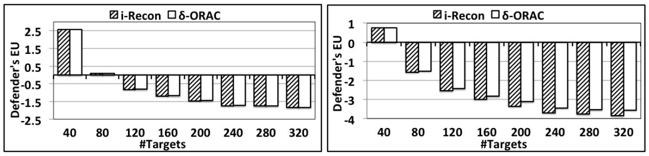
ensure any solution bound. As shown in Figure 5, while both algorithms achieve the similar expected utility when $\gamma = \eta = .01$, when the uncertainty increases, i.e., $\gamma = \eta = .05$, i-RECON obtains lower defender's utility than $\delta-$ORAC. For example, in Figure 5(b), in the case of 320-target games, $\delta-$ORAC obtains a defender's utility of -3.54 on average while i-RECON achieves only -3.84. Overall, our robust algorithms significantly outperform the existing robust algorithms for addressing uncertainties.



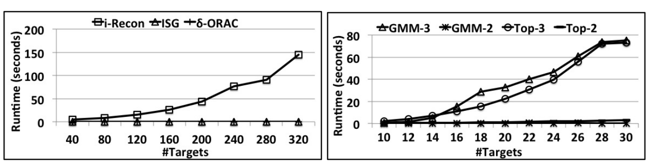
(a) $\gamma = \eta = .01$ (b) $\gamma = \eta = .05$

Figure 5: Solution quality, uncertainty in defender's strategy

8.2 Runtime performance

In addition to solution quality, we show that our approximate algorithms obtain an efficient runtime performance in comparison with other robust algorithms in large-scale games. The results are average over 100 payoff structures. In Figure 6, the y-axis indicates the runtime in seconds and the x-axis shows the number of targets. Figure 6(a) shows that $\delta-$ORAC runs significantly faster than i-RECON and its runtime is approximately the same as ISG; i-RECON's runtime grows quickly while $\delta-$ORAC's runtime is consistently fast as the number of targets increases. For example, i-RECON's runtime reaches 144.25 seconds while $\delta-$ORAC and ISG take only 0.05 and 0.046 seconds on average in 320-target games, respectively.

Furthermore, our GMM-p algorithm is shown to have approximately the same runtime as the Top-K algorithm (Figure 6(b)). While our approximate algorithms achieve higher quality without sacrificing runtime, some URAC versions are unable to scale-up. For example, when addressing a combination of all uncertainties (i.e., $\alpha = \beta = 0.5, \gamma = \eta = 0.05$, monotonic adversary), URAC-1's runtime is 85.17 seconds for 9-target games while our approximate algorithms take less than 1 second; of course, URAC-1 addresses a combination of uncertainties that no algorithm can.



(a) Uncertainty setting: $\alpha = \beta = .5, \gamma = \eta = .05$ (b) Uncertainty setting: monotonic adversary

Figure 6: Runtime performance, approximate algorithms

9. CONCLUSION

In this paper, we provide the following main contributions: 1) we present the first unified framework to handle all the uncertainties where robust algorithms have been defined in security games; 2) we provide a unified algorithmic framework from which we can derive different "unified" robust algorithms to address combinations of these uncertainties; 3) we introduce approximate robust scalable algorithms; 4) we show through our experiments that our algorithms improve runtime performance and/or solution quality.

10. ACKNOWLEDGEMENTS

This research was supported by MURI Grant W911NF-11-1-0332 and by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2010-ST-061-RE0001.

11. REFERENCES

[1] B. An, M. Brown, Y. Vorobeychik, and M. Tambe. Security games with surveillance cost and optimal timing of attack execution. In *AAMAS*, 2013.

[2] B. An, M. Tambe, F. Ordonez, E. Shieh, and C. Kiekintveld. Refinement of strong stackelberg equilibria in security games. In *AAAI*, 2011.

[3] N. Basilico, N. Gatti, and F. Amigoni. Leader-follower strategies for robotic patrolling in environments with arbitrary topologies. In *AAMAS*, 2009.

[4] V. Conitzer and T. Sandholm. Computing the optimal strategy to commit to. In *ACM*, 2006.

[5] A. X. Jiang, T. H. Nguyen, M. Tambe, and A. D. Procaccia. Monotonic maximin: A robust stackelberg solution against boundedly rational followers. In *GameSec*, 2013.

[6] C. Kiekintveld, T. Islam, and V. Kreinovich. Security games with interval uncertainty. In *AAMAS*, 2013.

[7] C. Kiekintveld, J. Marecki, and M. Tambe. Approximation methods for infinite bayesian stackelberg games: modeling distributional payoff uncertainty. In *AAMAS*, 2011.

[8] D. Korzhyk, V. Conitzer, and R. Parr. Complexity of computing optimal stackelberg strategies in security resource allocation games. In *AAAI*, 2010.

[9] J. Letchford and Y. Vorobeychik. Computing randomized security strategies in networked domains. In *AARM Workshop In AAAI*, 2011.

[10] R. McKelvey and T. Palfrey. Quantal response equilibria for normal form games. *Games and economic behavior*, 10(1):6–38, 1995.

[11] E. Nudelman, J. Wortman, Y. Shoham, and K. Leyton-Brown. Run the gamut: A comprehensive approach to evaluating game-theoretic algorithms. In *AAMAS*, 2004.

[12] J. Pita, M. Jain, F. Ordonez, M. Tambe, S. Kraus, and R. Magori-Cohen. Effective solutions for real-world stackelberg games: When agents must deal with human uncertainties. In *AAMAS*, 2009.

[13] M. Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, 2011.

[14] R. Wilcox. *Applying contemporary statistical techniques*. Academic Press, 2002.

[15] Z. Yin, M. Jain, M. Tambe, and F. Ordonez. Risk-averse strategies for security games with execution and observational uncertainty. In *AAAI*, 2011.

[16] Z. Yin and M. Tambe. A unified method for handling discrete and continuous uncertainty in bayesian stackelberg games. In *AAMAS*, 2012.