






Deceptive Labeling: Hypergames on Graphs for Stealthy Deception

Abhishek N. Kulkarni , *Student Member, IEEE*, Huan Luo , Nandi O. Leslie , *Member, IEEE*, Charles A. Kamhoua , *Senior Member, IEEE*, and Jie Fu , *Member, IEEE*

Abstract—With the increasing sophistication of attacks on cyber-physical systems, deception has emerged as an effective tool to improve system security and safety by obfuscating the attacker’s perception. In this paper, we present a solution to the deceptive game in which a control agent is to satisfy a Boolean objective specified by a co-safe temporal logic formula in the presence of an adversary. The agent intentionally introduces asymmetric information to create payoff misperception, which manifests as the misperception of the labeling function in the game model. Thus, the adversary is unable to accurately determine which logical formula is satisfied by a given outcome of the game. We introduce a model called hypergame on graph to capture the asymmetrical information with one-sided payoff misperception. Based on this model, we present the solution of such a hypergame and use the solution to synthesize stealthy deceptive strategies. Specifically, deceptive sure winning and deceptive almost-sure winning strategies are developed by reducing the hypergame to a two-player game and one-player stochastic game with reachability objectives. A running example is introduced to demonstrate the game model and the solution concept used for strategy synthesis.

Index Terms—Formal methods; game theory; temporal logic; hypergame theory; deception.

I. INTRODUCTION

WITH the increasing sophistication of the attacks on cyber-physical systems, deception has emerged as a tool to mitigate the strategic and informational disadvantages of the defender. In this paper, we consider a class of games where a control agent (P1, pronoun ‘he’) plays against its adversary (P2, pronoun ‘she’) to satisfy a temporal logic formula, which describes high-level constraints such as safety, reachability, liveness, and reactivity [1]. However, the task cannot be achieved if the adversary knows the exact game. Thus, the agent needs to falsify or obfuscate information to the adversary in order to satisfy its temporal logic specification. The question arises, how to synthesize *provably correct and deceptive* strategies that exploits the information advantages?

The class of games where players’ payoffs are Boolean valued temporal logic formulas (1 for satisfying the formula and 0 otherwise) is known as games on graphs (or ω -regular games). The solution concepts of the games on graphs have been studied in formal synthesis of reactive systems [2]–[4]

A. Kulkarni and J. Fu are with the Robotics Engineering Program and Dept. of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA. {ankulkarni, jfu2}@wpi.edu

H. Luo is a visiting student with Dr. Fu at the WPI from Sept to Nov, 2019. hluo@udel.edu

N. Leslie and C. Kamhoua are with U.S. Army Research Laboratory. {nandi.o.leslie.ctr, charles.a.kamhoua.civ}@mail.mil

and supervisory control [5]. However, existing work [3], [4] assumes that both players have access to the correct model of the game. This is not the case when one player (deceiver, P1) can provide misleading information or intentionally hide information to the other for strategic advantages. In this paper, we study a class of asymmetric information games in which P1 has complete information about the game, but he intentionally *falsifies or obfuscates P2’s perception of one game component—the labeling function*, which maps an outcome (sequence of game states) to a Boolean payoff of *one* if the temporal logic formula was satisfied or *zero* otherwise. Such deception techniques are commonly used in decoy-based cybersecurity (such as honey-X) and defense (such as camouflage) [6], [7].

To synthesize deceptive strategies for P1, we model the interaction between the two players as a hypergame [8]. A hypergame models the situation where the players have different perceptions of their interaction given their information, and higher-order information (information about other’s information). We extend the normal-form hypergame model to define the *hypergame on graph* model to capture the perceptual games of the players and their knowledge about the opponent’s perceptual game. To solve for P1’s deceptive strategies, we adopt the solution concept of subjective rationalizability [9] from games with incomplete information. A subjective rationalizable player behaves rationally and assumes the other player to act rationally in his/her subjective view of the game. Thus, whenever P1 deviates from his rational strategy in P2’s subjective view, we expect P2 to become aware of the information asymmetry. Using this observation, we establish the necessary and sufficient conditions for the deceptive strategies to be (a) stealthy sure winning, and (b) stealthy almost-sure winning (i.e., winning with probability one). A stealthy strategy ensures that P2 does not become aware of the information asymmetry until P1 can ensure to satisfy the temporal logic specification irrespective of P2’s actions. These solution concepts for hypergames on graphs not only provide the provably-correct deceptive strategies for P1 but also provide a way to assess the effectiveness of deception and its potential limitations.

Related Work: Game theory for deception has been investigated extensively using the two models of incomplete information games: hypergames [8], [10], [11] and Bayesian games [12], [13]. Hypergames were initially proposed and studied for the normal-form one-shot games [8], [10] and later studied by Gharesifard and Cortés [14], [15] for repeated games. Gharesifard and Cortés developed an H-digraph model

to monitor how a player’s perception evolves during repeated interactions and to design stealthy deceptive strategy in which the deceiver’s action does not contradict the perception of the mark. Bayesian games [16] are commonly used models to design deceptive strategies in cybersecurity applications [12], [13], [17]. Dynamic Bayesian games are used in [13] for active deception in cybernetwork, where the defender has incomplete information about the type of the attacker (legitimate user or adversary) and the attacker also is uncertain about the type of the defender (high-security awareness or low-security awareness). Ornkari et al. [17] formulate a security game (Stackelberg game) to allocate limited decoy resources in a cybernetwork to mask network configurations from the attacker. Existing models of deception in games describe players’ payoffs using rewards/costs. However, we choose to adopt the hypergame model over Bayesian games for two reasons [9]: a) hypergames do not require *the consistency of priors* assumption, which is an implicit assumption in Bayesian games model that requires both the players to know the set of possible values of all the unknowns *a priori*, and b) hypergames facilitate the study of higher-order information structures, which results in lower computational complexity to solve for equilibrium under the subjective rationalizability concept. Thus, we adapt the subjective rationalizability solution concepts in hypergames [18] to solve hypergames with payoffs specified in temporal logic.

II. PRELIMINARIES

We begin with a brief overview of ω -regular games [2]. An ω -regular game, hereafter referred to as a game, is a tuple $\mathcal{G} = \langle G, \varphi \rangle$ which consists of a game arena G , representing the dynamics of the interaction between P1 and P2, and a Linear Temporal Logic (LTL) specification φ for P1. In this work, we consider turn-based, deterministic game arenas and syntactically co-safe LTL specifications. We formalize these concepts below.

Game Arena: A turn-based, deterministic game arena is a tuple $G = \langle S, A, T, s_0, \mathcal{AP}, L \rangle$ where $S = S_1 \cup S_2$ is a finite set of states partitioned into P1’s states, S_1 , and P2’s states, S_2 ; $A = A_1 \cup A_2$ is the set of actions where A_1 and A_2 are the sets of actions for P1 and P2, respectively; $T : (S_1 \times A_1) \cup (S_2 \times A_2) \rightarrow S$ is a *deterministic* transition function that maps a state-action pair to a next state. If there exists a state $s' \in S$ such that $T(s, a) = s'$, then we say that action a is *enabled* at s ; $s_0 \in S$ is called the initial state of G ; \mathcal{AP} is the set of atomic propositions; $L : S \rightarrow 2^{\mathcal{AP}}$ is the labeling function that maps a state $s \in S$ to a subset $L(s) \subseteq \mathcal{AP}$ of propositions which evaluate ‘true’ at s .

A path $\rho = s_0 s_1 \dots$ in G is a sequence of states such that for any $i \geq 0$, there exists $a \in A$ for which $T(s_i, a) = s_{i+1}$. A path ρ can be mapped to a word over $2^{\mathcal{AP}}$ by using a labeling function $w = L(\rho) = L(s_0)L(s_1)\dots$, which can be evaluated against logical formulas.

Payoffs in Linear Temporal Logic: Given the set of atomic propositions, \mathcal{AP} , an LTL formula is inductively defined as:

$$\varphi := \top \mid \perp \mid p \mid \varphi \mid \neg\varphi \mid \varphi \wedge \varphi \mid \bigcirc\varphi \mid \varphi \text{U} \varphi,$$

where \top, \perp are universally true and false, respectively, $p \in \mathcal{AP}$ is an atomic proposition, \bigcirc is a temporal operator called the “next” operator. U is a temporal operator called the “until” operator. For details about the syntax and semantics of LTL, readers are referred to [1].

In this work, we restrict the objectives of P1 to a subclass of LTL called syntactically co-safe LTL (scLTL) [19]. An scLTL formula φ is equivalently expressed as a Deterministic Finite-State Automaton (DFA), defined by a tuple $\mathcal{A} = \langle Q, \Sigma, \delta, \iota, F \rangle$ which consists of a finite set Q of states; a finite set of symbols $\Sigma = 2^{\mathcal{AP}}$; a deterministic transition function $\delta : Q \times \Sigma \rightarrow Q$; an unique initial state $\iota \in Q$; and a set F of final states. We extend the transition function over words $u \in \Sigma^\omega$ to write $\delta(q, uw) = \delta(\delta(q, u), w)$. A word w is *accepted* by \mathcal{A} if and only if there exists a finite prefix u such that $w = uv$ for some $v \in \Sigma^\omega$, and $\delta(q, u) \in F$. Given a path ρ in G , we say ρ satisfies φ over G , if and only if $L(\rho)$ is accepted by the DFA \mathcal{A} .

Zero-sum Game on a Graph: Given a game arena G and the scLTL specification φ of P1, a zero-sum game on a graph is a tuple, $\mathcal{G} = \langle G, \varphi \rangle$. For a path $\rho \in S^\omega$ in G , if the labeling $L(\rho)$ satisfies φ , then the path is winning for P1. Otherwise, it is winning for P2.

Next, we construct a *product game* for solving the zero-sum game \mathcal{G} —that is, determining from the initial state s_0 , whether a player can enforce a path winning for him, regardless of the actions of the other player.

Definition 1 (Product game). Given an arena $G = \langle S, A, T, s_0, \mathcal{AP}, L \rangle$ and a DFA $\mathcal{A} = \langle Q, \Sigma, \delta, \iota, F \rangle$ equivalent to the LTL specification of P1 φ , the product game is a tuple $G \otimes \mathcal{A} = \langle S \times Q, A, \Delta, (s_0, q_0), S \times F \rangle$, where $S \times Q$ is a set of states partitioned into P1’s states $S_1 \times Q$ and P2’s states $S_2 \times Q$; $\Delta : (S_1 \times Q \times A_1) \cup (S_2 \times Q \times A_2) \rightarrow S \times Q$ is a *deterministic* transition function that maps a game state (s, q) and an action a to a next state (s', q') where $s' = T(s, a)$ and $q' = \delta(q, L(s'))$; $(s_0, q_0) \in S \times Q$ where $q_0 = \delta(\iota, L(s_0))$ is the initial state of the product game; $S \times F \subseteq S \times Q$ is a set of final states.

We slightly abuse the notation to denote the product game graph as $\mathcal{G} := G \otimes \mathcal{A}$. A path $\rho = (s_0, q_0), (s_1, q_1), \dots$ in the product game \mathcal{G} is a sequence of states in \mathcal{G} . By definition of this product game, the project of ρ onto S , $s_0 s_1 \dots$, is a path in G and satisfies φ if and only if there exists $(s_i, q_i) \in \rho$ for some $i \geq 0$ such that $(s_i, q_i) \in S \times F$.

Thus, P1 can win (or ensure a run to satisfy φ) by reaching the set $S \times F$ in the product game. P2 can win by always avoiding $S \times F$. Thus, the product game is a *reachability game* for P1 and a *safety game* for P2.

In the product game, a randomized, memoryless¹ *strategy* for player i , for $i \in \{1, 2\}$, is a function $\pi_i : S_i \times Q \rightarrow \mathcal{D}(A_i)$, where $\mathcal{D}(A_i)$ is the set of discrete probability distributions over A_i . A deterministic strategy $\pi_i : S \times Q \rightarrow A_i$ maps a state (s, q) to an action. We say that player i commits to a strategy π_i if and only if for a given state (s, q) , if $\pi_i(s, q)$ is defined,

¹A memoryless strategy in \mathcal{G} is a finite memory strategy in G , where the memory is represented by states in DFA \mathcal{A} .

then an action is sampled from the distribution $\pi_i(s, q)$ (or the action $\pi_i(s, q)$ is taken if π_i is deterministic), otherwise, player i selects an action at random. Let Π_i be the set of strategies of player i . A strategy $\pi_1 \in \Pi_1$ is said to *sure winning* at a state $(s, q) \in S \times Q$ if, for any $\pi_2 \in \Pi_2$, P1 is guaranteed to satisfy φ within $0 \leq k < \infty$ steps for a determined upper bound k on the number of steps. A strategy $\pi_1 \in \Pi_1$ is said to *almost-sure winning* at a state $(s, q) \in S \times Q$ if, for any $\pi_2 \in \Pi_2$, P1 is guaranteed to satisfy φ with probability one, i.e., P1 might require unbounded number of steps to satisfy φ . A pair $\langle \pi_1, \pi_2 \rangle$ of strategies is a *strategy profile*.

The games in Def. 1 are determined [20], [21]: From any state $(s, q) \in S \times Q$ exactly one of P1 and P2 has a memoryless sure winning strategy. This result allows us to partition the game state space as $S \times Q = \text{Win}_1 \cup \text{Win}_2$. Here, Win_1 includes all the states from which P1 has a sure winning strategy and Win_2 includes all the states from which P2 has a sure winning strategy. Readers are referred to [21] and Chapter 2 of [2] for the details of the game solution.

III. GAME ON GRAPH WITH LABELING MISPERCEPTION

In security and defense applications, players often have asymmetric incomplete information about the game. For instance, in a decoy-based deceptive defense approach, only the defender knows which hosts are decoys but the attacker does not. Such situations can be understood as the attacker ‘misperceives’ the labels of states in the game. We introduce a hypergame model to analyze the effect of P2 misperceiving the true labeling function and how P1 can leverage P2’s misperception to synthesize deceptive strategies.

A. Hypergame Model

Definition 2 (Hypergame [8]). A level-1 two-player hypergame is a pair $\mathcal{HG}^1 = \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$, where $\mathcal{G}_1, \mathcal{G}_2$ are games perceived by players P1 and P2, respectively. A level-2 two-player hypergame is a pair $\mathcal{HG}^2 = \langle \mathcal{HG}^1, \mathcal{G}_2 \rangle$, where P1 perceives the interaction as a level-1 hypergame and P2 perceives the interaction as game \mathcal{G}_2 . The first component of a hypergame is called *perceptual game* of P1; and the second component is called *perceptual game* of P2.

While it is possible to define a level- k hypergame (see [10]), we note that a level-2 hypergame is sufficient to model the game with asymmetric information studied in this paper, since P1 knows \mathcal{HG}^1 and P2 is only aware of \mathcal{G}_2 .

Information Structure In this paper, we are interested in games with asymmetric information of labeling function. Specifically, both P1 and P2 know the following components S, A, s_0, T of the arena G , and P1’s objective φ . However, P1 has complete information about the labeling function, $L_1(s) = L(s)$ for all $s \in S$, and P2 has misperception: There exists at least one state $s \in S$, $L_2(s) \neq L(s)$. Moreover, P1 is aware of P2’s perceived labeling function L_2 .

This information structure captures decoy-based deception and camouflage. For example, the attacker misperceives a honeypot to be a regular host and the defender is aware of the attacker’s misperception.

Definition 3 (Level-2 Hypergame with Labeling Misperception). Given the information structure and the perceptual games, $\mathcal{G}_1 = \langle G_1, \varphi \rangle$ with $G_1 = \langle S, A, T, s_0, \mathcal{AP}, L_1 \rangle$ and $\mathcal{G}_2 = \langle G_2, \varphi \rangle$ with $G_2 = \langle S, A, T, s_0, \mathcal{AP}, L_2 \rangle$, the interaction between P1 and P2 is a level-2 hypergame $\mathcal{HG}^2 = \langle \mathcal{HG}^1, \mathcal{G}_2 \rangle$, where $\mathcal{HG}^1 = \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ is the level-1 hypergame.

Given two games, \mathcal{G}_1 and \mathcal{G}_2 , we can use their product games to obtain the solutions, which yield different partitions of the product state space $S \times Q$. Let Win_1^k (resp., Win_2^k) represent the winning region of P1 (resp., P2) in \mathcal{G}_k . From the winning regions, the winning strategies can be extracted by construction (See Chapter 2 of [2] for details). To illustrate the solution, we introduce a running example.

Example 1. In the game arena, G , (see Fig. 1), we have two players: P1 (circle) and P2 (square). P1 chooses an action at a circle state, and P2 selects an action at a square state. Given the transitions are deterministic, we omit the action set and use the edges of the graph to refer to players’ actions.

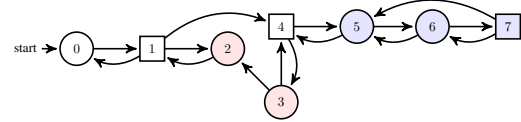


Fig. 1. A game arena, G . The red (resp. blue) nodes are P1’s winning region Win_1^2 in \mathcal{G}_2 (resp. Win_1^1 in \mathcal{G}_1).

Let L be defined such that $L(5) = \{A\}$ and $L(s) = \emptyset$ for $s \neq 5$. And L_2 is defined such that $L_2(2) = \{A\}$ and $L_2(s) = \emptyset$ for $s \neq 2$. The objective of P1 is $\varphi = \diamond A$, i.e., eventually reaching a state labeled A . The DFA equivalent to φ is shown in Fig. 2.

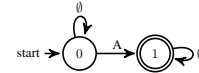


Fig. 2. The DFA for $\varphi = \diamond A$.

Due to the simplicity of DFA, we can directly solve \mathcal{G}_1 and \mathcal{G}_2 by marking the final set \mathcal{F} for P1 to reach in the arena. In \mathcal{G}_1 , the set to reach is $\{5\}$. The solution of \mathcal{G}_1 yields $\text{Win}_1^1 = \{5, 6, 7\}$ and $\text{Win}_2^1 = \{0, 1, 2, 3, 4\}$. Whereas, In \mathcal{G}_2 , the set to reach is $\{2\}$. The solution of \mathcal{G}_2 yields $\text{Win}_1^2 = \{2, 3\}$ and $\text{Win}_2^2 = \{0, 1, 4, 5, 6, 7\}$. In the true game \mathcal{G}_1 , P2 can win the game by choosing the edge $(4, 3)$, but in her perceptual game \mathcal{G}_2 , P2 considers the action $(4, 5)$ to be winning or, in other words, rational.

We now introduce the solution concept of subjective rationality to hypergames on graphs. Let S^+ be paths of length ≥ 1 . Let $u_1 : S^+ \times \Pi_1 \times \Pi_2 \rightarrow [0, 1]$ be the utility function of P1 such that $u_1(\rho, \pi_1, \pi_2)$ is the probability of satisfying the specification φ given that players commit to the strategy profile $\langle \pi_1, \pi_2 \rangle$ for a given history $\rho \in S^+$. The utility function for P2 is $u_2(\rho, \pi_1, \pi_2) = 1 - u_1(\rho, \pi_1, \pi_2)$. We denote u_i^j the *utility function of player i perceived by player j* .

Definition 4 (Subjective Rationalizability). Given a level-2 hypergame $\mathcal{HG}^2 = \langle \mathcal{HG}^1, \mathcal{G}_2 \rangle$ and the path $\rho \in S^+$, strategy $\pi_i^* : S^+ \rightarrow \mathcal{D}(A_i)$ (resp., π_j^*) is *subjective rationalizable* for P2 if and only if for all $\pi_i \in \Pi_i$, we have $u_i^2(\rho, \pi_i^*, \pi_j^*) \geq u_i^2(\rho, \pi_i, \pi_j^*)$, where $(i, j) \in \{(1, 2), (2, 1)\}$.

The strategy π_1^* is subjective rationalizable for P1 if and only for all $\pi_1 \in \Pi_1$, $u_1^1(\rho, \pi_1^*, \pi_2^*) \geq u_1^1(\rho, \pi_1, \pi_2^*)$, where π_2^* is subjective rationalizable for player 2.

In words, a strategy is called subjectively rationalizable for player i if it is the best response in that player's perceptual game to some strategy of player j , which, for player j , is the best response to player i in player j 's subjective view of player i 's perceptual game.

We now formally define the subjective rationalizable actions in \mathcal{G}_2 .

Definition 5 (Subjective rationalizable actions in \mathcal{G}_2). For a given state (s, q) in \mathcal{G}_2 , an action of player i , for $i = 1, 2$, is subjective rationalizable for P2 if it has a non-zero probability to be selected by a subjectively rationalizable strategy of player i in P2's perceptual game \mathcal{G}_2 .

Assumption 1. Subjective rationalizability is a common knowledge between P1 and P2.

Assumption 1 means that both players know that their opponent is subjectively rational and that the opponent is aware of this fact. Thus, we can say that P2 would become aware of her misperception, i.e., $\mathcal{G}_2 \neq \mathcal{G}_1$, whenever P1 uses an action which is not subjectively rationalizable in P2's perceptual game, \mathcal{G}_2 . Thus, we define the notion of a *stealthy* deceptive winning strategy over a graphical model—a hypergame transition system—that effectively allows P1 to track histories in both \mathcal{G}_1 and \mathcal{G}_2 .

Definition 6. Given games $\mathcal{G}_1 = \langle G_1, \varphi \rangle$ and $\mathcal{G}_2 = \langle G_2, \varphi \rangle$, a *hypergame transition system* (HTS) is a tuple,

$$\text{HTS} = \langle S \times Q \times Q, A, \Delta, (s_0, q_0, p_0), \text{Win}_1^1 \times Q \rangle,$$

where 1) the transition function Δ is defined as follows: given $(s, q, p), (s', q', p') \in S \times Q \times Q$, $\Delta((s, q, p), a) = (s', q', p')$ for some $a \in A$ if and only if $s' = T(s, a)$ and $q' = \delta(q, L_1(s'))$ and $p' = \delta(p, L_2(s'))$; and 2) the initial state is (s_0, q_0, p_0) where s_0 is the initial state in the game arena, $q_0 = \delta(\iota, L_1(s_0))$, and $p_0 = \delta(\iota, L_2(s_0))$. 3) $\text{Win}_1^1 \times Q = \{(s, q, p) \mid (s, q) \in \text{Win}_1^1\}$.

Definition 7 (Stealthy deceptive winning strategy). A strategy $\pi_1 : S \times Q \times Q \rightarrow \mathcal{D}(A_1)$ defined on the HTS is *stealthy deceptive (sure/almost-sure) winning* in the hypergame \mathcal{HG}^2 (in Def. 3) if the following two conditions are satisfied: 1) *Stealthy*: For any $(s, q, p) \in S_1 \times Q \times Q \setminus \text{Win}_1^1 \times Q$, $\pi_1((s, q, p), a) > 0$ only if action a is subjective rationalizable for P1 in \mathcal{G}_2 ; 2) *Winning*: By committing to π_1 , P1 ensures to visit a state in $\text{Win}_1^1 \times Q$, no matter which subjective rationalizable strategy that P2 commits to.

A state $(s, q, p) \in S \times Q \times Q$ is *stealthy deceptive (sure/almost-sure) winning* if P1 has a *stealthy deceptive (sure/almost-sure) winning* strategy at that state.

We now formally state our problem:

Problem 1. Given a hypergame on graph \mathcal{HG}^2 in Def. 3 and Assumption 1, how to synthesize a stealthy deceptive sure/almost-sure winning strategy for P1?

B. Synthesis of a stealthy deceptive sure winning strategy

For P1's deceptive strategy to be stealthy, he must choose actions that are subjective rationalizable in P2's perceptual game until reaching the winning region Win_1^1 . At the same time, a rational P2 takes subjective rationalizable actions in \mathcal{G}_2 unless she becomes aware of the misperception.

Lemma 1. In a turn-based deterministic perceptual game \mathcal{G}_2 , for a state $(s, q) \in S \times Q$, an action a is subjective rationalizable for player i if and only if it satisfies either condition: 1) $(s, q) \in \text{Win}_i^2$ and $\Delta((s, q), a) \in \text{Win}_i^2$; 2) $(s, q) \notin \text{Win}_i^2$ and a is enabled from s .

The first condition means that P2 thinks that a rational player should stay within his/her winning region; the second condition means that P2 thinks that it is rational for a player to take arbitrary actions if he/she has already lost the game from that state.

We introduce two functions π_i^2 , for $i \in \{1, 2\}$, that maps a state $(s, q) \in \text{Win}_i^2$ into a set of subjective rationalizable actions for player i in the game \mathcal{G}_2 . Formally, for each i , the function $\pi_i^2 : \text{Win}_i^2 \cap (S_i \times Q) \rightarrow 2^{A_i}$ is defined such that,

$$\pi_i^2(s, q) = \{a \mid \Delta_2((s, q), a) \in \text{Win}_i^2\}. \quad (1)$$

Theorem 1. Given HTS $= \langle S \times Q \times Q, A, \Delta, (s_0, q_0, p_0), \text{Win}_1^1 \times Q \rangle$, functions $\pi_2^2 : S \times Q \rightarrow 2^{A_2}$ and $\pi_1^2 : S \times Q \rightarrow 2^{A_1}$ defined by (1), P1 has a *stealthy deceptive sure winning* strategy if and only if he has a *sure winning* strategy in the following reachability game:

$$\widetilde{\mathcal{HG}} = \langle S \times Q \times Q, A, \tilde{\Delta}, (s_0, q_0, p_0), \text{Win}_1^1 \times Q \rangle$$

where $\tilde{\Delta}$ is obtained from Δ by restricting both players' actions as follows: For a given state $(s, q, p) \in S \times Q \times Q$ and action $a \in A$, if $(s, q) \in \text{Win}_1^1$, $\tilde{\Delta}((s, q, p), a) = \Delta((s, q, p), a)$, otherwise,

Case I: $(s, p) \in \text{Win}_2^2$ and $(s, q) \notin \text{Win}_1^1$,
 $\tilde{\Delta}((s, q, p), a) =$

$$\begin{cases} \Delta((s, q, p), a) & \text{if } s \in S_1, \\ \Delta((s, q, p), a) & \text{if } s \in S_2 \text{ and } a \in \pi_2^2(s, p), \\ \uparrow & \text{if } s \in S_2 \text{ and } a \notin \pi_2^2(s, p). \end{cases}$$

where \uparrow means that the transition is undefined.

Case II: $(s, p) \in \text{Win}_1^1$ and $(s, q) \notin \text{Win}_1^1$,

$$\tilde{\Delta}((s, q, p), a) =$$

$$\begin{cases} \Delta((s, q, p), a) & \text{if } s \in S_1 \text{ and } a \in \pi_1^2(s, p), \\ \uparrow & \text{if } s \in S_1 \text{ and } a \notin \pi_1^2(s, p), \\ \Delta((s, q, p), a) & \text{if } s \in S_2. \end{cases}$$

The winning condition is defined by $\text{Win}_1^1 \times Q$ —that is, P1 wins if he reaches the set $\text{Win}_1^1 \times Q$.

Proof: Before reaching the set $\text{Win}_1^1 \times Q$, at any state (s, q, p) where $s \in S_2$, if (s, p) is perceived winning by P2 (i.e., $(s, p) \in \text{Win}_2^2$), then P2 will select a subjectively rationalizable action $a \in \pi_2^2(s, p)$. If (s, p) is not in Win_2^2 , then any action from P2 is subjective rationalizable. At a state (s, q, p) where $s \in S_1$, if $(s, p) \in \text{Win}_1^1$ but $(s, q) \notin \text{Win}_1^1$, then P1 will select a subjectively rationalizable action $a \in \pi_1^2(s, p)$ so as not to contradict P2's perception. If $(s, p) \notin \text{Win}_1^1$ and

$(s, q) \notin \text{Win}_1^1$, then any action of P1 is deemed subjectively rationalizable by P2. The solution of reachability game $\tilde{\mathcal{H}}\mathcal{G}$, is a policy $\pi_1^* : S \times Q \times Q \rightarrow A_1$ that ensures starting from a state where π_1^* is defined, *no matter which action P2 selects in $\tilde{\mathcal{H}}\mathcal{G}$* , P1 can ensure to reach a state (s, q, p) with $(s, q) \in \text{Win}_1^1$ by following π_1^* , in finitely many steps. By construction, P2 will not know that a misperception exists as P1 takes only subjective rationalizable actions, until P1 reaches Win_1^1 . After reaching the set, P1 can follow the true winning strategy defined for Win_1^1 . ■

Example 2. Given the DFA shown in Fig. 2, we construct HTS and $\tilde{\mathcal{H}}\mathcal{G}$ shown in Fig. 3. In this figure, the red, dashed edges correspond to actions that are *not* subjective rationalizable in P2’s perceptual game and thus removed to obtain $\tilde{\mathcal{H}}\mathcal{G}$. For example, at state $(3, 0, 0)$, P2 thinks that it is irrational for P1 to reach $(4, 0, 0)$ instead of $(2, 0, 1)$ given P2 misperceives the labels of states and thinks that P1 needs to reach state 2.

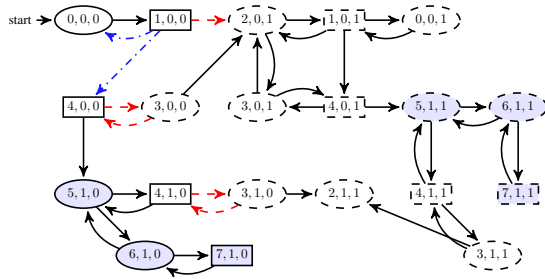


Fig. 3. A graph representing HTS and $\tilde{\mathcal{H}}\mathcal{G}$. The blue and dash dot edges are deterministic choices of P2 in two-player reachability game $\tilde{\mathcal{H}}\mathcal{G}$. The red and dashed edges are not subjectively rationalizable for P2 and thus removed in $\tilde{\mathcal{H}}\mathcal{G}$. Unreachable states in $\tilde{\mathcal{H}}\mathcal{G}$ and $\mathcal{H}\mathcal{G}_M$ are drawn dashed.

In the reachability game $\tilde{\mathcal{H}}\mathcal{G}$, we calculate the stealthy deceptive sure winning region for P1, which includes $\{(5, 1, 0), (6, 1, 0), (7, 1, 0), (4, 1, 0), (4, 0, 0)\}$. This means that P1 can satisfy his objective deceptively from states $\{4, 5, 6, 7\}$ —that is, one state more than the game where P2 does not have misperception. Due to P2’s misperception, P2 will not select to go to state 3 from state 4—making the state 4 deceptive sure winning for P1.

C. Synthesis of a deceptive almost-sure winning strategy

In synthesizing the deceptive sure winning strategy for P1, we assumed that P2 actively selects actions in the zero-sum game $\tilde{\mathcal{H}}\mathcal{G}$ to play against P1’s objective. However, P2 cannot construct this hypergame transition system and thus may make “mistakes”, exploitable by P1. To see this, let us consider the winning strategy for P2 in the reachability game $\tilde{\mathcal{H}}\mathcal{G}$, $\tilde{\pi}_2^* : S \times Q \times Q \rightarrow 2^{A_2}$. For P2 to exercise $\tilde{\pi}_2^*$, P2 should know the value of q in the tuple (s, q, p) , which means that P2 should have a knowledge about L_1 . This is not the case. Next, we consider a realistic assumption for P2.

Assumption 2. For a P2 state (s, q, p) in the HTS, any subjective rationalizable action at (s, p) in \mathcal{G}_2 will be selected by P2 with a non-zero probability.

The assumption on P2’s behavior has the following rationale: At any given state, the set of subjective rationalizable actions has the same values (either 1 or 0 depending on

whether $(s, p) \in \text{Win}_2^2$). The assumption allows P2 to select any action in this set at random, instead of the worst-case scenario (considered by solving stealthy deceptive *sure winning* strategy, in Sec. III-B). Besides, if P2 *never* selects a subjective rationalizable action in her perceptual game, then the game is entirely different as we would have eliminated that action from the arena. This P2’s random choice of subjective rationalizable actions can be considered as opportunities for P1 to exploit.

Theorem 2. Given HTS $= \langle S \times Q \times Q, A, \Delta, (s_0, q_0, p_0), \text{Win}_1^1 \times Q \rangle$, P1 has a *stealthy deceptive almost-sure winning* strategy if and only if he has an *almost-sure winning* strategy in the following one-player stochastic game:

$$\mathcal{H}\mathcal{G}_M = (V = V_1 \cup V_P, A_1, P, v_0, \mathcal{F} = \text{Win}_1^1 \times Q),$$

where the states are partitioned into two subsets: $V_1 = S_1 \times Q \times Q$ are a set of P1’s states and $V_P = S_2 \times Q \times Q$ are a set of *probabilistic states*. The transition function is partially defined as follows. First, any state in \mathcal{F} is a sink or absorbing state. At a state $(s, q, p) \in V_1 \setminus \mathcal{F}$, we distinguish two cases: *Case I-1:* $(s, p) \in \text{Win}_2^2$, for any action $a \in A_1$ enabled from s , $P((s', q', p')|(s, q, p), a) = 1$ where $(s', q', p') = \Delta((s, q, p), a)$. *Case I-2:* $(s, p) \in \text{Win}_1^1$, for any action $a \in \pi_1^2(s, p)$, $P((s', q', p')|(s, q, p), a) = 1$ where $(s', q', p') = \Delta((s, q, p), a)$.

At a state $(s, q, p) \in V_P$, we distinguish two cases: *Case II-1:* $(s, p) \in \text{Win}_2^2$, then for any action $a \in \pi_2^2(s, p)$, $P((s', q', p')|(s, q, p), a) > 0$ where $(s', q', p') = \Delta((s, q, p), a)$. *Case II-2:* $(s, p) \in \text{Win}_1^1$, then for any action $a \in A_2$ enabled from s , $P((s', q', p')|(s, q, p), a) > 0$ where $(s', q', p') = \Delta((s, q, p), a)$.

The almost-sure winning condition is defined by $\text{Win}_1^1 \times Q$ —that is, P1 wins if he reaches the set $\text{Win}_1^1 \times Q$ with probability one.

The proof is similar to that of Thm. 1, with small changes to consider randomized actions of P2. We omitted the proof due to the lack of space.

It is noted that only the support of $P((s, q, p), a)$ is known but not the exact probability distribution. The partial knowledge of the transition probability function gives us a *graph* of the underlying one-player stochastic game. The stealthy deceptive almost-sure winning strategy for P1 is to ensure, with probability one, a state in $\text{Win}_1^1 \times Q$ can be reached. Next, we describe Algorithm 1 to solve the almost-sure stealthy and deceptive winning strategy for P1.

The algorithm uses a function Pre defined as follows.

$$\begin{aligned} \text{Pre}(v, X) = \{v' \in V_1 \mid \exists a \in A_1, P(v|v', a) = 1\} \\ \cup \{v' \in V_P \mid P(v|v') > 0 \implies v \in X\} \quad (2) \end{aligned}$$

and $\text{Pre}(Y, X) = \cup_{v \in Y} \text{Pre}(v, X)$.

Intuitively, the set $\text{Pre}(Y, X)$ includes any state starting from which P1 can ensure to reach the set Y with a positive probability, while staying in X with probability one. The following result is readily obtained by construction.

Proposition 1. The fix-point $X^* = X_k = X_{k+1}$ is the almost-sure winning region for P1 in the one-player stochastic game \mathcal{HG}_M .

Given the fixed point X^* , let Y_0, Y_1, \dots, Y_k be a sequence of states computed using $X = X^*$ in the inner loop, we can extract P1's deceptive almost-sure winning strategy π_1 as follows. For each $v \in Y_i \setminus Y_{i-1}$, $i > 0$, $\pi_1(v, a) = 1$ if $P(Y_{i-1} \mid v, a) = 1$. After reaching \mathcal{F} , P1 follows his sure winning strategy in Win_1^1 .

Algorithm 1 Computation of the almost-sure winning region and strategy for P1 in the one-player stochastic game.

Inputs: $\mathcal{HG}_M = (S = V_1 \cup V_P, A_1, P, \mathcal{F})$.

Outputs: $X_k, \{Y_i\}$.

```

1:  $X_0 = V, Y_0 = \mathcal{F}, k \leftarrow 0$ ,
2: while True do  $i \leftarrow 0$ ,
3:   while True do
4:      $Y_{i+1} = \text{Pre}(Y_i, X_k) \cup Y_i$ 
5:     if  $Y_i = Y_{i+1}$  then
6:       Break.
7:      $i \leftarrow i + 1$ .
8:   if  $Y_i = X_k$  then Break.
9:    $X_{k+1} = Y_i, k \leftarrow k + 1$ ,

```

Example 3. The edges $(1, 0, 0) \rightarrow (0, 0, 0)$ and $(1, 0, 0) \rightarrow (4, 0, 0)$ (drawn in blue, dash dot lines) are in Fig. 3 are now probabilistic choices of P2. We compute 1) $Y_0 = \text{Win}_1^1 \times Q = \{(5, 1, 0), (6, 1, 0), (7, 1, 0)\}$. (here we omitted unreachable states.) 2) $Y_1 = \{(4, 1, 0), (4, 0, 0)\} \cup Y_0$. 3) $Y_2 = \{(1, 0, 0)\} \cup Y_1$, 4) $Y_3 = \{(0, 0, 0)\} \cup Y_2$. Because $Y_4 = Y_3$. The inner loop of Alg. 1 ends. Because now all reachable states in X_0 are in Y_3 . We have $X_0 = Y_3$ and the outer loop of Alg. 1 ends. Thus, P1 can satisfy his objective deceptively from states $\{0, 1, 4, 5, 6, 7\}$.

It is noted that the solutions of deceptive strategies are based on solving multiple games (two-player zero-sum, turn-based games and one-player stochastic games). The space/time complexity is linear in the size of HTS for solving the deceptive sure winning strategy, and polynomial for solving the deceptive almost-sure winning strategy.

IV. CONCLUSION AND DISCUSSIONS

This paper presents a theory of hypergame for synthesizing stealthy deceptive strategies with temporal logic specifications. We have shown that different from the games with complete information where the sure winning and almost-sure winning region overlap, the deceptive sure winning and almost-sure winning regions are different when one player has incomplete or incorrect information.

This work lays the foundation for multiple future directions for both theoretical advances and algorithmic development in game-theoretic deception for cyber-physical defense. One extension is to investigate the application of game-theoretic synthesis to cyber-physical security with decoy-based deception. This extension requires us to generalize the Assumption 1 to incorporate other inference mechanisms. For example, if P2

can detect the true labeling after interacting with the decoy nodes, then P1 could include safety (prevent P2 from reaching decoys) as part of stealthy deception objective. In addition, we will extend the theory of hypergames to concurrent games on graphs [22] and investigate the solution of this class of hypergames.

REFERENCES

- [1] 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.
- [2] E. Gradel and W. Thomas, *Automata, Logics, and Infinite Games: A Guide to Current Research*. Springer Science & Business Media, 2002, vol. 2500.
- [3] R. Bloem, K. Chatterjee, and B. Jobstmann, "Graph games and reactive synthesis," in *Handbook of Model Checking*. Springer, 2018, pp. 921–962.
- [4] K. Chatterjee and T. A. Henzinger, "A survey of stochastic ω -regular games," *Journal of Computer and System Sciences*, vol. 78, no. 2, pp. 394–413, 2012.
- [5] S. Lafortune, "Discrete event systems: Modeling, observation, and control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 2, pp. 141–159, 2019.
- [6] S. Jajodia, V. Subrahmanian, V. Swarup, and C. Wang, *Cyber Deception*. Springer, 2016.
- [7] M. I. Handel, *War, strategy and intelligence*. Routledge, 2012.
- [8] P. G. Bennett and R. R. Bussel, "Hypergame Theory and Methodology: The Current "State of the Art"," in *The Management of Uncertainty: Approaches, Methods and Applications*, L. Wilkin, Ed. Dordrecht: Springer Netherlands, 1986, pp. 158–181.
- [9] Y. Sasaki and K. Kijima, "Hierarchical hypergames and Bayesian games: A generalization of the theoretical comparison of hypergames and Bayesian games considering hierarchy of perceptions," *Journal of Systems Science and Complexity*, vol. 29, no. 1, pp. 187–201, Feb. 2016.
- [10] M. Wang, K. W. Hipel, and N. M. Fraser, "Solution concepts in hypergames," *Applied Mathematics and Computation*, vol. 34, no. 3, pp. 147–171, Dec. 1989.
- [11] N. S. Kovach, A. S. Gibson, and G. B. Lamont, "Hypergame Theory: A Model for Conflict, Misperception, and Deception," *Game Theory*, 2015.
- [12] T. E. Carroll and D. Grosu, "A Game Theoretic Investigation of Deception in Network Security," in *2009 Proceedings of 18th International Conference on Computer Communications and Networks*, Aug. 2009, pp. 1–6.
- [13] E. Al-Shaer, J. Wei, K. W. Hamlen, and C. Wang, "Dynamic bayesian games for adversarial and defensive cyber deception," in *Autonomous Cyber Deception*. Springer, 2019, pp. 75–97.
- [14] B. Gharesifard and J. Cortés, "Stealthy Deception in Hypergames Under Informational Asymmetry," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 6, pp. 785–795, Jun. 2014.
- [15] B. Gharesifard and J. Cortes, "Evolution of Players' Misperceptions in Hypergames Under Perfect Observations," *IEEE Transactions on Automatic Control*, vol. 57, no. 7, pp. 1627–1640, Jul. 2012.
- [16] J. C. Harsanyi, "Games with incomplete information played by "bayesian" players, i-iii part i. the basic model," *Management Science*, vol. 14, no. 3, pp. 159–182, 1967.
- [17] O. Thakoor, M. Tambe, P. Vayanos, H. Xu, C. Kiekintveld, and F. Fang, "Cyber camouflage games for strategic deception," in *International Conference on Decision and Game Theory for Security*. Springer, 2019, pp. 525–541.
- [18] Y. Sasaki, "Subjective rationalizability in hypergames," *Advances in Decision Sciences*, vol. 2014, 2014.
- [19] O. Kupferman and M. Y. Vardi, "Model checking of safety properties," *Formal Methods in System Design*, vol. 19, no. 3, pp. 291–314, 2001.
- [20] R. McNaughton, "Infinite games played on finite graphs," *Annals of Pure and Applied Logic*, vol. 65, no. 2, pp. 149–184, 1993.
- [21] W. Zielonka, "Infinite games on finitely coloured graphs with applications to automata on infinite trees," *Theoretical Computer Science*, vol. 200, no. 1–2, pp. 135–183, 1998.
- [22] L. De Alfaro, T. A. Henzinger, and O. Kupferman, "Concurrent reachability games," *Theoretical Computer Science*, vol. 386, no. 3, pp. 188–217, 2007.