symmetry

MDPI

Article

Goal Recognition Control under Network Interdiction Using a Privacy Information Metric

Junren Luo, Xiang Ji, Wei Gao , Wanpeng Zhang * and Shaofei Chen

College of Intelligence Science and Technology, National University of Defense and Technology, Changsha 410073, China

* Correspondence: wpzhang@nudt.edu.cn; Tel.: +86-0731-8457-6674

Received: 4 July 2019; Accepted: 13 August 2019; Published: 17 August 2019

Abstract: Goal recognition (GR) is a method of inferring the goals of other agents, which enables humans or AI agents to proactively make response plans. Goal recognition design (GRD) has been proposed to deliberately redesign the underlying environment to accelerate goal recognition. Along with the GR and GRD problems, in this paper, we start by introducing the goal recognition control (GRC) problem under network interdiction, which focuses on controlling the goal recognition process. When the observer attempts to facilitate the explainability of the actor's behavior and accelerate goal recognition by reducing the uncertainty, the actor wants to minimize the privacy information leakage by manipulating the asymmetric information and delay the goal recognition process. Then, the GRC under network interdiction is formulated as one static Stackelberg game, where the observer obtains asymmetric information about the actor's intended goal and proactively interdicts the edges of the network with a bounded resource. The privacy leakage of the actor's actions about the real goals is quantified by a min-entropy information metric and this privacy information metric is associated with the goal uncertainty. Next in importance, we define the privacy information metric based GRC under network interdiction (InfoGRC) and the information metric based GRC under threshold network interdiction (InfoGRCT). After dual reformulating, the InfoGRC and InfoGRCT as bi-level mixed-integer programming problems, one Benders decomposition-based approach is adopted to optimize the observer's optimal interdiction resource allocation and the actor's cost-optimal path-planning. Finally, some experimental evaluations are conducted to demonstrate the effectiveness of the InfoGRC and InfoGRCT models in the task of controlling the goal recognition process.

Keywords: information metric; goal recognition; network interdiction; Stackelberg game

1. Introduction

Goal recognition (GR), also called intention recognition, or more generally plan recognition, is the task of recognizing other agents' goals by analyzing the actions and/or the state (environment) changes caused by the actions [1], which has drawn the interest of researchers in the field of artificial intelligence and psychology for recent decades. Goal reasoning as one variant is the process in which intelligent agents continually reason about the goals they are pursuing [2]. Goal recognition design has been proposed to redesign the environment to facilitate goal recognition offline [3]. As one sub-problem of PAIR (plan activity and intent recognition) [4], goal recognition has been successfully applied to various applications, such as human–machine interaction (HMI) in social settings (home, offices, and hospitals) [5], agent modeling [6], critical infrastructure protection (CIP) [7], and some military applications about reasoning the goals of the terrorists or opponents [2,8]. Unlike manipulating asymmetric information in CIP, goal recognition is widely applied to "human–AI planning (HAIP)" [9], and "explainable planning (XAIP)" [10], where the focus is symmetric information understanding and

explicit information sharing respectively. But, in a parallel thread, new problems arise, such as the goals uncertainty in a fully observable and deterministic environment, the hard environment redesign can be replaced by soft interdiction with additional cost to actions. One simplified CIP scenario is illustrated in Figure 1, first mentioned in [7], in which the defender' objective is to protect critical infrastructure against the attacker whose goal (target) is unknown. The urban environment contains military and government facilities, physical (natural or artificial) obstacles and other environmental factors, where the ability of agents to perform certain actions is restricted. The actor is equipped with some explosive weapons, and these weapons enable the actor to carry out bomb attacks on vulnerable buildings. Owing to the different situation awareness of the urban environment, the defender has asymmetric information about the attacker's real goals [11], but bridge interdiction still could be performed by the defender to facilitate the goal recognition process.

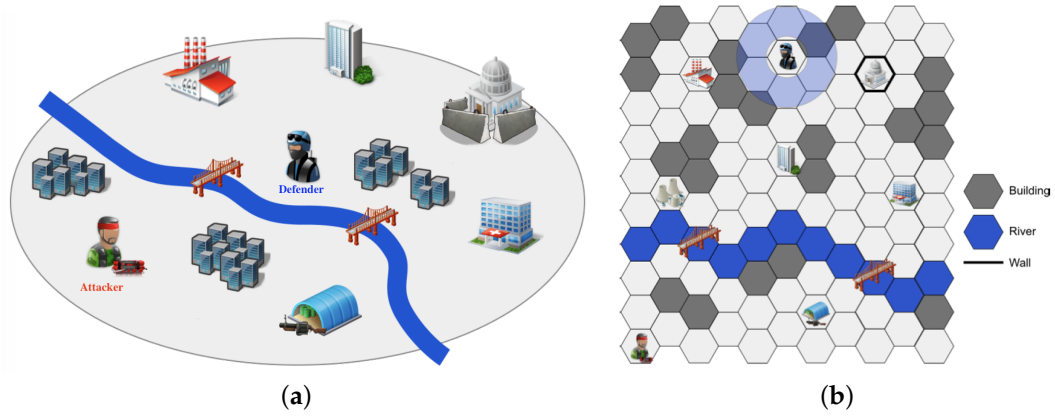


Figure 1. A simple tactical scenario of critical infrastructure protection (CIP) [7]: the defender would like to proactively recognize the goal of the attacker and make response plans. (**a**) A CIP domain. (**b**) A simple instance of the CIP domain.

Explainability, as one key AI enabling technology, has been used to develop robust AI applications and systems [12]. Explainability and obfuscation of the behavior are a pair of opposite requirements, since sharing and hiding the goals depict the opposite choice of the agents. Sharing goals drives the actor's behavior to be explainable (interpretable) with understandability [13], explicability [14], legibility [15], predictability [16], and transparency [17], while hiding goals drives the actor's behavior to be uninterpretable with obfuscation, deception, privacy, and security [18]. In the cooperative setting, the explainability and interpretability of behavior remain significantly challenging in developing human-aware AI agents [18] and human-agent systems [19]. Goal signaling assists behavior explanation in human-robot teaming [20]. In order to share explainable behavior, the human-aware agent should not only consider his own model, but also the observer model and the differences thereof [5]. In the adversarial setting, such as military mission planning and counter-planning [21,22], keeping the goal obfuscated is the most important. Many recent pieces of work explore deception [23] and privacy [24]. For example, deception was investigated in two classes, simulation and dissimulation [23], privacy was investigated in five classes, agent privacy, model privacy, decision privacy, topology privacy, and constraint privacy [25,26]. In cooperative and adversarial environment, a goal-driven intelligent agent would manipulate the goals in the goal-pursuing process, such as sharing or revealing the goals among teammates and meanwhile hide the goals against adversaries. The recursive reasoning process shows the cruel twist of situation awareness between agents, who continually react to their evolving situation, possibly abandoning current goals and switching to other goals [27]. Many unified frameworks have been proposed for the cooperative and adversarial environment, such as information bottleneck based intention reveal and hide [28–30], cooperative-competitive processes (CCP)-based multi-agent decision-making [31]. In fact,

many pieces of research revolved around the communication of goals implicitly using behavioral cues. The agents' action could be treated as special cases of implicit signaling behavior [18,20]. The highly interwoven decision-making process of the opposing players situated in these settings motivates the need for a comprehensive strategic analysis, which would help the observer to recognize the agents' real goals and identify the optimal interdiction strategies [32].

In different game models, the players are called differently. To be different from the pairing roles, such as attacker–defender, leader–follower, searcher–evader, and interdictor–intruder, in this paper, we use actor–observer as a more neutral pairing role to depict the interaction between the two players. When the actor performs an action privately in adversarial environment, the privacy information leakage from the actor's behavior is closely related to the goal uncertainty. Similar to the behavioral probability weighting technique, which has been used in interdependent security game [33], the actions or states of the agents can be measured by information metrics. In this paper, we quantify the privacy information leakage of actions or states with a min-entropy information metric, which is tightly associated with the goal uncertainty and can be used to aid in recognizing the goals. Aiming at assisting the observer to control the goal recognition process, in this paper, we follow the multi-model models, such as share (reveal, signal) or hide information [28,29], delay predictability [34] or assist recognition [3], reduce or improve uncertainty [35], and define the goal recognition control (GRC) problem under network interdiction with a privacy information metric as InfoGRC. Here, the observer will reduce the goal uncertainty value through limiting the action space that an actor can perform under network interdiction, while the actor manages to delay the goal recognition process through adding the goal uncertainty value by performing abnormal actions.

In summary, the main contributions of this paper are as follows:

- We start by introducing one game-theoretic decision-making framework, and then present the generative inverse path-planning and network interdiction for goal recognition, and some information metrics for the signaling behavior.
- We adopt a min-entropy based privacy information metric to quantify the privacy information leakage of the actions and states about the goal.
- We define the InfoGRC and InfoGRCT using the privacy information metric, and provide a more compact solution method for the observer to control the goal uncertainty by incorporating the information metric as additional path cost.
- We conduct some experimental evaluations to demonstrate the effectiveness of the InfoGRC and InfoGRCT model in controlling the goal recognition process under network interdiction.

The rest of the paper is organized as follows: the background and related work are introduced in Section 2. In Section 3, the min-entropy based privacy information metric is presented, the InfoGRC and InfoGRCT problems are defined, and a Benders decomposition based solution method is introduced. Section 4 presents experimental results, evaluation, and analysis. Finally, conclusion and future work are summarized in Section 5.

2. Background and Related Work

In the defense and security domain, critical facility protection, privacy security, and convoy protection are in need of goal recognition. In such situations, the observer (decision-maker) is threatened by the actor with some conflicting goals and need one enabler to read the actor's mind. Here, we first propose one game-theoretic decision-making framework for goal recognition under network interdiction, the goal recognition process can, therefore, be divided into two main subtasks, namely generative inverse planning, where the observer attempts to generate plans for the actor, and goal recognition for proactive response, where the observer has to identify the actor's goal and make proactively response plans. As shown in Figure 2, the observer will get the game situation from the generative courses of action (COA) of the hostile opponents and friendly teammates, then attempts to recognize the actor's goals under network interdiction. In fact, as one important carrier,

the network can be used to represent "critical infrastructure network" (road network, railway network, power network, and cyber network), "task plans" (HTN, attack graph, and Petri Net). In this paper, we simply use the road network for path-planning and network interdiction.

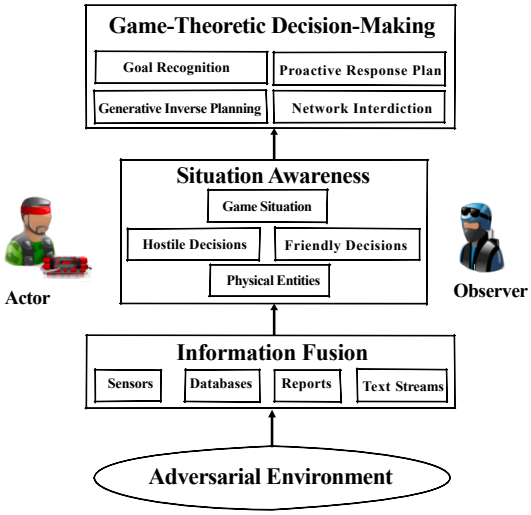


Figure 2. A game-theoretic decision-making framework for goal recognition under network interdiction.

2.1. Path-Planing and Network Interdiction

2.1.1. Path-Planning

Path-planning is a sub-problem of general task planning, which aims at finding a path through the map of a domain. One typical path planning scenario on the hexagonal grids is illustrated in Figure 3. Path-planning for an actor on the road network (discrete grid or connected graph representation) finds a path from the start location to the final goals. The path-planning problem can be defined as follow:

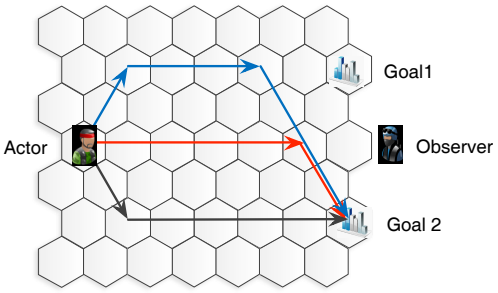


Figure 3. A simple path-planning scenario on the hexagonal grid, where the black path contains the least goal uncertainty, the red path contains the largest goal uncertainty, while the blue path contains some deceptive steps.

Definition 1 (PPD). *A path planning domain is a tuple:*

$$\mathcal{D} = \langle \mathcal{N}, \mathcal{E}, \mathrm{c} \rangle \tag{1}$$

- $\mathcal{N}$ *is a non-empty set of location nodes;*
- $\mathcal{E} \subseteq \mathcal{N} \times \mathcal{N}$ *is a set of actions related edges between nodes;*
- $\mathrm{c} : \mathcal{E} \mapsto R_0^+$ *returns the cost of traversing each edge.*

Definition 2 (GDPP). *A goal-driven path planning problem is a tuple:*

$$\mathcal{P}_{GP} = \langle \mathcal{D}, s, \mathcal{G}, \mathcal{P}_{po}, \Omega, \mathcal{O} \rangle \tag{2}$$

- $\mathcal{D}$ *is the path planning domain;*
- $s \in \mathcal{N}$ *is the start location;*
- $\mathcal{G} = \{g_r, g_0, g_1, \dots\}$*is a set of candidate goals, where* g_r *is the real goal;*
- $\mathcal{P}_{po}(\mathcal{G}|\mathcal{O}_n)$ *denotes the posterior probability of a goal given a sequence of observations (or last state in that sequence), which can be the model of the observer;*
- $\Omega = \{o_i | i = 1, \dots, m\}$ *is the set of m observations that can be emitted as results of the actions and the states;*
- $\mathcal{O} : (\mathcal{N} \times \mathcal{E}) \to \Omega$ *is a many-to-one observation function which maps the action taken and the next state reached to an observation in* Ω.

2.1.2. Network Interdiction

In the defense and security domain, interdiction refers to actions that serve to block or otherwise inhibit an adversary's operations [36]. Network interdiction is usually involved with two players, and it is a special class of network flow games [37], which has been widely studied in the fields of combinatorial optimization, artificial intelligence, and operations research. The interdiction and fortification between the two players can be described as one Stackelberg game model [38]. Generally, two basic models of network interdiction are considered: maximum-flow network interdiction (MXFI), shortest path network interdiction (SPNI). In this paper, we focus on maximizing the shortest path (MXSP), one variant of SPNI, where the actor attempts to travel along the shortest path through a road network from one start (origin) to one goal (destination), while the observer tries to interdict the edges to maximize the length of this shortest path. When the actor privately approaches a goal, the probability that the actor's goal is correctly recognized by the observer would be inversely proportional to the path cost or time cost that the actor is willing to take. So, we formulate this road network interdiction problem with one Stackelberg game model, in which observer aims at maximizing the expectation of "start-goal" path cost in a directed path network by interdicting nodes (states) or edges (actions) under bounded resource. In fact, the node interdiction problem can be transformed into one edge interdiction problem [39,40]. In such environment, the actor's past actions or states are increasingly difficult to conceal, the observer would proactively take some interdictions to accelerate the goal recognition process.

We consider that an actor executes a cost-critical task to travel from a start location S to a goal location G in minimum path cost, meanwhile, an observer seeks to interdict the actor path by choosing states (nodes) or actions (edges) along from S to G. The set of nodes between S and G define a secure road network represented by a directed graph $\mathcal{G}(\mathcal{N}, \mathcal{E})$, as shown in Figure 4, where the set $\mathcal{N}$ is the set of $|\mathcal{N}|$ nodes between S and G, and the set $\mathcal{E}$ is the set of connections between nodes.

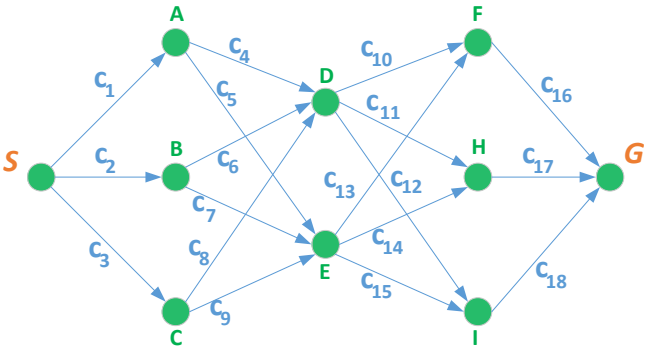


Figure 4. A simple road network with 10 nodes.

Each path will go through some nodes which are shared among different paths. An extremely patient actor without task but with a large time budget might start along a path that traverses the entire state space (e.g., a Hamiltonian path over the nodes) and stop when the goal is reached, so as to make the past actions reveal essentially nothing about the goal and make the observer's recognition difficult [34]. But one goal-driven actor would lie somewhere in the middle, by combining a cost-optimal path with some wasteful actions of goal obfuscation. In addition, owing to the bounded resources for interdiction, the observer is unable to separate the goal and the start node by interdicting the minimum-cut set. The basic mathematical formulation of MXSP is defined as follows:

$$[\text{MXSP-P}] \quad z^* = \max_{\mathbf{x}\in X} \min_{\mathrm{y}} \sum_{a\in\mathcal{E}} \left(c(a) + x(a)d(a)\right) y(a) \tag{3}$$

$$s.t. \quad \sum_{a\in \mathrm{Out(i)}} y(a) - \sum_{a\in \mathrm{In(i)}} y(a) = \begin{cases} 1 & \text{for } i = s \\ 0 & \forall i \in \mathcal{N}\setminus\{s,g\} \\ -1 & \text{for } i = t \end{cases} \tag{4}$$

where $X = \left\{\mathbf{x} \in \{0,1\}^{|\mathcal{E}|} | \mathbf{r}^T\mathbf{x} \le R\right\}$ with bounded resource R, $x(a), y(a) \in \{0,1\}$ indicate the observer's interdiction resource allocation and the actor's traverse respectively.

- $\mathbf{x}^*$ denotes an optimal interdiction solution for the observer.
- Flow-balance constraints of variables y, route one unit of flow from s to g, the inner minimum is a standard shortest path model with edge cost $c(a) + \alpha x(a)d(a)$.
- $c(a)$ is the nominal cost of edge a and $c(a) + d(a)$ is the interdicted cost; $d(a)$ represents the additional path cost, if sufficiently large, represents complete destruction of edge a.
- $r(a)$ is a small positive integer, representing how many resources are required to interdict edge a.
- R is the total available resource, the observer has $C_R^{|x|}$ possible interdiction combinations, which will grow exponentially with R.
- y denotes a traverse path of the actor.

If the outer variable $\mathbf{x}$ is fixed, we can take the inner minimization using Karush–Kuhn–Tucker (KKT) conditions, then the dual formulation that releases $\mathbf{y}$ is defined as follows:

$$[\text{MXSP-D}] \quad z^* = \max_{x\in X, \vec{\pi}} \pi(t) - \pi(s) \tag{5}$$

$$s.t. \quad \pi(j) - \pi(i) - d(a)x(a) \le c(a), \quad \forall a = (i,j) \in \mathcal{E} \tag{6}$$

$$\pi(s) = 0. \tag{7}$$

where we may interpret $\pi(i)$ as the post-interdiction shortest-path cost from s to i, $\pi(s) = 0$.

2.2. Goal Recognition

The ability to recognize the goals of others enables humans to reason about what they are doing, why they are doing it, and what they will do next [4]. Goal recognition problems can be divided into three kinds according to the role of the actor whose intention is being inferred. In keyhole recognition [41], the actor is unaware of being observed and recognized as if the actor is looking through a keyhole. In intended recognition [42], the actor wants to convey the goal to be understood. In adversarial recognition [7], the actor is actively hostile to the observations of the actions and the inference of the goals, and would hide the intention and attempt to thwart the recognition process by deception and concealment. Different kinds of intention recognition bring different challenges. More generally, adversarial plan recognition has been applied to the recognition of strategies and tactics of opponents, in which adversarial reasoning is needed to understand the minds of the opponents. Generic methods for plan recognition are based on plan-library [43], inverse-planning [44], and learning [45].

2.2.1. Probabilistic Goal Recognition

Among the approaches proposed for goal recognition, the probabilistic goal recognition model is highly regarded, and it is defined as follows:

Definition 3 (PGR). *A probabilistic goal recognition problem for path-planning is a tuple:*

$$\mathcal{P}_{GR} = \langle \mathcal{D}, \mathcal{G}, s, O, \mathcal{P}_{pr} \rangle \tag{8}$$

- $\mathcal{D} = \langle \mathcal{N}, \mathcal{E}, \mathrm{c} \rangle$ *is a path planning domain;*
- $\mathcal{G} \subseteq \mathcal{N}$ *is the set of candidate goals locations;*
- $s \in \mathcal{N}$ *is the start location;*
- $\mathcal{O} = o_1, \ldots, o_k$, *where* $k \geq 0$ *and* $o_i \in \mathcal{N}$ *for all* $i \in \{1, \ldots, k\}$, *is a sequence of observation;*
- $\mathcal{P}_{pr}$ *represents the prior probabilities of the goals.*

The solution to a probabilistic goal recognition problem is a posterior probability distribution $P_{po}(\mathcal{G}|\mathcal{O})$ over the set of possible goals. Given the start location and the sequence of observations, the posterior goal distribution will be computed by the Bayesian rule. One cost difference-based [46] Boltzmann distribution of the posterior probability is defined as follow:

$$\mathcal{P}_{po}(\mathcal{G}|\mathcal{O}) = \alpha \mathcal{P}(\mathcal{O}|\mathcal{G}) \mathcal{P}_{pr}(\mathcal{G}) = \alpha \frac{e^{-\lambda \delta}}{1 + e^{-\lambda \delta}} \tag{9}$$

$$\delta = \mathcal{C}_{diff}(s, g, \mathcal{O}_n) = optc(\mathcal{O}_n, g) - optc(s, g), \tag{10}$$

where α is a normalizing constant across all goals, λ is a positive constant which captures a soft rationality assumption, s is the start, g is a goal, $\mathcal{O}_n$ is the most recently observed of the actor.

This cost difference-based recognition method provides one single-observation recognition paradigm, since the start and goal-related cost difference can be computed offline, we only need to compute the current location-related cost difference.

2.2.2. Goal Recognition Design

Goal recognition design focuses on one controllable environment by modifying the configuration of the domain [43]. As for the observer, redesigning the environment will improve explainability of the actor's behavior. Many metrics have been proposed to redesign the environment, such as worst case distinctiveness (*wcd*) [3], expected-case distinctiveness (ecd) [47], all-goals *wcd* ($wcd_{(ag)}$) [47], and relative goal uncertainty (rgu) [35]. As for more general plan recognition design problem, the worst-case distinctiveness for plans (wcpd) measures the number of observations needed to unambiguously identify the agent's plan [43]. The *wcd* and goal recognition design (GRD) problem are defined as follow:

Definition 4 (*wcd*). *Let* $\Pi_D = \{\pi | \pi$ *is a non-distinctive path of* $D)$ *and let* $|\pi|$ *denote the length of a path* π, *then, worst case distinctiveness (wcd) of a model* $\mathcal{D}$, *denoted by* $wcd(\mathcal{D})$, *is:*

$$wcd(\mathcal{D}) = \max_{\pi \in \Pi_{\mathcal{D}}} |\pi| \tag{11}$$

Definition 5 (GRD). *A goal recognition design problem is defined as a tuple:*

$$\mathcal{D} = \langle \mathcal{P}_{\mathcal{D}}, \mathcal{G}_{\mathcal{D}} \rangle \tag{12}$$

- $\mathcal{P}_{\mathcal{D}}$ *is a planning domain formulated in STRIPS;*
- $\mathcal{G}_{\mathcal{D}}$ *is a set of possible goal;*

- *The output is* $\mathcal{P}_{\mathcal{D}}{}'$ *such that* $wcp\left(\mathcal{P}_{\mathcal{D}}{}'\right) \leq wcp\left(\mathcal{P}_{\mathcal{D}}{}''\right)$,

where all actions have the same cost, the objective is to find a subset of actions and remove them from the action space, then the wcd of the resulting problem is minimized.

These metrics for GRD are mainly formulated to optimize the maximum number of observations, which are required to unambiguously infer the goal or plan of the agent [43]. Such as the *wcd* of a domain $\mathcal{D}$ is an upper bound of the action number that the actor can perform in a stable model, before selecting a distinctive path to reveal the goal [3]. Figure 5 portrays two possible solutions for placing barriers or blocks to interdict the passage of the actor.

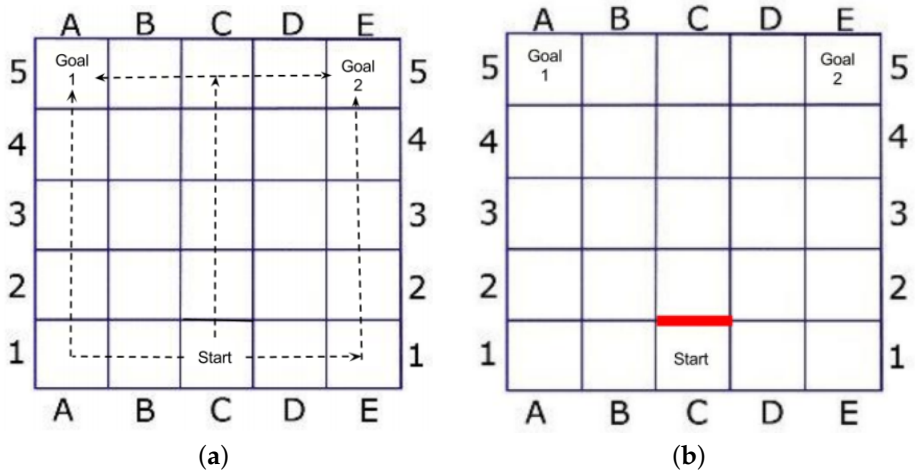


Figure 5. The goal recognition design problem with two kinds of redesign (interdiction): the *wcd* value is 4 in (**a**), the *wcd* value is 0 in (**b**) [3]. (**a**) A GRD domain; (**b**) redesign with one block.

In addition, the GRD problem can be reformulated into an optimization problem with some constraints: the cost of the cost-optimal plan to achieve each goal $g \in \mathcal{G}$ is the same before and after removing the subset of actions [48]. So, the objective is to find a subset of action $\delta\mathcal{E} \subset \mathcal{E}$, if they are removed from the set of actions $\mathcal{E}$, then the *wcd* of the resulting problem is minimized.

$$\delta\mathcal{E} = \text{argmin}_{\delta\mathcal{E}\subset\mathcal{E}} wcd(P) \tag{13}$$

$$s.t \quad \mathcal{C}\left(\pi_g^*\right) = \mathcal{C}\left(\hat{\pi}_g^*\right) \qquad \forall g \in \mathcal{G} \tag{14}$$

where $P = \langle \mathcal{D}, \mathcal{G} \rangle$ is the problem with the resulting domain $\hat{\mathcal{D}} = \langle \mathcal{N}, s_0, \mathcal{E} \backslash \delta\mathcal{E}, f, \mathcal{C} \rangle$ after removing actions $\delta\mathcal{E}$, π_g^* is a cost-optimal plan to achieve goal g in the original problem P, and $\hat{\pi}_g^*$ is a cost-minimal plan to achieve goal g in problem $\hat{P}$.

As for goal uncertainty, last deceptive point (LDP)-based deceptive path planning [23] and equidistant states based goal obfuscated plan [49] present two selective solutions. But, there are still a few standard assumptions in cryptography and multi-party computation. But what if the adversary knows the algorithms, which is realistic and complied with Kerckhoffs' principle used in cryptography [50], these closed formulated solutions of the deceptive path-planning will not incorporate deception. Goal recognition design aims at facilitating the recognition process. In order to reduce the *wcd*, three types of modification, i.e., sensor refinement (SR), action removal (AR), and action conditioning (AC), are widely used [51]. Owing to the strategic interaction between the actor and the observer in the GR and GRD problems, the solutions with cost-minimal or *wcd* do not reflect the strategic behaviors [52]. We are more interested in adopting soft measures such as additional action cost by interdiction so as to control the goal uncertainty.

2.2.3. Trend and Dual-Use

Three paradigms are widely used in recent research on goal recognition, such as the decision-theoretic paradigm based equi-reward utility maximizing design (ER-UMD) model, the environment is controlled by applying a sequence of modifications to maximize the agent's utility [53]. The game-theoretic paradigm-based goal recognition and design models were used to reason the opponents' minds, such as the adversarial intention recognition as inverse planning model, one generative stochastic game model was used for threat assessment [7]. As for the learning-based paradigm, inverse reinforcement learning [45], maximum entropy deep reinforcement learning [54], and information regularization-based deep reinforcement learning [30] are usually employed to explore the stochastic environment.

Network flow interdiction [55], plan interdiction games [56] and MDP interdiction [57] show one more potential research thread about interdiction. Network flow based game models such as network control under node disruptions and network routing under link disruptions [37] show one parallel thread of research about the goal and plan recognition.

From the perspective of explainability, goal obfuscation is the inverse problem of the goal legibility, while plan obfuscation is the inverse problem of the goal predictability [18]. Considering the duality property, road network interdiction is the inverse problem of network fortification [58].

2.3. Behavioral Information Metrics

Several information metrics for signaling behavior have been proposed in the literature. Such as the deception metric for deceptive path-planning, which involves finding a path such that the probability of an observer identifying the final destination is minimized [23]. As in the cost-optimal path-planning setting, simulation (simply deception) or dissimulation(concealment) can be employed to thwart the goal recognition process.

Simulation bound agents deliberately choose misleading actions to confuse the goal recognition process, i.e., there exists $g \in \mathcal{G} \backslash \{g_r\}$ s.t. the recognition probability $P\left(g_r|s_j\right) < P\left(g|s_j\right)$, where s_j is the j-th node, g_r is the real goal.

Definition 6 (S-SD). *The simulation based state information metric is defined as follows:*

$$\mathcal{I}_{S-SD}(s_j) = \max_{g_i \in G \backslash \{g_r\}} P\left(g_i|s_j\right) - P\left(g_r|s_j\right). \tag{15}$$

Definition 7 (A-SD). *The simulation based action information metric is defined as follows:*

$$\mathcal{I}_{A-SD}(a_i) = 1 - \lambda \mathcal{I}_{S-SD}(s_j). \tag{16}$$

Dissimulation-bound agents act covertly or intentionally select actions that are hard to detect. That is, there exists $g \in \mathcal{G} \backslash \{g_r\}$ s.t. the recognition probability $P\left(g_r|s_j\right) \leq P\left(g|s_j\right)$, where s_j is the j-th node, g_r is the real goal.

Definition 8 (S-DD). *The dissimulation-based state information metric is defined as follows:*

$$\mathcal{I}_{S-DD}(s_j) = -\kappa \sum_{g_i \in \mathcal{G}} P\left(g_i|s_j\right) \times \log\left(P\left(g_i|s_j\right)\right) \quad (\kappa = \log_2 |\mathcal{G}|) \tag{17}$$

Definition 9 (A-DD). *The dissimulation-based action information metric is defined as follows:*

$$\mathcal{I}_{A-DD}(a_i) = 1 - \lambda \mathcal{I}_{S-DD}(s_j) \tag{18}$$

Also, in some game-theoretic approaches of learning-based goal recognition frameworks, such as in [7], belief space and Kullback–Leibler (KL) divergence D_{KL} have been adopted to measure

the deception of strategy. Besides, in the reinforcement learning domain, the conditional mutual information between goal and action given state, $\mathcal{I}_{action}[\pi] := \mathcal{I}(\mathcal{A}; \mathcal{G}|\mathcal{S})$ was defined as the action information metric, and the mutual information between state and goal, $\mathcal{I}_{state}[\pi] := \mathcal{I}(\mathcal{S}; \mathcal{G})$ was defined as the state information metric [29]. Although these metrics have been defined for goal-related actions and states, the applicable scenarios and environment are diverse, we may need some neutral metrics if the actor knows the observer's algorithms or deliberately reveals the goal.

3. Goal Recognition Control

In this section, we will define the GRC problem in the context of defense and security with the road network to connect start locations and goals. Different from the GRD problem, we employ more applicable and soft measure, network interdiction under bounded resource, to control the goal recognition process. We propose to model the GRC problem under network interdiction as one Stackelberg game, where the observer owns asymmetric information about the actor's intended goal, and could proactively allocate security resources (such as road barrier, patrolling force) to protect goals against the actor.

3.1. Privacy Information Metrics

In the fully observable and deterministic environment with multiple goals, the observer may not be able to catch the real goal, since the actor's actions and states contain goal uncertainty. Given the possible goals and current observations, the posterior probability distribution over the goals reflects the goal uncertainty that the actor will encounter after selecting an action and reaching the next state. This enlightens us to measure the goal uncertainty associated with the conveyed information of the actions and states, in which the leaked privacy information can be quantified as the difference between the initial uncertainty and the remaining uncertainty. In this paper, we consider the actions (the adjacent edges between the nodes in the road network) as quantitative information flow [59], the leakage of the privacy information is based on the uncertainty of the observer about the input. We propose to use the min-entropy (an instance of Rényi entropy [60]) as the privacy information leakage metric. How much information about H can be deduced by the observer who obtains the output L is computed as follows:

$$Information \quad Leakage = Initial \quad uncertainty - Remaining \quad uncertainty \tag{19}$$

- initial uncertainty: $H_\infty(H) = -logV(H)$
- remaining uncertainty: $H_\infty(H|L) = -logV(H|L)$.
- information leakage $= H_\infty(H) - H_\infty(H|L)$

where $V(\mathrm{x}) = \max_{x \in \mathcal{X}} p(\mathrm{X} = x)$.

This privacy leakage metric represents the rate of information transmission, which has been widely used in quantifying the privacy leakage in the privacy-preserving planning domain [28]. In this section, we will define the state and action privacy information metrics to control the goal recognition process. Under the requirement of privacy-preserving, the actor may deliberately choose misleading actions to obfuscate the goal, i.e., if there exists $g \in \mathcal{G} \backslash \{g_r\}$ s.t. the recognition probability $P\left(g_r|s_j\right) < P\left(g|s_j\right)$, where s_j is the j-th node, g_r is the real goal. So, we define the metric of action at each state as follows:

Definition 10 (S-PI)**.** *The privacy information metric of the state is defined as follows:*

$$\mathcal{I}_{S-PI}(s_j) = H(\max_{g_i \in G \backslash \{g_r\}} P\left(g_i|s_j\right) - P\left(g_r|s_j\right)) = -log(\max_{g_i \in G \backslash \{g_r\}} P\left(g_i|s_j\right) - P\left(g_r|s_j\right)) \tag{20}$$

Definition 11 (A-PI). *The privacy information metric of action is defined as follows:*

$$\mathcal{I}_{A-PI}(a_i) = \frac{\sum_{a_j \in \mathcal{E}'(s)} I_{S-PI}(s)}{|\mathcal{E}'(s)|} \tag{21}$$

where $a_i \in \mathcal{E}(s)$, $a_j \in \mathcal{E}'(s)$, *and* $\mathcal{E}'(s) = \mathcal{E}(s) \backslash a_i$.

The metric $\mathcal{I}_{A-PI}(a_i)$ reflects the goal uncertainty associated with the action taken. The higher the privacy information metric is, more uncertainty the goal will be, which means the action taken by the actor gives less privacy information to the observer, and this will accelerate the goal recognition process. As shown in Figure 6, we compute the $\mathcal{I}_{A-PI}(a_i)$ of actions represented by arrow edges between nodes. As for the path-planning task, goal 1 and goal 2 are the actor's two goals from the start node 2, we use $c'(a) = c(a) + \mathcal{I}_{A-PI}(a)$ and $c(a) = 1$ to represent the additional path cost, which will be employed by the observer to control the goal recognition process. Generally, the actor would choose $path = \langle 2, 5, 8, 7 \rangle$ for the goal 1 and $path = \langle 2, 5, 8, 9 \rangle$ for goal 2. After the additional path cost with $\mathcal{I}_{A-PI}(a)$, the actor will choose $path = \langle 2, 1, 4, 7 \rangle$ for the goal 1 and $path = \langle 2, 3, 6, 9 \rangle$ for goal 2.

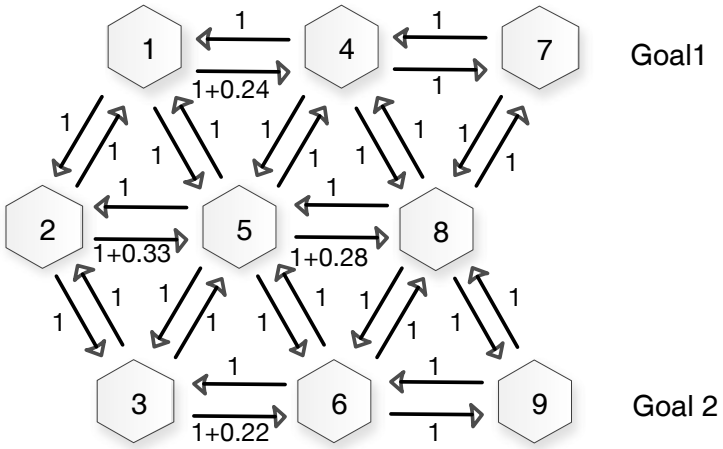


Figure 6. Path-planning on the hexagon grid with additional path cost $\mathcal{I}_{A-PI}(a)$.

3.2. InfoGRC and InfoGRCT

The GRC problem is a special case of static Stackelberg game. The observer attempts to facilitate the explainability of the actor's behavior and accelerate goal recognition by reducing the goal uncertainty under network interdiction, while the actor wants to delay the goal recognition process. Without requiring the cost-optimal paths to the goals to be the same before and after redesign the environment, as investigated in GRD, we will attempt to change the goal uncertainty by proactively allocating interdiction resource to add the action cost. Adding the information metric $\mathcal{I}$ proportionally as additional cost to the original action cost: $c'(a) = c(a) + \mathcal{I}_A(a)$, the GRC problem under network interdiction could be transformed into the problem of maximizing the expectation of "s-g" path cost. Here, we use optimization techniques to reformulate the GRC problems as mathematical programming problems. Some notations are shown in Table 1.

Table 1. Notations for the information metric based goal recognition control (GRC) under network interdiction (InfoGRC) and information metric based GRC under threshold network interdiction (InfoGRCT) problem.

Parameters	Meaning
Sets and indices	
$\mathcal{G} = (\mathcal{N}, \mathcal{E})$	Road graph network with nodes $\mathcal{N}$ and edges $\mathcal{E}$
$i \in \mathcal{N}$	Node i in $\mathcal{G}$
$a = (i, j) \in \mathcal{E}$	Edge (i, j) in $\mathcal{G}$
$s \in \mathcal{N}$	Start node s
$g \in \mathcal{N}$	Goal node g
In(i)/Out(i)	Edges set directed into or out of node i
Data	
$0 \leq c(a) < \infty$	Cost of edge a, vector form $\mathbf{c}$
$0 < d(a) < \infty$	Interdiction increment if edge a is interdicted, vector form $\mathbf{d}$
$\mathcal{I}_A(a)$	The privacy information metric of action a
$r(a) > 0$	Resource required to interdict edge a, vector form $\mathbf{r}$
R	Total amount of interdiction resource available
$\tilde{\theta} > 0$	Threshold of the shortest path
$\overline{\theta} > 0$	Upper bound with full interdiction
$\underline{\theta} > 0$	Lower bound without interdiction
Decision Variables	
$x(a)$	Observer's interdiction resource allocation, $x(a) = 1$ if edge a is interdicted
$y(a)$	Actor's traveling edge, $y(a) = 1$ if edge a is traveled by the actor

3.2.1. Accelerate and Delay

In order to formulate the accelerate model of the goal recognition process for the observer and the delay model of the goal recognition process for the actor, we use the network flow model to define these situations as follows:

$$[Accelerate] \quad z^* = \max_{\mathbf{x} \in X} \min_{\mathrm{y}} \sum_{a \in \mathcal{E}} \left(c(a) + x(a) d(a) (1 + \alpha \mathcal{I}_A(a)) \right) y(a) \tag{22}$$

$$[Delay] \quad z^* = \max_{\mathbf{x} \in X} \min_{\mathrm{y}} \sum_{a \in \mathcal{E}} \frac{\left(c(a) + x(a) d(a) \right)) y(a)}{1 + \beta \mathcal{I}_A(a)} \tag{23}$$

$$s.t. \quad \sum_{a \in Out(i)} y(a) - \sum_{a \in In(i)} y(a) = \begin{cases} 1 & \text{for } i = s \\ 0 & \forall i \in \mathcal{N} \setminus \{s, g\} \\ -1 & \text{for } i = t \end{cases} \tag{24}$$

where $X = \left\{ \mathbf{x} \in \{0,1\}^{|\mathcal{E}|} | \mathbf{r}^T \mathbf{x} \leq R \right\}$ with bounded resource R, $x(a), y(a) \in \{0,1\}$ indicate the observer's interdiction resource allocation and the actor's traverse path respectively, α, β are the controlling parameters of two opposite objectives.

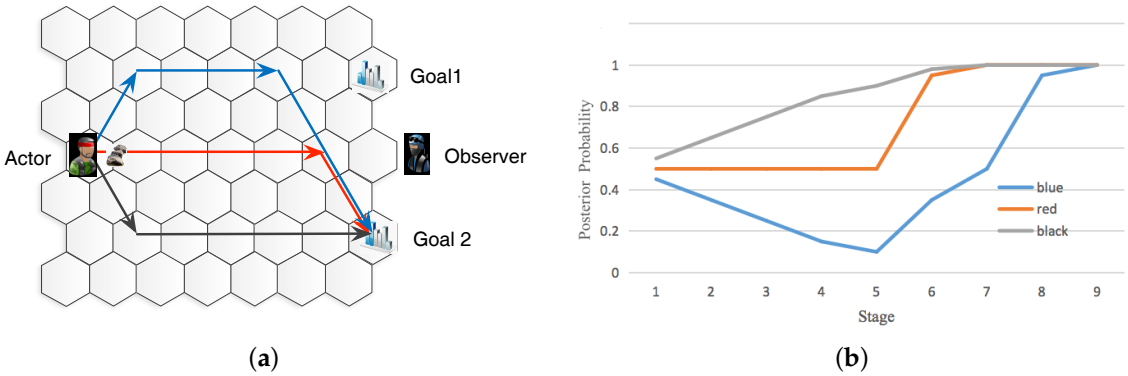
As shown in Figure 7, three paths of the actor under the observer's interdiction with a barrier before the start node s. The observer proactively interdicts to reduce the goal uncertainty and accelerate goal recognition. The actor attempts to minimize the privacy information leakage, so as to improve the goal uncertainty and hide the real goal.

We need to know the metric $\mathcal{I}_A(a)$ associated with the goal uncertainty, which is defined over actions available at each state and can be computed offline. The single observation based probabilistic goal recognition approach will not encounter online inconsistency.

3.2.2. Control and Threshold

Instead of individually analyze the accelerate and delay model, we may want to control the goal recognition process by adding additional path cost under bounded resource. Here, we mainly focus on

reformulating the GRC under network interdiction with bounded resource as one optimizing problem incorporating the metric $\mathcal{I}_A(a)$.



(**a**) (**b**)

Figure 7. (**a**) Three paths of the actor, (**b**) the observer's goal recognition results at every stage.

Definition 12 (InfoGRC). *The formulation of the action privacy information metric-based goal recognition control is defined as follows:*

$$[\text{InfoGRC}] \quad z^* = \max_{\mathbf{x}\in X} \min_{\mathrm{y}} \sum_{a\in\mathcal{E}} \frac{(c(a) + x(a)d(a)(1+\alpha\mathcal{I}_A(a)))\, y(a)}{1+\beta\mathcal{I}_A(a)} \tag{25}$$

$$s.t. \quad \sum_{a\in Out(i)} y(a) - \sum_{a\in In(i)} y(a) = \begin{cases} 1 & for\ i = s \\ 0 & \forall i \in \mathcal{N}\setminus\{s,g\} \\ -1 & for\ i = t \end{cases} \tag{26}$$

where $X = \left\{\mathbf{x} \in \{0,1\}^{|\mathcal{E}|} | \mathbf{r}^T\mathbf{x} \le R\right\}$ *with bounded resource* R, $x(a), y(a) \in \{0,1\}$ *indicate the observer's interdiction resource allocation and the actor's traverse path respectively,* α, β *are the controlling parameters of two opposite objectives. Equation (26) is the flow-balance constraint.*

Here, we define one variant InfoGRCT, a novel extension of the InfoGRC with threshold interdiction [61], in which the actor attempts to minimize the length of the metric $\mathcal{I}_A(a)$ added path cost, while the observer interdicts the path so that the path cost exceeds a specific threshold with least resource consumption. We designate this critical threshold as a trade-off between the maximum shortest path and resource consumption for the observer, which represents the longest shortest path cost that the actor will tolerate.

Definition 13 (InfoGRCT). *The formulation of the action privacy information metric based goal recognition control with a threshold is defined as follows:*

$$[\text{InfoGRCT}] \quad r^* = \min_{\mathbf{x}\in X} \sum_{a\in\mathcal{E}} x(a)r(a) \tag{27}$$

$$s.t. \quad \min_{\mathrm{x,y}} \sum_{a\in\mathcal{E}} \frac{(c(a) + x(a)d(a)(1+\alpha\mathcal{I}_A(a)))\, y(a)}{1+\beta\mathcal{I}_A(a)} \ge \tilde{\theta} \tag{28}$$

$$\sum_{a\in Out(i)} y(a) - \sum_{a\in In(i)} y(a) = \begin{cases} 1 & for\ i = s \\ 0 & \forall i \in \mathcal{N}\setminus\{s,g\} \\ -1 & for\ i = t \end{cases} \tag{29}$$

where $x(a), y(a) \in \{0,1\}$ *indicate the observer's interdiction resource allocation and the actor's traverse path respectively,* α, β *are the controlling parameters of two opposite objectives,* $\tilde{\theta}$ *is the threshold. Equation (29) is the flow-balance constraint.*

As illustrated in Figure 8a, one simple road graph network is composed of $|\mathcal{N}| = 11$ nodes and $|\mathcal{E}| = 21$ edges. Given that node S and node G_i as part of each path, we label the 18 paths, from S to G_1, as follows: $[S, \ldots, G_1] \triangleq [(A,D,F), (A,D,H), (A,D,I), (A,E,F), (A,E,H), (A,E,I), (B,D,F), (B,D,H), (B,D,I), (B,E,F), (B,E,H), (B,E,I), (C,D,F), (C,D,H), (C,D,I), (C,E,F), (C,E,H), (C,E,I)]$. We choose the path cost c_i for the i-th edge to be equal to $[c_1, c_2, \ldots, c_{21}] \triangleq [6, 3, 7, 4, 3, 3, 5, 4, 4, 6, 5, 5, 7, 3, 6, 6, 7, 4, 5, 5, 3]$. The three numbers in the tuple (c, d, r) represent the original path cost of the edge, added cost after interdiction and the resource required for edge interdiction, respectively. The actor has one fixed starting node S and two possible goals (G_1 and G_2). We link the actor's shortest path before and after the network interdiction using different lines with red arrows, and the interdicted edges are labeled with a red cross. Specifically, we assume that the observer has been assigned with a total of $R = 5$ units of resource to interdict, and the threshold for interdiction is $\tilde{\theta} = 20$.

The network interdiction solutions for the InfoGRC and InfoGRCT are shown in Figure 8. Taking the goal G_1 as an example, the actor would first traverse the optimal path $(S,B), (B,D), (D,H), (H,G_1)$ with a total length of 15. However, if the edge (H,G_1) is interdicted, the path cost of the original path would be added to 18, and then the other path $(S,B), (B,D), (D,I), (I,G_1)$ with a cost of 16 will be selected, as shown in Figure 8b. Similarly, if the actor takes G_2 as the real goal, as shown in Figure 8c, a new path $(S,B), (B,D), (D,I), (I,G_2)$ would be taken to replace the original $(S,B), (B,E), (E,H), (H,G_2)$ after the edge $(7,8)$ being interdicted. In this case, the path cost before and after network interdiction are 16 and 22 respectively, while the newly selected path after interdiction is 18. As shown in Figure 8d,e, considering the interdiction threshold, the optimal interdiction solution for G_1 is $(H,G_1), (I,G_1)$, and the solution for G_2 is $(H,G_2), (I,G_2)$.

3.3. Dual Reformulation

The InfoGRC and InfoGRCT can be transformed into bi-level optimization programming (BMIP) problems, in which the observer's interdiction resource allocation is transparent to the actor. Some algorithms cannot scale up to large road networks and are sensitive to network parameters, here we first propose to dual reformulate these problems. The matrix form of the InfoGRC problem is as follows:

$$[\text{InfoGRC-P}] \quad z^* = \max_{\mathbf{x} \in X} \min_{\mathbf{y}} \sum_{a \in \mathcal{E}} (\mathbf{c}' + \mathbf{M}\mathbf{x})^T \mathbf{y} \tag{30}$$

$$s.t. \quad \mathbf{K}^T \mathbf{y} = \mathbf{b}, \quad \mathbf{y} \geq \mathbf{0}, \tag{31}$$

where $c'_a = c_a / (1 + \beta \mathcal{I}_{AI}(a))$ is the additional action cost, $\mathbf{M} = \text{diag}\left(m_1, \cdots, m_{|\mathcal{E}|}\right)$, $\mathbf{b} = (1, 0, \cdots, 0, -1)$, $m_a = d(a)(1 + \alpha \mathcal{I}_A(a)) / (1 + \beta \mathcal{I}_A(a))$, $\mathbf{K}$ is the network matrix. Equation (31) is the vector-form flow-balance constraint.

Fixing the outer variable x, we can take the dual of the inner minimization using KKT conditions, then the dual reformulation of the InfoGRC is as follows:

$$[\text{InfoGRC-D}] \quad z^* = \max_{\mathbf{x} \in X, \vec{\pi}} \mathbf{b}^T \vec{\pi} \tag{32}$$

$$s.t. \quad \mathbf{K}^T \vec{\pi} = \mathbf{c}' + \mathbf{M}\mathbf{x}, \quad \pi_s = 0, \tag{33}$$

where $X = \left\{ \mathbf{x} \in \{0,1\}^{|\mathcal{E}|} | \mathbf{r}^T \mathbf{x} \leq R \right\}$ with bounded resource R, $\vec{\pi}$ is the dual variables. Hence, the dual problem can be solved by a standard branch-and-bound algorithm.

The matrix form and the dual reformulation of the InfoGRCT problem are as follows:

$$[\text{InfoGRCT-P}] \quad r^* = \min_{\mathbf{x} \in X} \mathbf{r}^T \mathbf{x} \tag{34}$$

$$s.t. \quad \mathbf{c}'^{T}\mathbf{y} + \mathbf{x}^{T}\mathbf{M}\mathbf{y} \geq \tilde{\theta} \quad \forall \mathbf{y} \in Y \tag{35}$$

$$\begin{aligned} \mathbf{K}^{T}\mathbf{y} &= \mathbf{b} \\ \mathbf{y} &\geq \mathbf{0}. \end{aligned} \tag{36}$$

$$[\text{InfoGRCT-D}] \quad r^{*} = \min_{\mathbf{x} \in X} \mathbf{r}^{T}\mathbf{x} \tag{37}$$

$$s.t. \quad \mathbf{A}\vec{\pi} \geq \tilde{\theta} \tag{38}$$

$$\begin{aligned} \mathbf{B}^{T}\vec{\pi} + \mathbf{M}^{T}\mathbf{x} &\geq -\mathbf{c} \\ \mathbf{x} &\geq \mathbf{0}, \end{aligned} \tag{39}$$

where $\tilde{\theta}$ is the threshold, $\mathbf{A} = [-1, 0, \ldots, 0, 1]_{1 \times m}$, and $\mathbf{B}_{|\mathcal{N}| \times |\mathcal{E}|} = (b_{ik})$ is the node-edge incidence matrix.

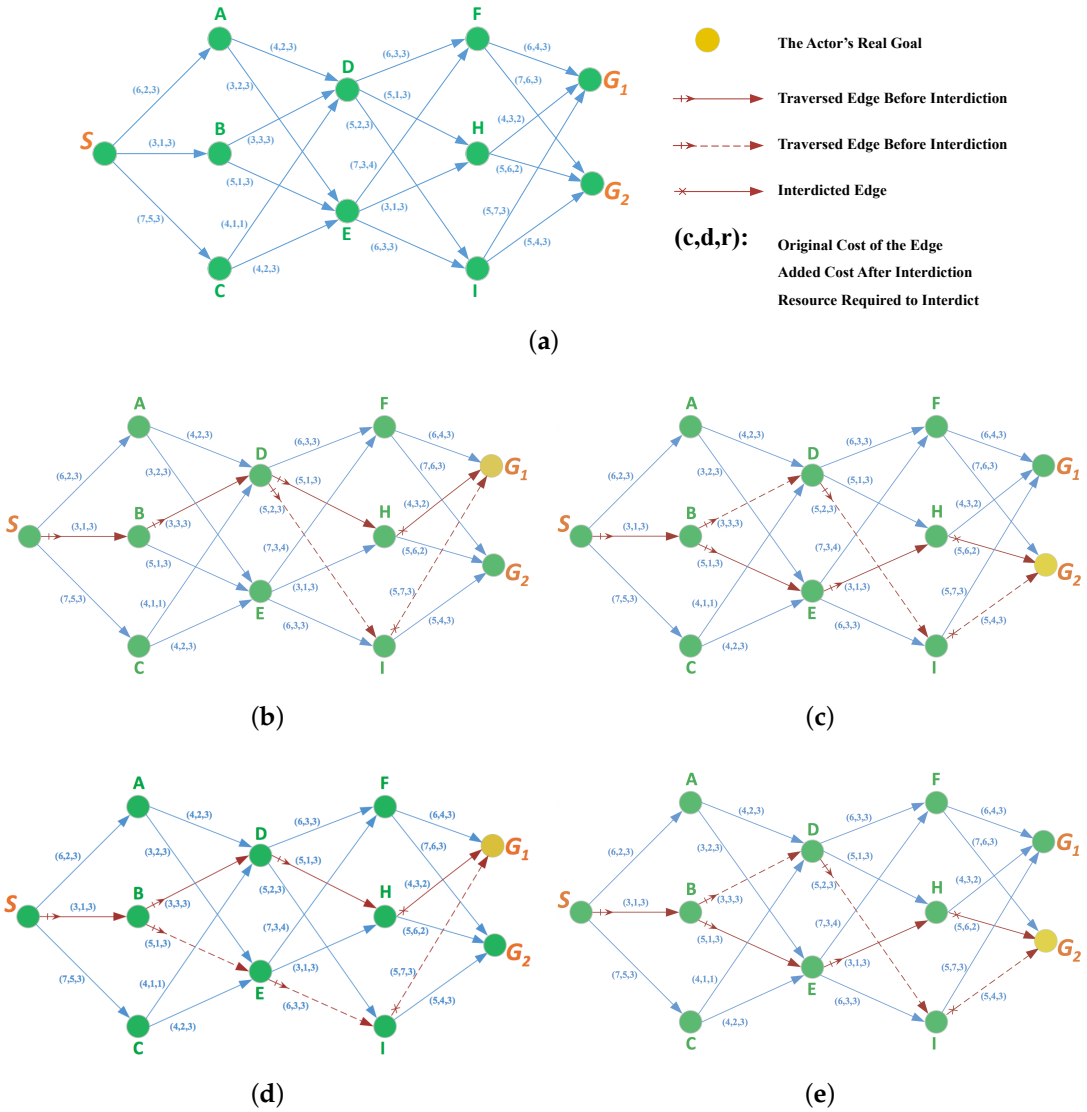


Figure 8. The network interdiction solutions for information metric based goal recognition control (GRC) under network interdiction (InfoGRC) and information metric based GRC under threshold network interdiction (InfoGRCT) on the 11 nodes graph network. (**a**) The road graph network with 11 nodes. (**b**) Interdiction for G_1. (**c**) Interdiction for G_2. (**d**) Interdiction for G_1 with the threshold. (**e**) Interdiction for G_2 with the threshold.

We will adopt a Benders decomposition based constraint generation approach [62]. The framework is depicted in Figure 9. The higher-level is the interdiction resource allocation problem for the observer, while the lower-level is the generative cost-optimal path-planning for the actor.

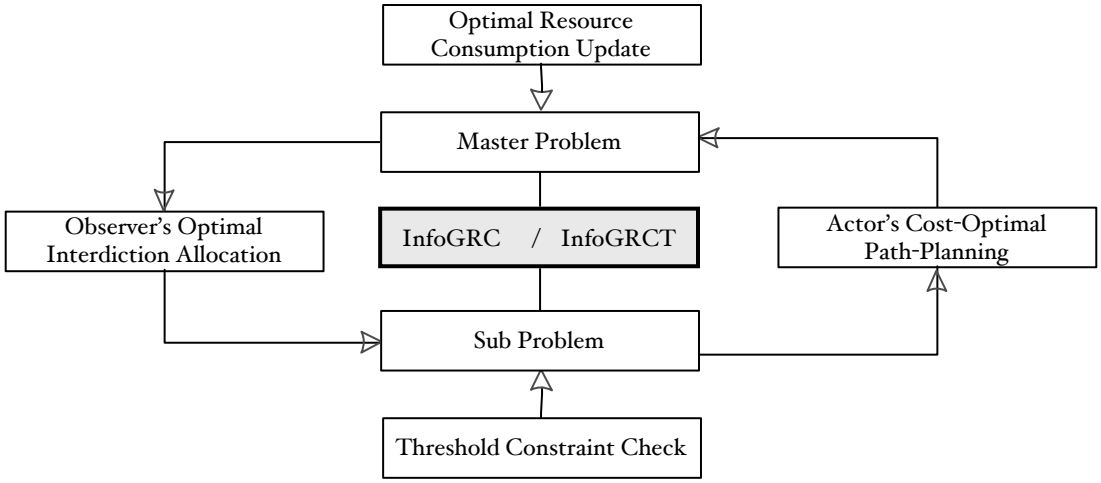


Figure 9. The Benders decomposition based problem-solving framework.

Benders decomposition is an efficient approach to solve large-scale optimization problems. The main idea is to separate the mixed decision variables into two-stage variables and generate two relatively independent problems denoted as the Master problem and the Subproblem respectively. Then we alternately solve the problems and iteratively update the results until a convergence condition is satisfied. Here, the InfoGRC and InfoGRCT can be reformulated to $[\text{Master}(\hat{Y})] - [\text{Sub}(\hat{x})]$ problems as follows:

$$[\text{InfoGRC-Master}] \quad z^* = \max_{\mathbf{x} \in X} z \tag{40}$$

$$s.t. \quad z \leq \mathbf{c'}^T \hat{y} + \mathbf{x}^T \mathbf{M} \hat{y} \quad \forall \hat{y} \in \hat{Y} \tag{41}$$

$$[\text{InfoGRC-Sub}(\hat{x})] \quad z_{\hat{x}} = \min_{y} \sum_{a \in \mathcal{E}} \left(c(a) + \hat{x}(a) d(a) \right) y(a) \tag{42}$$

$$\begin{aligned} s.t. \quad & \mathbf{K}^T \mathbf{y} = \mathbf{b} \\ & x(a) \in \{0,1\} \quad \forall a \in \mathcal{E} \end{aligned} \tag{43}$$

$$[\text{InfoGRCT-Master}(\hat{Y})] \quad r_{\hat{Y}} = \min_{x} \mathbf{r}^T \mathbf{x} \tag{44}$$

$$\begin{aligned} s.t. \quad & \mathbf{c'}^T \hat{y} + \mathbf{x}^T \mathbf{M} \hat{y} \geq \tilde{\theta} \quad \forall \hat{y} \in \hat{Y} \\ & x(a) \in \{0,1\} \quad \forall a \in \mathcal{E} \end{aligned} \tag{45}$$

$$[\text{InfoGRCT-Sub}(\hat{x})] \quad d_{\hat{x}} = \min_{\mathbf{y}} \sum_{a \in \mathcal{E}} \left(c(a) + \hat{x}(a) d(a) \right) y(a) \tag{46}$$

$$\begin{aligned} s.t. \quad & \mathbf{K}^T \mathbf{y} = \mathbf{b} \\ & x(a) \in \{0,1\} \quad \forall a \in \mathcal{E} \end{aligned} \tag{47}$$

where $\mathbf{Y}$ denotes the set of all simple $s-g$ paths, $\hat{y}$ (temporary optimal actor path in $[\text{Master}(\hat{Y})]$) and $\hat{x}$ (temporary observer's interdiction plan in $[\text{Sub}(\hat{x})]$) are fixed and known in their respective solutions. The basic Benders decomposition algorithm for InfoGRCT can be found in [63], and the Benders decomposition based problem-solving algorithm for InfoGRCT is proposed in Algorithm 1.

Algorithm 1 The Benders decomposition based problem-solving algorithm for InfoGRCT

Input: An instance of InfoGRCT.
Output: An optimal observer's interdiction plan for goal recognition
1: $\hat{x} \leftarrow \mathbf{1}$, solve $[\mathrm{Sub}(\hat{x})]$ to obtain the $\bar{\theta}$;
2: **while** $\tilde{\theta} \leq \bar{\theta}$ **do**
3: $\quad \hat{X}\hat{Y} \leftarrow \emptyset, \hat{x} \leftarrow 0$
4: $\quad$ **repeat**: solve $[\mathrm{Sub}(\hat{x})]$ to obtain $\hat{y}$ and θ;
5: $\quad\quad \hat{X}\hat{Y} \leftarrow \hat{X}\hat{Y} \cup (\hat{x}, \hat{y})$;
6: $\quad\quad$ solve $[\mathrm{Master}(\hat{y})]$ for $\hat{x}$ and $r_{\hat{y}}$;
7: $\quad$ **until** $\theta \geq \tilde{\theta}$
8: $\quad x^* \leftarrow \hat{x}, r^* = r_{\hat{y}}$
9: **end while**
10: **Return** x^*, r^*

4. Experiments

Experiments were conducted on synthetic path datasets upon two small artificially generated network and one real-world road network. Here, we assume the actor to be rational, which means the path datasets will contain some sub-optimal paths but without some loopy or zigzagging paths. We first evaluate the effectiveness and then compare the performance under different interdiction.

4.1. Experimental Setup

The experimental programs are coded with python, the experiments are run on one MacbookPro that runs macOS Sierra 10.12.6 with 4 CPU and 8 GB RAM. The InfoGRC/InfoGRCT have been reformulated as bi-level mixed-integer programming (BLMIP) problems and solved using the MIP solvers (Gurobi and MiniZinc). We simply set $\alpha = \beta = 1$, more details will be introduced below.

As for goal recognition, early prediction, precision and recall, are properties required. We use F-*measure* as the accuracy metric [4]. F-*measure* is an integration of precision and recall, where precision is used to scale the reliability of the recognized results and recall is used to scale the efficiency of the algorithm applied. They are computed as follows:

$$\text{F-}measure = \frac{2 \cdot precision \cdot recall}{precision + recall} \tag{48}$$

$$precision = \frac{1}{N_G} \sum_{i=1}^{N_G} \frac{TP_i}{TI_i} \tag{49}$$

$$recall = \frac{1}{N_G} \sum_{i=1}^{N_G} \frac{TP_i}{TT_i} \tag{50}$$

where N_G is the number of possible goals, TP_i, TI_i and TT_i are the true positives, total of true labels, and the total of inferred labels for class i respectively. The value of F-*measure* will be between 0 and 1, and a higher value means better performance.

As for early prediction, if the goal recognition model converged (the final prediction was correct), the convergence point metric [4] represents the point where the following predictions are correct, which can be defined as follow:

$$N_{CP} \in \mathcal{N} \tag{51}$$

$$s.t. \quad \mathcal{P}_{po}(g_r | \mathcal{O}_{N_{CP}}) \geq \gamma \tag{52}$$

where N_{CP} denoted the convergence point at which the posterior of the actor's real goal will not be less than γ, here we set $\gamma = 0.8$.

We may want to compare the relative early prediction ability between two goal recognition models given the path that contains the real goal:

$$R_{EP} = \frac{|N_{CP}^1 - N_{CP}^2|}{PS = |\langle s_0, \ldots N_i \ldots g_r \rangle|} \tag{53}$$

where R_{EP} represents the relative early prediction ability, PS is the path steps from the start node to the real goal.

As for network interdiction, we employ the path interdiction efficiency for evaluation [35], which is defined as follows:

$$e = \delta L / \mathbf{d}^T \mathbf{x}, \tag{54}$$

where δL is the increased path cost for the actor after interdiction and $\mathbf{d}^T \mathbf{x}$ is the total path cost increment in the network.

4.2. Experimental Scenarios

Different network topologies may indicate different application domains and greatly affect the efficiency of the InfoGRC and InfoGRCT. We adopt two small artificially generated networks to verify the feasibility, as shown in Figures 10 and 11, and then adopt one real-world road network to further verify the scalability, see Figure 12 for detail.

Hexagon grid network: We employ one 7×7 hexagonal discrete grid with 7 rows and 7 columns. Since the hexagonal discrete grid owns great symmetrical properties and is widely used in simulation systems to represent the environment. The hexagonal grid on Offset coordinate is shown in Figure 10, the start node is $(0,3)$, and the goal nodes are $(6,1)$ and $(6,5)$. The actor has one fixed starting node S and two possible goals (G_1 and G_2). The path cost between nodes $c(a)$, the interdiction increment $d(a)$, and resource consumption $r(a)$ are generated to be uniform distribution on $[1,10]$, $[1,10]$, $[1,10]$, respectively.

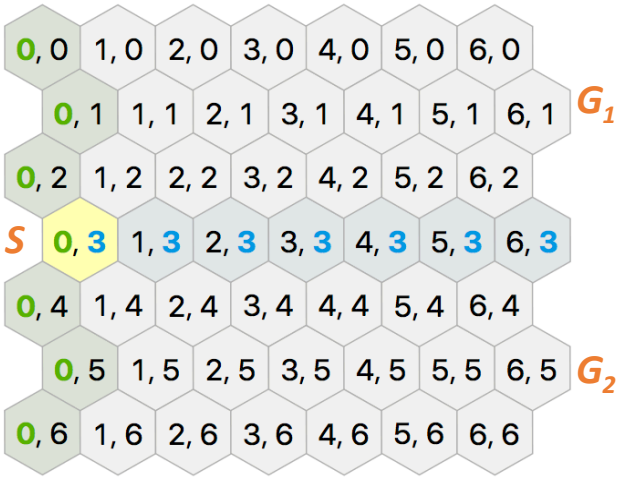


Figure 10. One 7×7 hexagonal grid on offset coordinate.

Random Graph Network: We employ the Erdős–Rényi model [64] to generate one random graph network, which is composed of $|\mathcal{N}| = 30$ nodes and $|\mathcal{E}| = 60$ edges, and the edges are added uniformly randomly. As shown in Figure 11, the actor has one fixed starting node S and two possible goals (G_1 and G_2). The path cost between nodes $c(a)$ is generated to be uniform distribution on $[1,10]$, the interdiction increment $d(a)$, and resource consumption $r(a)$ is linearly proportional to the node degree.

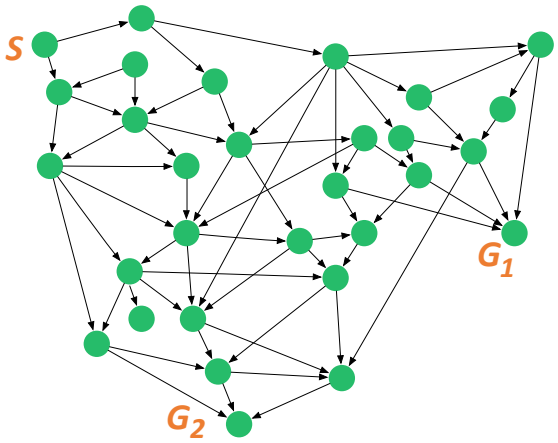


Figure 11. One random network with 30 nodes generated based on the Erdős–Rényi model.

Real-world road network: As shown in Figure 12, it is the real-world Chicago Sketch road network [65], which contains 933 nodes and 2950 edges. Here, the network is assumed to be undirected, the node indexes of the start and possible goals are $\{368\}$ and $\{377, 597, 575\}$, respectively. The cost of each edge $c(a)$ is an approximate integer of the real distance between two nodes, the interdiction increment $d(a)$ and resource consumption $r(a)$ are linearly proportional to the node degrees. A dataset consists of 50 labeled paths for each goal is generated with about 20 steps without goal switch during the midway. Each path is separated into 10 stages so as to evaluate paths with different steps.

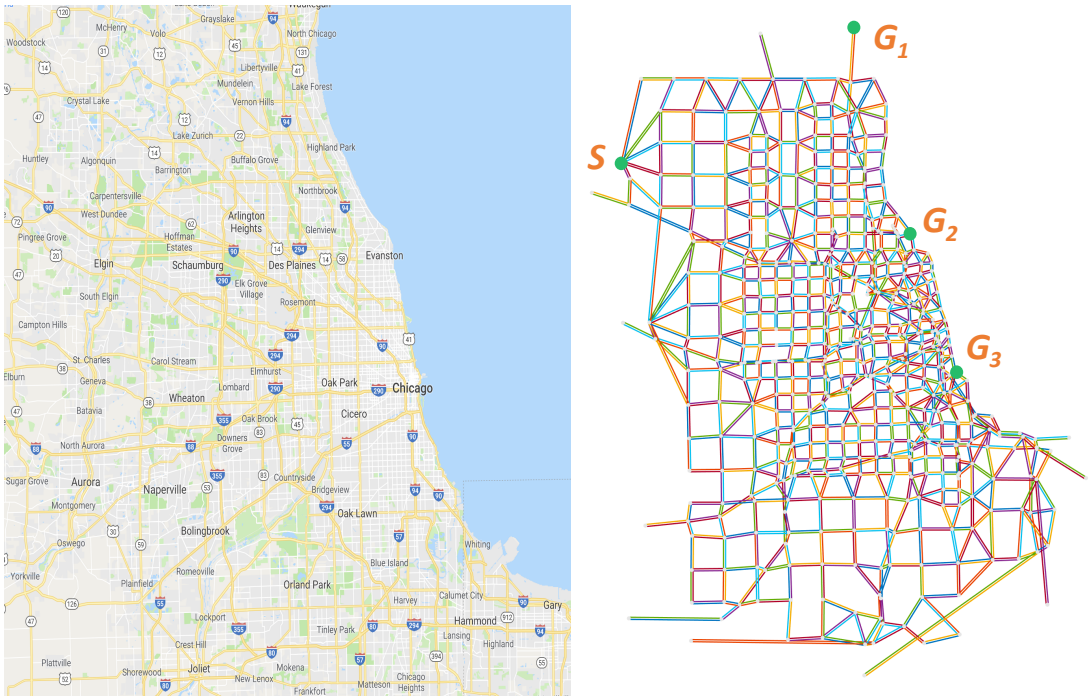


Figure 12. The Chicago Sketch road network. (**a**) The real-world Chicago Scketch road map from Google. (**b**) The real-world Chicago Scketch road network.

4.3. Goal Recognition Control under Network Interdiction

As for goal recognition, experimental evaluations are performed on four models, the "normal" without metric, "delay" and "accelerate" with metric, and the "control" model (InfoGRC). The actor

has one start state and two or three predefined possible goals, which are selected with equal probability at the beginning. If the actor reaches its goal, then the goal is achieved, otherwise, the probabilistic goal recognition module will generate goal distribution over goals. In the following test, we will statistically evaluate different goal recognition models with the metric F-*measure*, and R_{EP}, which are widely used to measure the performance of different goal recognition models. As shown in Figure 13, the statistical performance of different models for the three scenarios is measured by the F-*measure* value.

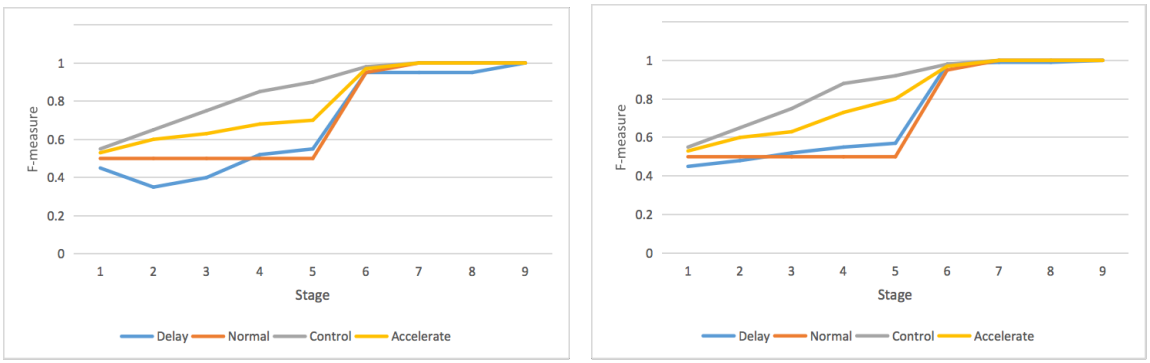
The actor's actions involve privacy information, which are tightly associated with the goal uncertainty and indeed seriously hinder the goal recognition of the observer. After incorporating the action privacy information metric, the F-*measure* values of the "Accelerate" model were greater than the "normal" and "delay" model, while the "delay" model performs poor compared to the "normal" model. The big gap of the F-*measure* values between the "accelerate" model and the "delay" model showed that the actor's actions are tightly associated with the goal uncertainty, the action privacy information metric $\mathcal{I}_A(a)$ could be employed by the observer during the goal recognition process. As for the "control" model, the values of F-*measure* under network interdiction were usually higher compared with the "normal", "accelerate", and "delay" model, which proves that the control model with $\mathcal{I}_A(a)$ metric assisted could be employed to control the goal recognition process.

Here, using the total 150 paths for the Chicago Sketch road network scenario, we compute the "relative early prediction" ability of the "normal" model and "dontrol" model on three different goals. As shown in Figure 14, there are still 54 paths whose R_EP is 0, when the actor traverse over these paths, no privacy information about the goal will be leaked. So, even if the actor could manipulate the asymmetric information about their action-goal, but there are still paths that possess little goal uncertainty.

After evaluating the performance of our models in goal recognition, here, we compared the network interdiction efficiency of InfoGRC and InfoGRCT under different network interdiction. As shown in Table 2, the expectation of the e are almost more than 50%, the values of the Chicago Sketch road network scenario are almost 80%. This demonstrates the average impact of InfoGRC and InfoGRCT model in network interdiction.

Table 2. The expectation of network interdiction efficiency on the three scenarios for each goal.

$E(e)$ (%)	Scenario 1	Scenario 2	Scenario 3
InfoGRC	65.4/63.7	62.7/78.4	88.7/77.5/90.8
InfoGRCT	65.1/63.3	62.1/78.1	88.2/77.2/90.4



(**a**) (**b**)

Figure 13. *Cont.*

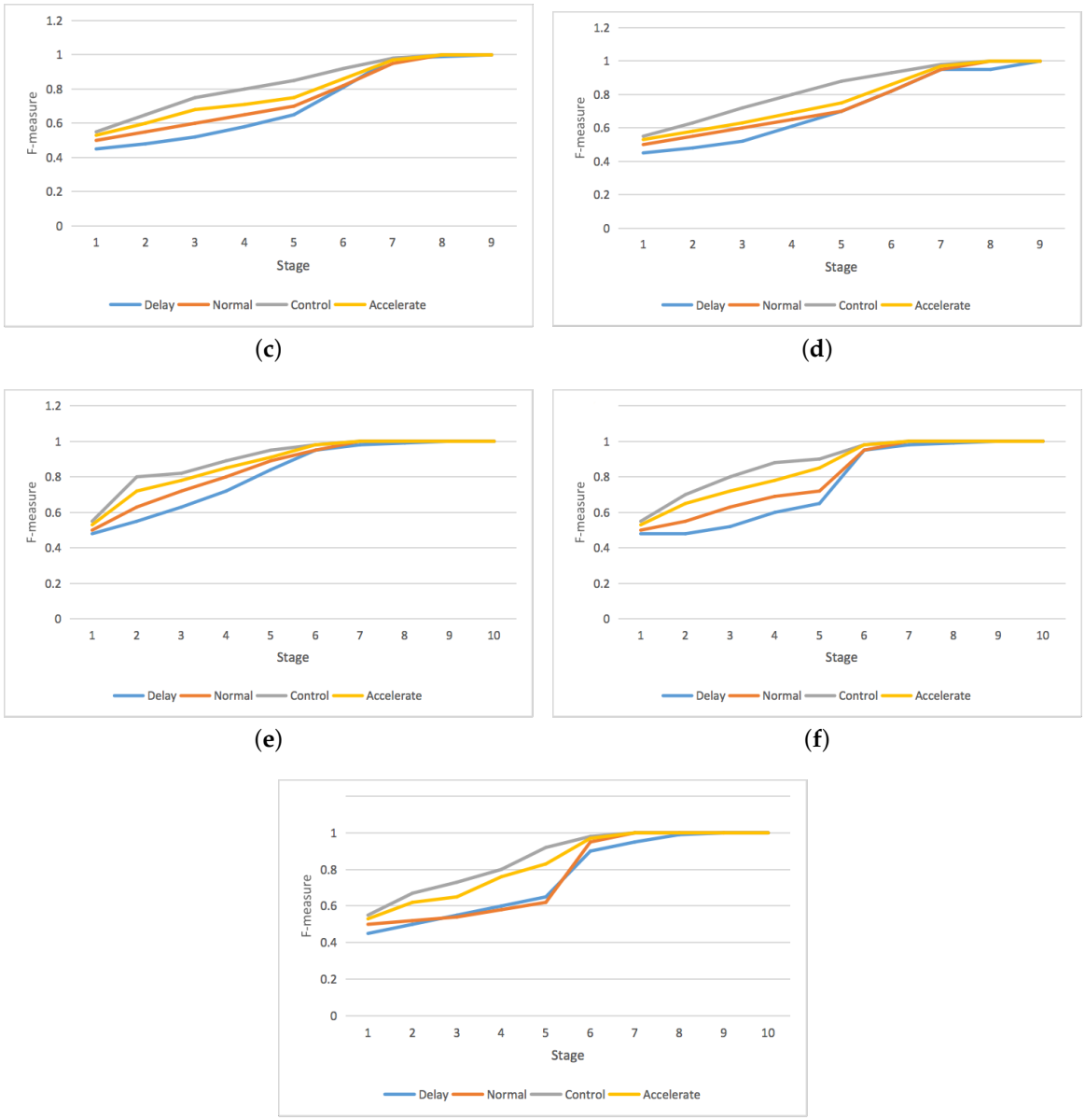


Figure 13. The statistical performance of different models for goal recognition on two synthetic road networks with two goals (G_1,G_2), and one real-world road network with three goals (G_1, G_2, G_3). (**a**) F-*measure* for goal 1 on the hexagonal grid. (**b**) F-*measure* for goal 2 on the hexagonal grid. (**c**) F-*measure* for goal 1 on the random graph network. (**d**) F-*measure* for goal 2 on the random graph network. (**e**) F-*measure* for goal 1 on the Chicago Sketch road network. (**f**) F-*measure* for goal 2 on the Chicago Sketch road network. (**g**) F-*measure* for goal 3 on the Chicago Sketch road network.

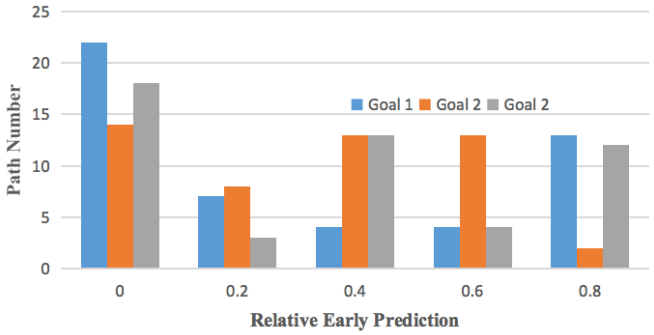


Figure 14. Relative early prediction (R_{EP}) of the "Normal" and "Control" model on the Chicago Sketch road network scenario with three goals.

5. Conclusions and Future Work

Goal recognition is vital in the defense and security domain, such as in CIP. Goals of the attacker are in need of timely recognized and the actions of the attacker should be restricted. In this paper, from the perspective of explainable agent behavior, we first adopt a privacy information metric to quantify the privacy information leakage of the actions taken by the actor, since these actions are tightly associated with the goal uncertainty. Then, we defined two different interdiction models (InfoGRC and InfoGRCT) to control the goal recognition process. Experimental results demonstrate the effectiveness of our models in the fully observable and deterministic environment with multiple goals. These models above provide one paradigm, from generative path planning, probabilistic goal recognition to proactively response interdiction resource allocation, which is simple but inspiring for decision-making (such as offline proactive planning, threat analysis) in the defense and security domain. Also, considering the dual use of these models, we could attempt to do inverse privacy-preserving path planning. Goal recognition control under network interdiction with bounded resource may be a suitable and soft method to facilitate goal recognition offline compared to the goal recognition design with the hard environment redesign.

However, it is noteworthy that our work is suggestive but still simple, the applicability of our models under network interdiction still face many challenges. As for the goal recognition, partial observable environment, noisy observation, adversarial goal recognition, and online recognition are very realistic need. As for the action model, durative action, midway goal change, deceptive action, active attacker, multiple attacker, higher dimensionality, and bounded rationality drive us to develop more robust opponent modeling methods. As for the interdiction model, nodal interdiction, threshold sensitivity, network resilience are still worthy of further study. As for the metric model, deceptive action metric and goal-related mutual information metric inspire us to design learning based goal recognition model. All of these are still open in our future work.

As a continuation of this work, allocating interdiction resource can be modeled as one dynamic process assisted with online goal recognition. In the future, we will attempt to use a stochastic game-theoretic framework to model the attacker-defender interaction in the partial observable environment, where the attacker would perform active deceptive actions or irrational actions to mislead the goal recognition process of the observer.

Author Contributions: J.L. and W.Z. proposed, designed the method; J.L. and X.J. performed the experiment; W.G. and S.C. participated in the experiment and analyzed the data; J.L. and X.J. wrote the paper; J.L. revised the paper; W.Z. supervised the overall process.

Funding: This work is partially sponsored by the National Natural Science Foundation of China under Grants No. 61702528, No. 61806212.

Conflicts of Interest: The authors declare that there is no conflict of interests regarding the publication of this paper.

Abbreviations

The following abbreviations are used in this manuscript:

GR	Goal recognition
GRD	Goal recognition design
GRC	Goal recognition control
CIP	Critical infrastructure protection
PAIR	Plan activity and intent recognition
HAIP	Human–AI planning
XAIP	Explainable planning
HMI	Human–machine interaction
COA	Course Of action
HTN	Hierarchical task network
BLMIP	Bi-level mixed-integer programming
wcd	worst-case distinctiveness
MXFI	Maximum-flow network interdiction
SPNI	Shortest path network interdiction
MXSP	Maximizing the shortest path
KKT	Karush–Kuhn–Tucker

References

1. Sadri, F. Logic-based approaches to intention recognition. In *Handbook of Research on Ambient Intelligence and Smart Environments: Trends and Perspectives*; IGI Global: Hershey, PA, USA, 2011; pp. 346–375.
2. Aha, D.W. Goal reasoning: Foundations, emerging applications, and prospects. *AI Mag.* **2018**, *39*, 3–24. [CrossRef]
3. Keren, S.; Gal, A.; Karpas, E. Goal recognition design. In Proceedings of the Twenty-Fourth International Conference on Automated Planning and Scheduling, Portsmouth, NH, USA, 21–26 June 2014.
4. Sukthankar, G.; Geib, C.; Bui, H.H.; Pynadath, D.; Goldman, R.P. *Plan, Activity, and Intent Recognition: Theory and Practice*; Newnes: Burlington MA, USA, 2014.
5. Chakraborti, T.; Kambhampati, S.; Scheutz, M.; Zhang, Y. AI challenges in human-robot cognitive teaming. *arXiv* **2017**, arXiv:1707.04775.
6. Albrecht, S.V.; Stone, P. Autonomous agents modelling other agents: A comprehensive survey and open problems. *Artif. Intell.* **2018**, *258*, 66–95. [CrossRef]
7. Le Guillarme, N. A Game-Theoretic Planning Framework for Intentional Threat Assessment. Ph.D. Thesis, Université de Caen, Caen, France, 2016.
8. Heinze, C. *Modelling Intention Recognition for Intelligent Agent Systems*; Technical Report; Defence Science and Technology Organisation Salisbury (AUSTRALIA): Melbourne, Australia, 2004.
9. Chakraborti, T.; Sreedharan, S.; Grover, S.; Kambhampati, S. Plan explanations as model reconciliation. In Proceedings of the 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI), Daegu, Korea, 11–14 March 2019; pp. 258–266.
10. Fox, M.; Long, D.; Magazzeni, D. Explainable planning. *arXiv* **2017**, arXiv:1709.10256.
11. Bayrak, H.; Bailey, M.D. Shortest path network interdiction with asymmetric information. *Networks* **2010**, *52*, 133–140. [CrossRef]
12. Vijay, G.; Justin, G.; Jeremy, K.; Albert, R.; Hayley, R.; Siddharth, S.; Jonathan, S.; David, M. AI Enabling Technologies: A Survey. *arXiv* **2019**, arXiv:1905.03592v1.
13. Hellström, T.; Bensch, S. Understandable robots-what, why, and how. *Paladyn J. Behav. Robot.* **2018**, *9*, 110–123. [CrossRef]
14. Štolba, M.; Tožička, J.; Komenda, A. Quantifying privacy leakage in multi-agent planning. *ACM Trans. Internet Technol.* **2018**, *18*, 28. [CrossRef]
15. Lichtenthäler, C.; Lorenzy, T.; Kirsch, A. Influence of legibility on perceived safety in a virtual human-robot path crossing task. In Proceedings of the IEEE RO-MAN: The 21st IEEE International Symposium on Robot and Human Interactive Communication, Paris, France, 9–13 September 2012; pp. 676–681.

16. Dragan, A.D.; Lee, K.C.; Srinivasa, S.S. Legibility and predictability of robot motion. In Proceedings of the 8th ACM/IEEE International Conference on Human-Robot Interaction, Tokyo, Japan, 3–6 March 2013; pp. 301–308.
17. Wortham, R.H.; Theodorou, A. Robot transparency, trust and utility. *Connect. Sci.* **2017**, *29*, 242–248. [CrossRef]
18. Chakraborti, T.; Kulkarni, A.; Sreedharan, S.; Smith, D.E.; Kambhampati, S. Explicability? legibility? predictability? transparency? privacy? security? The emerging landscape of interpretable agent behavior. *arXiv* **2019**, arXiv:1811.09722.
19. Rosenfeld, A.; Richardson, A. Explainability in human-agent systems. *Auton. Agents Multi-Agent Syst.* **2019**. [CrossRef]
20. Gong, Z.; Zhang, Y. Behavior Explanation as Intention Signaling in Human-Robot Teaming. In Proceedings of the 27th IEEE International Symposium on Robot and Human Interactive Communication, Nanjing and Tai'an, China, 27 August–1 September 2018; pp. 1005–1011.
21. Rowe, N.C.; Andrade, S.F. Counterplanning for Multi-Agent Plans Using Stochastic Means-Ends Analysis. In Proceedings of the 2002 IASTED IASTED Artificial Intelligence and Applications Conference, Malaga, Spain, 9–12 September 2002.
22. Pozanco, A.; E-Martín, Y.; Fernandez, S.; Borrajo, D. Counterplanning using Goal Recognition and Landmarks. In Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18), Stockholm, Sweden, 13–19 July 2018; pp. 4808–4814.
23. Masters, P.; Sardina, S. Deceptive Path-Planning. In Proceedings of the Twenty-sixth International Joint Conference on Artificial Intelligence, Melbourne, Australia, 19–25 August 2017.
24. Sarah, K.; Avigdor, G.; Karpas, E. Privacy Preserving Plans in Partially Observable Environments. In Proceedings of the Twenty-five International Joint Conference on Artificial Intelligence, New York, NY, USA, 9–15 July 2016.
25. Leaute, T.; Faltings, B. Protecting privacy through distributed computation in multi-agent decision making. *J. Artif. Intell. Res.* **2013**, *47*, 649–695. [CrossRef]
26. Wu, F.; Zilberstein, S.; Chen, X. Privacy-Preserving Policy Iteration for Decentralized POMDPs. In Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, LA, USA, 2–7 February 2018.
27. Wen, Y.; Yang, Y.; Luo, R.; Wang, J.; Pan, W. Probabilistic recursive reasoning for multi-agent reinforcement learning. *arXiv* **2019**, arXiv:1901.09207.
28. Štolba, M. Reveal or Hide: Information Sharing in Multi-Agent Planning. Ph.D. Thesis, Czech Technical University in Prague, Prague, Czech Republic, 2017.
29. Strouse, D.; Kleiman-Weiner, M.; Tenenbaum, J.; Botvinick, M.; Schwab, D. Learning to Share and Hide Intentions using Information Regularization. *arXiv* **2018**, arXiv:1808.02093.
30. Strouse, D. Optimization of Mutual Information in Learning: Explorations in Science. Ph.D. Thesis, Princeton University, Princeton, NJ, USA, 2018.
31. Wray, K.H.; Kumar, A.; Zilberstein, S. Integrated cooperation and competition in multi-agent decision-making. In Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, LA, USA, 2–7 February 2018.
32. Sanjab, A.; Saad, W.; Başar, T. Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6. [CrossRef]
33. Hota, A.R.; Sundaram, S. Interdependent security games on networks under behavioral probability weighting. *IEEE Trans. Control Netw. Syst.* **2016**, *5*, 262–273. [CrossRef]
34. Tsitsiklis, J.N.; Xu, K. Delay-predictability trade-offs in reaching a secret goal. *Oper. Res.* **2018**, *66*, 587–596. [CrossRef]
35. Xu, K.; Yin, Q.; Qi, Z. A New Metric and Method for Goal Identification Control. In Proceedings of the IJCAI Workshop on Goal Reasoning, Stockholm, Sweden, 13–19 July 2018; pp. 13–18.
36. Smith, J.C.; Song, Y. A Survey of Network Interdiction Models and Algorithms. *Eur. J. Oper. Res.* **2019**. [CrossRef]
37. Dahan, M.; Amin, S. Security Games in Network Flow Problems. *arXiv* **2016**, arXiv:1601.07216.

38. Smith, J.C.; Lim, C. Algorithms for network interdiction and fortification games. In *Pareto Optimality, Game Theory and Equilibria*; Springer Optimization and Its Applications; Springer: Berlin/Heidelberg, Germany, 2008, doi:10.1007/978-0-387-77247-9_24.
39. Kennedy, K.T.; Deckro, R.F.; Moore, J.T.; Hopkinson, K.M. Nodal interdiction. *Math. Comput. Model.* **2011**. [CrossRef]
40. Xiao, K.; Zhu, C.; Zhang, W.; Wei, X.; Hu, S. Stackelberg network interdiction game: Nodal model and algorithm. In Proceedings of the 2014 5th International Conference on Game Theory for Networks, GameNets 2014, Beijing, China, 25–27 November 2014. [CrossRef]
41. Avrahami-Zilberbrand, D.; Kaminka, G.A. Incorporating observer biases in keyhole plan recognition (efficiently!). In Proceedings of the Twenty-First AAAI Conference on Artificial Intelligence, Boston, MA, USA, 16–20 July 2006; Volume 7, pp. 944–949.
42. Cohen, P.R.; Perrault, C.R.; Allen, J.F. Beyond question answering. *Strateg. Nat. Lang. Process.* **1981**, *245274*.
43. Mirsky, R.; Gal, K.; Stern, R.; Kalech, M. Goal and Plan Recognition Design for Plan Libraries. *ACM Trans. Intell. Syst. Technol.* **2019**, *10*, 14. [CrossRef]
44. Ramírez, M.; Geffner, H. Plan recognition as planning. In Proceedings of the Twenty-First International Joint Conference on Artificial Intelligence, Pasadena, CA, USA, 14–17 July 2009.
45. Zeng, Y.; Xu, K.; Yin, Q.; Qin, L.; Zha, Y.; Yeoh, W. Inverse Reinforcement Learning Based Human Behavior Modeling for Goal Recognition in Dynamic Local Network Interdiction. In Proceedings of the Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, LA, USA, 2–7 February 2018.
46. Masters, P.; Sardina, S. Cost-Based Goal Recognition in Navigational Domains. *J. Artif. Intell. Res.* **2019**, *64*, 197–242. [CrossRef]
47. Wayllace, C.; Hou, P.; Yeoh, W. New Metrics and Algorithms for Stochastic Goal Recognition Design Problems. In Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, Melbourne, Australia, 19–25 August 2017; pp. 4455–4462.
48. Wayllace, C.; Hou, P.; Yeoh, W.; Son, T.C. Goal recognition design with stochastic agent action outcomes. In Proceedings of the IJCAI International Joint Conference on Artificial Intelligence, New York, NY, USA, 9–15 July 2016.
49. Kulkarni, A.; Klenk, M.; Rane, S.; Soroush, H. Resource Bounded Secure Goal Obfuscation. In Proceedings of the AAAI Fall Symposium on Integrating Planning, Diagnosis and Causal Reasoning, Arlington, VA, USA, 18–20 October 2018.
50. Braynov, S. Adversarial planning and plan recognition: Two sides of the same coin. In Proceedings of the Secure Knowledge Management Workshop, Brooklyn, NY, USA, 28–29 September 2006.
51. Wayllace, C.; Keren, S.; Yeoh, W.; Gal, A.; Karpas, E. Accounting for Partial Observability in Stochastic Goal Recognition Design: Messing with the Marauder's Map. In Proceedings of the 10th Workshop on Heuristics and Search for Domain-Independent Planning (HSDIP), Delft, The Netherlands, 26 June 2018; p. 33.
52. Ang, S.; Chan, H.; Jiang, A.X.; Yeoh, W. Game-theoretic goal recognition models with applications to security domains. In Proceedings of the International Conference on Decision and Game Theory for Security, Vienna, Austria, 23–25 October 2017; pp. 256–272.
53. Keren, S.; Pineda, L.; Gal, A.; Karpas, E.; Zilberstein, S. Equi-reward utility maximizing design in stochastic environments. In Proceedings of the HSDIP 2017, Pittsburgh, PA, USA, 20 June 2017; p. 19.
54. Shen, M.; How, J.P. Active Perception in Adversarial Scenarios using Maximum Entropy Deep Reinforcement Learning. *arXiv* **2019**, arXiv:1902.05644 .
55. Zenklusen, R. Network flow interdiction on planar graphs. *Discret. Appl. Math.* **2010**, *158*, 1441–1455. [CrossRef]
56. Vorobeychik, Y.; Pritchard, M. Plan Interdiction Games. *arXiv* **2018**, arXiv:1811.06162.
57. Panda, S.; Vorobeychik, Y. Near-optimal interdiction of factored mdps. In Proceedings of the Conference on Uncertainty in Artificial Intelligence, Sydney, Australia, 11–15 August 2017.
58. Sreekumaran, H.; Hota, A.R.; Liu, A.L.; Uhan, N.A.; Sundaram, S. Multi-agent decentralized network interdiction games. *arXiv* **2015**, arXiv:1503.01100.
59. Smith, G. On the foundations of quantitative information flow. In Proceedings of the International Conference on Foundations of Software Science and Computational Structures, York, UK, 22–29 March 2009; pp. 288–302.
60. Crooks, G.E. On measures of entropy and information. *Tech. Note* **2017**, *9*, v4.

61. Clark, C.R. *The Threshold Shortest Path Interdiction Problem for Critical Infrastructure Resilience Analysis*; Technical Report; Naval Postgraduate School Monterey United States: Monterey, CA, USA, 2017.
62. Geoffrion, A.M. Generalized Benders decomposition. *J. Optim. Theory Appl.* **1972**. [CrossRef]
63. Israeli, E.; Wood, R.K. Shortest-Path Network Interdiction. *Networks* **2002**. [CrossRef]
64. Erdős, P.; Rényi, A. On random graphs. I. *Publ. Math.* **1959**, *4*, 3286–3291.
65. Bar-Gera, H. Transportation Networks for Resear. Available online: https://github.com/bstabler/TransportationNetworks (accessed on 1 March 2019).