Synthesis of Deceptive Cyberdefense with Temporal Logic Constraints

***Abstract*—The design of provably correct systems from temporal logic specifications employs reactive synthesis, which models the interaction between the system and its dynamic environment as a two-player zero-sum game with complete information. However, most situations encountered in cybersecurity applications are characterized by asymmetric incomplete information: the adversary may not know the exact network configuration and the defender does not know the adversary's capabilities or intention. In this context, we discuss the recent developments in hypergame theory and omega-regular games with incomplete information which show that the solution concepts of this class of games lead to deceptive strategies that are surely or almost-surely (with probability one) guaranteed to satisfy a given security specification in Linear Temporal Logic (LTL).**

***Index Terms*—Formal specification, Logic-based design, Security protocols, Security policies, Privacy, Reactive synthesis**

I. Introduction and Background

Consider an interaction of a defender (P1, pronoun 'she') and an attacker (P2, pronoun 'he') over a network where P1 wants to prevent P2 from compromising the critical nodes. Such an interaction can be modeled as an incomplete (but perfect[1]) information game [2]. For instance, a honeypot deception problem can be formulated as an incomplete information game in which P2 wants to reach a critical node but does not know which nodes are honeypots, whereas P1 wants to configure the network such that P2 is distracted by the honeypots and, thereby, can be prevented from compromising the critical nodes. The problem of interest is *to synthesize a strategy for P1 that ensures P1 to satisfy the security objective, expressed as an LTL formula, for any rational strategy of P2, given P2 misperceives the locations of decoys*.

To solve this problem, it is necessary to develop solution concepts for games with asymmetric, incomplete information with Boolean payoffs captured by LTL formulas [3]. However, this class of games has not been investigated in the current literature for the games with LTL specifications [4]. In particular, we look into [5], [6] that extend the normal-form hypergame model (which, unlike Bayesian games, do not require consistency of priors [7]) to the game on graph model. These papers provide an interesting insight into questions such as 'under what conditions is the use of deception advantageous to P1?', 'how to synthesize a deceptive winning strategy for P1?' and 'how are the solution concepts from incomplete information games related to those from reactive synthesis?' In the next section, we discuss the game-theoretic modeling of attacker-defender interactions and the corresponding solution concepts from [6].

[1]Imperfect information games are characterized by imperfect recall. See [1] for comparison between incomplete and imperfect information games.

II. Deceptive Synthesis of Cyber Systems under Labeling Misperception

Traditionally, the games on graph are defined using a transition system and an LTL specification. A transition system consists of a labeling function that maps a game state to a subset of properties of interest (propositions) that hold in that state. For example, `IsAHoneypot` could be a valid proposition. When the true valuation of `IsAHoneypot` for all nodes in network is only known to P1 but not P2, we say P2 has misperception of the labeling function. Thus, we can capture the decoy-induced asymmetric information as follows: P1 knows the true labeling function and P2 misperceives some labels of states, and P1 knows P2's misperception.

Given this model, [6] proposes an algorithm that synthesizes an almost-sure winning strategy (a classical solution concept in reactive synthesis) that can leverage the misperception of P2 to ensure that, under the subjectively rational actions of P2, P1 has a strategy to ensure the security specification is satisfied with probability one.

The following contributions in [6] are noted. First, a dynamic hypergame on graph model is proposed that integrates P1's and P2's perceptual games (i.e. the game that P1 and P2 construct in their minds given the information they have) into a single graphical model. Second, the authors extend the solution concept of subjective rationalizability to the hypergame model. They show that an action is subjectively rational for P2 if it is permissive [8] in P2's perception. By assuming P2 only uses permissive actions, they solve for P1's subjectively rationalizable strategy, following which P1 is ensured to satisfy her security objective. Additionally, the synthesized strategy is also shown to be stealthy—that is, P1 is guaranteed to only choose actions that, in P2's mind, are subjectively rational for P1, until it reaches the sure-winning region of the game with complete information. Furthermore, the deceptive almost-sure winning strategy is proved to be more powerful (that is, including more states in the winning region) than the non-deceptive almost-sure winning strategy.

In conclusion, the work presented in [6] provides important insights for mechanism design of proactive and active defense with deception. The exploration is still in its nascent stages and has several open problems on both theoretical and practical side, including combining randomization and decoy-based deception for cybersecurity and decoy-allocation design under temporal logic constraints.

REFERENCES

[1] J. C. Harsanyi, "Games with Incomplete Information Played by "Bayesian" Players, I–III Part I. The Basic Model," *Management Science*, 1967.

[2] C. Bakker, A. Bhattacharya, S. Chatterjee, and D. L. Vrabie, "Learning and information manipulation: Repeated hypergames for cyber-physical security," *IEEE Control Systems Letters*, vol. 4, no. 2, pp. 295–300, 2020.

[3] A. Pnueli and R. Rosner, "On the synthesis of a reactive module," in *Proceedings of the 16th ACM SIGPLAN-SIGACT symposium on Principles of programming languages - POPL '89*, 1989, pp. 179–190.

[4] R. Bloem, K. Chatterjee, and B. Jobstmann, "Graph games and reactive synthesis," in *Handbook of Model Checking*. Springer, 2018, pp. 921–962.

[5] A. N. Kulkarni and J. Fu, "Synthesis of deceptive strategies in reachability games with action misperception," *ArXiv*, vol. abs/2002.07045, 2020 (accepted to IJCAI 2020).

[6] A. N. Kulkarni, H. Luo, N. O. Leslie, C. A. Kamhoua, and J. Fu, "Deceptive labeling: Hypergames on graphs for stealthy deception," *ArXiv*, vol. abs/2004.05213, 2020.

[7] Y. Sasaki and K. Kijima, "Hypergames and bayesian games: A theoretical comparison of the models of games with incomplete information," *Journal of Systems Science and Complexity*, vol. 25, no. 4, pp. 720–735, 2012.

[8] J. Bernet, D. Janin, and I. Walukiewicz, "Permissive strategies: from parity games to safety games," *RAIRO-Theoretical Informatics and Applications*, vol. 36, no. 3, pp. 261–275, 2002.