Reward-Poisoning Attacks on Offline Multi-Agent Reinforcement Learning

Young Wu, Jeremy McMahan, Xiaojin Zhu, and Qiaomin Xie

1 University of Wisconsin-Madison
yw@cs.wisc.edu, jmcmahan@wisc.edu, jerryzhu@cs.wisc.edu, qiaomin.xie@wisc.edu

Abstract
In offline multi-agent reinforcement learning (MARL), agents estimate policies from a given dataset. We study reward-poisoning attacks in this setting where an exogenous attacker modifies the rewards in the dataset before the agents see the dataset. The attacker wants to guide each agent into a nefarious target policy while minimizing the $L^p$ norm of the reward modification. Unlike attacks on single-agent RL, we show that the attacker can install the target policy as a Markov Perfect Dominant Strategy Equilibrium (MPDSE), which rational agents are guaranteed to follow. This attack can be significantly cheaper than separate single-agent attacks. We show that the attack works on various MARL agents including uncertainty-aware learners, and we exhibit linear programs to efficiently solve the attack problem. We also study the relationship between the structure of the datasets and the minimal attack cost. Our work paves the way for studying defense in offline MARL.

1 Introduction
Multi-agent reinforcement learning (MARL) has achieved tremendous empirical success across a variety of tasks such as the autonomous driving, cooperative robotics, economic policy-making, and video games. In MARL, several agents interact with each other and the underlying environment, and each of them aims to optimize their individual long-term reward (Zhang, Yang, and Başar 2021). Such problems are often formulated under the framework of Markov Games (Shapley 1953), which generalizes the Markov Decision Process model from single-agent RL. In offline MARL, the agents aim to learn a good policy by exploiting a pre-collected dataset without further interactions with the environment or other agents (Pan et al. 2022; Jiang and Lu 2021; Cui and Du 2022; Zhong et al. 2022). The optimal solution in MARL typically involves equilibria concepts.

While the above empirical success is encouraging, MARL algorithms are susceptible to data poisoning attacks: the agents can reach the wrong equilibria if an exogenous attacker manipulates the feedback to agents. For example, a third party attacker may want to interfere with traffic to cause autonomous vehicles to behave abnormally; teach robots an incorrect procedure so that they fail at certain tasks; misinform economic agents about the state of the economy and guide them to make irrational investment or saving decisions; or cause the non-player characters in a video game to behave improperly to benefit certain human players. In this paper, we study the security threat posed by reward-poisoning attacks on offline MARL. Here, the attacker wants the agents to learn a target policy $\pi^\dagger$ of the attacker's choosing ($\pi^\dagger$ does not need to be an equilibrium in the original Markov Game). Meanwhile, the attacker wants to minimize the amount of dataset manipulation to avoid detection and accruing high cost. This paper studies optimal offline MARL reward-poisoning attacks. Our work serves as a first step toward eventual defense against reward-poisoning attacks.

Our Contributions
We introduce reward-poisoning attacks in offline MARL. We show that any attack that reduces to attacking single-agent RL separately must be suboptimal. Consequently, new innovations are necessary to attack effectively. We present a reward-poisoning framework that guarantees the target policy $\pi^\dagger$ becomes a Markov Perfect Dominant Strategy Equilibrium (MPDSE) for the underlying Markov Game. Since any rational agent will follow an MPDSE if it exists, this ensures the agents adopt the target policy $\pi^\dagger$. We also show the attack can be efficiently constructed using a linear program.

The attack framework has several important features. First, it is effective against a large class of offline MARL learners rather than a specific learning algorithm. Second, the framework allows partially decentralized agents who can only access their own individual rewards rather than the joint reward vectors of all agents. Lastly, the framework only makes the minimal assumption on the rationality of the learners that they will not take dominated actions.

We also give interpretable bounds on the minimal cost to poison an arbitrary dataset. These bounds relate the minimal attack cost to the structure of the underlying Markov Game. Using these bounds, we derive classes of extremal games that are especially cheap or expensive for the attacker to poison. These results show which games may be more susceptible to an attacker, while also giving insight to the structure of multi-agent attacks.

In the right hands, our framework could be used by a benevolent entity to coordinate agents in a way that im-
proves social welfare. However, a malicious attacker could exploit the framework to harm learners and only benefit themselves. Consequently, our work paves the way for future study of MARL defense algorithms.

Related Work

**Online Reward-Poisoning:** Reward poisoning problem has been studied in various settings, including online single-agent reinforcement learners (Banihashem et al. 2022; Huang and Zhu 2019; Liu and Lai 2021; Rakshha et al. 2021a,b, 2020; Sun, Huo, and Huang 2020; Zhang et al. 2020), as well as online bandits (Bogunovic et al. 2021; Garcelon et al. 2020; Guan et al. 2020; Jun et al. 2018; Liu and Shroff 2019; Lu, Wang, and Zhang 2021; Ma et al. 2018; Yang et al. 2021; Zuo 2020). Online reward poisoning for multiple learners is recently studied as a game redesign problem in (Ma, Wu, and Zhu 2021).

**Offline Reward Poisoning:** Ma et al. (2019); Rakshha et al. (2020, 2021a); Rangi et al. (2022b); Zhang and Parkes (2008); Zhang, Parkes, and Chen (2009) focus on adversarial attacks on offline single-agent reinforcement learners. Gleave et al. (2019); Guo et al. (2021) study the poisoning attack on multi-agent reinforcement learners, assuming that the attacker controls one of the learners. Our model instead assumes that the attacker is not one of the learners, and the attacker wants to and is able to poison the rewards of all learners. For each period \( h \in [H] \), \( P_h : S \times A \rightarrow \Delta(S) \) is the transition function, where \( \Delta(S) \) denotes the probability simplex on \( S \), and \( P_h(s'|s,a) \) is the probability that the state is \( s' \) in period \( h+1 \) given the state is \( s \) and the joint action is \( a \) in period \( h \). \( R_{i,h} : S \times A \rightarrow \mathbb{R}^n \) is the mean reward function for the \( n \) players, where \( R_{i,h}(s,a) \) denotes the scalar mean reward for player \( i \) in state \( s \) and period \( h \) when the joint action \( a \) is taken. The initial state distribution is \( \mu \).

**Policies and value functions.** We use \( \pi \) to denote a deterministic Markovian policy for the \( n \) players, where \( \pi_h : S \rightarrow A \) is the policy in period \( h \) and \( \pi_{i,h}(s) \) specifies the joint action in state \( s \) and period \( h \). We write \( \pi_i = (\pi_{i,h})_{h \in [H]} \), where \( \pi_{i,h}(s) \) is the action taken by learner \( i \) and \( \pi_{i,h}(s) \) is the joint action taken by learners other than \( i \) in state \( s \) period \( h \). The value of a policy \( \pi \) represents the expected cumulative rewards of the game assuming learners take actions according to \( \pi \). Formally, the \( Q \) value of learner \( i \) in state \( s \) in period \( h \) under a joint action \( a \) is given recursively by

\[
Q_{i,h}^\pi(s,a) = R_{i,h}(s,a) + \sum_{s' \in S} P_h(s'|s,a) V_{i,h+1}^\pi(s') \, ,
\]

The value of learner \( i \) in state \( s \) in period \( h \) under policy \( \pi \) is given by \( V_{i,h}^\pi(s) = Q_{i,h}^\pi(s,\pi_i(s)) \), and we use \( V_{h}^\pi(s) \in \mathbb{R}^n \) to denote the vector of values for all learners in state \( s \) in period \( h \) under policy \( \pi \).

**Offline MARL.** In offline MARL, the learners are given a fixed batch dataset \( D \) that records historical plays of \( n \) agents under some behavior policies, and no further sampling is allowed. We assume that \( D = \{(s_k^{(k)},a_k^{(k)},r_k^{(k)})_{k=1}^K\} \) contains \( K \) episodes of length \( H \). The data tuple in period \( h \) of episode \( k \) consists of the state \( s_k^{(k)} \in S \), the joint action profile \( a_k^{(k)} \in A \), and reward vector \( r_k^{(k)} \in \mathbb{R}^n \), where the superscript \( 0 \) denotes the original rewards before any attack. The next state \( s_{k+1}^{(k)} \) can be found in the next tuple. Given the shared data \( D \), each learner independently constructs a policy \( \pi_i \) to maximize their own cumulative reward. They then behave according to the resulting joint policy \( \pi = (\pi_1,\ldots,\pi_n) \) in future deployment. Note that in a multi-agent setting, the learners’ optimal solution concept is typically an approximate Nash equilibrium or Dominant Strategy Equilibrium (Cui and Du 2022; Zhong et al. 2022).
An agent’s access to $D$ may be limited, for example due to privacy reasons. There are multiple levels of accessibility. In the first level, the agents can only access data that directly involves itself: instead of the tuple $(s_h, a_h, r_h)$, agent $i$ would only be able to see $(s_h, a_i, r_{i,h})$. In the second level, agent $i$ can see the joint action but only its own reward: $(s_h, a_h, r_{i,h})$. In the third level, agent $i$ can see the whole $(s_h, a_h, r_h)$. We focus on the second level in this paper.

Let $N_h(s, a) = \sum_{k=1}^{K} 1 \{s^{(k)}_h = s, a^{(k)}_h = a\}$ be the total number of episodes containing $(s, a, \cdot)$ in period $h$. We consider a dataset $D$ that satisfies the following coverage assumption.

**Assumption 1.** (Full Coverage) For each $(s, a)$ and $h$, $N_h(s, a) > 0$.

While this assumption might appear strong, we later show that it is necessary to effectively poison the dataset.

### Attack Model

We assume that the attacker has access to the original dataset $D$. The attacker has a pre-specified target policy $\pi^\dagger$ and attempts to poison the rewards in $D$ with the goal of forcing the learners to learn $\pi^\dagger$ from the poisoned dataset. The attacker also desires that the attack has minimal cost. We let $C(r^0, r^\dagger)$ denote the cost of a specific poisoning, where $r^0 = \{ (r^{0, h}_{i})_{h=1}^{H} \}_{h=1}^{K}$ are the original rewards and $r^\dagger = \{ (r^{\dagger, h}_{i})_{h=1}^{H} \}_{h=1}^{K}$ are the poisoned rewards. We focus on the $L^1$-norm cost $C(r^0, r^\dagger) = \|r^0 - r^\dagger\|_1$.

**Rationality.** For generality, the attacker makes minimal assumptions on the learners’ rationality. Namely, the attacker only assumes that the learners never take dominated actions (Monderer and Tennenholtz 2004). For technical reasons, we strengthen this assumption slightly by introducing an arbitrarily small margin $\epsilon > 0$ (e.g. representing the learners’ numerical resolution).

**Definition 1.** A $\epsilon$-strict Markov perfect dominant strategy equilibrium ($\epsilon$-MPDSE) of a Markov Game $G$ is a policy $\pi$ satisfying that for all learners $i \in [n]$, periods $h \in [H]$, and states $s \in S$,

$$\forall a_i \in A_i, a_i \neq \pi_{i,h}(s), a_{-i} \in A_{-i} : Q^\pi_{i,h}(s, (\pi_{i,h}(s), a_{-i})) \geq Q^\pi_{i,h}(s, (a_i, a_{-i})) + \epsilon.$$ 

Note that a strict MPDSE is one that,

**Assumption 2.** (Rationality) The learners will play an $\epsilon$-MPDSE should one exist.

**Uncertainty-aware attack.** State-of-the-art MARL algorithms are typically uncertainty-aware (Cui and Du 2022; Zhong et al. 2022), meaning that learners are cognizant of the model uncertainty due to finite, random data and will calibrate their learning procedure accordingly. The attacker accounts for such uncertainty-aware learners, but does not know the learners’ specific algorithm or internal parameters. It only assumes that the policies computed by the learners are solutions to some game that is plausible given the dataset. Accordingly, the attacker aims to poison the dataset in such a way that the target policy is an $\epsilon$-MPDSE for every game that is plausible for the poisoned dataset.

To formally define the set of plausible Markov Games for a given dataset $D$, we first need a few definitions.

**Definition 2.** (Confidence Game Set) The confidence set on the transition function $P_h(s, a)$ has the form:

$$\text{Cl}_h^P(s, a) := \left\{ P_h(s, a) \in \Delta(A) : \| P_h(s, a) - \hat{P}_h(s, a) \|_1 \leq \rho_h^P(s, a) \right\}$$

where

$$\hat{P}_h(s', a) := \frac{1}{N_h(s, a)} \sum_{k=1}^{K} \chi_{s^{(k)}_h = s', a^{(k)}_h = a}$$

is the maximum likelihood estimate (MLE) of the true transition probability. Similarly, the confidence set on the reward function $R_{i,h}(s, a)$ has the form:

$$\text{Cl}_h^R(s, a) := \left\{ R_{i,h}(s, a) \in [-b, b] : \| R_{i,h}(s, a) - \hat{R}_{i,h}(s, a) \| \leq \rho_h^R(s, a) \right\}$$

where

$$\hat{R}_{i,h}(s, a) := \frac{1}{N_h(s, a)} \sum_{k=1}^{K} r_{i,h}^{0, k}(s, a)$$

is the MLE of the reward. Then, the set of all plausible Markov Games consistent with $D$, denoted by $\text{Cl}_G^G$, is defined to be:

$$\text{Cl}_G^G := \{ G = (S, A, P, R, H, \mu) : P_h(s, a) \in \text{Cl}_h^P(s, a), R_{i,h}(s, a) \in \text{Cl}_h^R(s, a), \forall i, h, s, a \}.$$ 

Note that both the attacker and the learners know that all of the rewards are bounded within $[-b, b]$ (we allow $b = \infty$). The values of $\rho_h^P(s, a)$ and $\rho_h^R(s, a)$ are typically given by concentration inequalities. One standard choice takes the Hoeffding-type form $\rho_h^P(s, a) \propto 1/\sqrt{\max\{N_h(s, a), 1\}}$, and $\rho_h^R(s, a) \propto 1/\sqrt{\max\{N_h(s, a), 1\}}$, where we recall that $N_h(s, a)$ is the visitation count of the state-action pair $(s, a)$ (Xie et al. 2020; Cui and Du 2022; Zhong et al. 2022). We remark that with proper choice of $\rho_h^P$ and $\rho_h^R$, $\text{Cl}_G^G$ contains the game constructed by optimistic MARL algorithms with upper confidence bounds (Xie et al. 2020), as well as that by pessimistic algorithms with lower confidence bounds (Cui and Du 2022; Zhong et al. 2022). See the appendix for details.

With the above definition, we consider an attacker that attempts to modify the original dataset $D$ into $D^\dagger$ so that $\pi^\dagger$ is an $\epsilon$-MPDSE for every plausible game in $\text{Cl}_G^G$ induced by the poisoned $D^\dagger$. This would guarantee the learners adopt $\pi^\dagger$.

The full coverage Assumption 1 is necessary for the above attack goal, as shown in the following proposition. We defer the proof to appendix.

**Proposition 1.** If $N_h(s, a) = 0$ for some $(h, s, a)$, then there exist MARL learners for which the attacker’s problem is infeasible.

### 3 Poisoning Framework

In this section, we first argue that naively applying single-agent poisoning attack separately to each agent results in suboptimal attack cost. We then present a new optimal poisoning framework that accounts for multiple agents and thereby allows for efficiently solving the attack problem.
Suboptimality of single-agent attack reduction. As a first attempt, the attacker could try to use existing single-agent RL reward poisoning methods. However, this approach is doomed to be suboptimal. Consider the following game with $n = 2$ learners, one period and one state:

<table>
<thead>
<tr>
<th>$\mathcal{A}_1 \backslash \mathcal{A}_2$</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(3,3)</td>
<td>(1,2)</td>
</tr>
<tr>
<td>2</td>
<td>(2,1)</td>
<td>(0,0)</td>
</tr>
</tbody>
</table>

Suppose that the original dataset $D$ has full coverage. For simplicity, assume that each $(s, a) \in P$ pair appears sufficiently many times so $p^B$ is small. In this case, the target policy $\pi^1 = (1, 1)$ already is a MPDSE, so no reward modification is needed. However, if we use a single-agent approach, each learner $i$ will observe the following dataset:

$\begin{align*}
\mathcal{A}_i \quad r_i
\end{align*}$

In this case, to learner $i$ it is not immediately clear which of the two actions is strictly better. For example, when $1, 2$ appears relatively more often then $3, 0$. To ensure that both players take action 1, the attacker needs to modify at least one of the rewards for each player, thus incurring a nonzero (and thus suboptimal) attack cost.

The example above shows that a new approach is needed to construct an optimal poisoning framework tailored to the multi-agent setting. Below we develop such a framework, first for the simple Bandit Game setting, which is then generalized to Markov Games.

Bandit Game Setting

As a stepping stone, we start with a subclass of Markov Games with $|S| = 1$ and $H = 1$, which are sometimes called bandit games. A bandit game consists of a single stage normal-form game. For now, we also pretend that the learners simply use the data to compute an MLE point estimate $\hat{G}$ of the game and then solve the estimated game $\hat{G}$. This is unrealistic, but it highlights the attacker’s strategy to enforce that $\pi^1$ is an $\epsilon$-strict DSE in $\hat{G}$.

Suppose the original dataset is $D = \{(a^r(k), r^0(k))\}_{k=1}^K$ (recall we no longer have state or period). Also, let $N(a) := \sum_{k=1}^K 1\{a^r(k) = a\}$ be the action counts. The attacker’s problem can be formulated as a convex optimization problem given in (1).

$$
\min_{\{\rho^0, \rho^1\}} C(\rho^0, \rho^1)
$$

s.t. $\begin{align*}
R^i(a) := \frac{1}{N(a)} \sum_{k=1}^K r^+(k)1\{a^{(k)} = a\}, \quad \forall a; \\
R^i_\epsilon(\pi^1, a_{-i}) &\leq R^i(a) - \epsilon, \quad \forall i, a; \\
R^i_\epsilon(\pi^1, a_{-i}) &\geq R^i_\epsilon(\pi^1, a_{-i}) + \epsilon, \quad \forall i, a_{-i}, a_i \neq \pi^1_i; \\
r^+(k) &\in [-b, b]^n, \quad \forall k.
\end{align*}$

The first constraint in (1) models the learners’ MLE $\hat{G}$ after poisoning. The second constraint enforces that $\pi^1$ is an $\epsilon$-strict DSE of $\hat{G}$ by definition. We observe that:

1. The problem is feasible if $\epsilon \leq 2b - 2\rho^B(a), \forall a \in \mathcal{A}$.
2. If the cost function $C(\cdot, \cdot)$ is the $L^1$-norm, the problem is a linear program (LP) with $nK$ variables and $(A - 1)A^{n-1} + 2nK$ inequality constraints (assuming each learner has $|\mathcal{A}_i| = A$ actions);
3. After the attack, learner $i$ only needs to see its own rewards to be convinced that $\pi^1_i$ is a dominant policy, and learner $i$ does not need to observe other learners’ rewards.

This simple formulation serves as an asymptotic approximation to the attack problem for confidence bound based learners. In particular, when $N(a)$ is large for all $a$, the confidence intervals on $P$ and $R$ are usually small.

With the above idea in place, we can consider more realistic learners that are uncertainty-aware. For these learners, the attacker attempts to enforce an $\epsilon$ separation between the lower bound of the target action’s reward and the upper bounds of all other actions’ rewards (similar to arm elimination in bandits). With such separation, all plausible games in $C_1^G$ would have the target action profile as the dominant strategy equilibrium. This approach can be formulated as a slightly more complex optimization problem (2), where the second and third constraints enforce the desired $\epsilon$ separation. The formulation (2) can be solved using standard optimization solvers, hence the optimal attack can be computed efficiently.

$$
\min_{\{\rho^0, \rho^1\}} C(\rho^0, \rho^1)
$$

s.t. $\begin{align*}
R^i(a) := \frac{1}{N(a)} \sum_{k=1}^K r^+(k)1\{a^{(k)} = a\}, \quad \forall a; \\
C_l^R(\pi^1, a_{-i}) := \left\{ R_i(a) \in [-b, b] : \left| R_i(a) - R_i^1(a) \right| \leq \rho^B(a) \right\}, \quad \forall i, a; \\
\min_{R_i \in C_l^R(\pi^1, a_{-i})} R_i &\geq \max_{R_i \in C_l^R(\pi^1, a_{-i})} R_i + \epsilon, \quad \forall i, a_{-i}, a_i \neq \pi^1_i; \\
r^+(k) &\in [-b, b]^n, \quad \forall k.
\end{align*}$

We next consider whether this formulation has a feasible solution. Below we characterize the feasibility of the attack in terms of the margin parameter $\epsilon$ and the confidence bounds.

Proposition 2. The attacker’s problem (2) is feasible if $\epsilon \leq 2b - 2\rho^B(a), \forall a \in \mathcal{A}$.

Proposition 2 is a special case of the general Theorem 5 with $H = |S| = 1$. We note that the condition in Proposition 2 has an equivalent form that relates to the structure of the dataset. We later present this form for more general case.

When an $L^1$-norm cost function is used, we show in the appendix that the formulation (2) can also be efficiently solved.

Proposition 3. With $L^1$-norm cost function $C(\cdot, \cdot)$, the problem (2) can be formulated as a linear program.
Markov Game Setting

We now generalize the ideas from the bandit setting to derive a poisoning framework for arbitrary Markov Games. With multiple states and periods, there are two main complications:

1. In each period $h$, the learners’ decision depends on $Q_h$, which involves both the immediate reward $R_h$ and the future return $Q_{h+1}$.
2. The uncertainty in $Q_h$ amplifies as it propagates backward in $h$.

Accordingly, the attacker needs to design the poisoning attack recursively.

Our main technical innovation is an attack formulation based on $Q$ confidence-bound backward induction. The attacker maintains confidence upper and lower bounds on the learners’ $Q$ function, $Q$ and $\overline{Q}$, with backward induction. To ensure $\pi^1$ becomes an $\iota$-MPDSE, the attacker again attempts to $\iota$-separate the lower bound of the target action and the upper bound of all other actions, at all states and periods.

Recall Definition 2: given the training dataset $D$, one can compute the MLEs $R^*_h$ and corresponding confidence sets $CI^{R^*_h}_h$ for the reward. The attacker aims to poison $D$ into $D^*$ so that the MLEs and confidence sets become $R^*_h$ and $CI^{R^*_h}_h$, under which $\pi^1$ is the unique $\iota$-MPDSE for all plausible games in the corresponding confidence set. The attacker finds the minimum cost way of doing so by solving a $Q$ confidence-bound backward induction optimization problem, given in (3)–(7).

$$\min \ C (r^0, r^f) \tag{3}$$

s.t. $R^*_{i,h} (s, a) := \frac{1}{N_h (s, a)} \sum_{k=1}^K f^*_{i,h} (s^{(k)} = s, a^{(k)} = a)$,

$$\forall h, s, i, a$$

$CI^{R^*_i}_{i,h} (s, a) := \{ R_{i,h} (s, a) \in [-b, b] : |R_{i,h} (s, a) - R^*_{i,h} (s, a)| \leq \rho_\iota R^*_i (s, a) \}$,

$$\forall h, s, i, a$$

$Q_{i,H} (s, a) := \min_{R_{i,H} \in CI^{R^*_i}_{i,H} (s, a)} R_{i,H}, \forall s, i, a$

$Q_{i,h} (s, a) := \min_{R_{i,h} \in CI^{R^*_i}_{i,h} (s, a)} R_{i,h}$

$$+ \sum_{s' \in S} P_h (s') Q_{i,h+1} \left( s', \pi^*_h (s') \right), \forall h < H, s, i, a$$

$\overline{Q}_{i,h} (s, a) := \max_{R_{i,h} \in CI^{R^*_i}_{i,h} (s, a)} R_{i,h}, \forall s, i, a$

$\overline{Q}_{i,h} (s, a) := \max_{R_{i,h} \in CI^{R^*_i}_{i,h} (s, a)} R_{i,h}$

$$+ \sum_{s' \in S} P_h (s') \overline{Q}_{i,h+1} \left( s', \pi^*_h (s') \right), \forall h < H, s, i, a$$

The backward induction steps (4) and (5) ensure that $Q$ and $\overline{Q}$ are valid lower and upper bounds for the $Q$ function for all plausible Markov Games in $CI^\iota$, for all periods. The margin constraints (6) enforces a $\iota$-separation between the target action and other actions at all states and periods. We emphasize that the agents need not consider $Q$ at all in their learning algorithm; $Q$ only appears in the optimization due to its presence in the definition of MPDSE.

Again, pairing an efficient optimization solver with the above formulation gives an efficient algorithm for constructing the poisoning. We now answer the important questions of whether this formulation admits a feasible solution and whether these solutions yield successful attacks. The lemma below provides a positive answer to the second question.

**Lemma 4.** If the attack formulation (3)–(7) is feasible, $\pi^1$ is the unique $\iota$-MPDSE of every Markov Game $G \in CI^\iota$.

Moreover, the attack formulation admits feasible solutions under mild conditions on the dataset.

**Theorem 5.** The attacker formulation (3)–(7) is feasible if the following condition holds:

$$\iota \leq 2b - (H + 1) \rho_\iota^R (s, a), \forall h \in [H], s \in S, a \in A.$$  

We remark that the learners know the upper bound $b$ and may use it exclude implausible games. The accumulation of confidence intervals over the $H$ periods results in the extra factor $(H + 1)$ on $\rho_\iota^R$. Theorem 5 implies that the problem is feasible so long as the dataset is sufficiently populated; that is, each $(s, a)$ pair should appear frequently enough to have a small confidence interval half-width $\rho_\iota^R$. The following corollary provides a precise condition on the visit counts that guarantees feasibility.

**Corollary 6.** Given a confidence probability $\delta$ and the confidence interval half-width $\rho_\iota^R (s, a) = f (\frac{1}{N_h (s, a)})$ for some strictly increasing function $f$, the condition in Theorem 5 holds if

$$N_h (s, a) \geq \left( f^{-1} (\frac{2b - \iota}{H + 1}) \right)^{-1}.$$  

In particular, for the natural choice of Hoeffding-type $\rho_\iota^R (s, a) = 2b \sqrt{\log ((H |S| |A|) / \delta) / \max \{ N_h (s, a), 1 \} }$, it suffices that,

$$N_h (s, a) \geq \frac{4b^2 (H + 1)^2 \log ((H |S| |A|) / \delta)}{(2b - \iota)^2}.$$  

Despite the inner min and max in the problem (3)–(7), the problem can be formulated as an LP, thanks to LP duality.

**Theorem 7.** With $L^1$-norm cost function $C(\cdot, \cdot)$, problem (3)–(7) can be formulated as an LP.

The proofs of the above results can be found in appendix.
4 Cost Analysis

Now that we know how the attacker can poison the dataset in the multi-agent setting, we can study the structure of attacks. The structure is most easily seen by analyzing the minimal attack cost. To this end, we give general bounds that relate the minimal attack cost to the structure of the underlying Markov Game. The attack cost upper bounds show which games are particularly susceptible to poison, and the attack cost lower bounds demonstrate that some games are expensive to poison.

Overview of results: Specifically, we shall present two types of upper/lower bounds on the attack cost: (i) universal bounds that hold for all attack problem instances simultaneously; (ii) instance-dependent bounds that are stated in terms of certain properties of the instance. We also discuss problem instances under which these two types of bounds are tight and coincide with each other.

We note that all bounds presented here are with respect to the $L^1$-cost, but many of them generalize to other cost functions, especially the $L^\infty$-cost. The proofs of the results presented in this section are provided in the appendix.

Setup: Let $I = (\mathcal{D}, \pi^1, \rho^I, \rho^R, \iota)$ denote an instance of the attack problem, and $\hat{G}$ denote the corresponding MLE of the Markov Game derived from $D$. We denote by $I_h = (\mathcal{D}_h, \pi^1_h, \rho^R_h, \rho^R_h, \iota)$ the restriction of the instance to period $h$. In particular, $\hat{R}_h(s)$ derived from $\mathcal{D}_h$ is exactly the normal-form game at state $s$ and period $h$ of $\hat{G}$. We define $C^*(I)$ to be the optimal $L^1$-poisoning cost for the instance $I$; that is, $C^*(I)$ is the optimal value of the optimization problem (3)–(7) evaluated on $I$. We say the attack instance $I$ is feasible if this optimization problem is feasible. If $I$ is infeasible, we define $C^*(I) = \infty$. WLOG, we assume that $|A_1| = \cdots = |A_n| = n$. In addition, we define the minimum visit count for each period $h$ in $D$ as $N_h = \max_{s \in S} \sum_{a \in A} N_h(s, a)$, and the minimal over all periods as $\hat{N} := \min_{h \in \mathcal{H}} N_h$. We similarly define the maximum visit counts as $\tilde{N}_h = \max_{s \in S} \sum_{a \in A} N_h(s, a)$ and $\tilde{N} = \max_h \tilde{N}_h$. Lastly, we define $\rho = \min_{h \in \mathcal{H}, s, a} \rho^R(s, a)$ and $\bar{\rho} = \max_{h \in \mathcal{H}, s, a} \rho^R(s, a)$, the minimum and maximum confidence half-width.

Universal Cost Bounds

With the above definitions, we present universal attack cost bounds that hold simultaneously for all attack instances.

Theorem 8. For any feasible attack instance $I$, we have that,

$$0 \leq C^*(I) \leq \tilde{N} H |S| nA^n 2b.$$

As these upper and lower bounds hold for all instances, they are typically loose. However, they are nearly tight. If $\pi^1$ is already an $\iota$-MPDSE for all plausible games, then no change to the rewards is needed and the attack cost is 0, hence the lower bound is tight for such instances. We can also construct a high cost instance to show near-tightness of the upper bound.

Specifically, consider the dataset for a bandit game, $D = \{(a^{(k)}, r^{0,(k)})\}_{k=1}^K$, where $A = A^n$ and each action appears exactly $N$ times, i.e., $\hat{N} = \tilde{N} = N$ and $K = NA^n$.

The target policy is $\pi^1 = (1, \ldots, 1)$. The dataset is constructed so that $r^{0,(k)}_i = -b$ if $a^{(k)}_i = \pi^1_i(s)$ and $r^{0,(k)}_i = b$ otherwise. These rewards are essentially the extreme opposite of what the attacker needs to ensure $\pi^1$ is an $\iota$-DSE. Note, the dataset induces the MLE of the game shown in Table 1 for the special case with $n = 2$ players.

| $A_1/A_2$ | 1 | 2 | $\cdots$ | $|A_2|$ |
|-----------|---|---|---------|---|
| 1         | $-b, -b$ | $-b, b$ | $\cdots$ | $b, b$ |
| 2         | $b, b$   | $b, b$ | $\cdots$ | $b, b$ |
| $|A_1|$   | $b, b$   | $b, b$ | $\cdots$ | $b, b$ |

Table 1: MLE $\hat{R}_h(s, \cdot)$ before attack

For simplicity, suppose that the same confidence half-width $\rho^R(a) = \rho < b$ is used for all $a$. Let $\iota \in (0, b)$ be arbitrary. For this instance, to install $\pi^1$ as the $\iota$-DSE, the attacker can flip all rewards in a way that is illustrated in Table 2, inducing a cost as the upper bound in Theorem 8. The situation is the same for $n \geq 2$ learners.

| $A_1/A_2$ | 1 | $\cdots$ | $2, \ldots, |A_2|$ |
|-----------|---|---------|----------------|
| 1         | $b, b$ | $\cdots$ | $b, b$ |
| $|A_1|$   | $b - 2\rho - \iota, b$ | $\cdots$ | $b - 2\rho - \iota$ |

Table 2: MLE $\hat{R}_h(s, \cdot)$ after attack

Our instance-dependent lower bound, presented later in Theorem 12, implies that any attack on this instance must have cost at least $NnA^{n-1}(2b + 2\rho + \iota)$. This lower bound matches the refined upper bound in the proof of Theorem 9, implying the refined bounds are tight for this instance. Noticing that the universal bound in Theorem 8 only differs by an $O(A)$-factor implies it is nearly tight.

Instance-Dependent Cost Bounds

Next, we derive general bounds on the attack cost that depend on the structure of the underlying instance. Our strategy is to reduce the problem of bounding Markov Game costs to the easier problem of bounding Bandit Game costs. We begin by showing that the cost of poisoning a Markov Game dataset can be bounded in terms of the cost of poisoning the datasets corresponding to its individual period games.

Theorem 9. For any feasible attack instance $I$, we have that

$$C^*(I_H) \leq C^*(I) \text{ and},$$

$$C^*(I) \leq \sum_{h=1}^{H} C^*(I_h) + 2bnH|S|\hat{N} + H^2\bar{\rho}|S|nA^n\tilde{N}$$

Here we see the effect of the learner’s uncertainty. If $\rho^R$ is small, then poisoning costs slightly more than poisoning each bandit instance independently. This is desirable since it allows the attacker to solve the much easier bandit instances instead of the full problem.

The lower bound is valid for all Markov Games, but it is weak in that it only uses the last period cost. However,
this is the most general lower bound one can obtain without additional assumptions on the structure of the game. If we assume additional structure on the dataset, then the above lower bound can be extended beyond the last period, forcing a higher attack cost.

**Lemma 10.** Let $I$ be any feasible attack instance containing at least one uniform transition in $CI_P^n$ for each period $h$, i.e., there is some $P_h(s' | s, a) \in CI_P^n$ with $P_h(s' | s, a) = 1/|S|, \forall h, s', s, a$. Then, we have that

$$C^*(I) \geq \sum_{h=1}^H C^*(I_h).$$

In words, for these instances the optimal cost for poisoning is not too far off from the optimal cost of poisoning each period game independently. We note this is where the effects of $p^R$ show themselves. If the dataset is highly uncertain on the transitions, it becomes likely that a uniform transition exists in $CI_P^n$. Thus, a higher $p^R$ leads to a higher cost and effectively devolves the set of plausible games into a series of independent games.

Now that we have the above relationships, we can focus on bounding the attack cost for bandit games. To be precise, we bound the cost of poisoning a period game instance $I_h$. To this end, we define $\iota$-dominance gaps.

**Definition 3.** (Dominance Gaps) For every $h \in [H], s \in S, i \in [n]$ and $a_{-i} \in A_{-i}$, the $\iota$-dominance gap, $d_{i,h}^\iota(s, a_{-i})$, is defined as

$$d_{i,h}^\iota(s, a_{-i}) := \left[ \max_{a_i \neq \pi_{i,h}^\iota(s)} \left( \hat{R}_{i,h}(s, (a_i, a_{-i})) + \rho_h^R(s, (a_i, a_{-i})) \right) - \hat{R}_{i,h}(s, (\pi_{i,h}^\iota(s), a_{-i})) + \rho_h^R(s, (\pi_{i,h}^\iota(s), a_{-i})) + \iota \right].$$

where $\hat{R}$ is the MLE w.r.t. the original dataset $D$.

The dominance gaps measure the minimum amount by which the attacker would have to increase the reward for learner $i$ while others are playing $a_{-i}$, so that the action $\pi_{i,h}^\iota(s)$ becomes $\iota$-dominant for learner $i$. We then consolidate all the dominance gaps for period $h$ into the variable $\Delta_h(\iota)$,

$$\Delta_h(\iota) := \sum_{s \in S} \sum_{l=1}^n \sum_{a_{-i}} \left( d_{i,h}^\iota(s, a_{-i}) + \delta_{i,h}^\iota(s, a_{-i}) \right)$$

Where $\delta_{i,h}^\iota(s, a_{-i})$ is a minor overflow term defined in the appendix. With all this machinery set up, we can give precise bounds on the minimal cost needed to attack a single period game.

**Lemma 11.** The optimal attack cost for $I_h$ satisfies

$$\nabla_h \Delta_h(\iota) \leq C^*(I_h) \leq \overline{\nabla}_h \Delta_h(\iota).$$

Combining these bounds with Theorem 9 gives complete attack cost bounds for general Markov game instances.

The lower bounds in both Lemma 10 and Lemma 11 expose an exponential dependency on $n$, the number of players, for some datasets $D$. These instances essentially require the attacker to modify $\hat{R}_{i,h}(s, a)$ for every $a \in A$. A concrete instance can be constructed by taking the high cost dataset derived as the tight example before and extend it into a general Markov Game. We simply do this by giving the game several identical states and uniform transitions. In terms of the dataset, each episode consists of independent plays of the same normal-form game, possibly with a different state observed. For this dataset the $\iota$-dominance gap can be shown to be $d_{i,h}^\iota(s, a_{-i}) = 2b + 2\rho + \iota$. A direct application of Lemma 10 gives the following explicit lower bound.

**Theorem 12.** There exists a feasible attack instance $I$ for which it holds that

$$C^*(I) \geq NH |S| n A^{n-1} (2b + 2\rho + \iota).$$

Recall the attacker wants to assume little about the learners, and therefore chooses to install an $\iota$-MPDSE (instead of making stronger assumptions on the learners and installing a Nash equilibrium or a non-Markov perfect equilibrium). On some datasets $D$, the exponential poisoning cost is the price the attacker pays for this flexibility.

**5 Conclusion**

We studied a security threat to offline MARL where an attacker can force learners into executing an arbitrary Dominant Strategy Equilibrium by minimally poisoning historical data. We showed that the attack problem can be formulated as a linear program, and provided analysis on the attack feasibility and cost. This paper thus helps to raise awareness on the trustworthiness of multi-agent learning. We encourage the community to study defense against such attacks, e.g. via robust statistics and reinforcement learning.

**Acknowledgements**

McMahan is supported in part by NSF grant 2023239. Zhu is supported in part by NSF grants 1545481, 1704117, 1836978, 2023239, 2041428, 2202457. ARO MURI W911NF2110317, and AF CoE FA9550-18-1-0166. Xie is partially supported by NSF grant 1955997 and JP Morgan Faculty Research Awards. We also thank Yudong Chen for his useful comments and discussions.

**References**


