Online Appendix

Stop the Compartmentalization: Unified Robust Algorithms for Handling Uncertainties in Security Games

1 Appendix A: Proof of Theorem 4.2

Proof. In this proof, we focus on combinations of uncertainties with a monotonic adversary which is the most difficult uncertainty case. Any other uncertainty cases could be solved in a similar way. Given the defender’s original strategy, \( x \), denote \( v_1 = \min_{\hat{x} \in H(x)} \min_{y \in \Psi(x)} \sum_i y_i U^d_i(\hat{x}) \) and \( v_2 = \min_{y \in L(x)} \sum_i y_i U^d_{\min}(x, i) \), in the following, we show that \( v_1 = v_2 \).

a) Prove \( v_1 \leq v_2 \):

The optimal solution of the inner minimization, \( \min_{y \in L(x)} \sum_i y_i U^d_{\min}(x, i) \), corresponds to an extreme point of \( L(x) \). Moreover, all inequalities of \( L(x) \) are of the form \( y_i \geq 0 \) and \( y_i \geq y_j \) for certain pairs of targets \((i, j)\). Any extreme point of \( L(x) \) satisfies the following condition: For all \((i, j)\), if \( y_i, y_j > 0 \), then \( y_i = y_j \). Denote \( I_a(x) = \{i : y^*_i > 0, \ y^* = \arg\min_{y \in L(x)} \sum_i y_i U^d_{\min}(x, i)\} \) be the support of the optimal strategy of the adversary given the defender’s original strategy \( x \), we have \( \forall i \in I_a(x), y^*_i = \frac{1}{|I_a(x)|} \) and \( \forall j \notin I_a(x), y^*_j = 0 \). Moreover, the following constraint must hold:

\[
\forall i \in I_a(x), j \notin I_a(x) : U^a_{\max}(x, i) > U^a_{\min}(x, j). \tag{1}
\]

Given the defender’s original strategy \( x \) and the corresponding support \( I_a(x) \), consider the following defender’s executed strategy:

\[
\hat{x}^* = \begin{cases} 
\max \{0, x_i - \gamma_i\} & \text{, if } i \in I_a(x) \\
\min \{1, x_i + \gamma_i\} & \text{, otherwise}
\end{cases}
\]

According to the definition of \( H(x) \), we have: \( \hat{x}^* \in H(x) \). In addition, we have: \( U^a_{\max}(\hat{x}^*, i) = U^a_{\min}(x, i) \) for all \( i \in I_a(x) \) and \( U^a_{\min}(\hat{x}^*, j) = U^a_{\min}(x, j) \) for all \( j \notin I_a(x) \). Therefore, according to (1), we have \( y^* \in \Psi(\hat{x}^*) \). On the other hand, for all \( i \in I_a(x) \), we obtain \( U^d_i(\hat{x}^*) = U^d_{\min}(x, i) \). As the result,

\[
v_1 \leq \min_{y \in \Psi(\hat{x}^*)} \sum_i y_i U^d_i(\hat{x}^*) \leq \sum_i y^*_i U^d_i(\hat{x}^*) = \frac{1}{|I_a(x)|} \sum_{i \in I_a(x)} U^d_{\min}(x, i) = v_2.
\]

b) Prove \( v_1 \geq v_2 \):

Let \( \hat{x} \in H(x) \) be an executed strategy of the defender, we have: \( U^a_{\min}(x, i) \leq \hat{U}^a_{\min}(\hat{x}, i) \) and \( U^a_{\max}(x, i) \geq \hat{U}^a_{\max}(\hat{x}, i) \), for all \( i \). Therefore, given any pair of targets
According to the definition of \( \forall \), if \( U^a_{min}(x, i) \geq U^a_{max}(x, j) \), then \( \hat{U}^{a}_{min}(x, i) \geq \hat{U}^{a}_{max}(x, j) \) which implies that \( \forall y \in \Psi(x), y_i \geq y_j \). As the result, \( \forall y \in \Psi(x) \), we obtain the following condition: \( U^a_{min}(x, i) \geq U^a_{max}(x, j) \implies y_i \geq y_j \). According to the definition of \( L(x) \), we have: \( y \in L(x) \). Therefore, \( L(x) \supseteq \Psi(x) \). As the result, \( L(x) \supseteq \bigcup_{x \in \hat{H}(x)} \Psi(x) \).

Because \( L(x) \supseteq \bigcup_{x \in \hat{H}(x)} \Psi(x) \) and \( U^d_{min}(x, i) \leq U^d_i(x) \) for all \( i \), we obtain:

\[
\nu_2 = \min_{y \in L(x)} \sum_i y_i U^d_{min}(x, i) \leq \min_{y \in \hat{H}(x)} \sum_i y_i U^d_{min}(x, i)
\]

\[
= \min_{x \in \hat{H}(x)} \min_{y \in \Psi(x)} \sum_i y_i U^d_{min}(x, i) \leq \min_{x \in \hat{H}(x)} \min_{y \in \Psi(x)} \sum_i y_i U^d_i(x) = v_1.
\]

By combining a) and b), we show that \( v_1 = v_2 \) for all \( x \). Therefore, \( P1 \equiv P2 \).

### 2 Appendix B: Proof of Proposition 5.1

**Proof.** According to the definition of \( M(C(x)) \), we have:

\[
([M(C(x))]' y)_k = \begin{cases} 
\sum_i \sigma_{ik} y_i, & \text{if } k \in C(x) \\
0, & \text{otherwise}
\end{cases}
\]

Therefore, \([M(C(x))]' y \geq 0 \iff \forall k \in C(x), A_k(y) \geq 0\).

### 3 Appendix C: Proof of Theorem 7.1

**Proof.** Overall, the MILP (31-40) attempts to compute the optimal solution of the optimization problem: \( \max_{x \in \hat{F}_p} \min_{y \in \hat{S}_u(x)} \sum_i y_i U^d_i(x) \).

In particular, constraints (32-36) guarantee that all targets in the same group will have the same adversary’s expected utility and \( \forall i \in G_k, j \in G_{k'}, k < k' \), we have: \( U^d_i(x) > U^d_j(x) \). In particular, if \( h_{k-1, i} = 0 \) and \( h_{k, i} = 1 \) which mean that target \( i \) belongs to group \( k \), constraints (32) and (35) force \( U^d_i(x) = m_k \). If \( h_{k, i} = 0 \) which means that target \( i \) must belong to a group \( k' > k \) which means \( U^d_i(x) < m_k \), constraint (33) guarantees that \( U^d_i(x) \leq m_k - \epsilon < m_k \) where \( \epsilon \) is a given small positive number. Constraint (36) ensures that if \( h_{k-1, i} = 1 \), then \( h_{k, i} \) must be equal to 1, being consistent with the definition of the integer variable vector \( h_k \). Constraint (39) guarantees that each target must belong to a certain group.

Furthermore, constraints (37-38) guarantee that if \( t^* \) is the optimal objective value, then \( t^* = \min_{k=1}^{\bar{p}} \{ \overline{U}^d_i(x, k) \} \) where \( \overline{U}^d_i(x, k) \) is corresponding defender’s utility to a potential optimal strategy \( y^k \) of the adversary in \( \hat{S}_u(x) \). In particular, in constraint (38), if \( h_{k, i} = 0 \), then \( s_{k, i} = 0 \). In addition, as \( \sum_i s_{k, i} = 0 \), we have: \( \sum_{i \in \cup_{r=1}^{\bar{r}} G_r} s_{k, i} = 0 \) (*). On the other hand, in constraint (37), \( \forall i \in \cup_{r=1}^{\bar{r}} G_r \), which means that \( h_{k, i} = 1 \), we have: \( s_{k, i} + t \leq U^d_i(x) \) (**). By taking the sum of (**) over all \( i \in \cup_{r=1}^{\bar{r}} G_r \) and by using condition (*), we obtain the following derived inequality: for all \( k = 1, \bar{p} \), \( t \leq \overline{U}^d_i(x, k) \). As the objective of the MILP is to maximize \( t \), the optimal values of \( \{s_{k, i}\}_{k=1}^{\bar{p}}, i=1,\bar{T} \) will lead to \( t^* = \min_{k=1}^{\bar{p}} \{ \overline{U}^d_i(x, k) \} \).
Therefore, GMM-p will find the optimal solution through $B^d_p$. In addition, we have the following property of $B^d_p$: $\forall T \geq p > p' \geq 1: |B^d_p| \supseteq |B^d_{p'}|$. Therefore, $v^*_p \geq v^*_{p'}$. Finally, as any strategy of the defender will categorize the targets into $p$ groups for some $p \in \{1, 2, ..., T\}$, the optimal strategy of the defender will belong to $B_p$ for some $p$ which implies that GMM-p will provide the optimal solution.