Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 4
ICCIA 2024

Collaborative Optimization of Game Enemy Design and Network Security Defense Based on Deep Reinforcement Learning

Jianshu Liu

Shanghai Ocean University, Shanghai 200000, China

Abstract. The purpose of this paper is to explore the cooperative optimization strategy of game enemy design based on Deep Reinforcement Learning (DRL) and Network Security Defense (NSD). By analyzing the correlation between game enemy design and NSD, this paper puts forward a method of integrating DRL technology to improve the game experience and protect the security of the game system. Firstly, the paper introduces the basic concepts and existing research progress of game enemy design and NSD. Then, the paper introduces the design method of game enemies based on DRL in detail, including the training and behavior generation of enemy agents. Then, the paper discusses the application of DRL in NSD, including network traffic analysis and monitoring and intelligent defense strategy generation. Through experimental design and result analysis, the paper verifies the effectiveness and performance of collaborative optimization strategy, and shows its potential in improving game experience and protecting network security. Finally, the paper summarizes the research results and discusses the future research direction and development trend. This paper provides important reference and guidance for deeply understanding and applying DRL technology to game enemy design and NSD.

Keywords: Deep Reinforcement Learning; Game Enemy; Network Security Defense; Collaborative Optimization.

1. Introduction

With the rapid development of information technology, the game industry and network security have become an indispensable part of modern society. As a way of entertainment, games can not only bring people fun, but also constantly challenge players' intelligence and reaction ability. Network security is an important guarantee to protect the security of individuals, enterprises and even the country. However, with the development of technology, games and network security are facing more and more severe challenges [1].

In the gaming field, enemy design is an important component of the gaming experience [2-3]. The behavior design of enemies directly affects the gaming experience of players, and traditional enemy design methods are often limited to pre-defined rules and patterns, unable to adapt to different behaviors and strategies of players. At the same time, in the field of network security, the technology and means of network attackers are constantly being updated, and the traditional Network Security Defense (NSD) method also appears inadequate. Deep Reinforcement Learning (DRL), as an important technology in the field of AI, has the ability to autonomously learn and make decisions in complex environments, providing new possibilities for solving game enemy design and NSD [4-5]. By introducing DRL into the field of game enemy design and NSD, we can achieve intelligent behavior generation of game enemies and adaptive defense strategies against unknown attacks, thereby improving the gaming experience and network security level.

The purpose of this paper is to discuss the collaborative optimization of game enemy design and NSD based on DRL, which not only pays attention to the innovative application in the game field, but also involves the key technologies in the network security field. By studying and discussing the application of DRL in game enemy design and NSD, this paper aims to provide new ideas and methods for improving game experience and network security level.

2. Game enemy design and DRL

In traditional game development, the enemy's behavior is often based on predefined rules or simple patterns. This design method has some limitations, and the enemy's behavior lacks variability and personalization, which makes it difficult to adapt to the different strategies of players. The enemy's behavior pattern is relatively fixed, and it is easy for players to predict and respond, which leads to the reduction of the game experience. Enemy design for new scenes or new gameplay requires a lot of manpower and material resources, and is often not flexible and intelligent enough. Therefore, game developers urgently need a new method to realize the intelligent behavior generation of enemies, so as to enhance the game experience and challenge [6-7].

As a powerful AI technology, DRL has the ability of autonomous learning and decision-making, and is suitable for intelligent behavior generation in complex and uncertain environments. At this time, DRL can be applied to design the enemy's behavior. Each enemy in the game is regarded as an agent, and DRL algorithm is used to train them to learn the optimal behavior strategy.

Define the states in the game, including player position, enemy position, maze map information, etc., to form a state space. Define the actions that enemies can take, such as chasing players, attacking players, evading players, etc., to create an action space. Design a reward function that rewards enemies for taking different actions in different states. For example, if an enemy successfully defeats a player, they can receive higher rewards, while if defeated by a player, they can receive lower rewards. Using DRL algorithms such as Deep Q-Network (DQN) or Deep Deterministic Policy Gradient (DDPG), train each enemy agent to select the optimal action based on the current state [8-9].

Through this approach, enemies with intelligent behavior can be trained to respond accordingly to player behavior and strategies, providing a more challenging and interactive gaming experience. This design not only increases the fun of the game, but also allows players to immerse themselves in the game world and enjoy a more realistic and intense gaming experience.

3. NSD based on DRL

In today's digital age, the problem of network security is becoming more and more serious, and various network attacks, such as malicious software, data leakage and denial of service attacks, are emerging one after another, posing a serious threat to the security of individuals, enterprises and countries. Traditional NSD methods often rely on rules, features and signatures to detect and stop attacks, but these methods are often unable to effectively deal with new threats such as unknown attacks and zero-day vulnerabilities. Therefore, there is an urgent need for an adaptive and intelligent NSD method in the field of network security, which can detect and deal with all kinds of complex network attacks in time.

As a powerful AI technology, DRL has the ability of autonomous learning and decision-making, and shows excellent performance in a complex and uncertain environment. The DRL model is used to monitor and analyze network traffic in real time, and abnormal traffic and behavior, such as potential attack behavior and malware spread, are found [10]. Based on DRL model, the network attack is modeled and simulated, and the adaptive defense strategy is generated to deal with all kinds of unknown attacks and changes in time. Using DRL model, the threat level of network attacks is evaluated and classified, and corresponding coping strategies are formulated, including blocking attack traffic, fixing vulnerabilities and updating security policies.

DRL model can learn and make decisions independently according to the real-time network environment and attack situation, and has higher adaptability and flexibility. DRL model can learn the characteristics and patterns of different network environments and attack types, and provide intelligent and personalized solutions for NSD [11]. DRL model can realize real-time monitoring and response, and continuously improve the effect and performance of NSD through continuous learning and optimization.

NSD based on DRL has great potential and advantages in dealing with complex and dynamic network attacks, which provides new ideas and methods for the research and practice in the field of network security.

4. Collaborative optimization of game enemy design and NSD

4.1. Contact and challenge between enemy design and network security in games

The enemy's behavior design directly affects the player's game experience and fun. Well-designed enemies can increase the challenge and interest of the game and enhance the player's participation and satisfaction. The enemy's strength and behavior need to match the player's skill level to maintain the balance and fairness of the game. Unreasonable enemy design may lead to the game being too simple or too difficult, which will affect the playability and long-term attraction of the game. It takes a lot of manpower and time to design enemies for different game scenes and gameplay. Traditional enemy design methods often need frequent adjustment and optimization, which increases the cost and risk of game development.

Network attacks may cause the game system to crash, data to be lost or the player's account to be stolen, which will affect the player's game experience and trust. Security vulnerabilities and attacks may lead to the negative reputation of the game community and the loss of players, causing serious losses to game developers and operators. Using DRL and other technologies to design intelligent game enemies can enhance the security and anti-attack ability of the game system [12]. Designing intelligent game enemies can effectively deal with various behaviors of players and attackers, and improve the stability and security of the game system.

There is a close connection and challenge between enemy design and network security in the game. Using DRL and other technologies to design intelligent game enemies can not only enhance the game experience and challenge, but also enhance the security and anti-attack ability of the game system, bringing new opportunities and challenges to game development and NSD.

4.2. Collaborative optimization strategy of game enemy design and NSD based on DRL

State s_t represents the state of the environment at time t. Action selection $a_t = \pi(s_t)$ indicates the action selected in state s_t. The reward function $r_t = R(s_t, a_t)$ represents the instant reward obtained by selecting the action a_t in the state s_t. Each enemy is regarded as an agent with its own state, action and reward. Using DRL algorithm, DQN trains enemy agents to learn the optimal behavior strategy.

Using deep neural network to approximate Q value;

$$L(\theta) = E_{(s,a,r,s')}\left[\left(r + \gamma \max_{a'} Q(s', a'; \theta) - Q(s, a; \theta)\right)^2\right] \tag{1}$$

Gradient descent formula in DRL training;

$$\theta \leftarrow \theta - \alpha \nabla_{\theta} L(\theta) \tag{2}$$

Where θ is the parameter of the deep neural network, α is the learning rate and γ is the discount factor.

The DRL model is used to monitor and analyze the network traffic in real time and identify the potential intrusion behavior. Generate intelligent defense strategies based on DRL model to deal with various network attacks in time. Using DRL to train enemy agents, so that they can learn the optimal behavior strategy according to the game environment and player behavior. Through continuous optimization and training, the enemy agent is adaptive and intelligent.

The DRL model is used to analyze the network attack behavior and evaluate the threat level and risk of the attack. Based on the evaluation results, intelligent defense strategies are generated, including blocking attack traffic, fixing vulnerabilities, and updating security policies.

5. Application case analysis

A virtual multiplayer online combat game called "Battle Arena". In this game, players can choose different characters and play against other players in various scenes. At the same time, the game system needs to face the threat of network attacks, such as DDoS attacks and malware injection. Use DQN to train the game enemy agent, so that it can choose the best strategy according to the player's behavior and game environment. Off-line training of battle data through a large number of games makes enemy agents adaptive and intelligent. After the training, the enemy agent can choose the best combat action according to the current state in the real-time game environment, such as pursuit, evasion, attack and so on. Enemy agents are personalized and changeable, and can adjust strategies in real time according to players' behaviors and game scenes.

The deep learning model is used to monitor and analyze the network traffic of game servers in real time and identify potential network attacks. When abnormal traffic or attacks are detected, corresponding defensive measures should be taken immediately to protect the game system from attacks. Based on DRL model, the threat level and risk of network attacks are analyzed, and intelligent defense strategies are generated. According to different types of network attacks, we should formulate corresponding defense measures, including blocking attack traffic, updating security rules, and repairing loopholes.

From Figure 1, we can clearly see the performance of enemy agents in battle. Firstly, observing the decision pie chart of enemy agents, we can see that the distribution ratio is basically balanced among aggression, neutrality and defense. This shows that enemy agents have certain diversity and flexibility, and can make different decisions according to different game situations. Secondly, some interesting patterns can be observed in the heat map between player behavior and enemy agent decision-making. For example, when the player chooses to attack, the enemy agent tends to make defensive decisions, which shows that the enemy agent has certain intelligent response ability and can identify and deal with the player's attack behavior. In addition, when players choose defense, enemy agents tend to take neutral decisions, which may indicate that enemy agents will be vigilant, but not too radical or negative.

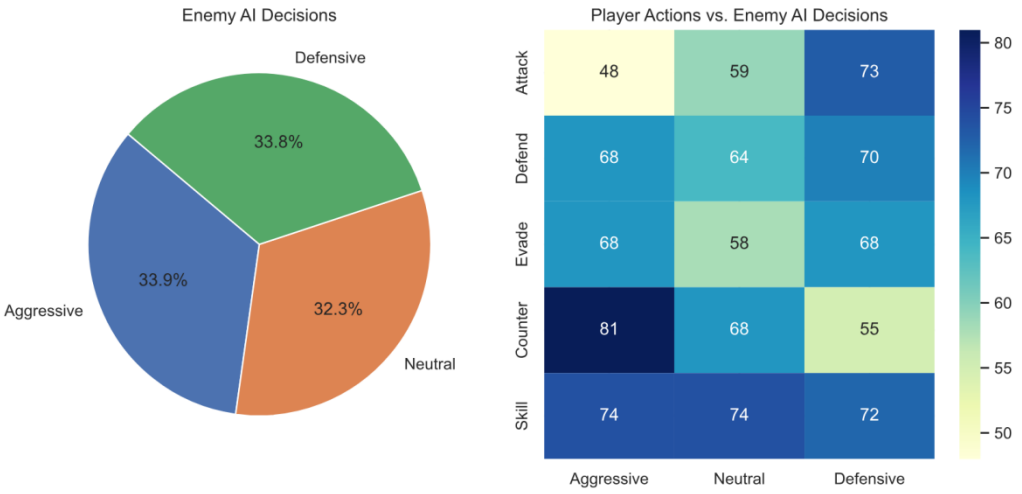

Figure 1. The performance of enemy agents in battle

It can be seen that the enemy agent's performance in battle is relatively good as a whole. Enemy agents can make appropriate decisions according to the player's behavior and game environment, and

have certain diversity and flexibility. However, further experiments and analysis are needed to evaluate the specific effects and advantages and disadvantages of enemy agents' performance in battle.

Table 1 lists several common types of network attacks, including DDoS attack, malware injection, SQL injection attack, XSS attack and CSRF attack. For each attack type, the defense success rate is recorded and divided into three sub-items: blocking attack traffic success rate, updating security rules success rate and repairing vulnerabilities success rate.

Table 1. Defensive success rate under different types of network attacks

Network attack type	Defense success rate (%)	Success rate of blocking attack traffic (%)	Success rate of updating security rules (%)	Success rate of fixing vulnerabilities (%)
DDoS attack	95	90	95	90
Malware injection	85	80	85	90
SQL injection attack	90	85	90	85
cross site scripting	88	85	90	85
CSRF attack	92	90	92	88

The defense success rate of DDoS attack is high, which is 95%. The success rate of blocking attack traffic and updating security rules are both high, which are 90% and 95% respectively. The success rate of fixing vulnerabilities is also high, at 90%. This shows that the defensive measures taken against DDoS attacks are effective and can effectively reduce the impact of attack traffic on the system.

The success rate of malware injection defense is 85%, which is slightly lower than DDoS attack. The success rate of blocking attack traffic and updating security rules is 80% and 85% respectively, and the success rate of fixing vulnerabilities is higher, which is 90%. This shows that the defense measures taken against malware injection are generally effective, and it is necessary to further strengthen the defense measures to improve the success rate.

SQL injection attack, XSS attack and CSRF attack, the defense success rate of these attack types is between 85% and 92%, and they perform well on the whole. The success rate of different defense means is relatively high, especially the success rate of updating security rules and fixing vulnerabilities is relatively high.

There are some differences in the success rate of defense under different types of network attacks, but the overall performance is good. Taking appropriate defensive measures, such as blocking attack traffic, updating security rules and fixing loopholes, can effectively improve the security of the system and reduce the impact of network attacks on the system. However, there are still some types of attacks with low success rate, and further research and improvement of defense strategies are needed to cope with the evolving network threats.

6. Conclusion

This study proposes an effective method to improve the game experience and protect the security of the game system by exploring the cooperative optimization strategy of game enemy design and NSD based on DRL. By analyzing the correlation between game enemy design and NSD, and combining with DRL technology, this paper realizes the intelligent design of game enemy agent and the intelligent response of NSD. DRL technology is used to train the game enemy agent, so that it can learn and optimize the strategy independently according to the player's behavior and game environment, which improves the playability and interest of the game. The individualization and variability of enemy agents are realized, and the strategy can be adjusted according to different players

and game scenes, which increases the challenge and diversity of the game. Based on DRL model, intelligent defense strategies are generated, including blocking attack traffic, updating security rules, and fixing vulnerabilities, which effectively improve the capabilities and effects of NSD. The cooperative optimization strategy of game enemy design and NSD based on DRL has great significance and potential in improving game experience and protecting game system security. In the future, we will further study and optimize related algorithms and technologies, continuously improve the performance and effect of the system, and make greater contributions to the development of the game industry and network security.

References

[1] Cao, L. , Jiang, X. , Zhao, Y. , Wang, S. , & Xu, X. (2020). A survey of network attacks on cyber-physical systems. IEEE Access, 2020(99), 1-1.

[2] Zhao, Y. , Xu, K. , Wang, H. , Li, B. , & Jia, R. (2021). Stability-based analysis and defense against backdoor attacks on edge computing services. IEEE Network, 35(1), 163-169.

[3] Shang, Z. , Zhang, T. , Tao, L. , Xiang, Z. , & Yang, W. (2021). Physical layer security in cognitive noma sensor networks with full-duplex technique:. International Journal of Distributed Sensor Networks, 17(12), 331-342.

[4] Rasool, R. U. , Ahmed, K. , Anwar, Z. , Wang, H. , Ashraf, U. , & Rafique, W. (2021). Cyberpulse plus plus : a machine learning-based security framework for detecting link flooding attacks in software defined networks. International journal of intelligent systems, 2021(8), 36.

[5] Febro, A. , Xiao, H. , Spring, J. , & Christianson, B. (2022). Edge security for sip-enabled iot devices with p4. Computer networks, 2022(11), 203.

[6] Bajic, A. , & Becker, G. T. (2022). Automated benchmark network diversification for realistic attack simulation with application to moving target defense. International Journal of Information Security, 2022(2), 21.

[7] Li, B. , Fei, Z. , Zhou, C. , & Zhang, Y. (2020). Physical-layer security in space information networks: a survey. IEEE Internet of Things Journal, 7(1), 33-52.

[8] Zhou, Z. , Kuang, X. , Sun, L. , Zhong, L. , & Xu, C. (2020). Endogenous security defense against deductive attack: when artificial intelligence meets active defense for online service. IEEE Communications Magazine, 58(6), 58-64.

[9] Hao, W. , Yao, P. , Yang, T. , & Yang, Q. (2021). Industrial cyber-physical system defense resource allocation using distributed anomaly detection. IEEE Internet of Things Journal, 2021(99), 1-1.

[10] He, D. , Gao, Y. , Liu, X. , Chan, S. , & Guizani, N. (2020). Design of attack and defense framework for 1553b-based integrated electronic systems. IEEE Network, 2020(99), 12-18.

[11] Mahfouz, A. , Abuhussein, A. , Venugopal, D. , & Shiva, S. (2020). Ensemble classifiers for network intrusion detection using a novel network attack dataset. Future Internet, 12(11), 180.

[12] Zhu, L. , Li, Y. , Yu, F. R. , Ning, B. , & Wang, X. (2020). Cross-layer defense methods for jamming-resistant cbtc systems. IEEE Transactions on Intelligent Transportation Systems, 2020(99), 1-13.