
Snooping Attacks on Deep Reinforcement Learning

Matthew Inkawhich
Duke University
mji5@duke.edu

Yiran Chen
Duke University
yiran.chen@duke.edu

Hai Li
Duke University
hai.li@duke.edu

Abstract

Adversarial attacks have exposed a significant security vulnerability in state-of-the-art machine learning models. Among these models include deep reinforcement learning agents. The existing methods for attacking reinforcement learning agents assume the adversary either has access to the target agent’s learned parameters or the environment that the agent interacts with. In this work, we propose a new class of threat models, called snooping threat models, that are unique to reinforcement learning. In these snooping threat models, the adversary does not have the ability to personally interact with the environment, and can only eavesdrop on the action and reward signals being exchanged between agent and environment. We show that adversaries operating in these highly constrained threat models can still launch devastating attacks against the target agent by training proxy models on related tasks and leveraging the transferability of adversarial examples.

1 Introduction

The deep learning revolution has put neural networks at the forefront of the machine learning research and production landscape. Recently, it has been shown that deep neural networks (DNNs) are effective function approximators for solving complex reinforcement learning (RL) problems. Mnih et al. [20] demonstrated that we can leverage the feature extraction capabilities of convolutional neural networks to enable RL agents to learn to play Atari games from raw pixels. Since then, there has been an influx of work dedicated to the field of deep RL (DRL), enabling powerful new solutions for tasks such as game playing [20, 22, 34, 31], continuous control [17, 32, 33], complex robot manipulation [16, 29, 27], and even autonomous vehicle operation [4, 30].

Despite the numerous successes of the applications of deep neural networks, these models have a significant Achilles’ heel. Studies show that these largely uninterpretable models are vulnerable to small adversarial perturbations to the input that cause the models to perform poorly [36, 10]. Recent work has uncovered a variety of adversarial attack algorithms in the domain of image classification [10, 6, 24, 8]. Alarming, results show that adversarial examples effective against one model are also effective against other models trained on the same task [10]. This transferability property has enabled attacks against models in black-box settings [25, 13].

As of now, adversarial attacks against DRL agents primarily consider the white-box threat model, in which the adversary is assumed to have access to the target model’s architecture and parameters. To our knowledge, the study of black-box attacks against DRL has been limited to the acknowledgement of the transferability of adversarial examples across policies and algorithms [12]. Thus, the current method for black-box attacks against DRL agents involves training a surrogate agent, which makes the rather unrealistic assumption that the adversary has unbounded access to the environment. In general, the black-box threat model in RL is more complex than it is in supervised learning. First, in the data generating process for supervised learning, the model draw samples i.i.d. from a static dataset. In RL, data generation is in the form of an environment from which new data samples are conditioned on the current environment state and the agent’s actions. This means that an RL adversary cannot trivially approximate the training data generating process the way a supervised learning adversary

can. Also, the RL problem consists of an exchange of a three signals between the environment and agent (state, action, reward). Even if an RL adversary seeks to approximate the agent or environment using some other method (e.g. inverse RL), they would need access to all signals.

In this work, we investigate threat models for DRL under the assumption that the adversary does not have access to the environment that the target agent interacts with. Specifically, we explore the potential effectiveness of an adversary that only has the ability to eavesdrop on a subset of the RL signals at each time step. We dub these the snooping threat models. We show that by training proxy models on tasks *similar* to the target agent’s task, we are able to craft adversarial inputs that significantly reduce the performance of target agents trained on various Atari environments. We feel this to be a more practical threat model for real-world systems. Overall, the contributions of this paper can be summarized as follows:

- We define the complex threat model for snooping attacks on DRL agents.
- We propose the use of proxy models for launching effective adversarial attacks under the different snooping threat models.
- We conduct extensive experiments using the attacks against the state-of-the-art DRL algorithms DQN [20] and PPO [32].
- We empirically show that adversarial examples transfer between models that are trained with very different objectives as long as the tasks are related.

2 Related work

Adversarial machine learning is a research area that investigates the vulnerabilities of deep neural networks to small adversarial perturbations. In this work, we focus on evasion attacks, which are test-time attacks designed to fool a trained model. This topic was popularized in the image classification domain in the white-box setting, where Szegedy et al. [36] discovered that adding imperceptible noise to an image causes the model to predict the incorrect class with high confidence. Goodfellow et al. [10] followed by suggesting a fast gradient method for crafting adversarial examples in an inexpensive way by assuming local linearity in the target model. [10] also observed that adversarial examples crafted using the gradients of one model transfer to other models trained on the same task. Papernot et al. [25] leveraged this concept of transferability and introduced a framework for black-box attacks that uses the target model as an oracle to train a surrogate model with a similar decision surface, and uses the surrogate to craft adversarial examples that also fool the target.

In the DRL domain, Huang et al. [12] showed that the fast gradient method [10] can be extended to fool agents on the Atari benchmark. Lin et al. [18] introduced a strategically-timed attack, which seeks to make perturbations sparse in time to render them more difficult to detect. [18] further presented an enchanting attack that strives to lure the target agent into a specified state. Behzadan and Munir [1] demonstrated that adversarial examples can be used during training to corrupt the learning process of an agent on the Atari Pong environment. Adversarial examples have also been used for hardening DRL models to environmental parameter variations in continuous control environments [28]. Overall, adversarial attacks on DRL agents have primarily been limited to the white-box setting.

3 Preliminaries

3.1 Adversarial example crafting

The goal of adversarial example crafting is to apply an imperceptible perturbation to a benign input such that the perturbed input fools the target model. In this work, we consider variants of the Fast Gradient Method (FGM) [10] because it is computationally efficient and generalizes to models other than classifiers. FGM is a one-step method that assumes linearity of the decision surface around a given sample. With this assumption, the optimal perturbation for an input x is in the direction to maximize the loss J . We consider constraining the perturbations under the L_∞ and L_2 norm bounds.

Under the L_∞ norm bound $\|x^* - x\|_\infty \leq \epsilon$, an adversarial example x^* is generated as

$$x^* = x + \epsilon * \text{sign}(\nabla_x J(x, y)) \quad (1)$$

where y is the label. Under the L_2 norm bound $\|x^* - x\|_2 \leq \epsilon$, x^* is generated as

$$x^* = x + \epsilon * \frac{\nabla_x J(x, y)}{\|\nabla_x J(x, y)\|_2}. \quad (2)$$

We also consider a momentum iterative variant of FGM (MIFGM) introduced by Dong et al. [8]. This variant disregards the linearity assumption and iteratively perturbs while accumulating a velocity vector in the direction of the gradient to stabilize the perturbation direction and combat overfitting.

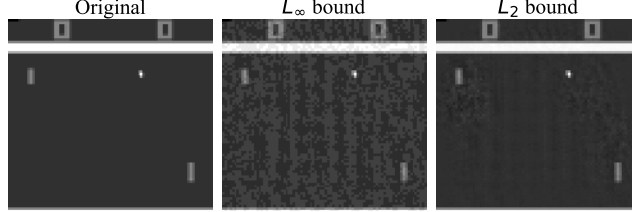


Figure 1: Adversarial example comparison between FGM attacks under different norm constraints on the Pong environment. The L_∞ bounded example was crafted with $\epsilon = 0.03$ and the L_2 bounded example used $\epsilon = 2.4$. These examples were crafted using the psychic proxy model (see 5.2).

3.2 Reinforcement learning

Reinforcement Learning is a machine learning paradigm based on sequential interactions between an agent and an environment in which the agent attempts to learn a policy π to maximize a total reward [35]. This interaction is formalized as a Markov Decision Process (MDP), which is the tuple $\langle \mathcal{S}, \mathcal{A}, \mathcal{P}, \mathcal{R}, \gamma \rangle$. \mathcal{S} is a finite set of states, \mathcal{A} is a finite set of actions, $\mathcal{P}(s, a, s') = P(S_{t+1} = s' | S_t = s, A_t = a)$ is the state transition function, $\mathcal{R}(s, a) = \mathbb{E}[R_{t+1} | S_t = s, A_t = a]$ is the reward function and $\gamma \in [0, 1]$ is a discount factor. The interaction can be described as follows: At each time step t , the environment sends a state s_t to the agent. The agent decides on an action a_t and dispatches it back to the environment. The environment responds by sending a reward r_{t+1} to the agent along with the next state s_{t+1} , and the process repeats. In this work, we consider the state-of-the-art value-based DRL method DQN [20] and policy-based PPO [32]. See Appendix for descriptions of these methods.

4 Snooping threat models

A high level view of the snooping threat model for DRL is portrayed in Figure 2. As in any threat model, we assume the adversary can intercept and manipulate the input game frames (i.e. the state). In the snooping family of threat models, the adversary does not have direct access to the environment, so training a surrogate DRL model and transferring examples from the surrogate to the target is ruled out. Instead, the adversary can only "snoop", or eavesdrop, on the natural interactions between the agent and environment. We define the **SRA** threat model to represent the scenario in which the adversary can snoop on reward and action signals, **SA** for when the adversary can only snoop on the actions, **SR** for when the adversary can only snoop on the rewards, and **S** for when the adversary only has access to the states. When the reward signal is hidden, the adversary is assumed to have no inclination about the goal of the agent. In the general case of game environments, this means that the adversary cannot explicitly infer the difference between winning and losing. When the action signal is hidden, not only is the adversary unable to determine which actions correspond to certain changes in the state space, but there is also no way of explicitly knowing the scope and magnitude of the action space at all.

5 Attack strategies

5.1 Methodology

Our general attack methodology is to leverage the transferability of adversarial examples. While this concept is not fully understood, recent efforts show that transferability is primarily enabled by decision boundary similarity between models [37, 36, 19]. We argue that this condition, however, generally overestimates the resources necessary to craft effective transferable adversarial examples.

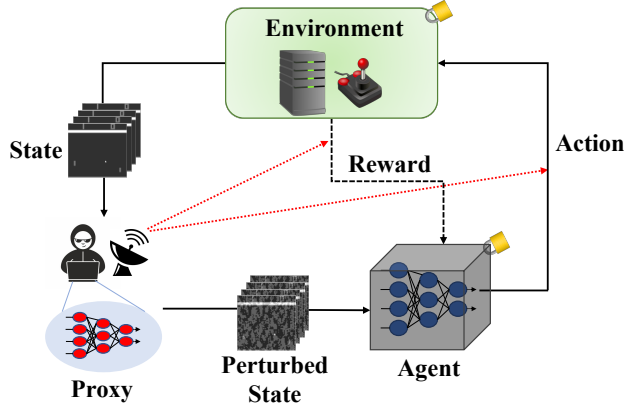


Figure 2: Snooping threat model overview for DRL.

The snooping threat models for RL provides one such counterexample, in which the adversary cannot train a surrogate DRL model that closely resembles the target agent. Instead, we posit that if the adversary can train a proxy model that learns a task that is *related* to the target agent’s policy to maximize reward, adversarial examples crafted to fool the proxy will also fool the agent. This implies that even proxy models with radically different decision surface dimensionality than the target can reliably produce transferable attacks. We hypothesize that by learning a related task, the proxy will learn to extract and use input features in a similar fashion to the target agent, which is the only necessary condition for crafting transferable attacks. Our explicit goal is to train a proxy model \mathcal{M} under a constraint subset $\kappa \in \{S, SR, SA, SRA\}$ parameterized by $\theta_{\mathcal{M}_\kappa}$ with loss $J_{\mathcal{M}_\kappa}$ that extracts similar input features and learns comparable implications of these features to the target agent \mathcal{T} parameterized by $\theta_{\mathcal{T}}$ trained with loss $J_{\mathcal{T}}$ (e.g. temporal difference error). Using input gradients as an indication of feature saliency, our intention is to train a constrained proxy \mathcal{M}_κ to optimize:

$$\arg \min_{\mathcal{M}_\kappa} \left[\frac{1}{N} \sum_{i=1}^N \left(\nabla_x J_{\mathcal{M}_\kappa}(\theta_{\mathcal{M}_\kappa}, x_i, y_i) - c \nabla_x J_{\mathcal{T}}(\theta_{\mathcal{T}}, x_i, z_i) \right) \right] \quad (3)$$

where N is an arbitrary number of inputs, x_i is an input, y_i is the true label for the proxy, z_i is the pseudo-true label [12] for the agent, and c is an unknown constant. We include c as a scaling constant as we desire \mathcal{M}_κ to produce similarly *shaped* input gradients to \mathcal{T} ’s, meaning the magnitude of the gradients do not necessarily have to align exactly. Note that this objective is a theoretical representation, and does not represent a tractable optimization objective. The exact choice of task and proxy \mathcal{M}_κ is determined by our discretion. Also note that since we are attacking RL agents during test time, we will not have access to truth labels required by the FGM method (i.e. the y in Equations 1 and 2), as RL data is inherently unlabeled. To work around this, we follow [12] and assume that our surrogates and proxies have converged to a reasonable minima, so we use their outputs as "truth". For surrogate agents or classifier proxies, we use the one-hot output of the model as truth, and for regressor proxies, we use the output (plus a small constant)¹ as truth.

5.2 S threat model

The **S** threat model is the weakest snooping threat model. The adversary only has access to a stream of states, and has no inclination about the motivations or capabilities of the agent. In this case, we propose a proxy \mathcal{M}_S that models the environment dynamics. Previous work shows that we can perform accurate next-frame prediction using the current state, action, and an L_2 reconstruction loss as long as \mathcal{P} is roughly deterministic [23, 38, 15]. This model directly approximates the state transition distribution $\mathcal{P}(s, a, s')$. In **S** however, we do not have access to \mathcal{A} , so the best we can do is approximate an expectation of \mathcal{P} under the target agent’s policy π_T using a *psychic* proxy model:

$$\text{psychic}(s_t, \theta_P) \approx \mathbb{E}_{\pi_T} [P(s_{t+1}|s_t)] = \mathbb{E}_{a_t \sim \pi_T} [P(s_{t+1}|s_t, a_t)]. \quad (4)$$

Because the psychic learns the dynamics \mathcal{P} under π_T , it effectively learns an encoding of π_T in the state space. In other words, the displacement of the agent’s representation in the state space (e.g. the

¹We must add a small constant to avoid computing a loss of zero.

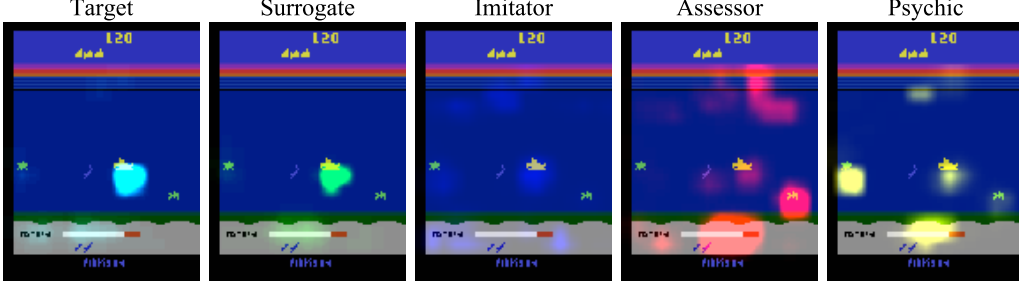


Figure 3: Comparison of features learned by target agent, surrogate agent, and proxy models on Seaquest environment using perturbation-based saliency map visualizations [11].

pixels of the paddle in Breakout) from s_t to s_{t+1} inherently encodes a representation of the action a_t taken and therefore an instance of the agent’s policy $\pi_T(s_t)$. This approximation will be noisy in general due to displacements in the state space that are not the consequence of the agent’s actions (e.g. the movement of the fish in Seaquest). Despite the noisiness, the key is that a subset of the features learned by the psychic will be similar to the features learned by the target agent.

5.3 SR threat model

In the **SR** threat model, we can intercept the states and snoop on the rewards. Because we do not have access to the actions, we again cannot make any presumptions about the policy π_T directly. However, by observing the rewards resulting from each state in a rollout we can get insight into the agent’s motivations by training an *assessor* proxy to estimate the value V of a given state under π_T . Since the reward signal is what drives the policy π_T , the features learned to approximate V^{π_T} must correspond to the features used by the agent itself.

$$assessor(s_t, \theta_A) \approx \mathbb{E}_{\pi_T} \left[\sum_{k=0}^{\infty} \gamma_t^{(k)} r_{t+k+1} \right] = V^{\pi_T}(s_t) \quad (5)$$

In our study we use empirical return to estimate value, meaning that we observe the immediate rewards at each step, and when the episode is over we retroactively calculate the (standardized) discounted sum of rewards at each state. During training, the assessor minimizes a Huber regression objective [9] between predicted value and empirical value. Despite the fact that the $J_{\mathcal{M}_{SR}}$ objective is different than J_T , the task of approximating V^{π_T} is directly related to π_T . For example, value-based agents directly approximate a value estimate $Q^{\pi_T}(s_t, \pi_T(s_t)) = V^{\pi_T}(s_t)$, and for policy-based agents, the explicit goal of the resulting policy is to maximize return, so implicitly the agent learns to assess the value of states.

5.4 SA threat model

In the **SA** threat model, we have access to a stream of states and can snoop on the actions taken by the agent at each step. Therefore, approximating π_T can be done directly with supervised learning. We can train an *imitator* model to predict the action that the target will take at a given state as:

$$imitator(s_t, \theta_I) \approx \pi_T(s_t). \quad (6)$$

Since the imitator is a classifier, we train it with cross-entropy loss ($J_{\mathcal{M}_{SA}}$) using the agent’s actions as labels. Although the imitator is trained with a different objective, it is directly related to the target agent’s goal. For value-based agents, the policy π is an ϵ -greedy extension of the learned Q-function and for policy-based agents, the function π_T is directly approximated. This methodology is homologous to the black-box attack strategy in [25], in which a substitute model is trained using the target model as an oracle. Note that if we were to have a continuous action space, the imitator would simply become a regression model.

5.5 SRA threat model

When we have the ability to eavesdrop on rewards *and* actions, we can attack with an imitator, assessor, or psychic. However, with this additional information we can improve our attacks by strategically timing the perturbations to make them less detectable. Lin et al. [18] show that we can accomplish

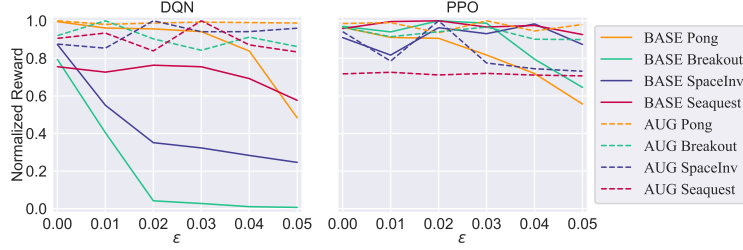


Figure 4: The effect of uniform random noise on trained agent performance. BASE agents are trained without noise and AUG agents are trained with noise. Rewards are averages over 10 episodes.

this in a white-box setting by defining a preference function $c(s_t) = \max_{a_t} [\text{Softmax}(Q(s_t, a_t))] - \min_{a_t} [\text{Softmax}(Q(s_t, a_t))]$ and attacking when $c(s) \geq \beta$ for some threshold β . At first glance, it may seem possible to use a similar preference-based approach with our imitator or assessor models. However, these proxies are only ever exposed to one particular policy π_T during training, so they lack the ability to assign credit to certain states or actions from the delayed reward signal. The RL agent, by contrast, learns this credit assignment through repeated trial and error during training. Nevertheless, we can approximate this ability using a combination of an assessor and an action-conditioned psychic (AC-psychic), which predicts s_{t+1} given s_t and a_t [38]. To perform the attack, we use the AC-psychic to generate a hypothetical next-state for every action given the current state, and value each of these with the assessor. We define a preference function whose output increases as the variation of potential future reward increases. In other words, we want to perturb s_t when there is a large difference in the different hypothetical values $V^{\pi_T}(s_{t+1}^H)$. To craft the perturbations, we can choose \mathcal{M}_{SRA} to be the proxy model of our choice (i.e. \mathcal{M}_S , \mathcal{M}_{SR} , or \mathcal{M}_{SA}). For details, see Algorithm 1.

Algorithm 1: Strategically-timed snooping attack

Input: Trained assessor, trained AC-psychic, trained proxy \mathcal{M}_κ , trained target agent \mathcal{T} , β

```

for  $t = 1, T$  do
    Initialize empty list  $q$ ;
    foreach  $a \in \mathcal{A}$  do
        Predict  $s_{t+1}^H$  with AC-psychic( $s_t, a$ );           ▷ Generate hypothetical next-state
        Estimate  $V^H$  with assessor( $s_{t+1}^H$ );           ▷ Value the hypothetical next-state
        Append  $V^H$  to  $q$ ;
    end
     $c(s_t) = \max [\text{Softmax}(q)] - \min [\text{Softmax}(q)]$ ;           ▷ Compute preference
    if  $c(s_t) \geq \beta$  then
        Perturb  $s_t$  using  $\nabla_x J_{\mathcal{M}_\kappa}$ ;           ▷ Attack if preference exceeds a threshold
    end
    Feed  $s_t$  to target  $\mathcal{T}$  for action decision;
end

```

6 Experiments and analysis

Although previous work has shown that DRL agents are vulnerable to adversarial noise, to our knowledge it is not clear whether it is the *adversarial* nature of the noise or simply the presence of noise that causes the agents to fail. Figure 4 shows that small uniform random noise significantly impacts agent performance. We believe that this fragility is due to the narrow training data distribution. Atari frames do not naturally contain the noise, occlusion, or lighting variations that natural images do, which leads to a higher risk of overfitting. In the interest of proving that our attacks are effective due to transferability between proxy and agent, for the remainder of the work we only consider agents that are hardened with uniform random noise perturbations during training. Our experiments show that this produces more robust models while not significantly reducing clean data performance.

To test the effectiveness of the attacks outlined in Section 5, we average the total reward accumulated by the target agent over 10 episodes of states perturbed by the FGM or MIFGM attacks at every time

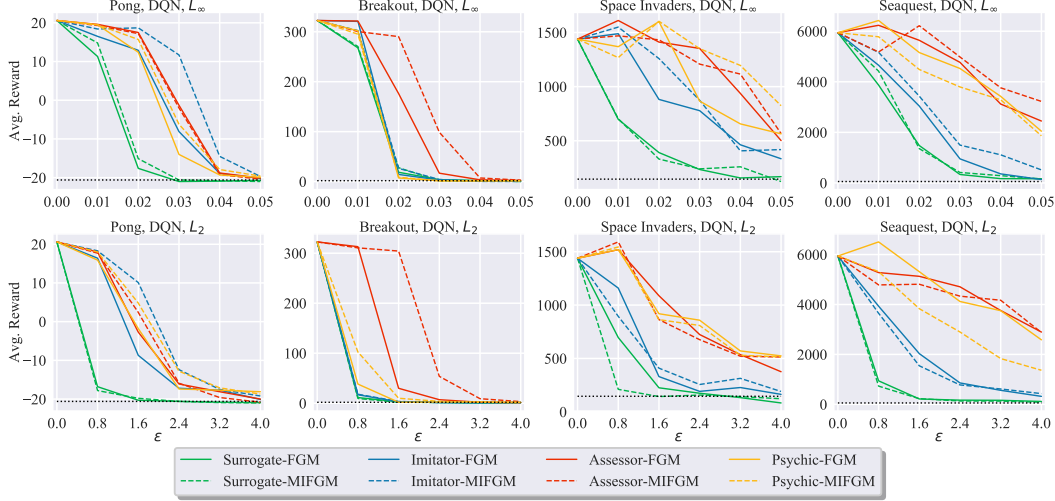


Figure 5: Performance reduction of DQN agents due to L_∞ and L_2 bounded perturbations. The black dotted line represents a random-guess policy.

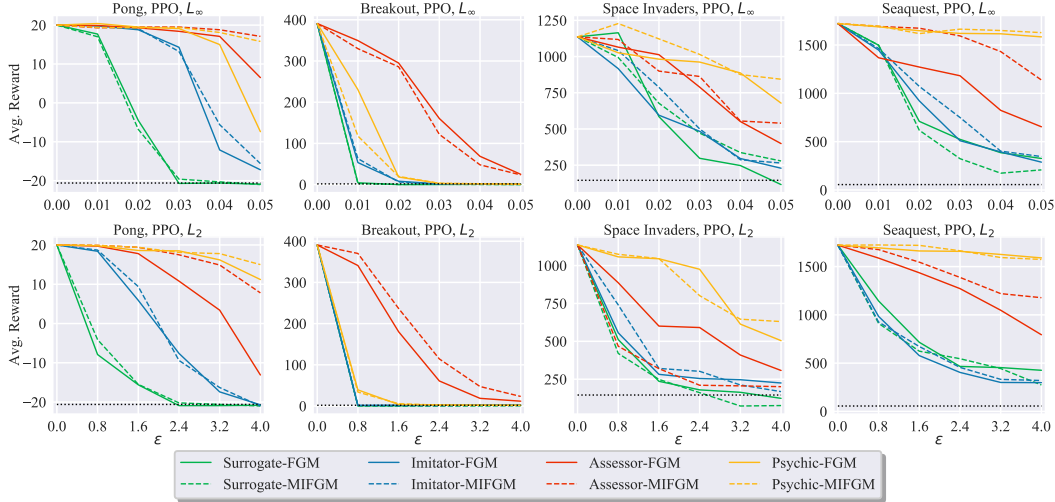


Figure 6: Performance reduction of PPO agents due to L_∞ and L_2 bounded perturbations. The black dotted line represents a random-guess policy.

step (using the proxy gradients $\nabla_x J_{\mathcal{M}_\kappa}$). We repeat this on each game for five ϵ values (i.e. attack strengths). For an upper-bound baseline attack, we use the policy-transfer methodology proven to be effective in [12] that assumes the adversary can train an identical model to the target agent, and use this model as a surrogate for crafting transferable adversarial examples. Figures 5 and 6 show the effectiveness of the transferred adversarial examples on the DQN and PPO agents, respectively. Note that the Appendix contains figures showing the attack success rates over time steps.

The imitators produce the most effective attacks out of the proxy models, performing comparably to the surrogate in all games. We believe this is because these models represent the most direct proxy to the agent’s policy π_T . The assessor attacks generally require a higher ϵ to reach the performance of the baseline and imitator attacks. Work by Tramèr et al. [37] gives the insight that better performing models yield more transferable adversarial examples. We therefore hypothesize that the reason for the lower performance of the assessor attacks is because the task of predicting the exact floating point value of a given state is a difficult objective to approximate precisely given the sparsity and variance of the reward signals. The attacks from the psychics perform worse than the surrogate and imitator attacks in general. This is not surprising, as the psychics operate under the most difficult threat model. In essence, the psychic model learns a noisy encoding of what the imitator learns directly. In some environments, the psychic attacks are more effective than the assessor attacks. This

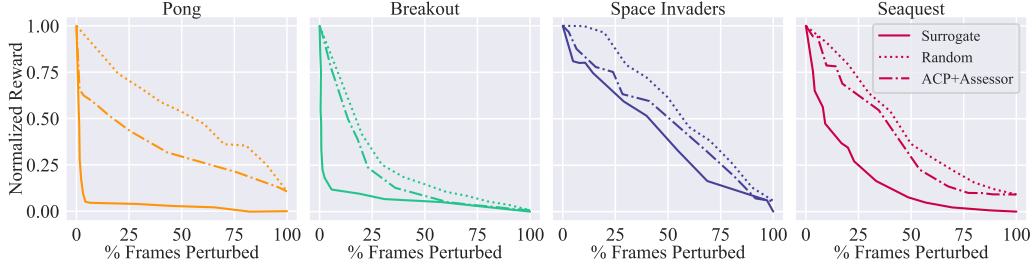


Figure 7: Effectiveness of strategically-timed attacks on DQN agents over 30,000 time steps. Our ACP+Assessor method and the random baseline use imitator gradients. We also compare to the technique in [18], which uses the stronger surrogate gradients. The FGM method is used for crafting.

result further supports our hypothesis that proxy models that approximate the policy directly will yield more transferable attacks.

To qualitatively evaluate the features that these models learn, we create perturbation-based saliency maps [11] designed to be human interpretable visualizations of $\nabla_x J(\theta, x_i, y_i)$ on Atari games. Figure 3 shows a representative example of what the saliency maps tell us about these models. As expected, the surrogate model’s map is very similar to the target’s. The imitator’s salient regions tend to be the most similar to the target’s out of the proxy models, which further supports our beliefs regarding attack effectiveness. The assessor tends to focus less on the agent itself (i.e. the submarine), and more on the objects around it which correspond to potential future reward. This intuition also helps to explain the inferior performance of the assessor’s attacks. Finally, because the psychic model predicts the entire next-frame, it must attend to any object in the state space that moves. Because the psychic learns an approximation of the state transition dynamics, a subset of the features that it learns (e.g. the submarine, fish, divers) do correspond to features that are important to the agent’s policy.

The results of the strategically-timed snooping attack on DQN agents can be seen in Figure 7. Note that we use the FGM crafting method with imitator gradients in this experiment. We compare this performance to (1) the black-box variant of the original strategically-timed attack described in [18] using FGM with surrogate gradients, and (2) an attack which perturbs at random time steps with FGM and imitator gradients. The strategically-timed attacks will typically be more effective on the paddle-based games such as Pong, as there is a clear distinction between time steps that are critical for good performance (i.e. as the ball approaches the paddle) and time steps when the actions of the agent do not matter. As expected, our method does not perform as well as the surrogate that was trained to assign credit to certain states and actions. Our method does show promise, however, as it performs markedly better than the random strategy without requiring any interaction with the environment. We believe that our method’s effectiveness is bottlenecked by the high-variance assessor predictions, and reducing the variance of the reward signal learned would lead to better performance.

An unexpected result of our experiments is the unimpressive performance of MIFGM compared to vanilla FGM. To understand why, we consider that iterative attacks like MIFGM create a more custom perturbation for the model that it is crafted by. This introduces the possibility that the resulting adversarial examples are overfit to a local maxima of the white-box model. In the case of the proxy models, we posit that because of the significant differences in the loss functions used by the agents and the proxies, adversarial examples that are more tailored to a specific objective will not perform as well. In the case of the baseline surrogate agents that *do* use the same objectives, the high variance of the RL data generation process is more likely to yield models with differently-shaped decision surfaces compared to supervised classifiers that draw data i.i.d. Again, this renders the more tailored perturbations less beneficial for transfer-based attacks.

7 Conclusions

It is often infeasible for an adversary to have access to a target agent’s parameters or train a DRL surrogate agent on a proprietary environment. However, we show that an adversary only needs the ability to intercept the states and optionally snoop on the action and reward signals to launch powerful adversarial attacks on a black-box agent. We believe this to be an important security vulnerability to consider and defend against before deploying these models to systems that we trust.

References

- [1] Vahid Behzadan and Arslan Munir. Vulnerability of deep reinforcement learning to policy induction attacks. In *MLDM*, 2017.
- [2] Marc G. Bellemare, Yavar Naddaf, Joel Veness, and Michael H. Bowling. The arcade learning environment: An evaluation platform for general agents. *J. Artif. Intell. Res.*, 47:253–279, 2013.
- [3] Richard Bellman. Dynamic programming. *Science*, 153 3731:34–7, 1966.
- [4] Mariusz Bojarski, Davide Del Testa, Daniel Dworakowski, Bernhard Firner, Beat Flepp, Prashoon Goyal, Lawrence D. Jackel, Miguel Pozuelo Monfort, Urs Muller, Jiakai Zhang, Xin Zhang, Junbo Jake Zhao, and Karol Zieba. End to end learning for self-driving cars. *CoRR*, abs/1604.07316, 2016.
- [5] Greg Brockman, Vicki Cheung, Ludwig Pettersson, Jonas Schneider, John Schulman, Jie Tang, and Wojciech Zaremba. Openai gym, 2016.
- [6] Nicholas Carlini and David A. Wagner. Towards evaluating the robustness of neural networks. *2017 IEEE Symposium on Security and Privacy (SP)*, pages 39–57, 2017.
- [7] Prafulla Dhariwal, Christopher Hesse, Oleg Klimov, Alex Nichol, Matthias Plappert, Alec Radford, John Schulman, Szymon Sidor, Yuhuai Wu, and Peter Zhokhov. Openai baselines. <https://github.com/openai/baselines>, 2017.
- [8] Yinpeng Dong, Fangzhou Liao, Tianyu Pang, Hang Su, Jun Zhu, Xiaolin Hu, and Jianguo Li. Boosting adversarial attacks with momentum. In *CVPR*, 2018.
- [9] Ross B. Girshick. Fast r-cnn. *2015 IEEE International Conference on Computer Vision (ICCV)*, pages 1440–1448, 2015.
- [10] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *CoRR*, abs/1412.6572, 2015.
- [11] Sam Greydanus, Anurag Koul, Jonathan Dodge, and Alan Fern. Visualizing and understanding atari agents. In *ICML*, 2018.
- [12] Sandy H. Huang, Nicolas Papernot, Ian J. Goodfellow, Yan Duan, and Pieter Abbeel. Adversarial attacks on neural network policies. *CoRR*, abs/1702.02284, 2017.
- [13] Nathan Inkawhich, Wei Wen, Hai Li, and Yiran Chen. Feature space perturbations yield more transferable adversarial examples. In *CVPR*, 2019.
- [14] Ilya Kostrikov. Pytorch implementations of reinforcement learning algorithms. <https://github.com/ikostrikov/pytorch-a2c-ppo-acktr-gail>, 2018.
- [15] Felix Leibfried, Nate Kushman, and Katja Hofmann. A deep learning approach for joint video frame and reward prediction in atari games. *CoRR*, abs/1611.07078, 2017.
- [16] Sergey Levine, Chelsea Finn, Trevor Darrell, and Pieter Abbeel. End-to-end training of deep visuomotor policies. *Journal of Machine Learning Research*, 17:39:1–39:40, 2016.
- [17] Timothy P. Lillicrap, Jonathan J. Hunt, Alexander Pritzel, Nicolas Heess, Tom Erez, Yuval Tassa, David Silver, and Daan Wierstra. Continuous control with deep reinforcement learning. *CoRR*, abs/1509.02971, 2016.
- [18] Yen-Chen Lin, Zhang-Wei Hong, Yuan-Hong Liao, Meng-Li Shih, Ming-Yu Liu, and Min Sun. Tactics of adversarial attack on deep reinforcement learning agents. In *IJCAI*, 2017.
- [19] Yanpei Liu, Xinyun Chen, Chang Liu, and Dawn Xiaodong Song. Delving into transferable adversarial examples and black-box attacks. *CoRR*, abs/1611.02770, 2017.
- [20] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Alex Graves, Ioannis Antonoglou, Daan Wierstra, and Martin A. Riedmiller. Playing atari with deep reinforcement learning. *CoRR*, abs/1312.5602, 2013.

- [21] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Andrei A. Rusu, Joel Veness, Marc G. Bellemare, Alex Graves, Martin A. Riedmiller, Andreas Fidjeland, Georg Ostrovski, Stig Petersen, Charles Beattie, Amir Sadik, Ioannis Antonoglou, Helen King, Dharshan Kumaran, Daan Wierstra, Shane Legg, and Demis Hassabis. Human-level control through deep reinforcement learning. *Nature*, 518:529–533, 2015.
- [22] Volodymyr Mnih, Adrià Puigdomènech Badia, Mehdi Mirza, Alex Graves, Timothy P. Lillicrap, Tim Harley, David Silver, and Koray Kavukcuoglu. Asynchronous methods for deep reinforcement learning. In *ICML*, 2016.
- [23] Junhyuk Oh, Xiaoxiao Guo, Honglak Lee, Richard L. Lewis, and Satinder P. Singh. Action-conditional video prediction using deep networks in atari games. In *NIPS*, 2015.
- [24] Nicolas Papernot, Patrick D. McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik, and Ananthram Swami. The limitations of deep learning in adversarial settings. *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 372–387, 2016.
- [25] Nicolas Papernot, Patrick D. McDaniel, Ian J. Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. Practical black-box attacks against machine learning. In *AsiaCCS*, 2017.
- [26] Adam Paszke, Sam Gross, Soumith Chintala, Gregory Chanan, Edward Yang, Zachary DeVito, Zeming Lin, Alban Desmaison, Luca Antiga, and Adam Lerer. Automatic differentiation in pytorch. 2017.
- [27] Deepak Pathak, Parsa Mahmoudieh, Guanhao Luo, Pulkit Agrawal, Dian Chen, Yide Shentu, Evan Shelhamer, Jitendra Malik, Alexei A. Efros, and Trevor Darrell. Zero-shot visual imitation. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 2131–21313, 2018.
- [28] Anay Pattanaik, Zhenyi Tang, Shuijing Liu, Gautham Bommanan, and Girish Chowdhary. Robust deep reinforcement learning with adversarial attacks. In *AAMAS*, 2018.
- [29] Lerrel Pinto, Marcin Andrychowicz, Peter Welinder, Wojciech Zaremba, and Pieter Abbeel. Asymmetric actor critic for image-based robot learning. *CoRR*, abs/1710.06542, 2018.
- [30] Ahmad El Sallab, Mohammed Abdou, Etienne Perot, and Senthil Yogamani. Deep reinforcement learning framework for autonomous driving. *CoRR*, abs/1704.02532, 2017.
- [31] John Schulman, Sergey Levine, Philipp Moritz, Michael I. Jordan, and Pieter Abbeel. Trust region policy optimization. In *ICML*, 2015.
- [32] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. *CoRR*, abs/1707.06347, 2017.
- [33] David Silver, Guy Lever, Nicolas Heess, Thomas Degris, Daan Wierstra, and Martin A. Riedmiller. Deterministic policy gradient algorithms. In *ICML*, 2014.
- [34] David Silver, Aja Huang, Chris J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Vedavyas Panneershelvam, Marc Lanctot, Sander Dieleman, Dominik Grewe, John Nham, Nal Kalchbrenner, Ilya Sutskever, Timothy P. Lillicrap, Madeleine Leach, Koray Kavukcuoglu, Thore Graepel, and Demis Hassabis. Mastering the game of go with deep neural networks and tree search. *Nature*, 529:484–489, 2016.
- [35] Richard S. Sutton and Andrew G. Barto. Reinforcement learning: An introduction. *IEEE Transactions on Neural Networks*, 16:285–286, 1988.
- [36] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian J. Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *CoRR*, abs/1312.6199, 2014.
- [37] Florian Tramèr, Nicolas Papernot, Ian J. Goodfellow, Dan Boneh, and Patrick D. McDaniel. The space of transferable adversarial examples. *CoRR*, abs/1704.03453, 2017.
- [38] Elias Wang. Deep action conditional neural network for frame prediction in atari games. 2017.
- [39] Christopher J. C. H. Watkins and Peter Dayan. Technical note: Q-learning. *Machine Learning*, 8:279–292, 1992.

A Deep reinforcement learning method descriptions

A.1 Deep Q-Networks

Q-learning is a value-based RL algorithm that estimates the cumulative discounted reward of each state-action pair, and chooses its policy based on these estimated returns. In Q-learning, we approximate the function $Q^*(s, a)$, which gives the cumulative discounted reward for taking action a in state s , and following an optimal policy π^* thereafter [39]. To train, we iteratively optimize with a temporal difference loss based on the Bellman equation [3]. Once we have an acceptable approximation of Q^* , a common policy is to act ϵ -greedily to aid in exploration. In an effort to apply Q-learning to problems with large state spaces such as Atari games, Mnih et al. [20] combine convolutional neural networks with Q-learning to create deep Q-learning. In practice, this requires the use of a replay memory buffer to enable off-policy learning and a target network for more stable updates.

A.2 Proximal policy optimization

PPO [32] is a policy-based RL method, meaning that it directly approximates the policy $\pi_\theta(a|s)$ with a neural network with parameters θ . The algorithm is typically implemented in an actor-critic framework which simultaneously learns to approximate a variance-reduced advantage estimate to stabilize the policy gradient. At each training step, PPO alternates between (1) collecting experience by running the current policy for a set number of time steps, (2) computing empirical returns and advantages, and (3) using batch learning to optimize a clipped surrogate objective that constrains the amount the updated policy can differ from the old policy.

B Implementation details

B.1 Agents

We train DQN [20] and PPO [32] agents on Pong, Breakout, Space Invaders, and Seaquest games in the Atari 2600 Arcade Learning Environment [2] via OpenAI Gym [5]. Preprocessing is primarily facilitated using the Atari wrappers in OpenAI’s baselines library [7], which converts frames from RGB to grayscale [0, 1], and resizes frames to 84x84. To make the environment Markovian, a state is created by stacking the last four consecutive frames, making the input volume to the models of shape 4x84x84. We use the PyTorch deep learning framework [26], the DQN implementation described in [21], and Ilya Kostrikov’s implementation of PPO [14].

B.2 Proxies

For the psychic and AC-psychic, we use a scaled-down implementation of the architecture described in [38], as they work with the raw RGB frames and we predict the preprocessed version of the frames. The imitator architecture that we use is identical to the smaller DQN that was initially introduced in [20], and apply a Softmax operation to the logits for use with the cross-entropy classification loss. Note that we intentionally use a different architecture from the target agents in the interest of strictly adhering to black-box assumptions. The assessor uses the same architecture as the imitator, but we replace the classification layer with a single output node, and train the model with the Huber regression loss [9]. To train these models, we alternate between (1) collecting a pool of states and "labels" using the signals that we are intercepting, and (2) running N iterations of optimization on the pooled data.

C More results

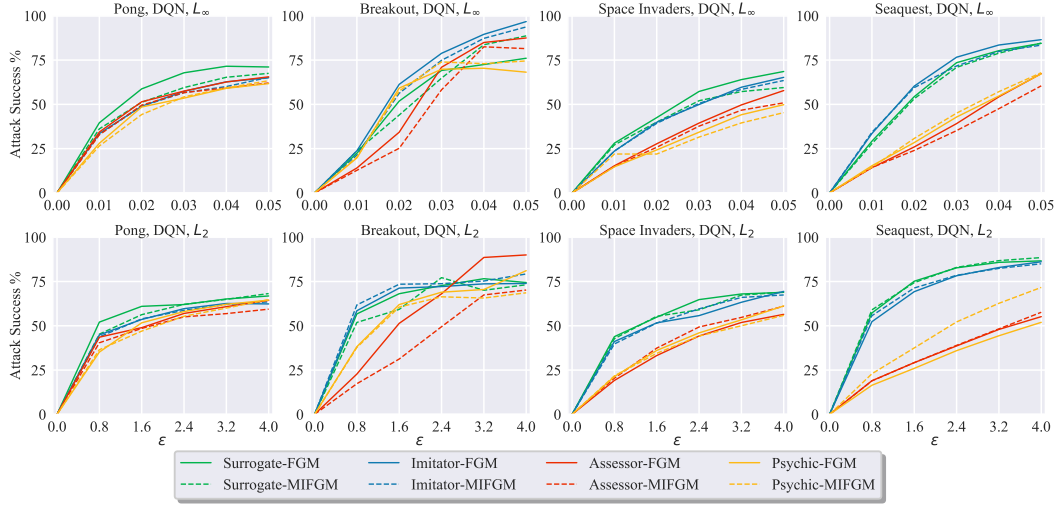


Figure 8: Attack success rates over 10 episodes of time steps on DQN agents due to L_∞ and L_2 bounded perturbations.

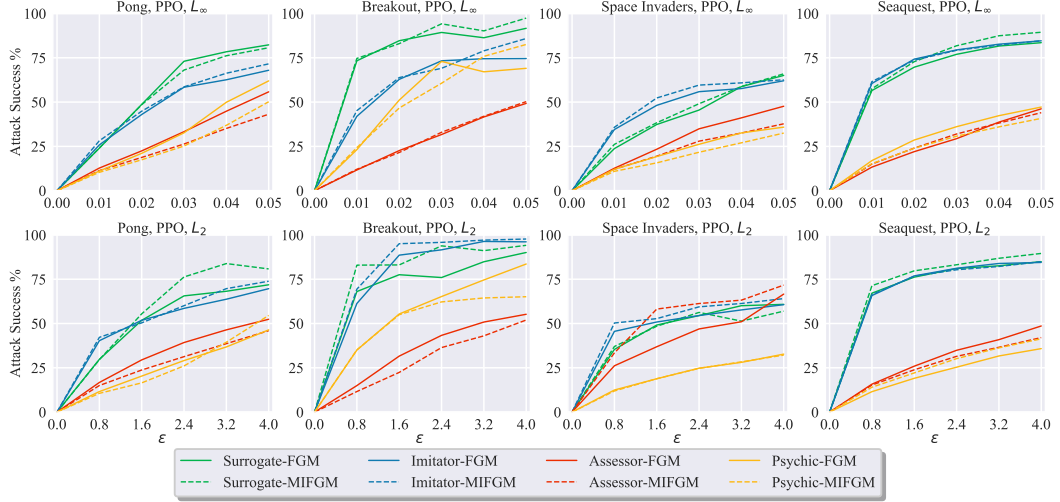


Figure 9: Attack success rates over 10 episodes of time steps on PPO agents due to L_∞ and L_2 bounded perturbations.

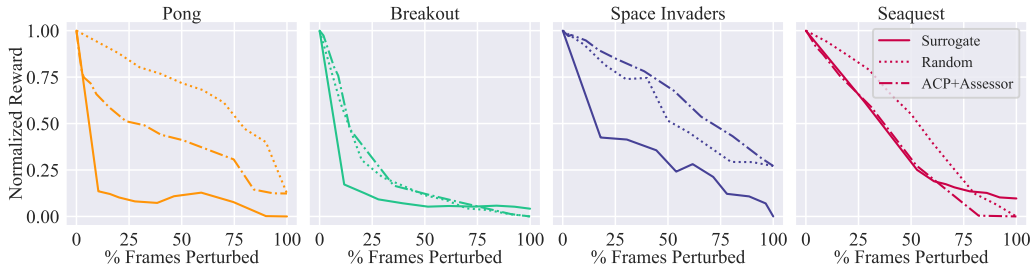


Figure 10: Effectiveness of strategically-timed attacks on PPO agents over 30,000 time steps. Our ACP+Assessor method and the random baseline use imitator gradients. We also compare to the technique in [18], which uses the stronger surrogate gradients. The FGM method is used for crafting.