Deceptive Routing in Relay Networks

Andrew Clark[†], Quanyan Zhu[‡], Radha Poovendran[†], and Tamer Başar[‡⋆]

[†]Department of Electrical Engineering
University of Washington
Seattle, WA 98195 USA,
Email: {awclark, rp3}@u.washington.edu

[‡]Coordinated Science Laboratory and
Department of Electrical and Computer Engineering,
University of Illinois at Urbana Champaign,
1308 W. Main St., Urbana, IL, USA, 61801,
Email: {zhu31, basar1}@illinois.edu

Abstract. Physical-layer and MAC-layer defense mechanisms against jamming attacks are often inherently reactive to experienced delay and loss of throughput after being attacked. In this paper, we study a proactive defense mechanism against jamming in multi-hop relay networks, in which one or more network sources introduce a deceptive network flow along a disjoint routing path. The deceptive mechanism leverages strategic jamming behaviors, causing the attacker to expend resources on targeting deceptive flows and thereby reducing the impact on real network traffic. We use a two-stage game model to obtain deception strategies at Stackelberg equilibrium for selfish and altruistic nodes. The equilibrium solutions are illustrated and corroborated through a simulation study.

Keywords: Game Theory, Stackelberg Equilibrium, Routing Algorithms, Jamming and Security, Relay Networks

1 Introduction

Wireless networks play a crucial role in many military and commercial applications. The open wireless medium, however, leaves such networks vulnerable to jamming attacks, in which an adversary broadcasts an interfering signal in the vicinity of a node, preventing any incoming packets from being correctly decoded. Jamming attacks are particularly harmful when the adversary can exploit weaknesses in the physical or MAC layer protocols used by the nodes [4], or target intermediate relay nodes in a multi-hop network to reduce the end-to-end-throughput [11]. Different classes of jamming adversary have been studied, including constant jammers that emit a constant interfering signal, random

⋆ The research was partially supported by the AFOSR MURI Grant FA9550-10-1-0573, ARO MURI Grant W911NF-07-1-0287, and also by an NSA Grant through the Information Trust Institute at the University of Illinois.

jammers that broadcast an interfering signal at random intervals, and intelligent jammers that can selectively target packets from different flows to maximize the damage of the attack [5].

Defense mechanisms against jamming are based on physical-layer techniques, such as beamforming, spread-spectrum, and directional antennas [7], or MAC-layer protocols such as channel surfing [12]. When multi-hop routing is used, the source nodes can also decrease the flow rate on paths that experience high packet-loss due to jamming, while increasing the rate on routes experiencing lower packet-loss [10]. This, however, is an inherently reactive defense that cannot be employed until the network has already been targeted by the adversary and experienced loss of throughput.

In this paper, we study a proactive defense mechanism against jamming for multi-hop wireless networks, in which one or more network sources introduce a deceptive network flow, consisting of randomly generated dummy packets, along a disjoint routing path. When the real and deceptive packets are encrypted, the adversary will be unable to distinguish between them, and will expend limited resources, such as jamming power, on targeting a false flow. This leaves fewer jamming resources available for targeting real packets, allowing those packets to escape jamming. The goal of this approach is to use the intelligent attributes of the adversary, such as the ability to target individual packets from specific flows, to create deception and thus mitigate the impact of the attack.

While this approach is promising, several challenges must first be addressed. First, the deceptive packets will traverse the same links as real packets, leading to increased congestion and delays. Second, each source node may have limited capacity to generate, encrypt, and transmit packets, and this scarce capacity must be divided between real and fake flows. Third, if the fake packets are not introduced according to an optimal strategy that leverages information on the adversary's capabilities and goals, then the deception may be ineffective in increasing the throughput of real nodes, and may be counterproductive due to the increase in congestion.

To address these issues, we introduce a game-theoretic framework for thwarting jamming attacks through deceptive flows. Our framework is based on a two-stage game between a set of sources and an adversary mounting the jamming attack. In the first stage of the game, the sources play a noncooperative game in order to select the real and deceptive flow allocations. In the second stage, the adversary observes the total flow allocation of each source and selects a jamming strategy accordingly in order to maximize the decrease in throughput. We study the deceptive jamming game under two types of source behavior, namely a selfish source that maximizes its own throughput while disregarding the delays experienced by other sources, and an altruistic source that incorporates the delays of other sources when choosing flow rates. We derive the equilibria of the game for each case, and provide efficient algorithms for allocating real and deceptive flows at each source based on the equilibria. Our results are illustrated through a simulation study.

The paper is organized as follows. In Section 2, we review related work on jamming attacks and defenses. In Section 3, the system and adversary models are introduced. Section 4 contains the game formulation and solution algorithms for each player. Section 5 presents our simulation results. Section 6 concludes the paper.

2 Related Work

The vulnerability of wireless networks to jamming attacks has been extensively explored [7]. In particular, the use of commodity wireless devices has led to efficient jamming attacks that target specific network protocols, such as 802.11 [4]. Jamming defenses at the physical layer are based on spread-spectrum communication [3], such as frequency hopping, in which jammed receivers change frequency in order to prevent the attacker from discovering the channel [8]. Spatial retreat, in which nodes that detect a jammer move away from the jammed region, was discussed in [12]. These lower-layer defenses are not affected by our proposed approach, and can be employed alongside our methods to further increase the robustness to jamming.

The impact of jamming attacks on multi-hop wireless networks, in which the jammer targets intermediate relay nodes in order to disrupt the end-to-end throughput, was studied in [11]. This work focuses on quantifying the impact of jamming for a given set of network flows and not on responding to jamming. In [10], a flow allocation approach to mitigating jamming was presented, in which each source responds to an increase in packet-loss rate, corresponding to increased jamming activity, by shifting flow to an alternative path with lower loss rate. The work of [10], however, does not explicitly model the goals and constraints of the adversary, and therefore does not enable a strategic approach to flow allocation, let alone introducing deception.

In [13], we proposed thwarting jamming attacks by introducing a deceptive flow, causing the adversary to waste resources and allowing valid packets to avoid being jammed. That work, however, focused on a single source selecting routing paths for real and deceptive flows. Multiple sources introducing deceptive flows leads to several challenges. First, the added deceptive flows may increase congestion and delay in the network. Second, the effect of the deceptive flow will depend on the flow allocations of other sources, resulting in a coupling between sources. For example, by introducing a deceptive flow that is jammed by an adversary, a source will not only improve its own throughput, but also the throughput of nearby sources, since the adversary will have fewer resources available to target those flows.

3 Model and Preliminaries

In this section, we introduce the network and adversary models along with relevant notations.

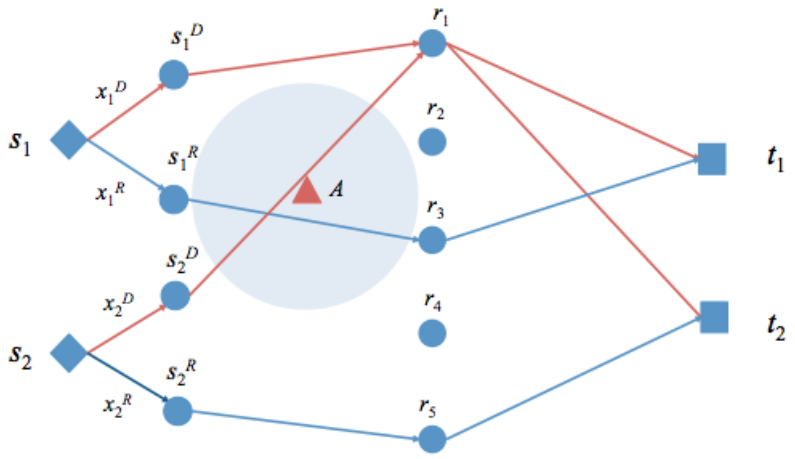

Fig. 1. Illustration of the network model with two source nodes s_1 and s_2, which transmit data to destination t_1 and t_2, respectively, via the relay network consisting of five relay nodes $r_1, r_2, \cdots, r_5$.

3.1 Network Model

We consider N source nodes, indexed in the set $\mathcal{S} = \{s_1, \ldots, s_N\}$. Source $s_i, i = 1, 2, \cdots, N$, has a corresponding destination node $d_i \in \mathcal{T}$, where $\mathcal{T} := \{t_1, t_2, \cdots, t_T\}$ denotes the set of T destinations. Each source s_i maintains a real flow to d_i, consisting of data packets, with rate x_i^R, as well as a deceptive flow consisting of randomly-generated fake packets at rate x_i^D, with $x_i^D + x_i^R \leq m_i, x_i^D \geq 0, x_i^R \geq 0$. The deceptive flow aims to deceive the attackers along the routing path between the source and destination pair in order to protect the real flow[1]. Since each source maintains two flows, we can equivalently represent each source node $s_i, i = 1, 2, \cdots, N$, with two virtual source nodes s_i^D and s_i^R, where s_i^D is the virtual node that transmits deceptive flows while s_i^R is the virtual node that sends real data. Let $\mathcal{S}^D := \{s_1^D, s_2^D, \cdots, s_N^D\}$ be the set of N deceptive source nodes , and likewise, let $\mathcal{S}^R := \{s_1^R, s_2^R, \cdots, s_N^R\}$ be the set of N real source nodes.

We consider a multi-hop relay network where sources have to send their data via intermediate nodes. Let $\mathcal{R} := \{r_1, r_2, \cdots, r_R\}$ be the set of R relay nodes deployed between sources and destinations. In general, the relay nodes can form a hierarchical structure for multi-hop routing. In this work, without loss of generality, we consider a two-hop routing scenario, where source nodes

[1] In principle, the deceptive flow could also contain duplicate copies of real packets. We assume, however, that the sources will not choose to send real packets along routes that are likely to be jammed.

first route data to relay nodes and then relay nodes to the destinations. We assume that the routing paths have been predetermined by standard routing protocols [2,6]. Let $a_i^e \in \mathcal{R}$ be the relay node chosen by the source node $s_i^e, i = 1, 2, \cdots, N, e \in \{R, D\}$, with $a_i^R \neq a_i^D$ for all $s_i \in \mathcal{S}$, and $B_j \subset \mathcal{T}$ be the set of destinations that receive packets from relay r_j. Let $\mathcal{L}_S^R$ be the set of links between sources and relays, and $\mathcal{L}_R^T$ be the set of links between relays and destinations. We can represent the routing network by the graph $\mathcal{G} := (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of vertices consisting of deceptive and real virtual source nodes, relay nodes and destinations, i.e., $\mathcal{V} := \mathcal{S}^D \cup \mathcal{S}^R \cup \mathcal{R} \cup \mathcal{T}$, and $\mathcal{E}$ is a set of data links between nodes, i.e., $\mathcal{E} := \mathcal{L}_S^R \cup \mathcal{L}_R^T$.

Each source node maintains two routes to its destination, one route for the real flow and one for the deceptive flow. The real flow of source s_i in the relay network can be represented by the set $f_i^R := \{(s_i^R, a_i^R), (a_i^R, d_i)\}, i \in \mathcal{S}$, and the deceptive flow of source s_i can be represented by the set $f_i^D := \{(s_i^D, a_i^D), (a_i^D, d_i)\}, i \in \mathcal{S}$. We let $\mathcal{F}^R := \{f_i^R, i = 1, 2, \cdots, N\}$ be the set of real flows, $\mathcal{F}^D := \{f_i^D, i = 1, 2, \cdots, N\}$ be the set of deceptive flows, and $\mathcal{F} := \mathcal{F}^D \cup \mathcal{F}^R$ be the set of flows in the relay network.

To conserve notation, we let f denote a particular flow in $\mathcal{F}$, and write x_f to denote the data rate for flow $f \in \mathcal{F}$ at the transmission rate, which may be real or deceptive. For example, the real flow $f_i^R, i \in \mathcal{S}$, has its transmission data rate $x_{f_i^R} = x_i^R$ and the data rates of deceptive flows $f_i^D, i \in \mathcal{S}$ are given by x_i^D. We let $\mathcal{L}$ denote the set of L bottleneck links in the network, and they consist of links directed to relay nodes and destination nodes. Hence $L = R + T$. We use $\mathcal{L}_f \subset \mathcal{L}$ to denote the set of those links traversed by flow $f \in \mathcal{F}$, with $\mathcal{L}_i^R \subset \mathcal{L}$ denoting the set of links traversed by real flow f_i^R and $\mathcal{L}_i^D \subset \mathcal{L}$ denoting the set of links traversed by deceptive flow f_i^D. The routes for real and deceptive flows for source i are assumed to be link-disjoint, with $\mathcal{L}_i^R \cap \mathcal{L}_i^D = \emptyset$. Each link l is assumed to have a finite capacity μ_l. Letting $\mathcal{F}_l$ denote the set of flows traversing link l, the capacity constraint can be expressed as $\sum_{f \in \mathcal{F}_l} x_f \leq \mu_l$. We assume that the delays $\tau_l \in \mathbb{R}_+$ experienced by each link follow an independent M/M/1 queueing model [9], with the delay on link l given by

$$\tau_l = \frac{1}{\bar{\mu}_l - \sum_{f \in \mathcal{F}^l} x_f}, \quad l \in \mathcal{L}, \tag{1}$$

where $\bar{\mu}_l = \mu_l - \epsilon$, for $\epsilon > 0$ sufficiently small. In addition, each source i has a capacity constraint m_i, so that $x_i^R + x_i^D \leq m_i$. The routing path of each source is represented by the routing matrix W, which is a $|\mathcal{L}| \times |\mathcal{F}|$ real matrix with a 1 in the (l, f) entry if flow f traverses link l and a 0 otherwise. The capacity constraint can be expressed in a more compact form as

$$W\mathbf{x} \leq \mu, \tag{2}$$

where $\mu = [\mu_1, \mu_2, \cdots, \mu_{|\mathcal{L}|}]$. We use $W_R \in \mathbb{R}^{|\mathcal{L}|} \times \mathbb{R}^{|\mathcal{F}^R|}$ to denote the routing matrix restricted to the set of real flows.

We illustrate the network model in Fig. 3. Sources s_1 and s_2 transmit data to destinations t_1 and t_2, respectively. Both sources split their traffic into two

flows: one is the deceptive flow containing randomly generated packets at rates x_1^D and x_2^D for sources s_1 and s_2 respectively; the other one is the legitimate flow containing the real data at rates x_1^R and x_2^R for sources s_1 and s_2 respectively. A relay network consisting of a set of relay nodes $\mathcal{R} = \{r_i, i = 1, 2, \cdots, 5\}$ is used to transmit data. The topology of the routing network can be represented by the graph $(\mathcal{V}, \mathcal{E})$, where $\mathcal{V} := \{s_1^D, s_1^R\} \cup \{s_2^D, s_2^R\} \cup \{t_1, t_2\} \cup \mathcal{R}$, and $\mathcal{E} = \{(s_1^D, r_1), (s_2^D, r_1), (s_1^R, r_3), (s_2^R, r_5), (r_1, t_1), (r_1, t_2), (r_3, t_1), (r_5, t_2)\}$. An attacker A can jam the flows within its range of influence. The network consists of four flows: $f_1^R = \{(s_1^R, r_3), (r_3, t_1)\}$, $f_1^D = \{(s_1^D, r_1), (r_1, t_1)\}$, $f_2^R = \{(s_2^R, r_5), (r_5, t_2)\}$ and $f_2^D = \{(s_2^D, r_1), (r_1, t_2)\}$, among which f_1^R and f_2^D are jammed by the attacker A. The relay network has 5 links associated with 5 relay nodes. Note that flows f_1^D and f_2^D share the same link and hence their rates are constrained by $x_{f_1^D} + x_{f_2^D} \leq \mu_1$, where μ_1 is the capacity constraint on link 1 associated with r_1.

3.2 Adversary Model

The network is deployed in the presence of an adversary mounting a jamming attack on a set of flows $\mathcal{F}_A \subseteq \mathcal{F}$. The adversary has knowledge of the routing topology for the flows in $\mathcal{F}_A$ as well as the flow rate x_f for all $f \in \mathcal{F}_A$. The adversary is capable of differentiating between packets from different flows and targeting individual packets for attack [11]. Since packets are encrypted, however, the adversary cannot differentiate between real and deceptive flows.

The adversary chooses a fraction of flow $f \in \mathcal{F}_A$ to target, denoted p_f. The cost to jam flow f is equal to $c_f p_f$, where c_f is a nonnegative constant determined by the jamming power, the distance between the jammer and the jammed receiver, and the channel characteristics. The total jamming power budget is equal to J, resulting in a jamming power constraint $\sum_{f \in \mathcal{F}_A} c_f p_f \leq J$.

We assume that the adversary does not attempt to differentiate between the real and deceptive flows by observing the flow rates or network topology, and instead assumes that all packets have an equal likelihood of being real. Otherwise, the sources could gain an advantage by choosing the rate or routing path of the deceptive flow in order to convince the adversary that it is real.

4 Game Formulation and Equilibria

In this section, the interaction between the adversary and network sources is described. We first describe the actions of the adversary, who observes the flow rates and routing topology and chooses a jamming strategy accordingly. We then discuss the actions of the sources, who determine the flow rates x_f.

4.1 Game Formulation

The deceptive jamming game consists of two stages. In the first stage, each source s_i selects real and deceptive flows x_i^R and x_i^D simultaneously. In the second stage,

the adversary observes the flow rates x_f for all $f \in \mathcal{F}_A$ and chooses the jamming rates p_f. When f is a real flow with source s_i, we write $p_f := p_i^R$, while p_i^D is the probability of jamming for a deceptive flow with source s_i. The adversary's goal is to find the optimal jamming strategy p_f^*, $f \in \mathcal{F}_A$, which is the solution to the optimization problem

$$\begin{array}{ll} \text{maximize} & \sum_{f\in\mathcal{F}_A} U_A(p_f, x_f) \\ p_f, f \in \mathcal{F}_A & \\ \text{s.t.} & \sum_{f\in\mathcal{F}_A} c_f p_f \le J \end{array} \tag{3}$$

The constant J is the adversary's total power budget. We select $U_A(p_f, x_f) = \ln p_f x_f$ for the analysis later in Section 4.3. At each source s_i, the goal is to optimize a utility function $U_i(x_i^R, x_i^D, x_{-i})$, where x_{-i} is the flow rates of the other sources. We consider two types of utility functions, selfish and altruistic. In the selfish case, source s_i's only goal is to maximize its own throughput while limiting the delay of real packets, leading to utility function

$$U_i^S(x_i^R, x_i^D, x_{-i}) = (1 - p_i^R(x_i^R, x_i^D, x_{-i}))x_i^R - \beta \sum_{l\in L_i^R} \frac{1}{\mu_l - \sum_{f\in\mathcal{F}_l} x_f}. \tag{4}$$

The second term of (4) quantifies the delay resulting from flow rates x_i^R and x_i^D, based on the M/M/1 model described in Section 3.1. In Section 4.3, a closed-form expression for the dependence of p_i^R on the x_i^R and x_i^D values will be derived. The formulation is illustrated in Figure 2(a).

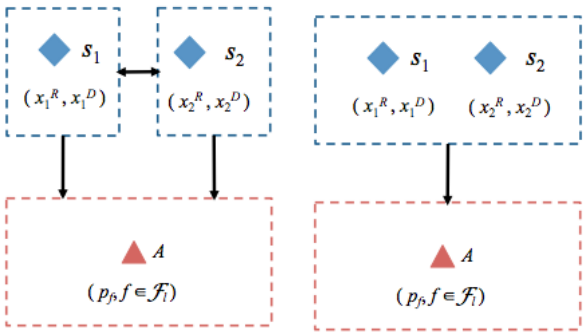

Fig. 2. Illustration of two-stage games and Stackelberg equilibrium is used as solution concept (a) Selfish source nodes: each source first decides on deceptive and real flows in a noncooperative way. (b) Cooperative source nodes: source nodes jointly optimize their data rates to achieve the best total utility. The attacker A sniffs the traffic of the network after source nodes decide on their data rates, and launches a jamming attack by choosing the power levels to affect the flows within its range of influence.

While introducing a deceptive flow on a separate path may increase the achieved throughput and reduce the error rate of a source, it will also increase the congestion, and hence the delays, experienced by the remaining sources. We denote sources that attempt to minimize the delay experienced by other sources, in addition to maximizing their own utility, as *altruistic*. An altruistic source has utility function defined by

$$U_i^T(x_i^R, x_i^D, x_{-i}) = (1 - p_i^R(x_i^R, x_i^D, x_{-i}))x_i^R - \beta \sum_{l \in L_i^R \cup L_i^D} \frac{1}{\mu_l - \sum_{f \in \mathcal{F}_l} x_f}. \quad (5)$$

The second (delay) term of (5) incorporates the delays experienced by both real and deceptive flows, as opposed to the delay term of (4) which only measures delay of real flows. The rationale is that increases in delay in fake packets are due to increased congestion, which will affect the real flows of other sources as well. Hence each source is penalized for the delays caused by fake packets. The altruistic user case is illustrated in Figure 2(b).

4.2 Equilibrium Concepts

The equilibrium concept for the game is dependent on the amount of information available to each player. For the game between the sources and the adversary, the adversary observes the sources' actions, equal to the source rates $x_1^R, x_1^D, \ldots$, before selecting a jamming strategy $p_1^R, p_1^D, \ldots$. Hence the adversary will select the jamming strategy p_f^* according to the optimization problem (3) after observing the actions of the sources.

In the case of selfish sources (see Fig. 2(a)), there are also strategic interactions among the sources. Since the sources cannot observe each others' actions before selecting real and deceptive flow rates, their interactions can be described by a normal-form game by fixing the behavior of the adversary. Hence, *Stackelberg equilibrium* solutions can be used to characterize the outcome for this $(n+1)$-person hierarchical game. Let $\tilde{\mathbf{p}}$ be a feasible action of the attacker as his response to the sources based on the attacker utility function, i.e.,

$$\tilde{p}_f = p_f^*(\mathbf{x}^R, \mathbf{x}^D), f \in \mathcal{F}_A,$$

where $\mathbf{x}^R = [x_i^R]_{i \in \{1,\ldots,N\}}, \mathbf{x}^D = [x_i^D]_{i \in \{1,\ldots,N\}}$, and $\tilde{p}_f : \mathbb{R}^{2N} \to \mathbb{R}^{|\mathcal{F}_A|}, f \in \mathcal{F}_A$, is the reaction map of the attacker.

Definition 1 (Stackelberg Equilibrium). *An action profile* $(\mathbf{x}^{R*}, \mathbf{x}^{D*}, \tilde{\mathbf{p}}) \in \mathbb{R}^{2S} \times \mathbb{R}^{|\mathcal{F}_A|}$ *is a Stackelberg equilibrium if*

$$\tilde{p}_f = p_f^*(\mathbf{x}^{R*}, \mathbf{x}^{D*}), f \in \mathcal{F}_A$$

and the source rates x_i^{R*}, x_i^{D*} *satisfy, for all* $i \in \mathcal{S}$,

$$U_i(x_i^{R*}, x_i^{D*}, \mathbf{x}_{-i}, p_f^*(x_i^{R*}, x_i^{D*}, \mathbf{x}_{-i})) \geq U_i(x_i^R, x_i^D, \mathbf{x}_{-i}, p_f^*(x_i^R, x_i^D, \mathbf{x}_{-i})), \quad (6)$$

for all feasible flow rates x_i^R, x_i^D.

4.3 Solution for Adversary

We consider an attacker with utility function $U_A = \exp\left\{\gamma \sum_{f\in\mathcal{F}_A} \alpha_f \ln x_f p_f\right\}$, where the log function reflects the fact that the adversary attempts to distribute the jamming impact among multiple flows and γ is a risk parameter. The coefficient α_f represents the relative importance of flow f, which is normalized so that $\sum_{f\in\mathcal{F}_A} \alpha_f = 1$. We define $\alpha_f = \frac{x_f}{\sum_{f'\in\mathcal{F}_A} x_{f'}}$, modeling an adversary who places a higher priority on flows that carry more network traffic.

The attacker then solves the optimization problem

$$\begin{aligned} \max_{p_f, f\in\mathcal{F}_A} \ & \exp\left\{\gamma \textstyle\sum_{x\in\mathcal{F}_A} \alpha_f \ln x_f p_f\right\}, \\ \text{s.t.} \ & \textstyle\sum_{f\in\mathcal{F}_A} c_f p_f \le J, \end{aligned} \tag{7}$$

Let $\bar{c}_f = c_f/J$. The solution to this optimization problem is given by

$$p_f = \alpha_f/\bar{c}_f. \tag{8}$$

4.4 Solution for Selfish Sources

We first consider the behavior of source nodes when each source attempts to maximize its own utility, represented by its throughput and delay. In this case, the utility of source i is given by

$$U_i^S(x_i^R, x_i^D) = (1-p_i^R)x_i^R - \beta \sum_{l\in L_i^R} \frac{1}{\mu_l - \sum_{f\in\mathcal{F}_l} x_f}.$$

Substituting the adversary's strategy for p_i^R yields

$$\begin{aligned} U_i^S(x_i^R, x_i^D) &= \left(1 - \frac{\alpha_i^R}{\bar{c}_i^R}\right) x_i^R - \beta \sum_{l\in L_i^R} \frac{1}{\mu_l - \sum_{f\in\mathcal{F}_l} x_f} \\ &= \left(1 - \frac{x_i^R}{\bar{c}_i^R \sum_{f\in\mathcal{F}_A} x_f}\right) x_i^R - \beta \sum_{l\in L_i^R} \frac{1}{\mu_l - \sum_{f\in\mathcal{F}_l} x_f} \end{aligned}$$

Furthermore, since the total flow originating at source i cannot exceed m_i, we have that each source's optimization problem, given the behavior of the other sources, is

$$\begin{aligned} \underset{x_i^R}{\text{maximize}} \ & \left(1 - \tfrac{x_i^R}{\bar{c}_i^R \sum_{f\in\mathcal{F}_A} x_f}\right) x_i^R - \beta \textstyle\sum_{l\in L_i^R} \frac{1}{\mu_l - \sum_{f\in\mathcal{F}_l} x_f} \\ \text{s.t.} \ & x_i^R + x_i^D \le m_i \end{aligned} \tag{9}$$

We observe that the objective function of (9) is strictly increasing in x_i^D, since the routes used by real and deceptive flows are link-disjoint. As a result,

the constraint $x_i^R + x_i^D \leq m_i$ will hold with equality. Moreover, in equilibrium, $x_i^R + x_i^D = m_i$ for all sources i. Letting $M = \sum_{i=1}^{N} m_i$, (9) can be rewritten as

$$\underset{x_i^R}{\text{maximize}} \left(1 - \frac{x_i^R}{M\bar{c}_i^R}\right) x_i^R - \beta \sum_{l \in L_i^R} \frac{1}{\mu_l - \sum_{f \in \mathcal{F}_l} x_f} \tag{10}$$

Taking a linear approximation around the origin to the second term, which models the case where the total data flow through each link is significantly less than the link capacity (as in sensor networks where the nodes themselves face energy constraints that prevent full utilization of the channel), yields

$$U_i^S(x_i^R) = \left(1 - \frac{x_i^R}{M\bar{c}_i^R}\right) x_i^R - \beta \sum_{l \in L_i^R} \frac{1}{\mu_l} \left(1 + \sum_{f \in \mathcal{F}_l} x_f\right) \tag{11}$$

The value of x_i^R that maximizes (11) is $x_i^R = \frac{\bar{c}_i M}{2}\left(1 - \beta \sum_{l \in L_i^R} \frac{1}{\mu_l}\right)$. Furthermore, a quadratic approximation yields

$$U_i^S(x_i^R) = \left(1 - \frac{x_i^R}{M\bar{c}_i^R}\right) x_i^R - \beta \sum_{l \in L_i^R} \frac{1}{\mu_l} \left(1 + \sum_{f \in \mathcal{F}_l} x_f + \left(\sum_{f \in \mathcal{F}_l} x_f\right)^2\right) \tag{12}$$

which attains its maximum at

$$x_i^R = \left(\frac{2}{\bar{c}_i M} + 2\beta \sum_{l \in L_i^R} \frac{1}{\mu_l^2}\right)^{-1} \left[1 - \beta \sum_{l \in L_i^R} \left(\frac{1}{\mu_l} + \frac{2\sum_{f \in \mathcal{F}_l} x_f}{\mu_l^2}\right)\right]. \tag{13}$$

Obtaining the equilibria for the games with responses (11) and (12) is equivalent to solving a system of linear equations. Define D to be a diagonal matrix with entries $D_{ii} = \left(\frac{2}{\bar{c}_i M} + 2\beta \sum_{l \in L_i^R} \frac{1}{\mu_l^2}\right)^{-1}$. Then (13) can be rewritten as

$$x_i^R = D_{ii} \left(1 - \beta \sum_{l \in \mathcal{L}} \frac{W_{il}}{\mu_l} - 2\beta \sum_{l \in \mathcal{L}} \left[\frac{W_{il}}{\mu_l^2} \sum_{f \in \mathcal{F}} W_{fl} x_f\right]\right).$$

Multiplying by W_{il} and W_{fl} allows us to sum over all entries in $\mathcal{F}$ and $\mathcal{L}$. Let U be a diagonal matrix with entries $U_{ll} = \mu_l$. Since the flow rates satisfy $x_i^R + x_i^D = m_i$, define

$$Z = \begin{pmatrix} 1 & 0 \cdots & 0 \\ -1 & 0 \cdots & 0 \\ & \vdots & \\ 0 & 0 \cdots & 1 \\ 0 & 0 \cdots & -1 \end{pmatrix}, \qquad \mathbf{m} = \begin{pmatrix} 0 \\ m_1 \\ \vdots \\ 0 \\ m_n \end{pmatrix},$$

where $Z \in \mathbf{R}^{2n \times 2n}$ and $\mathbf{m} \in \mathbf{R}^{2n}$, so that $\mathbf{x} = Z\mathbf{x}^R + \mathbf{m}$. Finally let ν be a vector with $\nu_l = 1/\mu_l$. Then the vector of real flow rates can be obtained by solving the matrix equation

$$(I + 2\beta D W_R^T (U^2)^{-1} W Z)\mathbf{x}_R = D(\mathbf{1} - \beta W_R^T \nu - 2\beta W_R^T (U^2)^{-1} W \mathbf{m}). \quad (14)$$

In the case where the quadratic approximation does not hold, the Stackelberg equilibrium of the game with selfish sources can be computed by observing that the best-response optimization problems (10) for each source define a potential game, with potential function

$$\Phi(x_1^R, \ldots, x_N^R) = \sum_{i=1}^{N} x_i^R \left(1 - \frac{x_i^R}{M\bar{c}_i^R}\right) - \beta \sum_{l \in \mathcal{L}} \frac{1}{\mu_l - \sum_{f \in \mathcal{F}_l} x_f} \quad (15)$$

Computing the equilibrium of the selfish-user game is equivalent to solving the optimization problem

$$\begin{array}{ll} \text{maximize} & \sum_{i=1}^{N} x_i^R \left(1 - \frac{x_i^R}{M\bar{c}_i^R}\right) - \beta \sum_{l \in \mathcal{L}} \frac{1}{\mu_l - \sum_{f \in \mathcal{F}_l} x_f} \\ x_1^R, \ldots, x_N^R & \\ \text{s.t.} & 0 \le x_i^R \le m_i \end{array} \quad (16)$$

Since the potential function $\Phi(\cdot)$ is a strictly concave function of $x_1^R, \ldots, x_N^R$, the optimization problem (16) has a unique solution that can be computed efficiently.

4.5 Solution for Altruistic Sources

When the sources behave altruistically, the utility function for source s_i is given by (5). In this case, we observe that the utility of s_i is no longer increasing in x_i^D, and hence we may have $x_i^R + x_i^D < m_i$. The best response of s_i to the other sources and the attacker is then given by the optimization problem

$$\begin{array}{ll} \text{maximize} & \left(1 - \frac{x_i^R}{\sum_{f \in \mathcal{F}_A} x_f \bar{c}_i^R}\right) x_i^R - \beta \sum_{l \in L_i^R \cup L_i^D} \frac{1}{\mu_l - \sum_{j \in \mathcal{F}_l} x_f} \\ x_i^R, x_i^D & \\ \text{s.t.} & Wx \le \mu \\ & x_i^R + x_i^D \le m_i \;\; i = 1, \ldots, N \end{array} \quad (17)$$

Lemma 1. *The utility function U_i^T is a strictly concave function of x_i^R and x_i^D.*

Proof. The function $(x_i^R)^2 / \sum_{f \in \mathcal{F}} x_f$ is a quadratic-over-linear function, and hence is strictly convex, implying that the first term of U_i^T is strictly concave. The concavity of the second term can be verified by computing its second derivative.

Lemma 1 yields the following theorem.

Theorem 1. *The simultaneous-move game, in which player s_i has utility function U_i^T, has a pure-strategy Stackelberg equilibrium.*

Proof. By [1, Theorem 4.4], an equilibrium in pure strategies exists if the set of feasible flow allocations $(x_1^R, x_2^R, \ldots)$ is compact and convex and the utility function U_i^T is a strictly concave function of x_i^R and x_i^D. The second condition holds by Lemma 1. The set of feasible flow allocations is convex and closed due to the convexity of the constraints $W\mathbf{x} \leq \mu$ and $0 \leq x_i^R + x_i^D \leq m_i$. Furthermore, since $0 \leq x_i^R, x_i^D \leq m_i$ for all i, the set of feasible flow allocations is bounded, and hence compact.

A heuristic algorithm for approximating a solution to the altruistic sources game is as follows. Each source initializes its flow rate to a feasible value, such as 0. At each iteration, each source computes its best-response to the observed flows of the other sources, based on (17). The algorithm terminates when no source can improve its utility by changing its strategy, or after a fixed number of iterations. The algorithm is summarized in Figure 3.

Approximate-Equilibrium: Algorithm for approximating a Stackelberg equilibrium when sources are altruistic.
Input: Link capacities μ, source capacities m_i, $i = 1 \ldots, N$
Routing matrix W, number of iterations K
Output: Real flow rate x_i^R and deceptive flow rate x_i^D for each $s_i \in \mathcal{S}$

$x_i^R, x_i^D \leftarrow 0$, $\forall i = 1, \ldots, N$, $k \leftarrow 0$
while $k < K$
 $b \leftarrow 0$
 for $i = 1, \ldots, N$
 $x_i^{R,old} \leftarrow x_i^R$, $x_i^{D,old} \leftarrow x_i^D$
 x_i^R, $x_i^D \leftarrow$ solution to (17) with x_{-i}^R, x_{-i}^D as input
 $b \leftarrow 1$ **if** $x_i^R \neq x_i^{R,old}$ or $x_i^D \neq x_i^{D,old}$
 end for
 if $b == 0$
 exit while loop; **return** $x_1^R, x_1^D, \ldots, x_N^R, x_N^D$
end while
return $x_1^R, x_1^D, \ldots, x_N^R, x_N^D$

Fig. 3. Algorithm for approximating a Stackelberg equilibrium of the altruistic sources game.

We observe that the sources can update their rates in an arbitrary order (i.e., source 1 does not have to update first, as in Figure 3).

5 Simulation Results

We illustrate our proposed approach through a Matlab simulation study. We consider a network with four sources, four relays, and one destination. Each source has a capacity of 1. All network links have equal capacity, which we

varied from $\mu = 2$ to $\mu = 3$. We simulated both selfish and altruistic sources, with trade-off parameter $\beta = 1$. An adversary is assumed to be active in the presence of the relay nodes, with jamming cost proportional to the square of its distance to each relay. The adversary's jamming budget is normalized to 1.

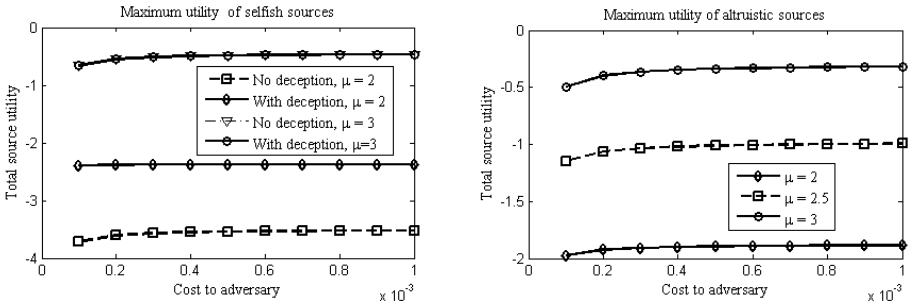

Fig. 4. Illustration of our proposed approach for a network of four sources, four relays, and one destination, with $\beta = 1$ and adversary cost proportional to the distance to each relay. (a) Case where sources are selfish. The utility achieved by the sources increases as the capacities of links and the adversary's cost increase. Deception increases the source utilities. (b) Case of altruistic sources. The utility achieved is higher on the average than the utility of selfish sources.

Figure 4(a) shows the utility achieved by selfish sources. The benefit of deception is reflected by an increase in utility. Each source's utility increases as the adversary's cost of jamming increases, since the adversary requires more power to jam the deceptive flows. Furthermore, a higher capacity results in lower delays, further increasing the utility. In the case where the capacities are low, the use of deceptive flows increases the utility of the sources. Increasing the capacity reduces the benefit of deception.

We also observe that altruistic sources yield higher overall utility (Figure 4(b)), since these sources minimize the congestion and delays caused by deceptive flows. As in the selfish source case, an increase in the adversary's cost results in higher utility for the sources. An increase in link capacity will also result in lower delays and higher throughput, increasing the source utility.

6 Conclusion

In this paper, we have studied the problem of mitigating jamming attacks through deception. We considered a defense mechanism in which each source generates a false traffic flow, causing the attacker to expend resources targeting a deceptive flow and enabling real packets to avoid jamming. We formulated deceptive jamming as a two-stage game between the sources and the jammer. In the first stage, the sources simultaneously choose both real and deceptive

flow rates to maximize throughput and minimize delay. In the second stage, the attacker observes the real and deceptive flow rates and selects a jamming strategy, represented by the fraction of each flow to jam. We derived a closed-form expression for the attacker's optimal strategy, which shows the fraction of the adversary's jamming resources that will be used to target deceptive flows, as well as the additional throughput of the real flows resulting from using deception. For the sources, we proved the existence of pure-strategy Stackelberg equilibria for two cases, namely the case where each source allocates flow in order to maximize its own utility (selfish users) and the case where each source incorporates the congestion of other sources when choosing a flow rate (altruistic users). We proposed algorithms for computing the equilibria for both cases, resulting in efficient methods for allocating real and deceptive flows at each source in order to maximize throughput and minimize delay. We illustrated our approach through a simulation study. Our simulations show that altruistic behavior improves the overall utility of the sources. In future work, we intend to analyze the loss of efficiency caused by selfish source behavior, and develop metrics for quantifying the value of deception. We will also study the case where the sources have imperfect information regarding the adversary's utility function and cost.

References

1. Başar, T., Olsder, G.J.: Dynamic Noncooperative Game Theory, vol. 23. Society for Industrial and Applied Mathematics (SIAM) (1999)
2. Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., Viennot, L.: Optimized link state routing protocol for ad hoc networks. In: Proceedings of IEEE International Multi-Topic Conference (INMIC) 2001
3. Liu, Y., Ning, P., Dai, H., Liu, A.: Randomized differential dsss: Jamming-resistant wireless broadcast communication. In: Proceedings of the 29th IEEE Conference on Computer Communications (INFOCOM) 2010. pp. 1–9
4. Noubir, G., Rajaraman, R., Sheng, B., Thapa, B.: On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming. In: Proceedings of the 4th ACM Conference on Wireless Network Security (WiSec). pp. 97–108. ACM (2011)
5. Pelechrinis, K., Iliofotou, M., Krishnamurthy, S.: Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys and Tutorials 13(2), 245–257 (2011)
6. Perkins, C., Royer, E.: Ad-hoc on-demand distance vector routing. In: Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA). pp. 90–100 (1999)
7. Poisel, R.: Modern Communications Jamming Principles and Techniques. Artech House Publishers (2011)
8. Pöpper, C., Strasser, M., Čapkun, S.: Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. IEEE Journal on Selected Areas in Communications (JSAC) 28(5), 703–715 (2010)
9. Ross, S.: Introduction to Probability Models. Academic Press (2009)
10. Tague, P., Nabar, S., Ritcey, J., Poovendran, R.: Jamming-aware traffic allocation for multiple-path routing using portfolio selection. IEEE/ACM Transactions on Networking 19(1), 184–194 (2011)

11. Tague, P., Slater, D., Poovendran, R., Noubir, G.: Linear programming models for jamming attacks on network traffic flows. In: Proceedings of the 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt). pp. 207–216. IEEE (2008)
12. Xu, W., Wood, T., Trappe, W., Zhang, Y.: Channel surfing and spatial retreats: defenses against wireless denial of service. In: Proceedings of the 3rd ACM Workshop on Wireless Security (WiSE). pp. 80–89. ACM (2004)
13. Zhu, Q., Clark, A., Poovendran, R., Başar, T.: Deceptive routing games. to appear in Proceedings of IEEE Conference on Decision and Control (CDC), Maui, Hawaii (2012)