반도체디스플레이기술학회지 제22권 제3호(2023년 9월)
Journal of the Semiconductor & Display Technology, Vol. 22, No. 3. September 2023.

네트워크 공격 시뮬레이터를 이용한 강화학습 기반 사이버 공격 예측 연구

김범석[*] · 김정현[*] · 김민석[**†]
[*]상명대학교 전자정보시스템공학과, [**†]상명대학교 휴먼지능로봇공학과

A Study of Reinforcement Learning-based Cyber Attack Prediction using Network Attack Simulator (NASim)

Bum-Sok Kim[*], Jung-Hyun Kim[*] and Min-Suk Kim[†]**
[*]Dept. of Electronic Information Systems Engineering, Graduate School, Sangmyung University,
[**†]Dept. of Human Intelligent Robotics Engineering, Sangmyung University

ABSTRACT

As technology advances, the need for enhanced preparedness against cyber-attacks becomes an increasingly critical problem. Therefore, it is imperative to consider various circumstances and to prepare for cyber-attack strategic technology. This paper proposes a method to solve network security problems by applying reinforcement learning to cyber-security. In general, traditional static cyber-security methods have difficulty effectively responding to modern dynamic attack patterns. To address this, we implement cyber-attack scenarios such as 'Tiny Alpha' and 'Small Alpha' and evaluate the performance of various reinforcement learning methods using Network Attack Simulator, which is a cyber-attack simulation environment based on the gymnasium (formerly Open AI gym) interface. In addition, we experimented with different RL algorithms such as value-based methods (Q-Learning, Deep-Q-Network, and Double Deep-Q-Network) and policy-based methods (Actor-Critic). As a result, we observed that value-based methods with discrete action spaces consistently outperformed policy-based methods with continuous action spaces, demonstrating a performance difference ranging from a minimum of 20.9% to a maximum of 53.2%. This result shows that the scheme not only suggests opportunities for enhancing cybersecurity strategies, but also indicates potential applications in cyber-security education and system validation across a large number of domains such as military, government, and corporate sectors.

Key Words : Reinforcement Learning, Network Attack Simulator, Cyber-attack, Security, Markov Decision Process, Deep-Q-Network

1. 서 론

현대 사회에서는 정보기술의 발달과 초고속 인터넷 보급으로 인해 사이버 공격에 대한 대비 및 강화 필요성이 점점 더 중요한 문제로 대두되고 있다. 또한, 코로나19[1]와 같은 전염병의 확산으로 원격 교육, 재택근무 및 기타 비대면 서비스의 수요가 급증하여[2] 랜섬웨어, 피싱 등의 사이버 공격 및 위협이 급격히 증가하고 있다[3, 4]. 특히 재택근무 시스템을 이용하는 직원의 VPN 계정 정보를 획득하여 기업의 내부망에 침투하는 사례가 보고되고 있으며[5], 원격 수업 파일을 이용한 랜섬웨어 공격 및 악성코드 감염과 같은 사이버 공격도 증가하고 있다[6, 7]. 더

[†]E-mail: minsuk.kim@smu.ac.kr

나아가 사이버 공간의 확대로 인해 개인, 산업 및 국가 시설과 같은 다양한 분야에서 사이버 공격이 발생하고 있어 막대한 피해가 발생하고 있으며[8] 이러한 상황으로 인해 다양한 분야에서 사이버 훈련장의 필요성은 더욱 증가하고 있다[9].

일반적으로 실제 훈련 환경에서는 제약 사항과 위험 부담으로 인해 실제와 유사한 상황을 모의하기 위한 훈련의 다양성 구성 및 공격 도구를 위한 시나리오 실행은 매우 어려운 문제이다[10, 11]. 이를 해결하기 위해, 사이버 작전에서는 공격자와 방어자의 의사결정 모델을 고려하여 Network Attack Simulator (NASim), Cyber Battle Simulation (CBS), CALDERA와 같은 지능형 사이버 시뮬레이터를 활용한 다양한 모의 테스트를 진행하는 것이 필요하다.

본 논문에서는 사이버 시뮬레이션 환경을 활용하여 다양한 공격기술을 지능적으로 학습하기 위한 다양한 시나리오를 구성하였다. 또한, 인공지능 기법 중 하나인 강화학습을 이용하여 보다 다양한 사이버공격 기술을 효율적으로 학습하고 이를 효과적으로 대응할 수 있는 능력을 분석하는 방법을 제안하고 있다. 본 연구는 사이버 전투의 핵심인 지능형 시뮬레이션 개발을 목표로 하고 있으며, 사이버 보안 분야에서 효과적인 해결 방법을 찾는데 중요한 역할을 할 것으로 기대한다.

2. 관련 연구

2.1 Cyber Security Emulation

사이버 공격의 지속적인 위협으로 인해 개인과 기업 모두 이를 대응하기 위한 다양한 전략 기술들이 요구된다[12, 13]. CALDERA는 이러한 공격에 대응하기 위한 오픈소스 프레임워크이며 실제 공격자의 전술, 기법, 절차(TTPs)를 모방하여 다양한 공격 시나리오를 생성할 수 있다[14, 15]. 그러나 프레임워크의 복잡성 때문에 설정과 관리가 어려울 수 있다[16]. Cuckoo Sandbox는 파일 레벨의 악성코드 분석에 특화되어 있는 오픈소스 도구이다. 하지만, 네트워크 레벨에서의 복잡한 공격 시나리오를 완전히 재현하기 위해서는 다소 무리가 있다[17].

2.2 Network Attack Simulation

사이버 공격 및 대응 기술은 지속적으로 진화되고 있는 분야이며 이를 오직 전통적인 방어 메커니즘만으로만 대응하기는 매우 어렵다. 따라서 이를 해결하기 위해 인공지능 방법 중 하나인 강화학습을 활용하여 위협에 대응하기 위한 노력들이 지속적으로 이뤄지고 있다. Network Attack Simulator(NASim) [18]은 강화학습을 활용하여 네트워크 취약점을 분석하고 이를 검증하는 시뮬레이터이며 다양한 공격 시나리오를 구성할 수 있다. NASim은 실제 네트워크 공격의 모든 세부 사항을 재현하기보다는 주로 펜 테스트의 핵심 요소에 초점을 맞춰 시뮬레이션 환경을 테스트할 수 있고, 사용자는 효과적으로 공격 에이전트를 구성하여 학습을 진행할 수 있다. CyberBattleSim(CBS) [19, 20]는 Microsoft의 Defender Research Team에서 제작한 시뮬레이션 환경으로 공격과 방어 시나리오를 모두 구성하여 네트워크 내의 상호작용을 모의할 수 있다. 공격 에이전트는 사이버 환경 내의 미리 정의된 취약성 및 고정 네트워크를 악용하여 네트워크의 일부를 탈취하는 것을 목표로 하며 방어 에이전트는 이러한 네트워크 활동을 모니터링할 수 있으며 침입하는 공격자를 식별하고 노드를 다시 설치하거나 방화벽을 변경하는 등의 다양한 방어적 행동을 취할 수 있다.

3. 강화학습 기반 사이버 공격 기술

본 논문은 시뮬레이션 환경을 이용한 사이버 공격 전략 기술 방법 및 강화학습 기반 사이버공격 시나리오를 제안한다.

3.1 Cyber-Attack Simulation Strategy

NASim은 네트워크 구성 요소와 침투 테스트 상호작용을 모델링 하기 위해 설계된 시뮬레이션 환경이다. 본 논문에서는 NASim에서 제공하는 환경 요소를 이용하여 실제 환경과 유사한 네트워크 환경을 구성하여 네트워크의 복잡성과 상호작용을 보다 정밀하게 재현할 수 있도록 구성하였다. 기존에 NASim에서 제공하고 있는 Tiny와 Small 환경은 강화학습을 통한 최대 보상을 얻기 위해 기본 노드만 존재한다. 이러한 구성은 실제 네트워크 환경에서 사이버공격을 다양하게 반영하는데 한계가 있다. 따라서 이를 해결하기 위해서는 목표 노드에 도달하기 위한 다양한 경로를 제공할 수 있는 전략기술 및 환경 구성이 필요하다. 본 논문에서는 기존 문제점을 개선하기 위해 필수적으로 통과해야 하는 노드의 수를 줄이고 복잡한 네트워크 토폴로지를 반영하여 다양한 우회 경로가 추가된 Tiny-Alpha와 Small-Alpha를 구현하였다. 해당 시뮬레이션 환경은 2개의 추가 호스트와 다양한 서비스 및 운영 체제 설정을 통해 보다 높은 네트워크의 복잡성을 구성하여 서브넷, 운영 체제, 호스트 등 다양한 네트워크 구성 요소를 상황에 따라 보다 효과적인 학습할 수 있도록 설계하였다.

Fig. 1과 Fig. 3에서 볼 수 있듯이 기존 시뮬레이션 환경들은 목표까지의 경로가 고정되어 있어 실세계의 복잡한 네트워크 구조를 충분히 반영하지 못하고 있다. 또한 이

환경에서는 목표 노드에 도달하기 위한 단일 경로만을 제공하고 있기 때문에 최대 보상을 얻기 위해 필수적으로 통과해야 하는 추가 노드가 필요하다. 그러나 실제 네트워크 환경에서는 거미줄 같이 복잡한 네트워크 환경으로 구성되어 이 있어 목표 노드에 도달하기 위한 다양한 형태의 경로와 전략이 추가로 필요하다. Fig. 2와 Fig. 4는 본 논문에서 제안한 개선된 시뮬레이션 환경인 Tiny-Alpha와 Small-Alpha이며 이 환경은 필수적으로 통과해야 하는 노드의 수를 줄이고 다양한 우회 경로와 복잡한 네트워크 연결을 추가하여 실제 네트워크 환경과 유사한 시뮬레이션 환경을 제공하고 있다. 이는 실제 환경과 유사한 네트워크 연결 구조를 보다 정확하게 모사하여 모델링할 수 있으며 다양한 공격 패턴과 대응책에 대한 검증 또한 효과적으로 수행할 수 있다.

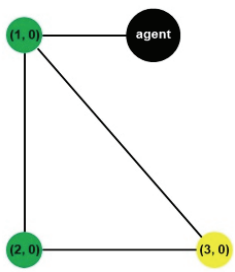

Fig. 1. Old Simulation Environment: Tiny.

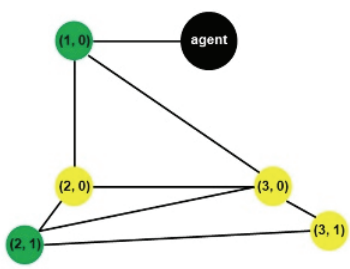

Fig. 2. New Simulation Environment: Tiny-Alpha.

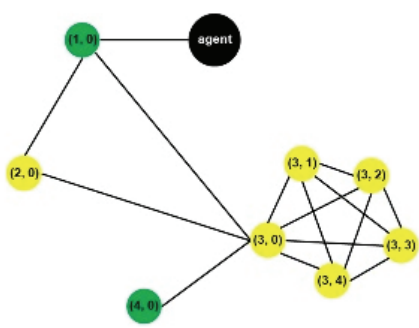

Fig. 3. Old Simulation Environment: Small.

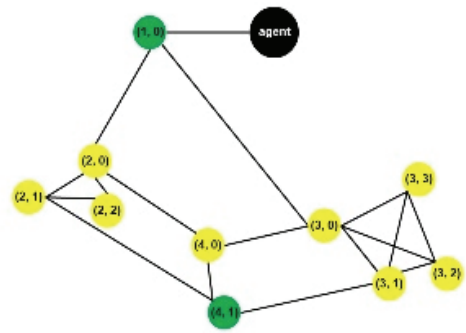

Fig. 4. New Simulation Environment: Small-Alpha.

3.2 Cyber-Attack Scenarios Based on Reinforcement Learning

본 논문에서는 제안된 NASim 환경을 기반으로 다양한 강화학습 방법을 적용하여 Markov Decision Process (MDP)[21]를 기반으로 Markov Game 형태의 최적 모델링을 진행하였다. 이 방법은 에이전트(Agent)가 환경을 탐색하며 선택한 행동(Action)는 환경 정보에 적극적으로 영향을 미치며, 환경 상태(State) 정보 따른 최적 보상(Reward)을 통해 에이전트는 지속적으로 학습을 진행하여 최적의 모델링을 찾는 방법이다. 이러한 모델링은 네트워크의 다양한 동적 요소를 지속적으로 고려할 수 있으므로 복잡한 네트워크 환경에서 매우 효과적으로 결과를 산출할 수 있다.

3.1에서 제안한 시뮬레이션 환경은 NASim을 기반으로 강화학습이 적용 가능할 수 있도록 사이버공격 시나리오를 설계되었다. 이 환경을 통해 공격 에이전트는 네트워크의 다양하고 복잡한 구성 요소를 상호작용하며 학습할 수 있으며 적대적인 시나리오에서도 최적의 공격 전략을 선택할 수 있다.

Table 1. Environment Configuration by Network Attack Simulator (NASim)

	Observation Space	Action Space
Components	Subnet	Subnet Scan
	OS	OS Scan
	Host	Host Scan
	Services	Service Scan
	Processes	Process Scan
	Network Topology	Privilege Escalation
		Exploit
		NoOp

Table 1과 Table 2에는 강화학습 에이전트가 학습에 사용할 수 있는 관찰 공간, 행동 공간, 그리고 각 시나리오의

핵심 변수들에 대한 상세 정보를 나타내고 있다. Table 1에서는 서브넷, 운영 체제, 호스트, 서비스, 프로세스 그리고 네트워크 토폴로지 등 다양한 관찰 공간의 변수들이 나열되어 있고 이러한 변수들은 강화학습 에이전트가 공격 전략을 효과적으로 학습하고 최적화하는데 사용된다. Action Space는 에이전트가 실행할 수 있는 다양한 행동들을 나열하고 있다. 이 행동은 에이전트가 네트워크의 중요 정보를 취득하고 권한을 상승시키며 다양한 공격 시나리오를 실행할 수 있는 모든 행동들이 포함된다. 에이전트는 이러한 행동을 통해 적대적 환경에서의 공격 전략을 학습하고 네트워크 내의 취약점과 공격 목표에 대한 정보를 추출할 수 있다. 또한, 서브넷, 운영체제, 호스트, 서비스 그리고 프로세스 등 네트워크에서 중요한 정보를 취득하기 위한 행동들과 취득한 정보를 토대로 네트워크 토폴로지를 점령하기 위해 권한 상승, 익스플로잇(Exploit)과 NoOp 등의 행동들이 있으며 이를 바탕으로 에이전트는 공격 전략을 개발하고 환경을 탐색하며 최적의 행동을 선택하기 위해 반복적인 학습을 진행한다. 뿐만 아니라, 에이전트는 네트워크 내의 취약점이나 공격 목표에 대한 정보를 분석하고 공격 체인을 형성하여 목표 노드에 도달하기 위해 취약점을 찾는 과정을 수행한다. 이를 통해 복잡한 네트워크 환경에 적응할 수 있고 보안 위협에 효과적으로 대응할 수 있는 최적의 전략을 학습하고 실행할 수 있다.

Table 2. Benchmark Scenario and Fundamental Learning Components on Network Attack Simulator (NASim)

Scenario / Obs	Tiny	Tiny Alpha	Small	Small Alpha
Subnets	3	3	4	4
Host	3	5	8	10
OS	1	1	2	1
Service	1	2	3	2
Process	1	1	2	2
Exploit	1	2	3	2
PrivEsc	1	1	2	2
Step limit	1000	1000	1000	1000
Action	18	21	72	80

Table 2에서는 각 시나리오의 복잡성을 나타내는 변수들, 즉 서브넷, 호스트, 운영 체제, 서비스, 프로세스, 익스플로잇, 권한 상승, 단계 제한, 행동의 개수와 같은 관찰 공간의 개수가 정리되어 있다. 강화학습을 적용하면 네트워크 취약점과 공격 목표를 식별하고 최적의 공격 및 방어 전략을 학습할 수 있다. 이를 통해 사이버 보안 전략과 그에 따른 대응책을 더욱 효과적으로 준비할 수 있을 것이며 이와 더불어 동적 학습(Dynamic Learning Process)과 같은 실시간 의사결정을 제공할 수 있기 때문에 빠르게 변화하는 사이버 위협 요소에 보다 민첩하고 효과적으로 대응할 수 있으며, 이를 바탕으로 사이버 전략 체계를 구성할 수 있을 것이다.

4. 실험 및 결과

본 논문에서는 개선된 NASim 환경에서 정책 기반(Policy-based) 강화학습과 값 기반 (Value-based) 강화학습을 수치적으로 비교하여 실험을 진행하였으며 어떤 학습방법이 이산적인 행동 공간에서 더욱 효과적인지, 혹은 얼마나 빠르게 수렴하는지 등에 대한 성능을 분석하였다.

4.1 Results of RL-based Learning Process

Table 3은 앞절에서 제안한 Table 1과 Table 2의 실험 환경을 바탕으로 도출된 실험 결과이다. NASim은 이산적인 Action Space와 선택된 강화학습 방법의 성능을 바탕으로 Action Space 특정 관찰 공간에서 가능한 이산적인 행동의 결과가 다르게 나타날 수 있다. 특히, 공격 시나리오에서 정의된 노드의 값에 따라 공격자가 취할 수 있는 행동의 수와 각 행동에 대한 보상 함수가 정의되어 있으므로 사이버공격 시뮬레이션 환경에서 Action Space는 연속적인 행동이 아닌 이산적인 행동으로 구성되어 있음을 알 수 있다.

Table 3의 Actor-Critic은 정책 기반의 강화학습 방법 중 하나이며 Actor가 정책을, Critic이 값을 학습하는 구조이다. 이 방법은 연속적인 행동(Continuous Action Space)을 취하는 데 유리하다. 따라서, Actor-Critic은 다른 강화학습 방법들에 비해 빠른 수렴 속도를 보였지만, 학습 결과의 불안정성 때문에 낮은 평균 보상(Mean Reward) 값이 실험 결과에 나타나고 있다.

Table 3. RL-based Learning Process

	Model	Tiny	Tiny Alpha	Small	Small Alpha
Mean / Max Reward	Actor Critic	152.8	146	85.4	126.1
		192	191	175	183
	Q-Learning	192.9	189.8	184.2	187.2
		194	191	186	189
	Deep Q-Learning	193.3	190.2	184.8	188.1
		194	191	186	189
	Duel Deep Q-Network	193.2	190.1	184.8	188.1
		194	191	186	189

반면 값 기반의 강화학습 방법들(Q-Learning, Deep-Q-Network, Double Deep-Q-Network)은 주로 이산적인 행동(Discrete Action Space)을 취하는 시뮬레이션 환경에 최적화되어 있다. 일반적으로 이 방법들은 값(value)을 사용하며 각

상태에 대한 행동 결과를 Q-Table 혹은 Neural Network에 적용하여 결과를 계산한다. 따라서 NASim과 같이 이산적인 행동을 요구하는 환경에서는 높은 평균 보상(Mean Reward) 값과 환경 내에서 획득 가능한 최대 보상(Max Reward)을 얻을 수 있기 때문에 매우 적합한 학습 방법임을 알 수 있다.

실험 데이터의 수치적 분석 결과에서 평균 보상(Mean Reward) 값은 Small과 Small-Alpha 시나리오에서 약 53.2%의 성능 차이를 나타내고 있으며, Tiny와 Tiny-Alpha 시나리오에서는 평균 보상의 차이가 약 20.9%의 성능 차이를 보이는 것을 알 수 있다.

4.2 Results of Performance and Convergence Comparison

본 논문에서는 Fig. 5~12과 같이 시각화를 통한 강화학습 방법들의 수렴 결과를 확인할 수 있다. 상대적으로 작은 시나리오인 Fig.5의 Tiny와 Fig.6의 Tiny Alpha 시뮬레이션 환경에서 Actor-Critic(Blue)의 정책(policy) 기반의 강화학습 방법이 값(value) 기반의 강화학습 방법들과 비교하였을 때 빠르게 수렴하는 경향을 보여주고 있지만, 낮은 보상 값으로 인해 매우 불안정한 학습 결과를 나타내고 있다.

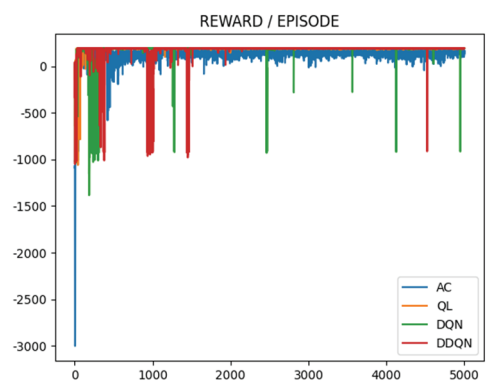

Fig. 5. Reward/Episode Results in Tiny.

Fig. 6. Reward/Episode Results in Tiny-Alpha.

학습이 종료된 후 결과값에서도 Actor-Critic(Blue)은 수렴 폭이 매우 넓게 나타나고 있으며, 반면에 Q-Learning (Orange)의 결과값은 전반적으로 안정적으로 수렴하는 경향을 보여주고 있다. DQN(Green)과 DDQN(Red) 또한 일부 구간에서 수렴하지 않는 모습을 보였지만, 최종적으로 안정된 학습 곡선을 나타내고 있다. 시나리오가 확대된 Fig.7의 Small과 Fig.8의 Small Alpha에서는 Actor-Critic(Blue)의 경우, 수렴 폭이 넓어졌고, Q-Learning(Orange), DQN(Green), 그리고 DDQN(Red)은 모두 초기 학습 성능이 좋지 않지만 이후 빠르게 수렴하는 경향을 보이고 있다.

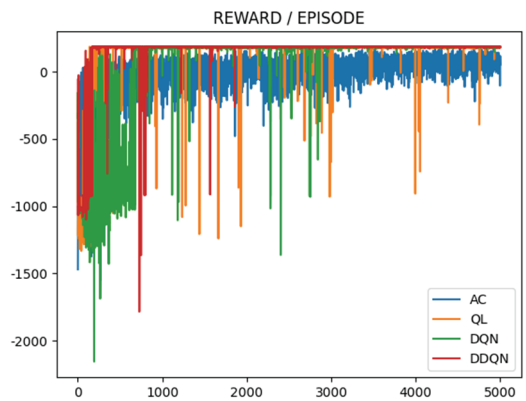

Fig. 7. Reward/Episode Results in Small.

Fig. 8. Reward/Episode Results in Small-Alpha.

에피소드에 따른 보상만을 고려한다면 학습의 효율성을 정확하게 평가할 수 없지만 학습 과정에서의 다른 중요한 지표인 에피소드별 스텝의 변화량도 함께 분석해야 결과를 보다 정확하게 판단할 수 있다. 변화량의 그래프는 Fig. 9~12에서 나타내고 있다. 스텝 수의 변화와 보상 값의 변화량은 유사한 형태를 보이지만, 학습의 진척도에 따라 같은 스텝 수를 사용해도 얻는 보상은 다를 수 있다.

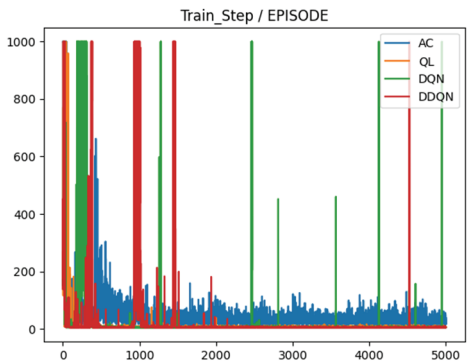

Fig. 9. Step/Episode Results in Tiny.

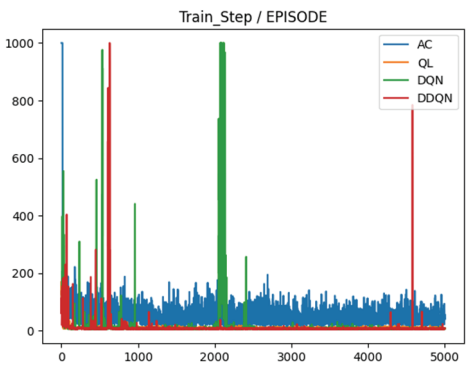

Fig. 10. Step/Episode Results in Tiny-Alpha.

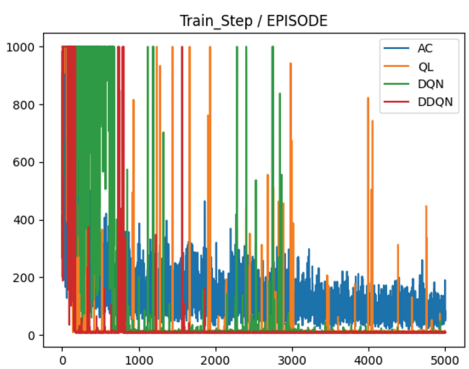

Fig. 11. Step/Episode Results in Small.

결과적으로 전체적인 실험결과를 살펴보면 Step/Episode 결과값은 이전 Reward/Episode 실험 결과에서 확인한 것과 같이 유사한 그래프 경향을 나타내고 있다. Fig. 9와 Fig. 10의 시나리오에서는 적은 수의 에피소드만으로도 공격이 성공할 가능성이 높은 것을 확인할 수 있고 이보다 넓고 복잡한 상태 공간을 가진 Fig. 11와 Fig. 12의 시뮬레이션 환경에서는 값(value) 기반의 강화학습 방법에서는 학습 성능 향상을 위해 더 많은 스텝이 필요한 것을 알 수 있다.

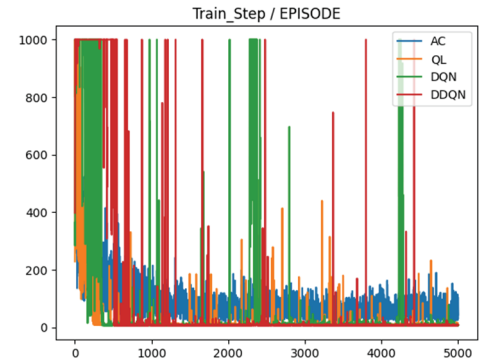

Fig. 12. Step/Episode Results in Small-Alpha.

5. 결 론

본 논문은 사이버 공격 시뮬레이션 환경(NASim)을 활용하여 다양한 사이버 공격 시나리오를 구현하였고 이를 기반으로 다양한 강화학습 방법의 학습 성능을 비교 분석하였다. 또한, 시뮬레이션 환경 및 사이버 공격 시나리오를 추가 개발하여 네트워크 크기와 복잡도에 따른 학습 성능 변화도 관찰하였으며 그 결과 강화학습 보상 값 외에도 에피소드별 스텝의 변화량과 같은 다른 지표를 고려해야만 학습의 전반적인 효율성을 정확하게 평가할 수 있음을 확인할 수 있었다. 또한, 연속적인 행동 중심의 정책(policy) 기반 강화학습 방법은 빠른 수렴 속도를 보였으나 불안정성과 수렴 결과와 낮은 평균 보상의 문제가 있음을 확인할 수 있었으며, 반면 값(value) 기반의 강화학습 방법들은 작은 사이즈의 시뮬레이션 환경에서 보다 높은 성능을 보였으며 복잡한 환경에서도 정책(policy) 기반의 학습 방법에 비해 상대적으로 좋은 성능을 보여주고 있는 것을 알 수 있었다. 이러한 실험 결과는 향후 사이버공격 강화 훈련에서 인공지능 기술을 적용하기 위한 좋은 성능 지표를 제공할 것이며 군사, 정부, 기업 등에서의 사이버 보안 교육과 시스템 보안 검증에도 도움이 될 것으로 보인다.

향후 연구로서 보다 다양한 공격 및 방어 전략 훈련을 위해 멀티 에이전트 기반의 사이버 공격/방어 기술을 개발하여 보다 효과적인 보안 기술 강화에 대비할 필요가 있다.

감사의 글

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Government (MSIT) (No.2022-0-00961).

참고문헌

1. Kim, D. W., Lee, M. S., Jeong, J. Y., Kim, and H. C., “COVID19 Related Keyword Analysis: Based on Topic Modeling and Semantic Network Analysis,” Journal of the Semiconductor & Display Technology, Vol. 21, No. 2, pp.127-132, 2022.
2. Kang, Y. G., Yoo, J. D., Park, E.J., Kim, D. H., and Kim, H.K., “Design and Implementation of Cyber Attack Simulator based on Attack Techniques Modeling,” Journal of the Korea Society of Computer and Information, Vol.25, pp.65-72, 2020.
3. Taherdoost, H., “Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview,” Electronics, Vol. 11, pp. 2181, 2022.
4. Lee, J. Y., Moon, D. S. and Kim, I. K., “Technological Trends in Cyber Attack Simulations.” Electronics and Telecommunications Trends, Vol. 35, pp. 34–48, 2020.
5. Rabie, A. R., Bassam, W. A., Jalawi, S. A., Abdullah, J. A., Ayman, E.S., and Mohamed, M. D., “Cybersecurity and Countermeasures at the Time of Pandemic", Journal of Advanced Transportation, Vol. 2021, pp. 1-19, 2021.
6. Al‐Qahtani, A. F., and Cresci, S., “The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19,” IET Information Security, Vol.16, pp.324-345, 2022.
7. Singh, S., Sharma, P. K., Moon, S. Y., Moon, D. S., and Park, J. H., “A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions”, The Journal of Supercomputing, Vol. 75, pp. 4543-4574, 2019.
8. Choi,Y. K., Jang I. S., Whoang, I., Kim, T. G., Hong, S. J., Park, I. S., Yang, J. S., Kwon, Y. J., and Kang, J. M., “Design and Implementation of Cyber Range for Cyber Defense Exercise Based on Cyber Crisis Alert.” Journal of the Korea Institute of Information Security & Cryptology, Vol. 30, pp. 805–821, 2020.
9. Milian, E. Z., Spinola, M. D. M., and Carvalho, M. M., “Fintechs: A literature review and research agenda", Electronic Commerce Research and Applications, Vol. 34, 2019.
10. Jiang, H., Choi, T., and Ko, R. K. L., “Pandora: A cyber range environment for the safe testing and deployment of autonomous cyber-attack tools,” Security in Computing and Communications, Vol. 1364, pp. 1-20, 2021.
11. Yamin, M. M., Katt, B., and Gkioulos, V., “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” Computers & Security, Vol. 88, pp. 101636, 2020.
12. Yamin, M. M., and Katt, B., “Use of cyber attack and defense agents in cyber ranges: A case study,” Computers & Security, Vol. 122, pp. 102892, 2022.
13. Katina, P. F., and Keskin, O. F., “Complex system governance as a foundation for enhancing the cybersecurity of cyber-physical systems,” International Journal of Cyber Warfare and Terrorism, Vol. 11, pp. 1-14, 2021.
14. Kim, D. H., Kim, Y. H., Ahn, M. K., and Lee, H. J., “Automated cyber threat emulation based on ATT&CK for cyber security training,” Journal of the Korea Society of Computer and Information, Vol. 25, pp. 71-80, 2020.
15. Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., and Kim, H. K., “Cyber attack and defense emulation agents,” Applied Sciences, Vol. 10, pp. 2140, 2020.
16. Mohamed, N., “Study of bypassing Microsoft Windows Security using the MITRE CALDERA framework” F1000 Research, Vol. 11, pp. 16-25, 2022.
17. Sainadh, J., Navya, Y. S., Raja, P., Tagore, G., and Rao, G. R. K., “Dynamic Malware Analysis Using Cuckoo Sandbox”, 2018 Second International Conference on Inventive Communication and Computational Technologies, pp. 1056-1060, 2018.
18. Jjschwartz, “NetworkAttackSimulator (Version 0.9.1).” Retrieved August 12, 2021, from https://github.com/Jjschwartz/NetworkAttackSimulator (Publication Date: N/A).
19. Microsoft, “CyberBattleSim (Version 2.4.0).” Retrieved August 26, 2021, from https://github.com/microsoft/CyberBattleSim.
20. Walter, E., Ferguson-Walter, K., and Ridley, A., “Incorporating Deception into CyberBattleSim for Autonomous Defense.” Retrieved May 18, 2023, from https://arxiv.org/abs/2108.13980, 2021.
21. Xiang, X., Foo, S., and Zang, H., “Recent Advances in Deep Reinforcement Learning Applications for Solving Partially Observable Markov Decision Processes (POMDP) Problems Part 2 - Applications in Transportation, Industries, Communications and Networking and More Topics”, Machine Learning and Knowledge Extraction, Vol. 3, pp. 863-878, 2021.

접수일: 2023년 9월 8일, 심사일: 2023년 9월 15일,
게재확정일: 2023년 9월 18일