51st IEEE Conference on Decision and Control
December 10-13, 2012. Maui, Hawaii, USA

Deceptive Routing Games

Quanyan Zhu, Andrew Clark, Radha Poovendran and Tamer Başar

Abstract— **The use of a shared medium leaves wireless networks, including mobile ad hoc and sensor networks, vulnerable to jamming attacks. In this paper, we introduce a jamming defense mechanism for multiple-path routing networks based on maintaining deceptive flows, consisting of fake packets, between a source and a destination. An adversary observing a deceptive flow will expend energy on disrupting the fake packets, allowing the real data packets to arrive at the destination unharmed. We model this deceptive flow-based defense within a multi-stage stochastic game framework between the network nodes, which choose a routing path and flow rates for the real and fake data, and an adversary, which chooses which fraction of each flow to target at each hop. We develop an efficient, distributed procedure for computing the optimal routing at each hop and the optimal flow allocation at the destination. Furthermore, by studying the equilibria of the game, we quantify the benefit arising from deception, as reflected in an increase in the valid throughput. Our results are demonstrated via a simulation study.**

I. Introduction

Multi-hop wireless networks have been deployed or envisioned in applications ranging from infrastructure monitoring to battlefield communication [1]. The use of an open wireless medium, however, leaves wireless networks vulnerable to jamming attacks, in which an adversary broadcasts an interfering signal in the vicinity of a receiving node and thereby prevents packets from being correctly decoded [2]. The jamming attack can severely limit the throughput of a communication session unless defense measures are taken.

Current approaches to mitigating jamming attacks use randomization techniques at one or more layers to prevent the adversary from targeting packets. At the physical layer, frequency hopping is used to prevent the adversary from identifying the frequency band used by the nodes [3]. Generalized mechanism-hopping methods are employed at higher layers, in which the network nodes switch between different communication protocols in order to prevent protocol-specific attacks [4]. Jamming has also been mitigated by dividing traffic flows among multiple paths, so that network flows can be shifted away from paths that are being jammed [5], [6]. These defense methods are inherently *reactive*, in that they are not activated until the adversary has already reduced the network throughput. Furthermore, while their main objective is to hide information on the frequency channel, communication protocol, or network routing topology, they do not employ deception to actively mislead the adversary.

In this paper, we introduce a proactive deception mechanism for mitigating wireless jamming, in which the source node introduces a false flow, consisting of randomly generated packets. If all traffic is encrypted, then an adversary will not be able to distinguish between real and false flows. The adversary will then expend its limited resources, such as jamming power, on attacking the false flow, thereby reducing the impact on the real flow.

We introduce a game-theoretic framework for modeling and developing deceptive flow-based jamming mitigation between a single source and a destination. Our framework consists of two components. First, at the intermediate nodes between the source and the destination, we formulate a multi-person Stackelberg game, in which the intermediate node moves first and chooses the next hop for both the real and false flows. The adversary then selects how much power to allocate to jamming each flow at that hop. We introduce the concept of *path Stackelberg equilibrium*, describing the optimal strategies of both the intermediate node and the adversary, and prove the existence of such an equilibrium in behavioral mixed strategies.

Second, we consider the rates chosen for the real and deceptive flows at the source. Under this formulation, the source first chooses the flow rates, and then the intermediate nodes and adversary respond by choosing routing and jamming strategies, respectively. We introduce a *rate Stackelberg equilibrium* describing the optimal flow allocation by the source, and prove the existence of such an equilibrium.

We provide an efficient procedure for computing both the path and rate Stackelberg equilibria for a given network. We demonstrate this approach by analyzing a network in which the source has a logarithmic utility function and the adversaries pursue independent strategies at each hop. The effectiveness of our approach is demonstrated through numerical examples.

We also introduce the notion of *value of deception* in order to evaluate the benefit of deception in multi-hop routing games. When the value is greater than 1, deception is valuable to the source node for mitigating the attack, and the utility gain of deceptive routing is measured by the difference between the equilibrium utility of the game and the utility under routing strategies without deception.

The rest of this paper is organized as follows. In Section III, we present our system model and game formulations. We discuss the existence of equilibrium solutions and a backward induction method to compute the equilibrium. In

The research was partially supported by the AFOSR MURI Grant FA9550-10-1-0573, and also by an NSA Grant through the Information Trust Institute at the University of Illinois.

Q. Zhu and T. Başar are with the Coordinated Science Laboratory and Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA. Email: {zhu31, basar1}@illinois.edu

Andrew Clark and Radha Poovendran are with the Department of Electrical Engineering, University of Washington, Seattle, WA 98195 USA. Email: {awclark, rp3}@u.washington.edu

978-1-4673-2066-5/12/$31.00 ©2012 IEEE

Section IV we provide analysis for the special case where each hop is independent and the source has a logarithmic utility function. Section V contains our simulation results. Section VI concludes the paper and points out future work.

II. Related Work

Game-theoretic approaches have been widely applied to routing problems in communication networks [15], [12]. In recent years, hierarchical multi-hop network architectures have emerged as an essential aspect of emerging communication networks. For instance, while cellular-based communication has been the leading architecture in the past decade, recent advances in wireless networking, such as the need for distributed multi-hop communication has imposed a hierarchical architecture on many next generation wireless networks [13], [14]. In [8], we have introduced a distributed dynamic routing algorithm for secondary users to minimize their interference with the primary users in multi-hop cognitive radio networks. We have used a temporal and spatial dynamic non-cooperative game to model the interactions among secondary users as well as their influences from primary users in the multi-hop structure of the network. In [7], we have proposed a dynamic secure routing game framework to effectively combat jamming attacks in distributed cognitive radio networks. A stochastic multi-stage zero-sum game framework adopted is based on the directional exploration of ad hoc on-demand distance vector (AODV) algorithms. The zero-sum game captures the conflicting goals between malicious attackers and honest nodes, and considers packet error probability and delay as performance metrics. In [9], we have formulated a noncooperative game to analyze the complex interactions between wireless users and a malicious node in the context of relay station-enabled wireless networks.

Our work is also related to the following works that apply game theory to deception. In [10], the authors have studied a leader-follower game where the actions of the leader determine the information available to the follower. By concealing information, the leader degrades the performance of the follower that attempts to choose one out of several resources with the best state among all. In [11], the authors have formulated a general two-player, zero-sum game, that takes into account the possibility that one player may implement deception to neutralize the other player's information. In [16], the authors have introduced a diagrammatic hypergame representation termed as hypergame perception model (HPM). HPM is derived from the established hypergame approach, and is used to model misperception and deception.

III. System Model

In this section, we introduce a general multi-hop framework for deceptive routing in communication networks. Let S be the source node and D be the destination node. A source sends its data to two different nodes. One is a legitimate node, denoted by R_G, which seeks the best routing path for data from its source to destination. The other one, denoted by R_D, is chosen to deceive attackers along the path. The

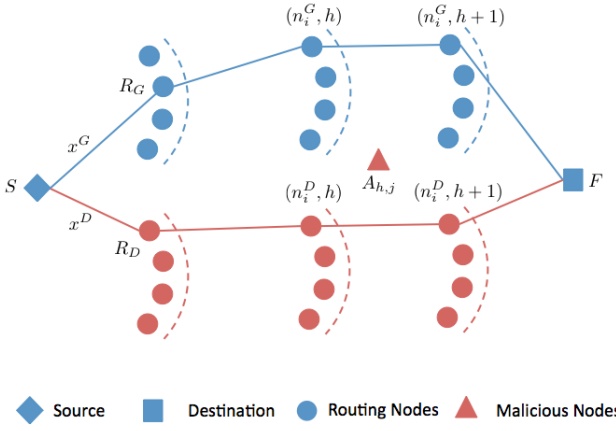

Fig. 1. Illustration of deceptive routing in sensor networks: A source node S splits its rates into two routes, one being legitimate and the other one being deceptive.

source splits its data rate between R_G and R_D. It sends to R_G at rate x^G and sends to R_D at rate x^D, where

$$x^D + x^G = 1. \tag{1}$$

After R_G and R_D are chosen, each node explores the routing path by seeking the node for the next hop. Let L_D, L_G be the number of explorations before reaching destination D. We assume that $L_D = L_G = L$. This assumption is valid since the legitimate and the deceptive nodes are often close to the source node and they share the same destination. Let $\mathscr{L} := \{l_1, l_2, \cdots, l_L\}$ be the set of L stages of exploration. Nodes R_G and R_D start with the first stage of exploration by discovering the sets of nodes $\mathscr{N}_1^D$ and $\mathscr{N}_1^G$, respectively. Let $\mathscr{N}_{l_h}^e, e \in \{D,G\}, l_h \in \mathscr{L}$, be the set of explored nodes at stage l_h for legitimate and deceptive paths. Let $(n_i^e, l_h) \in \mathscr{N}_{l_h}^e, e \in \{D,G\}, h \in L, i = 1,2,\cdots,N_{l_h}^e$, denote the node chosen at stage l_h, where $N_h^e = |\mathscr{N}_l^e|$. For the final stage l_L, it is clear that the sets $\mathscr{N}_{l_L}^e, e \in \{D,G\}$, are singletons only containing the destination node F. A node at stage l_h chooses a node to connect to at stage l_{h+1} for $h = 1,2,\cdots,L-1$. And also by default, we see nodes R_D and R_G are nodes at initial stage l_0, $\mathscr{N}_0^D := \{R_D\}$ and $\mathscr{N}_0^G := \{R_G\}$.

Denote by $A_{h,j}$ attacker j who is present at stage h. An attacker allocates his resources to cause maximum damage on the routing path. Let C_h be the resource budget of the attacker at stage h, and $q_{h,j}^e \in [0, C_{h,j}]$ be the resource allocated to two different routes such that

$$\sum_{e \in \{G,D\}} c_{h,j}^e (q_{h,j}^e, (n_i^e, h+1)) \leq \bar{C}_{h,j}, \tag{2}$$

where $\bar{C}_{h,j}$ are the resource budgets; $c_{h,j}^e : [0, C_{h,j}] \times \mathscr{N}_{h+1}^e \to \mathbb{R}$, are monotonically increasing differentiable functions of $q_{h,j}^e$. The costs depend on the connecting nodes $(n_i^e, h+1)$ as the costs are higher when the attacker is farther away from the nodes. An attacker $A_{h,j}$ has a belief $\pi = \{\pi_{h,j}^e \in [0,1], e \in \{G,D\}\}$ on the routes, i.e., the attacker believes with probability $\pi_{h,j}^G$ that the legitimate path is the true path and with probability $\pi_{h,j}^D$ that the deceptive path is

the true path. Let $\mathcal{N}_A$ be the set of N_A attackers along the path, and $\mathcal{N}_{A,h}$ be the set of $N_{A,h}$ attackers at stage l_h. Let $\mathbf{q}_{h,j} = [q^e_{h,j}, e \in \{D,G\}]$ be the attack strategy of an attacker $A_{h,j}$ at stage l_h. Denote by $\mathbf{q}^e_h = [q^e_{h,j}, j \in \mathcal{N}_{A,h}]$ the attack on route e at stage h, and $\mathbf{q}^e = [q^e_{h,j}, j \in \mathcal{N}_{A,h}, h = 0, \cdots, L]$ the attack on legitimate or deceptive path.

The deceptive routing framework is illustrated in Fig. 1. In the first stage of the game, the source splits its data rate into two paths: one sends to the deceptive node R_D and the other sends to the legitimate node R_G. In the following stages, R_D and R_G search for connecting nodes to reach the destination F. An attacker is located at stage h to jam the traffic between nodes (n^G_i, h) and $(n^G_i, h+1)$, (n^D_i, h) and $(n^D_i, h+1)$.

A. Utility Functions

The stage utility function of node $(n^e_i, h), e \in \{G,D\}$, at stage l_h depends on the currently connected node (n^e_i, h), the connecting node $(n^e_i, h+1)$, the actions of the attackers $\mathbf{q}^e_h$, and the initial data rate x^e_h determined by the source node S. Moreover, in general, the stage utility is also influenced by routing behaviors from other paths. In this model, the stage utility of (n^G_i, h) of the legitimate path depends on the choice of the connecting nodes $(n^D_i, h+1)$ from the deceptive one, and likewise for (n^D_i, h).

Let $(\mathbf{n}, h) := [(n^G_i, h), (n^D_j, h)]$, $(n^G_i, h) \in \mathcal{N}^G_h$, $(n^D_j, h) \in \mathcal{N}^D_h$, be the profile of connected nodes of the legitimate and the deceptive paths at stage h. We denote the stage utility by $u^e_h\left((\mathbf{n}, h), (\mathbf{n}, h+1), \mathbf{q}^e_h, x^e\right) : \prod_{e\in\{G,D\}} \mathcal{N}^e_h \times \prod_{e\in\{G,D\}} \mathcal{N}^e_{h+1} \times \prod_{j=1}^{N_{A,h}} [0, C_{h,j}] \times [0,1] \to \mathbb{R}$. We assume that it is a continuous and non-decreasing function of x^e_h and a continuous and non-increasing function of $q^e_{h,j}$.

At each stage, the decision is made by the current connected node on the following node at stage l_{h+1}. Hence, distributed decisions lead to a path P^e formed by the chain of nodes $R_e \to (n^e_i, l_1) \to (n^e_i, l_2) \cdots \to (n^e_i, l_L) \to F$. Let $\mathscr{P}^e(R_e, F), e \in \{G,D\}$, be the set of all admissible paths from the source to destination. The goal of the legitimate node R_G connected to the source is to find the best route to maximize the path utility $U^G(P^G(R_G,F), P^D(R_D,F), \mathbf{q}^G, x^G) : \mathscr{P}^G(R_G,F) \times \mathscr{P}^D(R_D,F) \times \prod_{h=1}^{L-1} \prod_{j=1}^{N_{A,h}} [0, C_{h,j}] \times [0,1] \to \mathbb{R}$ of R_G which is given by the sum of the stage utilities from l_1 to l_L, i.e.,

$$U^G(P^G, P^D, \mathbf{q}^G, x^G) = \sum_{h=1}^{L} u^G_h. \tag{3}$$

On the contrary, the goal of the deceptive node R_D is to find a deceiving path so that the path is most vulnerable to attacks. In other words, R_D seeks to minimize its path utility $U^D(P^D(R_D,F), P^G(R_G,F), \mathbf{q}^D, x^D) : \mathscr{P}^D(R_D,F) \times \mathscr{P}^G(R_G,F) \times \prod_{h=1}^{L-1} \prod_{j=1}^{N_{A,h}} [0, C_{h,j}] \times [0,1] \to \mathbb{R}$ from stage $h=1$ to $h=L$, given by

$$U^D(P^D, P^G, \mathbf{q}^D, x^D) = \sum_{h=1}^{L} u^D_h. \tag{4}$$

Since node (n^e_i, h) can only decide on the next connecting node $(n^e_i, h+1)$ to optimize the path in the future, node (n^e_i, h) maximizes (or minimizes) its utility-to-go $U^e_{(n_i,h)}$, given by

$$U^e_{(n_i,h)}\left(P^G\left((n^G_i,h),F\right), P^D\left((n^D_i,h),F\right), \{\mathbf{q}^e_{h'}\}^L_{h'=h}, x^e\right) = \sum_{h'=h}^{L} u^e_{h'}\left((\mathbf{n},h),(\mathbf{n},h+1),\mathbf{q}^e_h, x^e\right). \tag{5}$$

An attacker $A_{h,j}$ at stage h aims to minimize the stage cost function according to his belief subject to his resource constraint (2). Denote by $u^A_{h,j} : \prod_{e\in\{D,G\}} \mathcal{N}^e_h \times \prod_{e\in\{D,G\}} \mathcal{N}^e_{h+1} \times [0, C_{h,j}] \times [0,1] \to \mathbb{R}$ the payoff function of attacker $A_{h,j}$, which is given by

$$u^A_{h,j} = \sum_{e\in\{G,D\}} \pi^e_{h,j} u^e_h. \tag{6}$$

Remark 1: The utility functions of R_D and R_G in (3) and (4) are interdependent on the routing strategies of each path. Since there is lack of communications between R_D and R_G and it is so for their future connecting nodes, the strategic behaviors between two routing paths lead to a noncooperative game.

Remark 2: In utility functions (3) and (4), we have explicitly emphasized the dependence of utility of one path on the other. The coupling results from the fact that (i) $\mathcal{N}^e_h$ can be overlapping, i.e., $\mathcal{N}^D_h \cap \mathcal{N}^G_h \neq \emptyset$, for $h = 1, 2, \cdots, L-1$; (ii) the coupled constraints (2) lead to interdependencies through attack strategies. The framework described above can be easily extended to more general cases with multiple deceptive routes with nodes $R_{D_1}, R_{D_2}, \cdots, R_{D_M}$ at the first stage.

B. Stackelberg Game

Since the source node proactively chooses deceptive routes, we can view the interaction between the defender and the attackers as a multi-stage Stackelberg game, where at every stage the defender is the leader and the attackers are the followers. We assume that there are no collusions between the attackers, i.e, $N_{A,h}$ attackers at stage l_h choose their attack strategies $\mathbf{q}_{h,j}, j \in \mathcal{N}_{A,h}$ independently. If collusion happens, we can group the colluding attackers as a single one. Given the rates $x^e, e \in \{D,G\}$, and the connecting node $(n_i, h+1)$ for node (n_i, h), we have an $N_{A,h}$-person non-cooperative game $\Xi_{A,h} := \langle \mathcal{N}_{A,h}, \{\mathscr{Q}^e_{h,j}\}_{A_{h,j}\in\mathcal{N}_{A,h}, e\in\{G,D\}}, \{u^A_{h,j}\}_{A_{h,j}\in\mathcal{N}_{A,h}} \rangle$ among the group of attackers at every stage h, where the set of players is $\mathcal{N}_{A,h}$, the action set for each player $A_{h,j}$ is $\mathscr{Q}^e_{h,j} := [0, C_{h,j}]$, for all $e \in \{G,D\}$, and the payoff function of each player is $u^A_{h,j}$. Since the payoff function is continuous and convex in $q^e_{h,j} \in \mathscr{Q}^e_{h,j}$, and $q^e_{h,j} \in \mathscr{Q}^e_{h,j}$ are compact and convex, the game admits a Nash equilibrium in pure strategies according to Theorem 4.3 in [17]. Denote by $\kappa_{h,j} = [\kappa^e_{h,j}, \kappa^e_{h,j} \in \mathscr{Q}^e_{h,j}, e \in \{D,G\}]$ the best response strategy of each attacker $A_{h,j}$, where $\kappa^e_{h,j} : \mathcal{N}^e_h \times \mathcal{N}^e_{h+1} \times [0,1] \to \mathscr{Q}^e_{h,j}$. We assume that this game $\Xi_{A,h}$ admits a unique best response for every stage l_h. Denote by $\kappa^*_{h,j}$ the unique Nash equilibrium attack strategy in response to (n^e_i, h) and its connecting node $(n^e_i, h+1)$ and rates x^e for $e \in \{G,D\}$.

With the best response $\kappa^*_h = [\kappa^*_{h,j}, j \in \mathcal{N}_{A,h}]$ of the attackers, at each stage h, nodes R_G and R_D aim to find the

best routing path by choosing the next connecting node. At every stage, (n_i^G,h) chooses a connecting node $(n_i^G,h+1)$ at the next stage by maximizing its utility-to-go $U^G_{(n_i^G,h)}$, while the deceptive node chooses a connecting node $(n_i^D,h+1)$ to minimize its utility-to-go $U^D_{(n_i^D,h)}$, i.e., node (n_i^G,h) finds $(n_i^G,h+1)\in\mathscr{N}_h^G$ to maximize

$$U^G_{(n_i^G,h)} = \sum_{h'=h}^{L} u^G_{h'}((n_i^G,h'),(n_i^G,h'+1),(n_i^D,h'),(n_i^D,h'+1),\kappa^*_{h'},x^G), \tag{7}$$

and node (n_i^D,h) finds $(n_i^D,h+1)\in\mathscr{N}_h^D$ to minimize

$$\sum_{h'=h}^{L} u^D_{h'}((n_i^D,h'),(n_i^D,h'+1),(n_i^G,h'),(n_i^G,h'+1),\kappa^*_{h'},x^D). \tag{8}$$

The optimal strategies of nodes (n_i^G,h) at each stage l_h lead to optimal paths $P^G(R_G,F)$ and $P^D(R_D,F)$, which yield the optimal utilities U^{G*} and U^{D*}, respectively. The coupling between the legitimate route and the deceptive one comes explicitly from the interdependence in the utility as well as implicitly from the attacker strategies. Note that U^{G*} and U^{D*} are functions of rates x^G and x^D. At the source node S, the decision is made to maximize U^{G*}, i.e., the source node S solves the following source problem (SP):

$$\text{(SP)}\quad U^{G\star} := \max_{x^G,\ x^D\in[0,1]} U^{G*}(x^G,x^D) \quad \text{s.t.} \quad \text{constraint (1) holds.}$$

We define formally the Stackelberg game as follows.

Definition 1 (Stackelberg Game): Let Ξ_S be the (N_A+3)-person Stackelberg game, with the set $\mathscr{N}_A$ of N_A attackers as the followers and S,R_D,R_G, as the leaders. Source S splits its data to the legitimate node R_G and the deceptive node R_D by solving (SP). Nodes R_G and R_D choose routing paths to maximize (or minimize) their utility functions (3) and (4), respectively. In response to the actions of the leaders, every attacker $A_{h,j}\in\mathscr{N}_A$ at stage l_h minimizes his stage payoff function $u^A_{h,j}$ in (6).

Remark 3: Note that the Stackelberg game Ξ_S has three leaders S,R_D,R_G. Strictly speaking, there is also a leader-and-follower relationship between these three players. S is the leader who decides on the data rates while R_G and R_D are players who decide on the routing path in response to the determined rates. In the case where S makes both rate and routing decisions, including decisions on choices of R_D and R_G, we call the game an (N_A+1)-person Stackelberg game.

In Fig. 2, we illustrate the Stackelberg game framework at each stage l_h associated with the system model in Fig. 1. Attackers $A_{h,j}, j=1,2,3$, behave as followers and choose attack strategies κ_h in response to the defending actions. (n_i^G,h) and (n_i^D,h) act as leaders choosing the connecting nodes $(n_i^G,h+1)$ and $(n_i^D,h+1)$, respectively.

In Fig. 3, we illustrate the strategic interactions between S,R_G,R_D. The source node first determines the data rates x^D and x^G. In response to them, R_G and R_D seek to find the best routing paths that lead to the destination F.

C. Stackelberg Equilibrium

In this subsection, we define the equilibrium solution concepts associated with the Stackelberg game defined above and use an iterative backward induction method to find the equilibrium of the game.

Definition 2: (Path Stackelberg Equilibrium in Pure Strategies) Assume that κ_h^* is unique and $\kappa^* = [\kappa_h^*]_{h=1,2,\cdots,L-1}$. Given a rate profile (x^G,x^D), routing paths $P^{e*}(R_e,F)\in\mathscr{P}^e(R_e,F), e\in\{G,D\}$, are called *pure path Stackelberg equilibrium* (PPSE) strategies for the leaders R_D,R_G of the game Ξ_S if

$$\begin{aligned} U^{G*}(x^G,x^D) &:= U^G(P^{G*},P^{D*},\kappa^{G*}(P^{G*},P^{D*}),x^G) \\ &\geq U^G(P^G,P^{D*},\kappa^{G*}(P^G,P^{D*}),x^G), \\ U^{D*}(x^G,x^D) &:= U^D(P^{D*},P^{G*},\kappa^{D*}(P^{G*},P^{D*}),x^D) \\ &\leq U^D(P^D,P^{G*},\kappa^{D*}(P^{G*},P^D),x^D), \end{aligned}$$

for all $P^e\in\mathscr{P}^e(R_e,F)$.

Note that in $U^e, e\in\{D,G\}$, above, we have suppressed the dependence of x^G,x^D in P^e,P^{e*}, and κ^e, κ^{e*}. The equilibrium outcomes of PPSE are denoted by functions $U^{G*}(\cdot),U^{D*}(\cdot)$ for the legitimate and the deceptive paths, respectively. Following (SP) and Definition 1, we can define *rate Stackelberg Equilibrium* (RSE) as follows.

Definition 3 (Rate Stackelberg Equilibrium): Suppose that κ_h^* is unique and $\kappa^* = [\kappa_h^*]_{h=1,2,\cdots,L-1}$. In addition, $P^{e*}, e\in\{D,G\}$, is a unique PPSE by Definition 2, and we use $P^e(x^G)$ to denote explicitly the dependence of the routing paths on the data rates. Then, a rate profile $x^{e*}\in[0,1], e\in\{G,D\}$, with constraint (1) is called rate Stackelberg equilibrium (RSE) strategies for the leader S of the game Ξ_S if

$$\begin{aligned} U^{G\star} &:= U^G(P^{G*}(x^{G*}),\kappa^{G*}(P^{G*},P^{D*},x^{G*}),x^{G*}) \\ &\geq U^G(P^{G*}(x^G),\kappa^{G*}(P^{G*},P^{D*},x^G),x^G), \end{aligned}$$

for all $x^G\in[0,1]$, where $P^{e*}(R_e,F), e\in\{G,D\}$, are PPSE defined in Definition 2.

Note that from (1), $x^D = 1-x^G$. Hence we can express U^e,P^e all in terms of x^G above. Every RSE defined maximizes (SP) and a global optimal solution to (SP) satisfies the definition. Hence the notion of RSE is equivalent to finding the global optimal solution to (SP). Definition (2) describes a pure strategy path Stackelberg equilibrium. However, due to the noncooperative behaviors between R_D and R_G, there may not exist an equilibrium in pure strategies. Hence, we need to study the equilibrium under mixed strategies. We let $\mathbf{p}_h^e = [p_h^e((n_i^e,h)),(n_i^e,h)\in\mathscr{N}_h^e]\in\Gamma_h^e$ be the probability distribution over the action set $\mathscr{N}_h^e$, where

$$\Gamma_h^e := \left\{ p_h^e((n_i^e,h))\in\mathbb{R}_+ \;\middle|\; \sum_{(n_i^e,h)\in\mathscr{N}_h^e} p_h^e((n_i^e,h)) = 1 \right\}, \quad e\in\{G,D\},\ h=1,\cdots,L-1.$$

We consider behavioral mixed strategies (BMS) in which every node (n_i^e,h) randomizes over $\mathscr{N}_h^e$ at every stage h [17]. Denote by $\mathbf{p}^e = [\mathbf{p}_h^e, h=1,2,\cdots,L-1]$ the behavioral

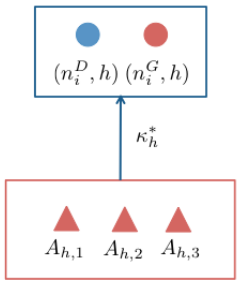

Fig. 2. Stackelberg game at each stage l_h: Attackers $A_{h,1},A_{h,2},A_{h,3}$ behave as followers using equilibrium attack strategies κ_h, and defending nodes (n_i^G,h) and (n_i^D,h) act as leaders choosing the connecting nodes.

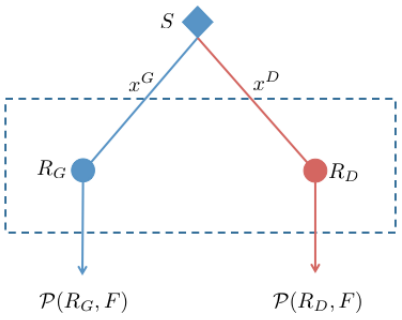

Fig. 3. Stackelberg game between S,R_G,R_D. The source node S first determines the data rates. R_G and R_D behave as followers in response to x^G and x^D, respectively, to find the best routing paths $\mathscr{P}(R_G,F)$ and $\mathscr{P}(R_D,F)$.

path mixed strategies (BPMS), and $\mathbb{U}^e, e\in\{G,D\}$, the utility functions under BPMS given by $\mathbb{U}^e(\mathbf{p}^e,\bar{\kappa}^e(\mathbf{p}^e),x^e)$, where $\bar{\kappa}$ is attacker's best response to BPMSs with constraint (2) being averaged over $\mathbf{p}_h^e$, i.e.,

$$\sum_{e\in\{G,D\}}\sum_{(n_i^e,h)\in\mathscr{N}_h^e} p_h^e((n_i^e,h))c_{h,j}^e\left(q_{h,j}^e,(n_i^e,h+1)\right)\le\bar{C}_{h,j}, \tag{9}$$

Definition 4 (Path Stackelberg Equilibrium in BMS): Assume that $\bar{\kappa}_h^*$ is the unique best response to BMS at each stage, and $\bar{\kappa}^*=[\bar{\kappa}_h^*]_{h=1,2,\cdots,L-1}$. Given a rate profile (x^G,x^D), routing paths $\mathbf{p}^{e*}, e\in\{G,D\}$, are called *behavioral mixed path Stackelberg equilibrium* (BMPSE) strategies for the leaders R_D,R_G of the game Ξ_S if

$$\begin{aligned}\mathbb{U}^{G*}(x^G,x^D) &:= \mathbb{U}^G(\mathbf{p}^{G*},\mathbf{p}^{D*},\bar{\kappa}^{G*}(\mathbf{p}^{G*}),x^G)\\ &\ge \mathbb{U}^G(\mathbf{p}^G,\mathbf{p}^{D*},\bar{\kappa}^{G*}(\mathbf{p}^G),x^G),\\ \mathbb{U}^{D*}(x^G,x^D) &:= \mathbb{U}^D(\mathbf{p}^{D*},\mathbf{p}^{G*},\bar{\kappa}^{D*}(\mathbf{p}^{D*}),x^D)\\ &\le \mathbb{U}^D(\mathbf{p}^D,\mathbf{p}^{G*},\bar{\kappa}^{D*}(\mathbf{p}^D),x^D),\end{aligned}$$

for all $\mathbf{p}_h^e\in\Gamma_h^e, h=1,\cdots,L-1$.

Note that RSE that corresponds to BMPSE can also be defined in a similar fashion as in Definition 3 by replacing P^e with $\mathbf{p}^e$ and κ^e with $\bar{\kappa}^e$. The RSE for BMPSE can be found by solving a source problem similar to (SP). We call it a mixed source problem (MSP), i.e.,

$$\begin{aligned}\text{(MSP)}\quad \mathbb{U}^{G\star} := \max_{x^G,\ x^D\in[0,1]} \quad & \mathbb{U}^{G*}(x^G,x^D)\\ \text{s.t.}\quad & \text{Constraint (1) holds.}\end{aligned}$$

Proposition 1: Assume that $\bar{\kappa}^e, e\in\{G,D\}$, are unique. Then the Stackelberg game Ξ_S admits a BMPSE solution.

Proof: Given that $\bar{\kappa}^e$ are unique, we can view the game at each stage l_h as a strategic game in normal form, and hence it follows from Theorem 3.2 in [17] that Ξ_S admits a BMPSE solution. ∎

Proposition 2: Assume that $\bar{\kappa}^e, e\in\{G,D\}$, are unique and are continuous mappings from $\prod_{e\in\{D,G\}}\prod_{h=1}^{L-1}\Gamma_h^e\times[0,1]$ to $\prod_{A_{h,j}\in\mathscr{N}_{A,h}}\mathscr{Q}_{h,j}^e$. In addition, $\mathbf{p}^{e*}$ are unique and continuous in x^G,x^D. Then, the Stackelberg game Ξ_S admits a RSE described by (MSP).

Proof: Following Proposition 1, the Stackelberg game Ξ_S admits a BMPSE solution $\mathbf{p}^{e*}, e\in\{G,D\}$. By fixing $\mathbf{p}^{e*}$, due to the uniqueness and continuity of $\bar{\kappa}^e$ and $\mathbb{U}^G$, it follows from Theorem 4.8 in [17] that Ξ_S admits a RSE associated with the BMPSE solution. ∎

Proposition 3: Assume that $\bar{\kappa}_h^*$ is unique for every h. The BMPSE of the game Ξ_S can be found using backward induction, i.e.,

$$\begin{aligned}(\mathbf{p}_h^{G*},\mathbf{p}_h^{D*}) &\in \arg\,\text{NE}\left\{\mathbb{U}^{G*}_{(n_i^G,h+1)}+\mathbf{u}_h^G,\right.\\ &\qquad \left.\mathbb{U}^{D*}_{(n_i^D,h+1)}+\mathbf{u}_h^D\right\}, \qquad (10)\\ \left(\mathbb{U}^{G*}_{(n_i^G,h)},\mathbb{U}^{D*}_{(n_i^D,h)}\right) &\in \text{NE}\left\{\mathbb{U}^{G*}_{(n_i^G,h+1)}+\mathbf{u}_h^G,\right.\\ &\qquad \left.\mathbb{U}^{D*}_{(n_i^D,h+1)}+\mathbf{u}_h^D\right\},\\ &\qquad h=1,2,\cdots,L-2, \qquad (11)\\ \mathbb{U}^{e*}_{n_i^e,L-1} &= u_F^e,\end{aligned}$$

where $u_F^e, e\in\{G,D\}$, is the utility of the legitimate and the deceptive path connecting from $(n_i^e,L-1)$ to the final destination F, respectively. The mixed strategy $\mathbf{p}_{L-1}^e$ is a point distribution over the singleton sets $\mathscr{N}_L^e$. arg NE$\{\cdot\}$ is an operator that yields the mixed strategy Nash equilibria of two-person nonzero-sum games in normal form with utility functions specified in the argument, and NE is an operator that yields the corresponding equilibrium utilities at the mixed strategy equilibrium $(\mathbf{p}_h^{G*},\mathbf{p}_h^{D*})$.

Sketch of the Proof: Note that the multi-level structure of the game allows us to write

$$\mathbb{U}^e := \mathbb{U}^e_{(n_i^e,1)} = \mathbf{u}_1^e + \mathbb{U}^e_{(n_i^e,2)}, e\in\{G,D\}, \tag{12}$$

which is composed of two parts: one is the current stage utility and the other is the utility-to-go. Given a unique $\bar{\kappa}$ and rate profile (x^D,x^G), the maximizing (or minimizing) decisions are not coupled across the stages, i.e.,

$$\max_{P^G(R_G,F)}\mathbb{U}^G = \max_{(n_i^G,1)\in\mathscr{N}_1^G}\mathbf{u}_1^G + \max_{P^G((n_i^G,2),F)}\mathbb{U}^G_{(n_i^G,2)}, \tag{13}$$

and likewise for minimizing $\mathbb{U}^D$. The process of (13) continues until it reaches the last stage where nodes $(n_i^e,L-1), e\in\{D,G\}$, connect to F with probability 1. Therefore, we can apply the dynamic programming principle and arrive at the recursion.

Note that the solution obtained using this backward induction approach has the following properties [17].

Definition 5: Let Ξ_h be the dynamic routing game starting at stage l_h with utility functions $\mathbb{U}^e_{(n_i^e,h)}$ for $e \in \{D,G\}$. Given a rate profile (x^G,x^D), a BMPSE $P^{e*}(R_e,F), e \in \{G,D\}$, solving the dynamic game Ξ_1, is *strongly time-consistent* or *subgame perfect* if the truncated equilibrium $P^{e*}((n_i^e,h),F), e \in \{G,D\}$, solves the truncated game $\Xi_h, h \geq 2$, for every $h = 2,\cdots,L$.

D. Value of Deception

In this section, we study the value of deception as a metric to evaluate the benefit of deception in routing. Define ρ_P as the ratio between the equilibrium utility of the legitimate path under RSE of deceptive routing scheme and its counterpart utility without deception under PPSE, i.e.,

$$\rho_P := \frac{U^{G\star}}{U^{G*}(1,0)} = \frac{U^{G*}(x^{G*},1-x^{G*})}{U^{G*}(1,0)}, \tag{14}$$

where x^{G*} is a RSE, $U^{G\star}, U^{G*}$ are defined in (SP) and Definition 2, respectively. Likewise, we can define the ratio for equilibrium in mixed strategies given by

$$\rho_M := \frac{\mathbb{U}^{G\star}}{\mathbb{U}^{G*}(1,0)} = \frac{\mathbb{U}^{G*}(x^{G*},1-x^{G*})}{\mathbb{U}^{G*}(1,0)}, \tag{15}$$

where $\mathbb{U}^{G\star}, \mathbb{U}^{G*}$ are defined in (MSP) and Definition 4, respectively. Deception is advantageous when the ratio ρ_P or ρ_M is greater than 1. The ratio can be evaluated in a closed form in special cases (Section IV).

IV. Case of Logarithmic Utility for Source

In this section, we analyze this deceptive flow allocation model for a multi-hop connection between the source and destination. We take a logarithmic function to reflect the risk-adversity of the source, $u_h((n_i^G,h-1),(n_i^D,h-1),q_G^h,q_D^h,x^G) = \ln(1+q_G^h x^G)$. In this example, we assume that the stage l_h costs are independent of other stages for simplified analysis. Hence, we only need to solve the game of the same structure at each stage after R_D and R_G. We assume that, if there is no adversary present in the vicinity of a link, then $q_R^h = q_D^h = 1$, i.e. all real and deceptive packets are delivered correctly. At the same time, we assume that the adversary attempts to minimize the total throughput at stage l_h, $u^A_{h,j} = \pi_G \frac{x^G}{a_G^h} + \pi_D \frac{x^D}{a_D^h}$.

We first analyze the adversary's optimal jamming strategy at hop h via the following lemma.

Lemma 1: For given costs c_G^h and c_D^h, the adversary's optimal strategy at hop l_h is given by

$$a_G^h = \frac{C^h}{\sqrt{\frac{\pi_D}{\pi_G}\frac{x^D}{x^G}c_G^h c_D^h} + c_G^h}, \quad a_D^h = \frac{C^h}{\sqrt{\frac{\pi_D}{\pi_G}\frac{x^G}{x^D}c_D^h c_G^h} + c_D^h} \tag{16}$$

Proof: For a given routing and flow allocation, the adversary's strategy can be determined by solving the optimization problem

$$\begin{aligned} \text{minimize} \quad & \pi_G \tfrac{x^G}{a_G^h} + \pi_D \tfrac{x^D}{a_D^h} \\ a_G^h, a_D^h \quad & \\ \text{s.t.} \quad & c_G^h p_G^h + c_D^h p_D^h \leq C^h \end{aligned} \tag{17}$$

Since the adversary's objective is a convex function of a_G and a_D, the optimal strategy (a_G^*, a_D^*) can be obtained as a solution to the Lagrangian equations

$$\begin{aligned} -\frac{\pi_G x^G}{(a_G^h)^2} + \mu c_G^h &= 0, \\ -\frac{\pi_D x^D}{(a_D^h)^2} + \mu c_D^h &= 0, \\ c_G^h a_G^h + c_D^h a_D^h &= C^h. \end{aligned}$$

Solving the above system of equations yields (16). ∎

The network nodes choose a receiver for the next hop in order to maximize the utility of the good session, based on knowledge of the adversary's optimal response. In this case, at each hop h the sender chooses (n_e,h), $e \in \{G,D\}$ in order to maximize $\ln(1+\frac{x^G}{a_G^h})$. To achieve this, the goal is to maximize $\frac{1}{a_G^{h*}}$, or equivalently, to minimize a_G^{h*}.

By (16), the adversary's best response a_G^* is decreasing in C_R and increasing in C_D. Hence a_G is minimized when C_R is maximized and C_D is minimized. Intuitively, this implies that the real flow should be as far from the adversary's position as possible, while the deceptive flow is located close to the adversary. Since the deceptive flow has lower cost to attack, the adversary will target this flow instead of the real flow.

After selecting a next node at each intermediate hop and at the source, the final step is for the source to allocate the real and deceptive flows. In order to maximize the source utility function, the real and deceptive flow rates are chosen according to

$$\begin{aligned} \text{maximize} \quad & \textstyle\sum_{h=1}^L \ln\left(1+\frac{x^G}{a_G^h(x^G,x^D)}\right) \\ x^G, x^D \quad & \\ \text{s.t.} \quad & \text{Constraint (1) holds.} \end{aligned} \tag{18}$$

By Lemma 1, optimization problem (18) is equivalent to

$$\begin{aligned} \text{maximize} \quad & \textstyle\sum_{h=1}^L \ln\left(1+\frac{\sqrt{\frac{\pi_D}{\pi_G}x^G(1-x^G)c_G^h c_D^h}+x^G c_G^h}{C^h}\right) \\ x^G \quad & \\ \text{s.t.} \quad & 0 \leq x^G \leq 1. \end{aligned} \tag{19}$$

Efficient algorithms for finding the optimal flow allocation under (18) can be readily obtained in view of the following lemma.

Lemma 2: The problem described in (19) is a convex optimization problem.

Proof: The function $\frac{\pi_D}{\pi_G}c_G^h c_D^h x^G(1-x^G)$ is concave and increasing in x^G on the interval $[0,1]$. The concavity of the objective function of (19) then follows from composition rules. ∎

The results of this section are summarized in the following theorem.

Theorem 1: Suppose that each hop is independent and the utility function of the network is logarithmic. Then the

pure-strategy path Stackelberg equilibrium is given by

$$a_G^h = \frac{C^h}{\sqrt{\frac{\pi_D}{\pi_G}\frac{x^D}{x^G}c_G^h c_D^h} + c_G^h}, \tag{20}$$

$$a_D^h = \frac{C^h}{\sqrt{\frac{\pi_D}{\pi_G}\frac{x^G}{x^D}c_D^h c_G^h} + c_D^h}, \tag{21}$$

$$n_G^h = \arg\max_{n \in \mathcal{N}_h^G} c_n^h, \tag{22}$$

$$n_D^h = \arg\min_{n \in \mathcal{N}_h^D} c_n^h, \tag{23}$$

while the pure-strategy rate Stackelberg equilibrium is given by (20)–(23) together with the solution to (19).

Based on these equilibria, the value of deception ρ_P can be computed. In this case, it is always advantageous to introduce deception, as described by the following proposition.

Proposition 4: For the equilibria of Theorem 1, $\rho_P > 1$.

Proof: We have $\rho_P > 1$ if there exists x^G such that $U_G(x^G, 1-x^G) > U_G(1,0)$. This will occur if, at each hop, $u_G^h(x^G, 1-x^G) > u_G^h(1,0)$. By the monotonicity of the logarithm function, this is equivalent to

$$\sqrt{\frac{\pi_D}{\pi_G}x^G(1-x^G)c_G^h c_D^h} + x^G c_G^h > c_G^h. \tag{24}$$

Rearranging the terms of (24) yields

$$\alpha x^G(1-x^G) > \beta(1-x_G)^2,$$

where $\alpha = \frac{\pi_D}{\pi_G}c_G^h c_D^h$ and $\beta = (c_G^h)^2$. Eq. (24) is therefore equivalent to

$$(\alpha+\beta)(x^G)^2 - (2\beta+\alpha)x^G + \beta < 0. \tag{25}$$

We have that $\rho_P > 1$ if the left-hand side of (25) has two positive roots. The roots are given by

$$\frac{2\beta+\alpha \pm \sqrt{(2\beta+\alpha)^2 - 4\beta(\alpha+\beta)}}{2(\alpha+\beta)}. \tag{26}$$

One of the roots is equal to 1, while the other root is equal to $\beta/(\alpha+\beta)$, which is always positive and strictly between 0 and 1. Hence there always exists x^G such that $U_G(x^G, 1-x^G) > U_G(1,0)$. ∎

V. Simulation Results and Analysis

A multi-hop wireless network was simulated using Matlab. The simulated network topology consisted of L hops, with each node at hop h capable of communicating with each node at hop l_{h+1}. The destination was placed at the $L-$th hop. The source was assumed to have a logarithmic utility function as described in Section IV.

A total of L adversaries were simulated, with the $h-$th adversary operating at a random location within 400m of the nodes in hop l_h. The unit cost for an adversary at hop l_h to jam was set equal to d_h^α, where d_h represents the distance to the receiver at hop l_h and α is the path-loss constant, equal to 2. The adversary jamming strategy was chosen to maximize the utility given in Section IV. Each data point represents an average over 50 independent trials. Unless otherwise noted, the adversary's belief π_G was set equal to 0.5, the adversary's level of resources, representing the jamming power available to each adversary, was set equal to $C^h = 10^5$ at each hop. The number of hops $L = 4$.

The adversary's belief that the legitimate path is the true path, denoted π_G, influenced both the flow allocation strategy at the source and the resulting utility. As π_G increases, the adversary becomes less likely to target the deceptive flow, making deception less effective. As a result, the utility of the network using deception will decrease (Figure 4(a)) and the gap between the utility of deceptive and non-deceptive networks will decrease. At the same time, as π_G increases, the rate of the deceptive flow will also decrease (Figure 4(b)).

The utility for both deceptive and non-deceptive flows experiences roughly linear growth in the number of hops (Figure 4(c)). This behavior follows from the fact that the utility is additive over each hop and the routing decisions at each hop are independent. We observe that the benefit of using deception increases as the number of hops increases. Since deception provides an incremental benefit at each hop, increasing the number of hops increases the total benefit of deception.

As the resources available to the adversary increase, the utilities of both deceptive and non-deceptive strategies are reduced (Figure 4(d)). We observe a more graceful degradation arising from the use of deception. We note that C^h alone does not affect the flow allocation of the source, since C^h can be viewed as a constant offset in the objective of (19).

VI. Conclusions

Deception is used to distract attackers from attacking the legitimate routes for real data. In this paper, we have proposed a game-theoretic framework for deceptive routing in communication networks. The framework is composed of multiple stages. At the first stage of the game, the source strategically splits its data into two intermediate routing nodes. One is legitimate and the other is deceptive. The second stage of the game involves search of optimal multi-hop paths to the destination in response to jamming behaviors from adversaries as well as the interference from the other route at each hop. The deceptive routing game considers many roles of the players, the source, legitimate and deceptive nodes, intermediate routing nodes, and jammers. The complex interactions among these players are defined by a $N_A + 3$-person Stackelberg game. We have introduced solution concepts such as path Stackelberg equilibrium (PSE), rate Stackelberg equilibrium (RSE) and their behavioral mixed strategy counterparts for the game. We have proposed a backward induction method to find the routing path and studied the routing consistency of the solution. We have illustrated further with logarithmic utility functions and provided PSE and RSE solutions in closed form. The proposed game-theoretic framework can be applied to routing problems in many communication networks such as ad hoc networks, wireless sensor networks, and wireless mobile networks. Our future work will entail development of routing

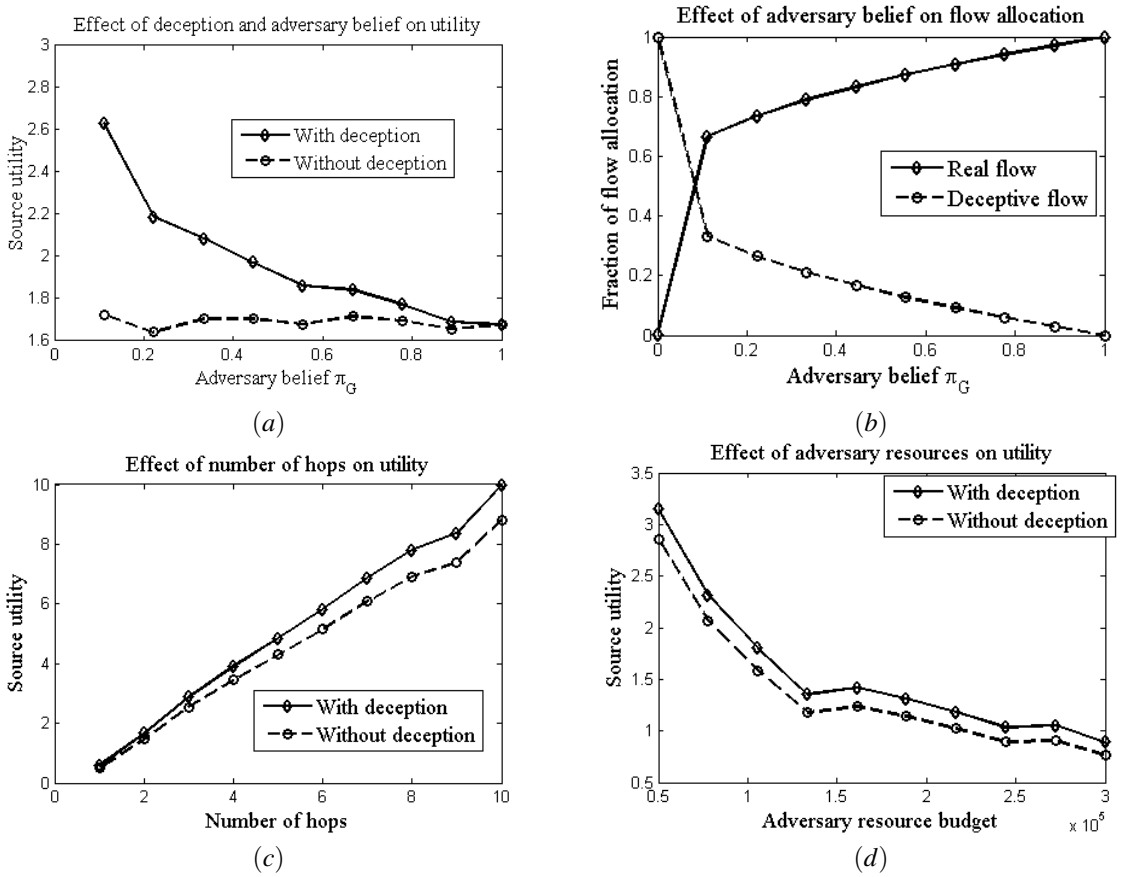

Fig. 4. Simulation of deceptive routing and flow allocation in a multi-hop network. (a) The effect of the adversary's belief that the legitimate path is the true path, π_G, on the source utility. The use of deception increases the achieved utility. (b) The effect of the adversary's belief on the flow allocation. As the adversary grows more certain that the correct flow is real, the benefit of deception, and hence the rate of deceptive flow, decreases. (c) The utility of the source grows roughly linearly in the number of hops. (d) As the adversary's resources increase, the utility with and without deception decreases. Deception provides consistently higher utility than the non-deceptive case.

algorithms based on learning techniques, and generalization of the framework here to multiple deceptive paths.

REFERENCES

[1] I.F. Akyildiz, W. Su, and Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46–57, 2005.

[3] R. Poisel, *Modern Communications Jamming Principles and Techniques*, Artech House Publishers, 2011.

[4] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "Spread: Foiling smart jammers using multi-layer agility," in Proc. of the 26th IEEE International Conference on Computer Communications (INFOCOM), pp. 2536-2540, 2007.

[5] A.D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no.10, pp. 54-62, Oct. 2002.

[6] P. Tague, S. Nabar, J. A. Ritcey and R. Poovendran, "Jamming-aware traffic allocation for multiple-path routing using portfolio selection," *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 184-194, February 2011.

[7] Q. Zhu, J. B. Song and T. Başar, "Dynamic secure routing game in distributed cognitive radio networks," in Proc. of IEEE Global Communications Conference (GLOBECOM), Houston, Texas, Dec. 5 - 9, 2011.

[8] Q. Zhu, Z. Yuan, J. B. Song, Z. Han, and T. Başar, "Dynamic interference minimization routing game for on-demand cognitive pilot channel," in Proc. of IEEE Global Communication Conference (GLOBECOM), Miami, FL, 2010.

[9] Q. Zhu, W. Saad, Z. Han, H. V. Poor and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in Proc. of IEEE Military Communications Conference (MILCOM), Baltimore, MD, Nov. 7-10, 2011.

[10] S. Sarkar, E. Altman and P. Vaidyanathan, "Information concealing games," *IEEE Transactions on Information Theory*, vol.56, no.9, pp. 4608–4630, Sept. 2010.

[11] Z. Fuchs and P. P. Khargonekar, "Games, deception, and Jones' lemma," in the Proc. 2011 American Control Conference (ACC), pp. 4532–4537, June 29 -July 1 2011.

[12] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, J.-P. Hubaux, "Game theory meets network security and privacy," ACM Survey, September 2013.

[13] The Relay Task Group of IEEE 802.16, "The p802.16j baseline document for draft standard for local and metropolitan area networks," 802.16j-06/026r4, Tech. Rep., Jun. 2007.

[14] Y. D. Lin and Y. C. Hsu, "Multihop cellular: a new architecture for wireless communications," in Proc. IEEE Conf. on Comp. Comm. (INFOCOM), Tel Aviv, Israel, Mar. 2000.

[15] E. Altman, T. Boulogne, R. Elazouzi, T. Jimenez, L. Wynter, "A survey on networking games in telecommunications, *Computers & Operations Research*, vol. 33, no. 2, pp. 286-311, 2006.

[16] M. E. Mateski, T.A. Mazzuchi and S. Sarkani, "The hypergame perception model: A diagrammatic approach to modeling perception, misperception, and deception," Military Operations Research, vol. 15, no. 2, pp. 21-37, 2010.

[17] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, SIAM Series in Classics in Applied Mathematics, Philadelphia, January 1999.