study suggests an advanced deception paradigm for zero-day attack management in order to overcome these issues. This will be accomplished by implementing an Advanced Game Theory (AGT) technique. The AGT model will manage attack by treating the interaction between attackers and defenders as a strategic game, where defender actions are based on anticipating the most likely vulnerabilities attackers will exploit. It dynamically adapts its deception strategies in real time, responding to attacker behaviour and making vulnerabilities harder to exploit. By optimizing resource allocation and prioritizing critical vulnerabilities, the model ensures efficient defence against zero-day threats while minimizing risks to the system. This proactive, strategic approach enhances the overall management and mitigation of vulnerabilities, especially those not yet known or fully understood.

RESEARCH METHODOLOGY

The type of research design used is the quantitative. The research methodology used is experimental design which takes a systematic approach that includes identification of the problem, proposing solution to the problem identified, modelling the proposed solution, programming it on a testbed, testing and then validating its performance. The research method takes a systematic which began with the modelling of the problem through description of the network environment and then potential zero-day vulnerability. This modelling forms the testbed under study. Then behavioural analytical model was modelled using stochastic game theory approach. The decoy environment was modelled with honeypot, while decoy vulnerability was introduced on the decoy environment using honeytoken. The methods were integrated as decoy approach for zero-day attack management. To simulate the solution, data as collected from Ethnos cyber limited and then applied to implement the solution through python programming language. Simulation approach was applied for the testing process, while comparative analysis was applied as technique to validate the system. The Figure 1 summarized the research methodology.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

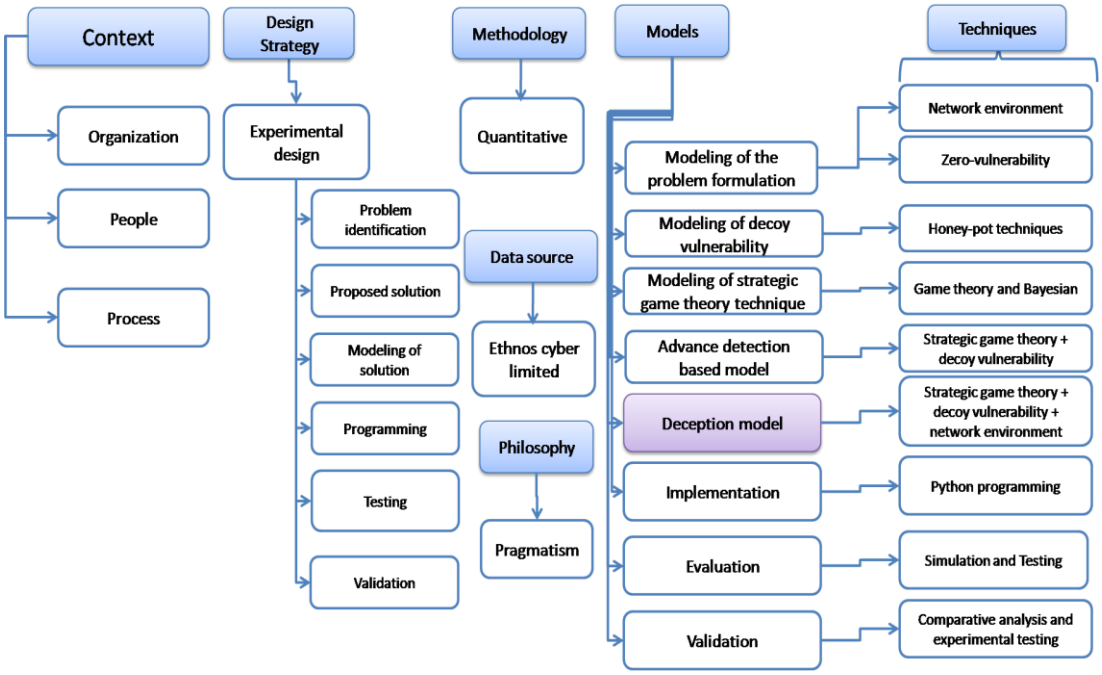

Figure 1: Block diagram of the research methodology

Data collection

The data used for this was collected from Ethnos Cyber Limited, No: 2071 Muri Okunola St, Victoria Island, Lagos Nigeria. The collected data model a network environment with zero-day vulnerabilities, simulated threat features, and several attack vectors as shown in Table 1

Table 1: Simulation parameters (Source: Ethonos Cyber Limited)

Variable	Description	Value
S_i	Real system (target)	1
H_i	Honeypots in the network	3
T_j	Honeytokens in each honeypot	3
$P(H_i)$	D	0.4-0.7
SGT	Simulated threat features	30000
$B(T_j)$	Believability of honeytoken T_j	0.5-0.9
$E(T_j)$	Exploitability of honeytoken T_j	0.6-0.8
u_d	Defender's utility function	5-10
u_A	Attacker's utility function	1-3
T_{delay}	Time delay before attacker identifies a decoy	30-120
$P(detection)$	Probability of detecting an attacker interaction	0.8-0.95
$P(interaction\ wi$	Probability of interacting with honeytoken T_j	0.5-0.85
t_{attack}	Time window for each attacker action	30-600
$t_{simulaiton}$	Total simulation time	100
$n_{attacker}$	Number of attackers involved in the simulation	1-5
n_{normal}	Number of normal users interacting with the system	10-20
$P(S_r)$	A))	0.1-0.2

The Proposed Deception Technique for Zero-Day Attack Management

The proposed system is made of three different approaches which are an improved game theory approach, honeypot and honeytoken. The improved game theory optimizes decision making to differentiate between

attacker and legitimate user. Upon attacker identification, access to decoy facility is granted which looks exactly like the main network facility and developed using honeypot techniques. To ensure that the attacker remains on the decoy facility, decoy vulnerabilities are strategically placed on the network environment using honeytoken technique. This ensures that the attacker remains on the fake network facility, while the threat intelligence and response are automatically initiated. The Figure 2 presents the proposed system block diagram.

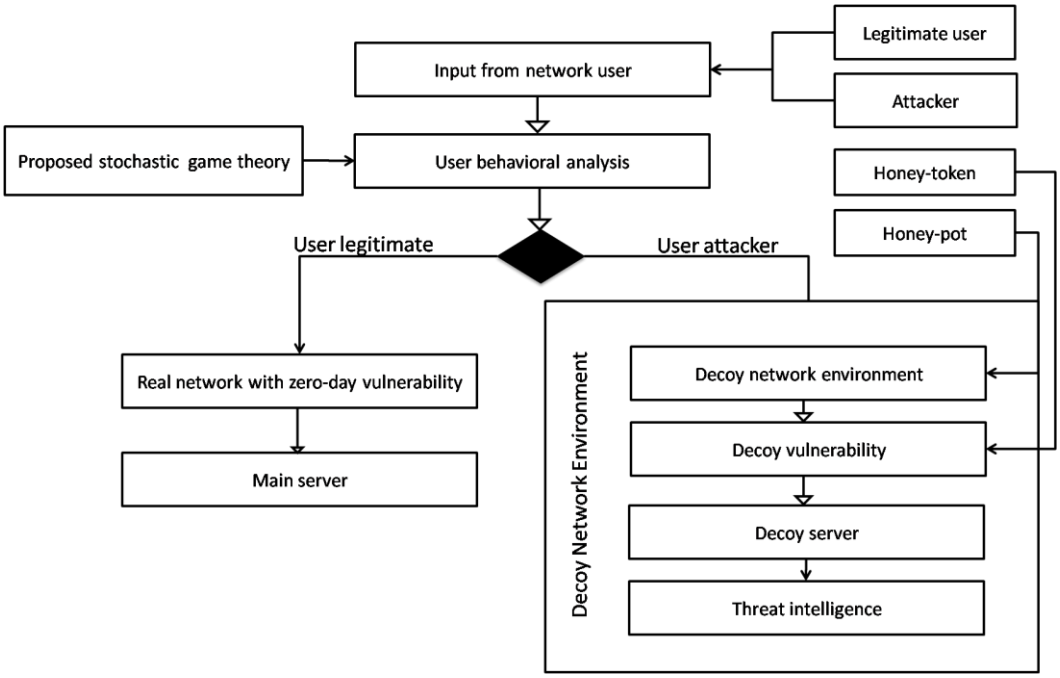

Figure 2: Proposed deception technique for zero-day attack management

The Proposed User Behavioral Analytical Model using Optimized Stochastic Game Theory Approach (GTA)

Behavioral analysis is aimed at identifying an attacker and a legitimate user through actions. Normally attackers always masquerade themselves to appear like a legitimate user and exploit vulnerability, while legitimate users always interact with the network normally as expected. Game theory is a popular approach employed in cyber security studies to characterize this behavior and classify legitimate users and attacker (Hausken et al., 2024). However, due to the dynamic nature of attacker's behavior, conventional game theory approaches suffer issues of false positive, misclassification and hence raise a question of reliability, thus necessitating the need for optimized game theory approach for behavioral analysis (Hattori et al., 2018; Douha et al., 2023). The basic component of game theory is made of players, state space, action and payoff functions as shown in Figure 3. The state space is defined as equation 1;

$$S = \{s_1, s_2, s_3, s_4\} \quad (1.0)$$

Where s_1 is suspicious activities, s_2 behavior of potential suspected attacker, s_3 is the confined attacker and s_4 is legitimate user. The actions are grouped into the defender action A_d, attacker action A_a and legitimate users actions A_l. Let A_d= $[a_d^1$ (continuous monitoring),a_d^2 $(allow\ decoy\ if\ attacker)$,$a_d^3$ $(allow\ if\ legitimate)]$. Let $A_a = [a_a^1(attempt\ to\ exploit), a_a^2\ (masqurade\ as\ legitimate\ user)]$; While Let $A_l = [a_l^1(access\ to\ system), a_l^2$(exit access). The payoff function for each payer is determined based on the behavioral analysis for legitimate user, defender or attacker. The defender payoff attacker is defined as equation 2.0.

$$P_d = [s, a_d, a_A\ and\ a_l] \quad (2.0)$$

Where attacker payoff is $P_A\ [s, a_d, a_A]$, while legitimate user payoff $P_l = [s, a_d, a_l]$. (Mejdi and Ezzedine, 2024). The transition state is defined as equation 3;

$T: S * A_d * A_a * A_l \; tends \; to \; [0,1].$ (3.0)

This transition probabilities is the state change from s to s' when action is taken.

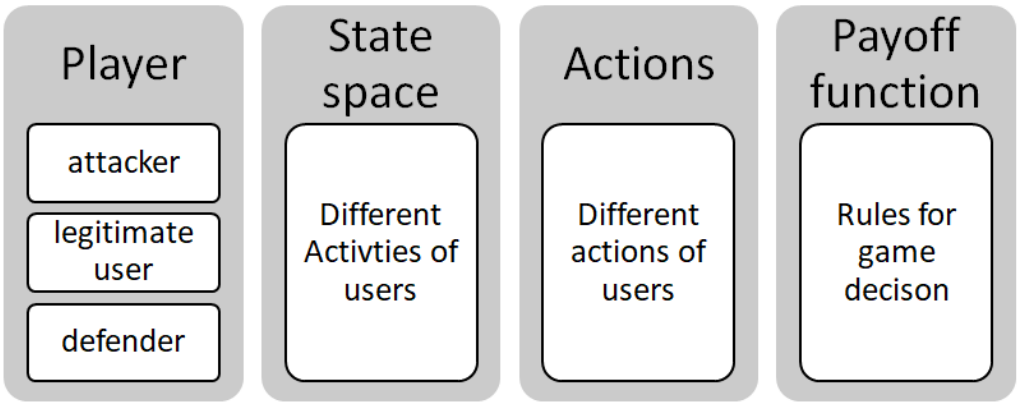

Figure 3: Component interaction diagram of game theory

The players in Figure 3 are the defender, attacker and legitimate users.

The rules for game decision are as follows;

1. Receive reward R_{wd} if the defender's identification of the attack is accurate.
2. Else if, incur C_d^A (where C is the cost function) if the defender set a valid user to decoy if true.
3. Else if, you will pay C_d^A if the defence is unable to identify the attacker. If the attacker avoids detection, then the reward is R_{wdA}.
4. Else if, suffer C_A if the attacker is set to decoy. Otherwise, receive the reward R_{wdl} if legitimate access is granted.
5. Else if, incur C_l if the legitimate is set to decoy.

The Deception Network Model Using Honeypot

In achieving this objective, the aim is to create a decoy network environment which looks similar with the real network, but has several decoy vulnerabilities. The network decoy network environment was developed with honeypot while the decoy vulnerabilities are deployed with honeytoken (Sivamohan et al., 2022).

Let the Real system (S_r), represents the actual network, Honeypots (H_i) which constitutes the decoy system made of $H_1, H_2, \ldots \ldots \ldots \ldots \ldots \ldots \ldots H_n$ to mimic the real network. Then the honeynet H_{net}, which is a collection of several honeypots. The honeynet presents the attacker to with multiple decoy vulnerabilities, while the honeytoken are placed inside the honeypot to model vulnerabilities. To make these honeypots adaptive and hard for attackers to detect, the Equation 1 was to model the honeypot as high interactive adaptive system, considering the state of the honeypot $\sigma_i(t)$, attack vector $A_i(t)$ and defence strategy $D_i(t)$ at H_i at time t.

$$\sigma_i(t+1) = f\big(\sigma_i(t), A_i(t), D_i(t)\big) \quad (4.0)$$

These adaptive honeypot models can switch between multiple decoy configurations $\sigma_i(t)$, to mimic real world vulnerabilities. To model the interaction between the attacker and the adaptive honeypot, a Markov decision model was applied in Equation 5 (Sivamohan et al., 2022).

$$P\left(\sigma_i(t+1) | \sigma_i(t), A_i(t), D_i(t)\right) = \pi(\sigma_i(t+1)) \quad (5.0)$$

Where $\pi(\sigma_i(t+1))$ is the probability of transition to new state of honeypot to ensure that attackers continuously face difficulty in differentiating a real and decoy facility.

Honeytoken are deployed as potential decoy vulnerability inside the honeypot and are explorable by attackers. Let the honeytoken based dynamic vulnerability be defined as T_j. Each honeypot H_i is injected with multiple

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

honeytokens defined as $T_1, T_2, \ldots\ldots\ldots\ldots\ldots\ldots T_n$, with n representing the number of placed honeytoken within the honeypots, while T_n model different decoy vulnerabilities within the network. To dynamic nature of the T_n is described as a state function θ_j and changes over (t). The conviction rate of B (T_j) and the exploitation rate $E(T_j)$ by attacker is defined as Equation 6 and 7;

$$B(T_j) = \frac{1}{1+e^{-\alpha_j \cdot A(t)}} \quad (6)$$

$$E(T_j) = \frac{1}{1+e^{-\beta_j \cdot A(t)}} \quad (7)$$

Where the function of attractiveness and exploitability by an attacker $A(t)$ of the vulnerabilities are represented as α_j and β_j. These Equations 3 and 4 implied that as attacker interacts with honeypot, the honeytokens adapts to make the attacker believe that vulnerabilities are real and exploitable.

Integrating the Stochastic Game Theory (SGT) Model with Honeypot and Honeytoken

This section presents a system integration of the stochastic game theory with the decoy network environment for the management of zero-day vulnerability. In this case let the strategy of attacker and defender was used to define the state transition and outcomes as a stochastic game. The defender objective function is minimizing chances hatattacker reaches the main network environment, though the maximization of $H_i$and T_n. Let the real network S_r and H_i be used to maximize the goal as in Equation 8;

$$u_d = \sum_{i=1}^{n} P(H_i|D) \sum_{j=1}^{k} . B(T_j).E(T_j) \quad (8)$$

Where u_d is the utility function of the defender and models the overall effectiveness of diverting attacker to the decoy honeypot environment and trapped with the honeytoken decoy vulnerabilities. The attacker objective function is to identify S_r , while avoiding $H_i$and T_n. This goal can be minimized by the defender as Equation 9. The architecture of the honeypot network with decoy vulnerability is presented as Figure 4.

$$u_A = P(S_r|A).\ (1 - \sum_{i=1}^{n} P(H_i|A) .B(T_j).E(T_j) \quad (9)$$

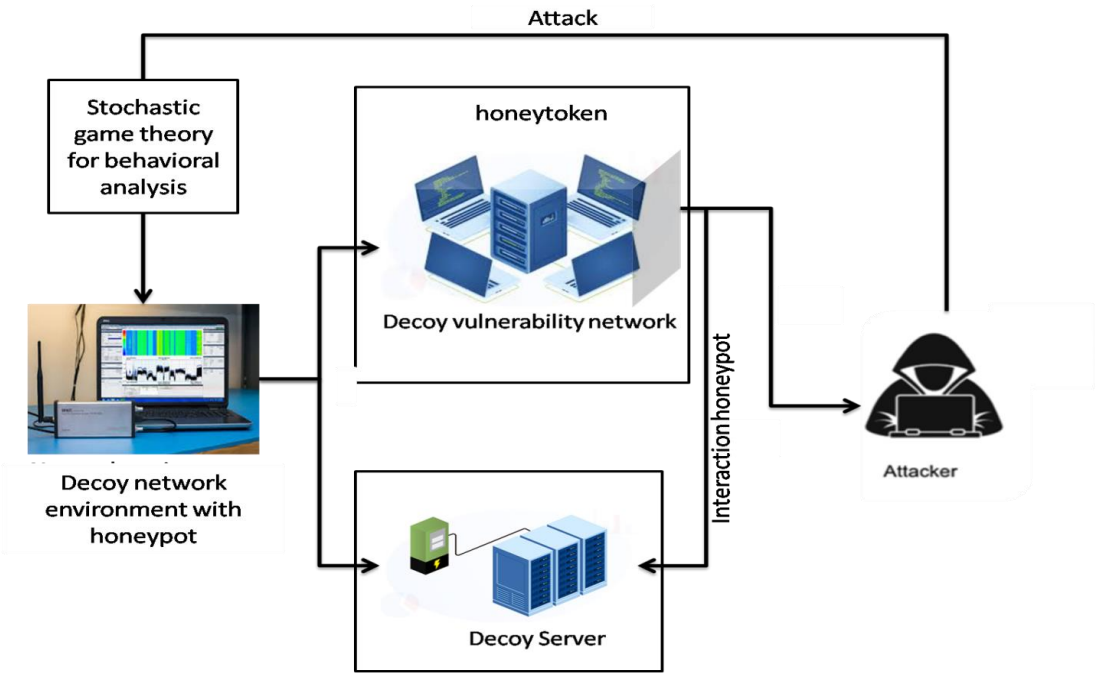

Figure 4: Architectural model of the decoy network with deception vulnerability

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

The Figure 4 presents the architecture of the decoy network with deception vulnerability. The attacker upon identifying the network types to login. The input information was analyzed through the stochastic game theory and then allow access to the decoy network environment which was modelled with adaptive honeypot to mimic the real network environment, while the honeytoken was applied to create decoy vulnerability, which ensures that the attacker remained on the decoy network and tries to exploit them. Threat information of the attacker is collected from the decoy server and used to update the main network. The complete architectural diagram which showcased the system integration of the deception technique for the management of zero-day vulnerability was presented in Figure 5;

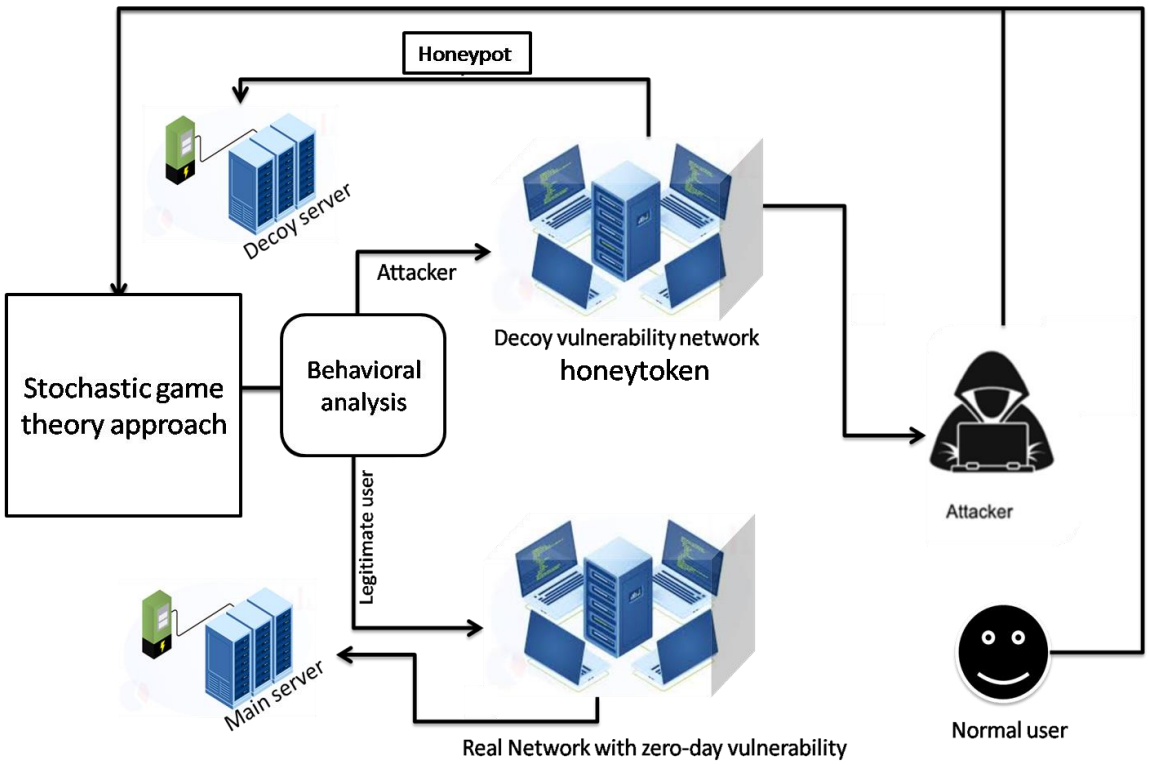

Figure 5: Architectural model the deception technique for zero-day attack management

The Figure 5 presents the architecture which showed the management of zero-day vulnerability through stochastic game theory, adaptive honeypot and honeytoken. When users (attacker or legitimate normal user) try to access the network, based on their behavior the stochastic game theory was applied to analyze user activity and upon classification as normal user is granted access to the real network with zero-day vulnerability. However, upon classified as attacker is granted access to the deception network developed with honeypot techniques. To ensure that the attacker is trapped on the network, honeytoken was applied to create vulnerabilities, which the attacker keep on exploiting while wasting time and their threat information collected at the back end as the threat intelligence.

Simulation of the deception based zero-day attack management system

Python environment was used to implement the deception model for zero-day vulnerability. This was achieved using libraries such as NumPy, Matplotlib, and NetworkX for effective data processing, statistical analysis, and network visualization, respectively. The decoy network environment was first created using a graph-based technique, in which nodes were color-coded balls to represent honeypots, legitimate users, and zero-day vulnerabilities. Stochastic game theory was used in the behavioural analysis to model interactions between attackers and authorized users. This allowed for the management of zero-day vulnerabilities with the use of honeytokens and the redirection of possible threats toward honeypots. The study employed simulations to quantitatively assess several performance metrics, such as Attack Diversion Rate (ADR), Honeytoken Activation Rate (HAR), Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate (FPR). The Figure 6 presented the integrated network environment with our decoy solution, while the parameters we used to simulate the network are those in Table 1.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

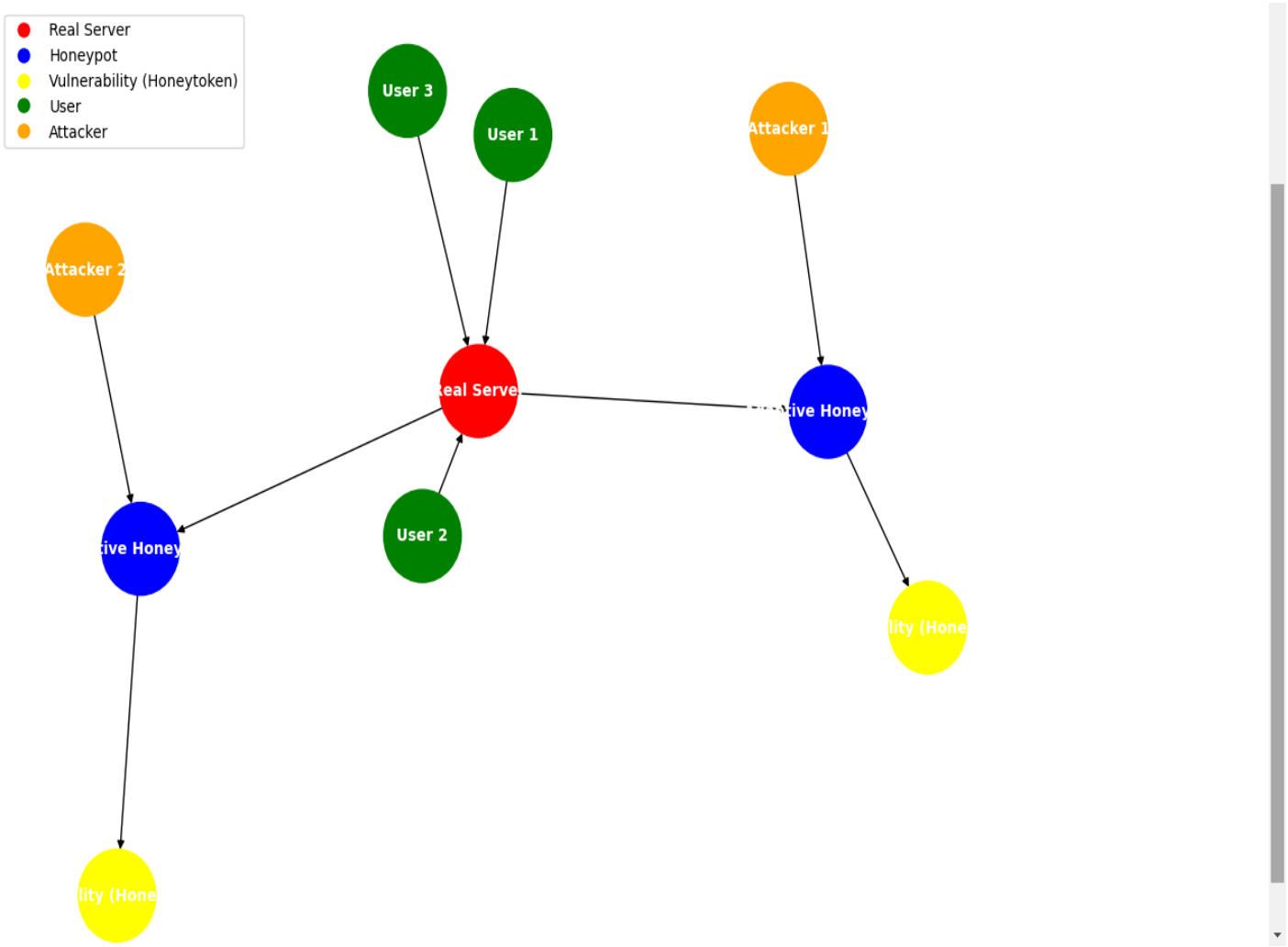

Figure 6: The simulated network environment with SGT based deception technique

RESULTS AND DISCUSSIONS

This section begins with the result of the behavioral analysis, showing the cumulative number of feature classified by the Stochastic Game Theory (SGT) as attacker reward and as legitimate user reward. Then the next results discussed the performance evaluation of the deception based network with integrated SGT, honeypot and honeytoken technique made of adaptive honeypot and honeytoken, against zero-day attack. Experiments were performed on the network using several threat features and results were evaluated.

Results of the features behavioural analysis with SGT

The SGT model in equation 3.10 was proposed to optimize decision of the traditional game theory approach in the classification of attacker and legitimate users. To evaluate the model after integration on the network environment with dynamic state transition state in equation 3.7. 200, 000 feature vectors of cumulative attacker and normal users were introduced through simulation over 100 secs to test the effectiveness of the SGT during behavioural analysis. The results were reported in Figure 7. The results reported the accumulation of rewards for legitimate users and reward for attackers over the number of iterations rounds for attack. From the results, it was observed that the reward for legitimate user and defender increased significantly, while the rewards for attacker decreased. The results for defender implied as posited in equation 3.8 which presents the optimal stochastic defender behaviour is that increased rewards were consistently achieved with defenders' ability to correctly classify attacker, and rarely misclassify legitimate user as attacker. More so the legitimate user behavioural analysis, the results showed that the SGT correctly allows access for the user and get reward consistently, while for attacker, the decrease in results implies that the masquerading was not successful as it was sent to decoy facility by the SGT, thereby incurring cost instead of rewards and this resulted to the steady decrease in the rewards as shown in the graph.

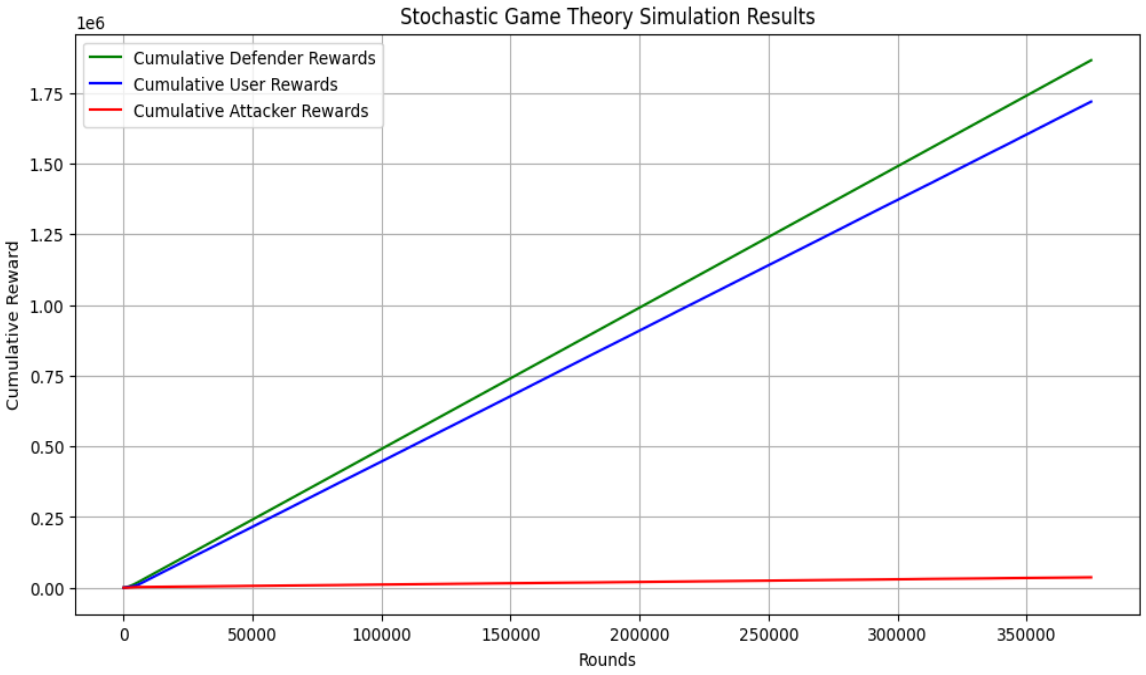

Figure 7: Result of the behavioural analytical model with SGT

Figure 7 revealed that the SGT model was able to correctly classify attacker, defender and legitimate users' action and allocate appropriate access to them. The results were very good due to the dynamic user activities modelled as a stochastic process and then their Nash equilibrium adopted as the optimal threshold for decision based and classification of user based on their activities

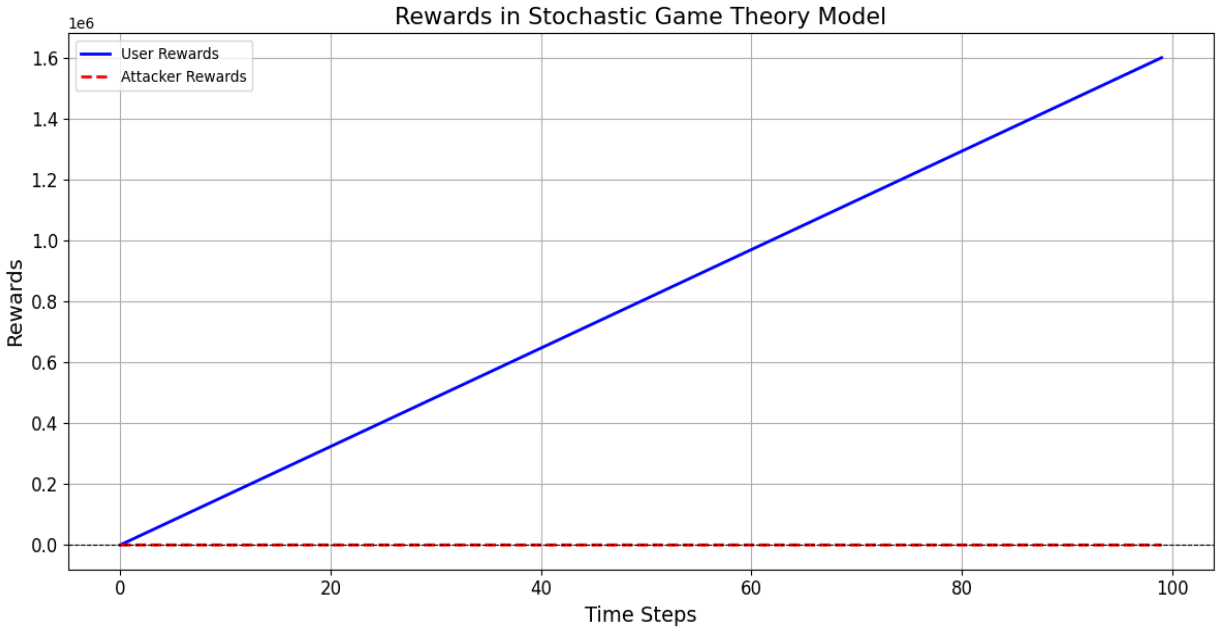

Figure 8: Result of the SGT during zero-day attack

Figure 8 reported the performance of the behavioural analysis after 100 secs of simulation with zero-day attack. From the result it was observed that the actions of the users were identified at each period and classified as attacker or legitimate user. With each successful correct action, rewards were allocated to help access the model effectiveness. In the context of attacker, it was observed that the rewards consistently decreased, while for legitimate user, the rewards consistently increased. This implied that the attacker was not able to achieve its goal because the SGT detected it and classified it to decoy facility, while eh legitimate user achieved its goal as it was classified as normal user and given access to the network. The heat map chart in Figure 9 was also applied to evaluate the SGT model for behavioural analysis.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

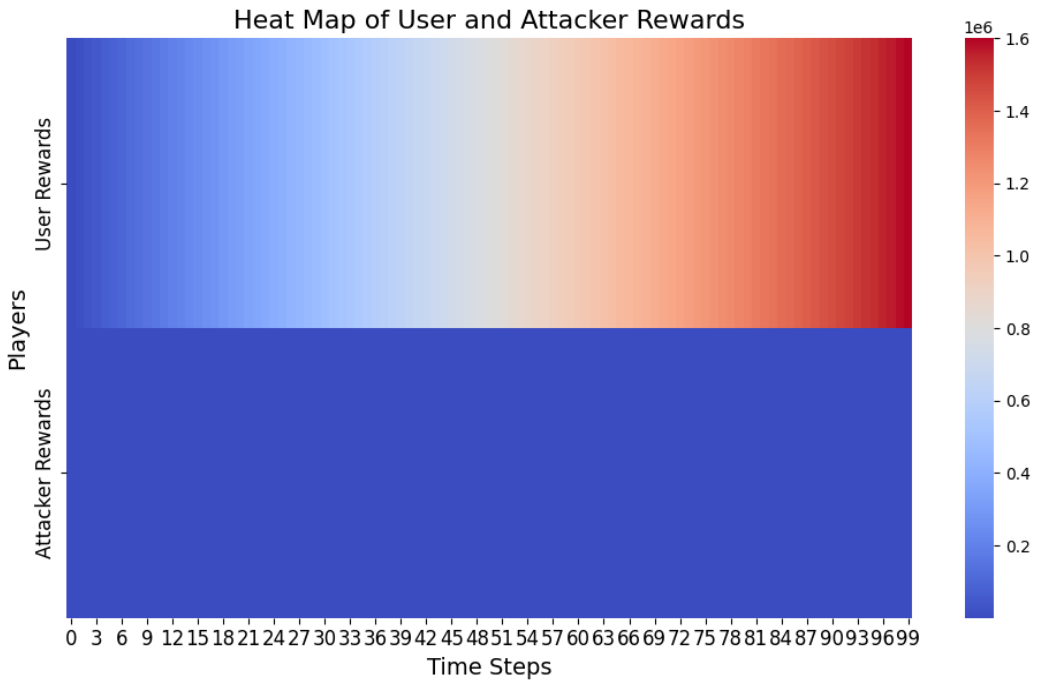

Figure 9: Heat map of the SGT behavioural analytical performance

In this heat map, two of the main players which are attacker and legitimate users were considered for the analysis. The reward score was measured from the colour candle range of 0 to 1.6. From the result, it was observed that in the context of attacker reward, the heat map was all deep blue which range from the score value of 0-0.6. This poor heat map results implied that the attacker has very poor reward it consistently did not achieve its aim, thus resulting to the poor reward recorded. In the context of the legitimate user reward heat map, it was observed at after the first few seconds of here the rewards was poor, over time the rewards was consistently very good with heat map of rewards at the optimal level. This implied that our model was able to correctly classify normal user to the access the network legitimately without access restriction or diversion to decoy as a threat. The mean rewards for the attacker and user interaction by the SGT based behavioural analysis was measured in Figure 10.

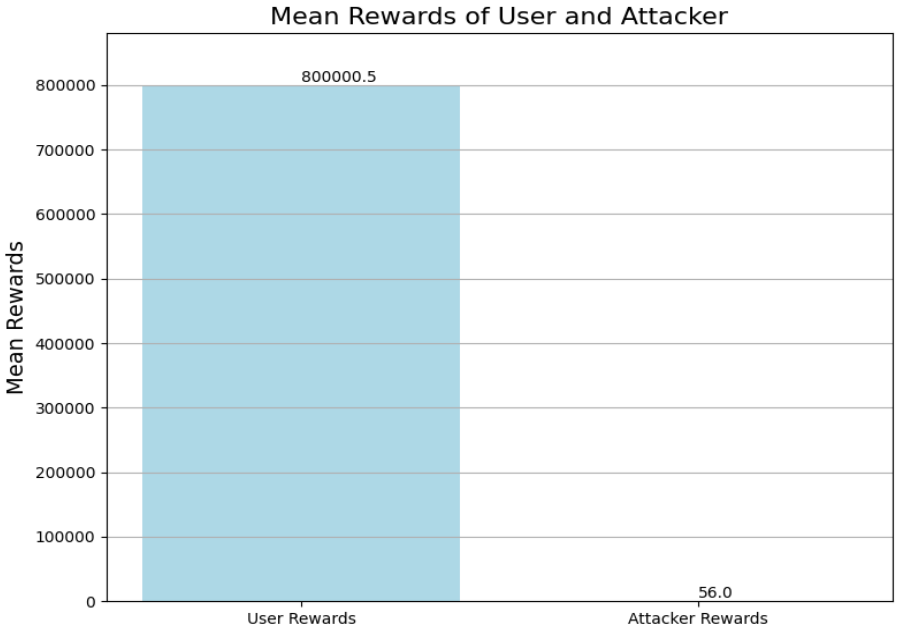

Figure 10: Mean reward evaluation score

From the mean reward evaluation result in Figure 10, the user rewards over 900,000 features of zero-day attack were measured with the user reward recording 800000.5 score, while the attacker reward recorded 56 rewards.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

This result implies that legitimate user behaviour was correctly classified as normal and allows access to the network by the defender. It also showed that legitimate users were not wrongly diverted to decoy facility as attackers. The attacker rewards score which is significantly low suggested the inability of the attacker to achieve its goal of penetration as normal user to exploit the network vulnerability.

Simulation of the network environment with SGT based deception technique

Upon user classification by the SGT in the previous section, attackers are allowed access to a decoy facility, while legitimate users are allowed access to normal network server for data management. The deception technique was developed with a combination of honeypot and honeytoken combined. The adaptive honeypot model in Equation 1 was used for the recreation of the real network as a decoy system, while the honeytoken was applied as the decoy vulnerability which traps the attacker on the network, while protecting the main infrastructure. To evaluate the deception model on the network environment, zero day attack was introduced for 100secs and Figure 11 presents results obtained.

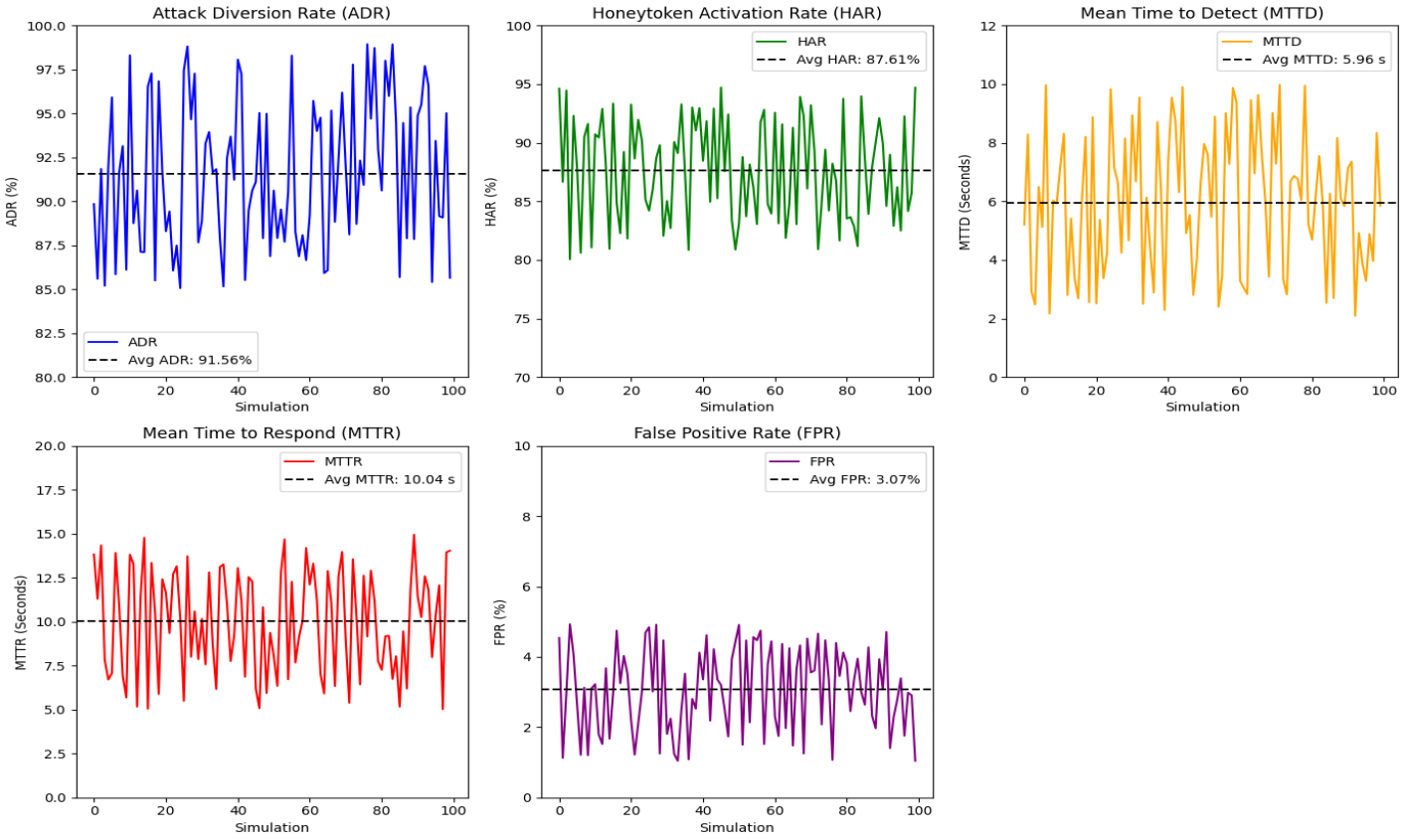

Figure 11: Result of the deception solution against zero-day vulnerability

Figure 11 reported the result of the deception technique. During zero-day attack, the behaviour of the player was classified by the SGT and diverted to the decoy facility. The ADT was reported as 91.56% which indicated that during the 100 secs of zero-day attack simulation on the network, the SGT was able to correctly classify the player action ac threat and divert to the decoy network. The average detection speed of the SGT which is the MTTD is recorded as 5.96s, while the rate of honeypot activation was measured as 87.45%. This interaction was achieved using the Markov model in equation 3.12. This implied that upon diversion to the network, the attacker was successful allowed access and remained on the network. The reason was due to the honeytoken based vulnerabilities which traps the attacker on the decoy network environment. The exploitability and conviction rate of the honeytoken was evaluated in figure 4.6. The result of the deception solution against zero-day attack was also evaluated considering mean time of response which reported 10.04s, while the false positive rate reported an average of 3.07%. The MTTR reported the response time of the zero-day attack by the SGT, while the FPR measures the percentage of legitimate activities classified as attack. The Figure 12 presents the exploitability rate in Equation 4 of the honeytoken and also the conviction rate in Equation 3.

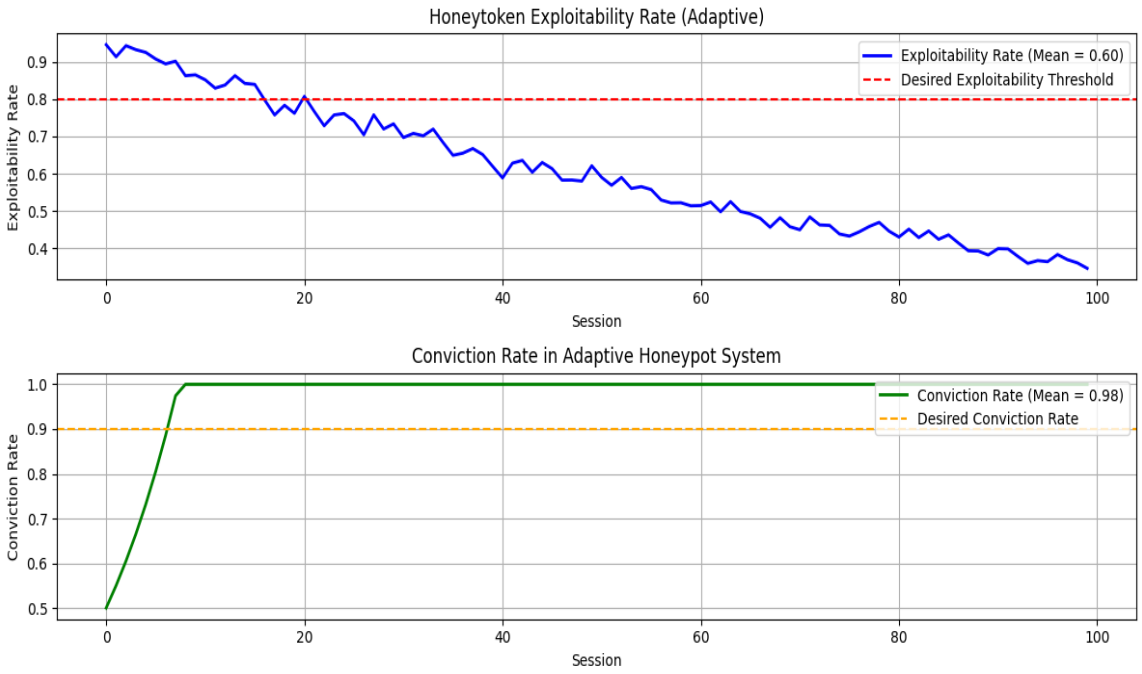

Figure 12: Honeypot vulnerability performance

The Figure 12 presents the exploitability performance and the conviction rate of the honeypot vulnerability. The exploitability value reported 0.60, which means that 60% of the attackers at the decoy network exploited the honeytoken vulnerability, thereby wasting time on the network with assumption it is the main network facility. The conviction rate of the honeypot vulnerability was 0.98, which means that the vulnerability is 98% as the traditional zero-day vulnerabilities.

Experiment with several types of zero-day attack vector

Having tested our SGT decoy model through simulation in the previous section, with the outcome showing high effectiveness against zero-day attack, this section experimented further on the model considering several attack vectors such as DDoS, zero-day, and SQL injection attack.The experimental performance summary of the deception model was reported in Table 2

Table 2: Experimental result of the model against several attacks

Metrics	Zero-day attack	DDoS	SQL injection	Average
ADR (%)	94.28	89.77	93.08	92.37667
HAR (%)	87.53	82.85	77.53	82.63667
MTTD (s)	4.63	8.58	5.77	6.326667
MTTR (s)	6.68	9.97	8.42	8.356667
FDR (%)	1.03	2.90	2.04	1.99

The results in Table 2 reported the experimental performance of the SGT based deception model for the management of zero-day attack. From the results, it was observed that overall, the ADR for the three threat vectors all reported an average ADR of 92.38%, HAR of 82.63%, MTTD of 6.3s, MTTR of 8.4s and FDR of 1.99%. These results consistently revealed that our model was able to correctly detect attacker with SQL injection, DDoS and zero-day respectively and then divert to the decoy facility. The high-performance score recorded was due to the SGT which was able to identify the dynamic threat model of attacker as the game and then classify attacker to the decoy facility which was justified by the high ADR and HAR valued reported.

Comparative analysis with other state of the art zero-day management algorithms

In this section, a comparative analysis of existing model in literature tailored towards zero day attack management with our model was performed and all the results reported in Table 3.

Table 3: Comparative analysis with existing algorithms

Author and year	Technique	Detection accuracy (%)
Manish et al. (2021)	Machine learning	98.00
Sharukh (2020)	CNN	87.50
Berna (2019)	DL	97.00
Ibraheem and Tasha (2024)	SVM	92.00
Ekong et al. (2023)	RF	95.00
Nkongolo et al. (2021)	ELM	99.00
	RF	44.00
	DT	99.00
Ali et al. (2022)	Stacker based model	98.80
Peppes et al. (2023)	GAN	96.42
Reddy et al. (2024)	RL	92.5
Singh et al. (2019)	Priority based approach	96.00
Cen et al. (2024)	SA-CNN-IS	96.31
Our model	SGT- based deception	94.28
	Traditional honeypot	77.82

From the results reported in the plotted graphs of Table 3, it was observed that while our model with SGT based deception as among the top best models for zero day attack management. However, our model is the most reliable for zero day attack management because it uses SGT and decoy to divert the attackers from the main network infrastructure and also uses decoy vulnerability to ensure attacker remain on the decoy environment, thereby protecting completely the main real network.

CONCLUSION

This study has successfully a stochastic based decoy technique for the management of zero-day vulnerability. This was achieved through behavioural analytical model which through the action of players classify attacker and legitimate users. The classified attackers are diverted to a decoy environment developed with adaptive honeypot, while to ensure that the attacker remained trapped on the network, decoy vulnerability was integrated using honeytoken. These models were integrated on a network environment using python programming language. The results after simulation considering zero-day attack reported ADR of 94.28%, HAR of 87.53%, MTTD of 4.63s, MTTR of 6.68s and FDR of 1.03% respectively. Another simulation was carried out with zero-day attack considering traditional honeypot deception on the network environment. ADR reported 77.82%, which indicated that the existing game theory was able to detect attack with 77.82% accuracy. The activation of honeypot reported 60.47% which indicated that successful diversion of attackers to the decoy facility is at 60.47%. The MTTD and MTTR both reports 6.82s and 8.54s respectively, while the average FPR reported 4.55%. Experiments were carried out considering other attacker vectors such as SQL injection and DDoS, and averagely the ADR recorded 92.28%, HAR reported 82.64%, MTTD of 6.3s, MTTR of 8.3s and FDR of 1.99s. The limitation of the study is the inability to test the solution in real life network, however this is recommended for future studies.

Data Availability

Data used for the work were used confidentially without violation of company's ethics.

Ethical Concerns

The data collected from Ethos Limited was handled in strict compliance with data protection regulations, of the Nigeria's Data Protection Act. The data while used does not disclose in any information which can be used to cause harm to the company. The purpose of using the data was strictly for academic and research advancement, with appropriate ethical oversight to avoid misuse. Furthermore, the research was guided by principles of fairness, transparency, and accountability to prevent bias, ensure responsible data usage, and uphold trust between stakeholders.

REFERENCES

1. Ali, S.; Rehman, S.U.; Imran, A.; Adeem, G.; Iqbal, Z.; Kim, K.-I. Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics 2022, 11, 3934. https://doi.org/10.3390/electronics11233934
2. Berna C., (2019) Zero-Day Attack Detection with Deep Learning. The Graduate School Of Natural And Applied Sciences Of Middle East Technical University.
3. Chakraborty, T., Jajodia, S., Katz, J., Picariello, A., Sperli, G., &Subrahmanian, V. S. (2019). A fake online repository generation engine for cyber deception. IEEE Transactions on Dependable and Secure Computing, 18(2), 518-533.
4. Chen, W. and Wei, Q. (2024). "A new optimal adaptive backstepping control approach for nonlinear systems under deception attacks via reinforcement learning". ElSevier. Journal of Automation and Intelligence 3 (2024) 34–39. journal homepage: www.keaipublishing.com/en/journals/journal-of-automation-and-intelligence/
5. Douha, N.Y.-R.; Sasabe, M.; Taenaka, Y.; Kadobayashi, Y. An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users against Cyberattacks. *Appl. Sci.* **2023**, *13*, 4645. https://doi.org/10.3390/app13074645
6. Ekong A., Etuk A., Inyang S., & Ekere-Obong M., (2023) Securing Against Zero-Day Attacks: A Machine Learning Approach for Classification and Organizations' Perception of its Impact. Journal of Information Systems and Informatics Vol. 5, No. 3, September 2023 e-ISSN: 2656-4882 p-ISSN: 2656-5935https://doi.org/10.51519/journalisi.v5i3.546
7. Hattori, M.; Satoh, A.; Tanaka, Y. Minimax theorem and Nash equilibrium of symmetric multi-players zero-sum game with two strategic variables. *arXiv* **2018**, arXiv:1806.07203
8. Hausken, K.; Welburn, J.W.; Zhuang, J. A Review of Attacker–Defender Games and Cyber Security. *Games* **2024**, *15*, 28. https://doi.org/10.3390/g15040028
9. Ibraheem I., & Tasha A., (2024) Zero Day Attack Vulnerabilities: Mitigation using Machine Learning for Performance Evaluation. Journal of Computers for Society 5(1) (2024) 43-58https://doi.org/10.17509/jcs.v5i1.70795
10. Manish A., Vivek S., Vishal K., Mahesh S., & Madhuri J., (2021) Detection of Zero-Day Security Threat Using Machine Learning. International Journal Of Current Engineering And Scientific Research (IJCESR).
11. Mejdi, H.; Ezzedine, T. Novel Dynamic Defense Strategies in Networked Control Systems under Stochastic Jamming Attacks. *Mathematics* **2024**, *12*, 2143. https://doi.org/10.3390/math12132143
12. Morozov D., Vakaliuk T., Yefimenko A., Nikitchuk T., &Kolomilets R., (2023) Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure. doors-2023: 3rd Edge Computing Workshop, April 7, 2023, Zhytomyr, Ukraine
13. Nandakumar D., Schiller R., Redino C., Choi K., Rahman A., Bowen E., Vucovich M., Nehila J., Weeks M., & Shaha A., (2022) Zero Day Threat Detection Using Metric Learning Autoencoders. arXiv:2211.00441v1 [cs.CR]
14. Niakanlahaji, A., Jafarian, H.J., Chu, B.-T., Al-Shaer, E. (2020). "HoneyBug: Personalized Cyber Deception for Web Applications". Proceedings of the 53rd Hawaii International Conference on System Sciences 2020.
15. Nkongolo, M.; van Deventer, J.P.; Kasongo, S.M. UGRansome1819: A Novel Dataset for Anomaly Detection and Zero-Day Threats. Information 2021, 12, 405. https://doi.org/10.3390/info12100405
16. Oluoha, O.U., Yange, T.S., Okereke, G.E. and Bakpo, F.S. (2021) Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey. Journal of Information Security, 12, 250-269. https://doi.org/10.4236/jis.2021.124014
17. Peppes, N.; Alexakis, T.; Adamopoulou, E.; Demestichas, K. The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers. Sensors 2023, 23, 900. https://doi.org/10.3390/s23020900
18. Perkins, R. C., & Howell, C. J. (2021). Honeypots for cybercrime research. Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, 233-261. FErguson-M

19. Reddy B., Shaik S., & Gaddam V., (2024) Reinforcement Learning for Zero-Day Vulnerability Detection in IoT Devices: A Proactive Approach. Research Square: https://doi.org/10.21203/rs.3.rs-4086508/v1
20. Roumani Y., (2021) Patching zero-day vulnerabilities: an empirical analysis. Journal of Cybersecurity, 2021, 1–13 https://doi.org/10.1093/cybsec/tyab023
21. SakthiMurugan S., Sanjay K., Vishnu V.,& Santhi P., (2023) Assessment of Zero-Day Vulnerability using Machine Learning Approach. EAI Endorsed Transactions on Internet of Things
22. Sarhan M., Layeghy S., Gallagher M., & Portmann M., (2023) From zero-shot machine learning to zero-day attack detection. International Journal of Information Security (2023) 22:947–959 https://doi.org/10.1007/s10207-023-00676-0
23. Sayed A., Anwar A., Kiekintveld C., Bosansky B., &Kamhoua C., (2023) Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach. Springer Nature Switzerland AG 2023https://doi.org/10.1007/978-3-031-26369-9_3
24. Schiaffino A., Reina M., Aragon R., Solinas A., & Epifania F., (2023) Detecting Zero-Day Vulnerabilities in CMS Platforms: An In-depth Analysis Using DeepLog. AIABI 2023: 3rd Italian Workshop on Artificial Intelligence and Applications for Business and Industries, November 9, 2023, Milano, Italy
25. Sharukh S., (2020) A hybrid deep learning approach for detecting zero-day malware attacks.VNRVignana Jyothi Institute of engineering and technology, Hyderabad, IndiaEasyChair Preprint
26. Singh U., Joshi C., & Kanellopoulos D., (2019) A framework for zero-day vulnerabilities detection and prioritization. Journal of Information Security and Applications 46 (2019) 164–172https://doi.org/10.1016/j.jisa.2019.03.011
27. Sivamohan, S., Sridhar, S.S., Krishnaveni, S. (2022). Efficient Multi-platform Honeypot for Capturing Real-time Cyber Attacks. In: Hemanth, D.J., Pelusi, D., Vuppalapati, C. (eds) Intelligent Data Communication Technologies and Internet of Things. Lecture Notes on Data Engineering and Communications Technologies, vol 101. Springer, Singapore. https://doi.org/10.1007/978-981-16-7610-9_21
28. Tan, F., Zhou, L., and Xia, J. (2022). “Adaptive quantitative exponential synchronization in multiplex Cohen-Grossberg neural networks under deception attacks”. ElSevier. Journal of the Franklin Institute 359 (2022) 10558–10577 www.elsevier.com/locate/jfranklin.
29. Teymourlouei H., Stone D., & Jackson L., (2023) Identifying Zero-Day Attacks with Machine Learning and Data Reduction Methods. 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)DOI 10.1109/CSCE60160.2023.00372
30. Topcu, A.E.; Alzoubi, Y.I.; Elbasi, E.; Camalan, E. Social Media Zero-Day Attack Detection Using TensorFlow. Electronics 2023, 12, 3554. https://doi.org/10.3390/electronics12173554
31. Zahoora U., Rajarajan M., Pan Z., & Khan A., (2022) Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier. Applied Intelligence https://doi.org/10.1007/s10489-022-03244-6