Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 453947, 14 pages
doi:10.1155/2011/453947

Research Article

MAC Layer Jamming Mitigation Using a Game Augmented by Intervention

Zhichu Lin and Mihaela van der Schaar

Department of Electrical Engineering, University of California Los Angeles (UCLA), Los Angeles, CA 90095-1594, USA

Correspondence should be addressed to Zhichu Lin, linzhichu@gmail.com

Received 13 April 2010; Revised 21 August 2010; Accepted 11 November 2010

Academic Editor: Ashish Pandharipande

MAC layer jamming is a common attack on wireless networks, which is easy to launch by the attacker and which is very effective in disrupting the service provided by the network. Most of the current MAC protocols for wireless networks, for example, IEEE 802.11, do not provide sufficient protection against MAC layer jamming attacks. In this paper, we first use a non-cooperative game model to characterize the interactions among a group of self-interested regular users and a malicious user. It can be shown that the Nash equilibrium of this game is either inefficient or unfair for the regular users. We introduce a policer (an intervention user) who uses an intervention function to transform the original non-cooperative game into a new *non-cooperative game augmented by the intervention function*, in which the users will adjust to play a Nash equilibrium of the augmented game. By properly designing the intervention function, we show that the intervention user can effectively mitigate the jamming attacks from the malicious user, and at the same time let the regular users choose more efficient transmission strategies. It is proved that any feasible point in the rate region can be achieved as a Nash equilibrium of the augmented game by appropriately designing the intervention.

1. Introduction

Due to the broadcast nature of the wireless medium, wireless networks are not only sensitive to the mutual interferences among the legitimate (regular) users, but also highly vulnerable to malicious attacks from adversarial users. Malicious attacks are usually more detrimental than interference from legitimate users because they *intentionally* disrupt the network service. One of the most effective and simple attacks on wireless networks is a Denial-of-Service (DoS) or jamming attack [1]. These attacks from one or more adversarial users make a network and its service unavailable to the legitimate users. DoS attacks can be carried out at different layers of the wireless networks. For example, a DoS attack at the physical layer [2] can be launched by a wireless jammer which sends high power signal to cause an extremely low signal-to-interference and noise ratio (SINR) at a legitimate user's receiver. A MAC layer DoS attacker [1, 3] can disrupt legitimate users' packet transmission by sending jamming packets to a contention-based network. At the application layer, a brute force DoS attack [4] is to flood a network with an overwhelming number of requests of service.

In this paper, we will focus on mitigating MAC layer DoS attacks, for the following reasons: (i) unlike a physical layer jammer, a MAC layer jammer does not need special hardware such as directional antenna or power amplifier, hence it can be easily implemented and deployed; (ii) higher-layer antijamming techniques will simply fail if MAC layer is not well-protected from jamming attacks; most importantly, (iii) the existing IEEE 802.11 MAC protocol, which is widely adopted in most current wireless ad hoc networks, does not provide sufficient protection to even simple and oblivious jamming attacks, as shown in [5].

Various research works have been devoted to analyzing the performance of wireless networks under MAC layer jamming attacks, and designing new protocols to defend against these attacks. The performance of the current 802.11 protocol under jamming attacks is analyzed in [5], and it shows that 802.11 protocol is vulnerable even to simple jamming schemes. The damages of various DoS attacks to both TCP and UDP flows are also evaluated in [6]. In [7], a

cross-layer protocol-hopping scheme is proposed to provide resiliency to jamming attacks in wireless networks. However, this approach can significantly complicate the protocols of all the users. Optimal jamming attack and defense strategies are developed in [1] by formulating a game between attacker and defenders in wireless sensor networks. Reactive and proactive jamming mitigation methods are compared in [8] in multi-radio wireless networks using max-min game formulation. There are also research works focusing on physical layer jamming. For example, a nonzero-sum power-control game between a legitimate user and a jammer is analyzed in [2].

In this paper, we propose a novel method to mitigate MAC layer jamming attacks in a contention-based (e.g., ALOHA) network. Unlike the above mentioned existing techniques and protocols to combat MAC layer jamming, which all require modifications to the protocol stack or algorithms of existing legitimate users, our proposed method introduces a new intervention user which allows the legitimate users to keep their protocols unchanged. The intervention user designs an intervention rule which prescribes the desired transmission strategies of all the other users in the network. The intervention rule is announced to all the users or learned by them through repeated interactions. After the legitimate and malicious users act, the intervention is implemented according to their actions. The objective of the intervention user is to appropriately shape the incentive of both legitimate and malicious users such that the legitimate users can achieve higher utilities. Our solution does not require any assumption about the utility functions of legitimate users, therefore it can be applied to networks with various applications.

The idea of using an intervention user to networking problems was first introduced in [9], where an intervention function transforms a non-cooperative contention game into an augmented game with intervention, and the Nash equilibriums of the augmented game are shown to be more efficient than the Nash equilibriums of the original game. With similar network settings, the main difference between this paper and [9] is that the users in [9] are all *self-interested*, but they do not intend to decrease the utilities of other users; however, in this work we consider a non-cooperative game with *malicious* users, who intentionally try to decrease the utilities of all the other users. This key difference leads to some important distinctions between our intervention function and the one in [9]. For example, in [9] when all the other users transmit according to the target strategies set by the intervention user, the intervention user will not intervene; however, in our case with a malicious user, the intervention user has to intervene even when its target strategies are fulfilled by all the other users. In this paper, we also show that a single intervention function can intervene in order to shape the behavior of both the self-interested regular users and malicious users. Hence, the proposed solution can mitigate the adversarial attacks from the malicious users, while at the same time help to avoid network collapse caused by selfish behaviors of regular users. Furthermore, we consider a multi-channel case in which multiple malicious users may exist.

The rest of this paper is organized as follows. In Section 2, the considered network setting is described and the problem is formulated as a non-cooperative game, and an intervention user is introduced to transform the original game into an augmented game. Section 3 investigates the benefit of introducing intervention user in the single channel case, and it is shown that by using a properly designed intervention function, any point in the feasible rate region can be achieved as a Nash equilibrium of the augmented game. The solution is extended to multi-channel case in Section 4. Section 5 discussed the information requirement for different users to play the original and also the augmented game. Some illustrative numerical examples are given in Sections 6 and 7 concludes the paper.

2. Problem Formulation

2.1. Network Setting. We consider a set $\mathcal{N} = \{1, 2, \ldots, N\}$ of users sharing a group of independent channels $\mathcal{K} = \{1, 2, \ldots, K\}$. The network is slotted and the time slots are synchronized across all the channels [10]. For user n, we let $\mathcal{K}_n \in \mathcal{K}$ denote the set of channels it can access, and we assume that these $\{\mathcal{K}_n\}_{n\in\mathcal{N}}$ do not change over time. When a user has traffic to transmit at the beginning of a time slot, it will choose one of the channels it can access to transmit the packet. We let P^n $(0 \le P^n \le 1)$ be the probability that user n has traffic to transmit at a certain time slot (or its traffic load), and let $p_{n,k}$ be the probability that user n transmits on channel k. For simplicity, we let $\mathbf{p}_n = (p_{n,1}, \ldots, p_{n,K})$ the *transmission strategy* for user n, $\mathbf{p} = (\mathbf{p}_1, \ldots, \mathbf{p}_N)$ be the strategy profile of all the users, and $\mathbf{p}_{-n}$ the strategy profile for all the users in $\mathcal{N}$ other than user n. We denote $\mathcal{P}_n$ as the set of all possible transmission strategies of user n, that is,

$$\mathcal{P}_n = \left\{ \mathbf{p}_n \mid \sum_{k\in\mathcal{K}_n} p_{n,k} \le P^n, p_{n,k} = 0 \ \ (k \ne \mathcal{K}_n) \right\} \quad (1)$$

and $\mathcal{P}$ as the set of all the possible strategy profiles across all the users.

We assume that we have a slotted-ALOHA-type MAC [11, 12]. Hence, a transmission is successful if and only if there is only one user transmitting in a certain time slot.

The set of users $\mathcal{N}$ consists of both regular and malicious users, and they have different interests. The users $\mathcal{N}_{\text{reg}} = \{1, 2, \ldots, N-1\}$ are *regular* (i.e., legitimate) users, and user n's utility is defined as a function of its average throughput (over all the channels), that is, the utility for user n is

$$u_n(\mathbf{p}) = U_n\left(\sum_{k\in\mathcal{K}_n} p_{n,k} \prod_{m\ne n} (1 - p_{m,k}) \right), \quad \text{for } 1 \le n \le N-1, \quad (2)$$

where U_n is an increasing function. As noted in [13], not all network applications have concave utilities. For example, delay-tolerant applications (also referred to as *elastic* traffic, and including file transfer, email service, etc.) usually have diminishing marginal improvement with increasing rate, which results in concave utility functions; on the other

hand, some applications (referred to as *inelastic* traffic, and including real-time video transmission, online games, etc.) have stringent delay deadlines and their performances degrade greatly when the rate is below a certain threshold, which makes their utilities nonconcave [13, 14]. Hence, we do not make any further assumption about the concavity of U_n. Note that our assumptions for the regular user's utility function also includes the case of heterogeneous regular users, in which regular users can have different utility functions u_n due to their applications, and so forth.

The user N is a *malicious* user whose objective is to decrease the sum utility of all the regular users. Since the utility functions of the regular users are usually unknown to the malicious user, we assume that the malicious user can only observe the sum throughput of all the regular users (This can be done, as shown in [15], by listening to the wireless medium and estimating the probability that there is a successful transmission), and try to lower the sum throughput by transmitting its jamming packets. We assume the malicious user has a certain power budget P^N, and hence the set of all possible transmission strategies of the malicious user can be defined as $\mathcal{P}_N = \{\mathbf{p}_N \mid \sum_{k=1}^{K} p_{N,k} \le P^N\}$. We also assume the malicious user has a transmission cost which is linear to its total transmission power. Therefore, we can define the utility of the malicious user similar to the formulation in [2], as

$$u_N(\mathbf{p}) = U_N\left(\sum_{k=1}^{K} q_k(\mathbf{p}_{-N})(1-p_{N,k})\right) - c_N\left(\sum_{k=1}^{K} p_{N,k}\right), \quad (3)$$

where $\mathbf{p}_N = (p_{N,1}, \ldots, p_{N,K})$ is the jamming strategy of the malicious user, c_N is the cost of user N for each unit of its transmission, and $q_k(\mathbf{p}_{-N}) = \sum_{n=1}^{N-1} p_{n,k} \prod_{m=1, m\neq n}^{N-1} (1-p_{m,k})$ is the sum-throughput of all the regular users over channel k if there is no jamming attack. We note that the form of function U_N depends on regular users' utility functions. For example, if there is only one regular user then the malicious user can have $U_N(r) = U_1(r_{\max}) - U_1(r)$, where $r_{\max}$ is the maximum rate which the regular user can get. We can find out that if $U_1(r)$ is concave then $U_N(r)$ is a convex function; if $U_1(r)$ is nonconcave, $U_N(r)$ is also not convex. Since we do not make any assumption about the concavity of U_n, U_N can also be convex or non-convex, depending on whether the malicious user models regular users traffic as elastic or inelastic traffic. We also assume that $U_N(r)$ satisfies the following conditions in its domain $(0, +\infty)$:

(1) $U_N(r)$ is continuous and differentiable;

(2) $U_N(r) \ge 0$ for any $r \ge 0$ and it is decreasing in r.

2.2. A Non-Cooperative Game Model. We use a non-cooperative game model to characterize the behavior of both the self-interested regular users and also the malicious user. We define the non-cooperative game by the tuple $\Gamma = \langle \mathcal{N}, (\mathcal{P}_n), (u_n) \rangle$, where $\mathcal{N}$, $\mathcal{P}_n$, and u_n are defined as in Section 2.1. It is easy to show that Γ is a nonzero-sum game (similar to the formulation in [2]), because of the transmission cost of the malicious user.

Each user in the game Γ chooses its best-response transmission strategy $\mathbf{p}_n^{BR}$ to maximize its utility by taking all the other users' transmission strategies $\mathbf{p}_{-n}$ as given, that is,

$$\begin{aligned}\mathbf{p}_n^{BR}(\mathbf{p}_{-n}) &= \arg\max_{\mathbf{p}_n} u_n(\mathbf{p}_n, \mathbf{p}_{-n}) \\ &= \arg\max_{\mathbf{p}_n} U_n\left(\sum_{k\in\mathcal{K}_n} p_{n,k} \prod_{m\neq n} (1-p_{m,k})\right)\end{aligned} \quad (4)$$

for the regular users, and

$$\begin{aligned}&\mathbf{p}_N^{BR}(\mathbf{p}_{-N}) \\ &= \arg\max_{\mathbf{p}_N} u_N(\mathbf{p}_N, \mathbf{p}_{-N}) \\ &= \arg\max_{\mathbf{p}_N}\left[U_N\left(\sum_{k=1}^{K} q_k(\mathbf{p}_{-N})(1-p_{N,k})\right) - c_N\left(\sum_{k=1}^{K} p_{N,k}\right)\right]\end{aligned} \quad (5)$$

for the malicious user. The outcome of this non-cooperative game can be characterized by the solution concept of *Nash equilibrium* (NE), which is defined as any strategy profile $\mathbf{p}^{\mathrm{NE}} = (\mathbf{p}_1^{\mathrm{NE}}, \ldots, \mathbf{p}_N^{\mathrm{NE}})$ satisfying

$$u_n\left(\mathbf{p}_n^{\mathrm{NE}}, \mathbf{p}_{-n}^{\mathrm{NE}}\right) \ge u_n\left(\mathbf{p}_n, \mathbf{p}_{-n}^{\mathrm{NE}}\right), \quad \text{for any } \mathbf{p}_n \in \mathcal{P}_n,\ n \in \mathcal{N}. \quad (6)$$

It is straightforward to verify that this definition is equivalent to

$$\mathbf{p}_n^{\mathrm{NE}} = \mathbf{p}_n^{BR}\left(\mathbf{p}_{-n}^{\mathrm{NE}}\right), \quad \text{for any } n \in \mathcal{N}. \quad (7)$$

Note that the game we defined in the paper is generally not zero-sum, because we do not make specific assumptions about either the regular or malicious user's utility function. However, if their utility functions are chosen such that the game is zero-sum, all the analysis and results still apply. Hence if the game is zero-sum, it will just be a special case of the game we defined.

Existing research has investigated the inefficiency of Nash equilibrium in various networking problems [9, 16]. We will next introduce an intervention user to transform the game Γ into a new game which can yield higher utility for regular users at its equilibriums. Later we will also discuss how the same intervention user can mitigate the jamming effect while simultaneously leading the regular users to play a more efficient equilibrium.

2.3. A Non-Cooperative Game Augmented by an Intervention User. We introduce an intervention user (user 0), which has an intervention function $g : \mathcal{P} \to \mathcal{P}_0$, where $\mathcal{P}_0$ is the set of all the possible transmission strategies of the intervention user within its power budget P^0, that is, $\mathcal{P}_0 = \{\mathbf{p}_0 \mid \sum_{k=1}^{K} p_{0,k} \le P^0\}$. We assume that user 0 can access any channel in $\mathcal{K}$, that is, $\mathcal{K}_0 = \mathcal{K}$. The intervention user's transmission strategy (also referred to as *intervention level*) is given by $\mathbf{p}_0 = (p_{0,1}, \ldots, p_{0,K}) = g(\mathbf{p})$. Hence, the intervention

Table 1: The timing of the game with intervention user.

At the beginning of a time-slot
(a) the intervention user determines its intervention function g and announces it to all the regular and malicious users;
(b) knowing the intervention function, each user chooses its own transmission strategy;
(c) intervention user calculates its intervention level after observing all the users' strategies;
During the time slot
(d) all the users transmit according to its selected strategy;
At the end of the time slot
(e) all the users payoffs are realized

function can be considered as a reaction to all the regular and malicious users' *joint* transmission strategy. The idea of using intervention function in networking problems was first investigated by [9], in which an intervention user was introduced to prevent the regular users from playing at inefficient Nash equilibriums in contention-based networks. In this paper, besides enforcing the regular users to behave less selfishly, the intervention user also prevents the malicious user from jamming the regular users with a high transmission rate.

In each time-slot, the new game augmented by an intervention user is played as in Table 1. If the set-up time, that is, the duration before (d), is negligibly short compared to a time-slot, then the new utility functions of the regular users can be defined in a similar way as u_n, but taking the intervention into account, that is,

$$\widetilde{u}_n(\mathbf{p},g) = U_n\left(\sum_{k\in\mathcal{K}_n} p_{n,k}(1-p_{0,k})\prod_{m\neq n}(1-p_{m,k})\right), \quad (8)$$

for $1 \le n \le N-1$. The intervention level $\mathbf{p}_0 = (p_{0,1},\ldots,p_{0,K})$ is determined by intervention function g as

$$\mathbf{p}_0 = (p_{0,1},\ldots,p_{0,K}) = g(\mathbf{p}). \quad (9)$$

For the malicious user, we will have the following utility after considering the intervention:

$$\widetilde{u}_N(\mathbf{p},g) = U_N\left(\sum_{k=1}^{K} q_k(\mathbf{p}_{-N})(1-p_{N,k})(1-p_{0,k})\right) - c_N\left(\sum_{k=1}^{K} p_{n,k}\right), \quad ((p_{0,1},\ldots,p_{0,K}) = g(\mathbf{p}_N)). \quad (10)$$

The introduction of the intervention user (and its intervention function g) transforms the game $\Gamma = \langle\mathcal{N},(\mathcal{P}_n),(u_n)\rangle$ into a new game $\widetilde{\Gamma}_g = \langle\mathcal{N},(\mathcal{P}_n),(\widetilde{u}_n(\mathbf{p},g))\rangle$. We call the game $\widetilde{\Gamma}_g$ an *non-cooperative game augmented by an intervention function g*. The intervention user has a target strategy profile $\widetilde{\mathbf{p}}$, and its objective is to let all the other players operate according to its target strategy, while applying a minimal level of intervention. A strategy profile $\widetilde{\mathbf{p}}^{\mathrm{NE}}$ is a Nash equilibrium of the augmented game $\widetilde{\Gamma}_g$ if

$$\widetilde{u}_n\left(\widetilde{\mathbf{p}}_n^{\mathrm{NE}},\widetilde{\mathbf{p}}_{-n}^{\mathrm{NE}},g\right) \ge \widetilde{u}_n\left(\mathbf{p}_n,\widetilde{\mathbf{p}}_{-n}^{\mathrm{NE}},g\right), \quad \text{for any } \mathbf{p}_n\in\mathcal{P}_n,\ n\in\mathcal{N}. \quad (11)$$

Table 2: Key notations.

User 1, 2, …, $N-1$: regular users
User N: intervention user
User 0: intervention user
$\mathcal{K} = \{1,2,\ldots,K\}$: set of channels
$\mathbf{p}_n$: user n's transmission strategy
u_n: user n's utility function
$g : \mathcal{P} \to \mathcal{P}_0$: intervention function
$\Gamma = \langle\mathcal{N},(\mathcal{P}_n),(u_n)\rangle$: the non-cooperative game
$\widetilde{\Gamma}_g = \langle\mathcal{N},(\mathcal{P}_n),\widetilde{u}_n\rangle$: the augmented non-cooperative game
$\widetilde{\mathbf{p}}$: intervention user's target strategy profile

In the following sections, we will show that with a properly designed intervention function, the regular users can get higher payoffs at an NE of game $\widetilde{\Gamma}_g$ than at an NE of the original game Γ.

We have summarized some key notations in this section in Table 2.

3. The Single Channel Case

3.1. Using Intervention to Mitigate Malicious Jamming. We first consider a single channel case ($\mathcal{K} = \{1\}$) and assume that the malicious and intervention user have $P^0 = P^N = 1$. The intervention user's objective is to *both* mitigate jamming as well as to enforce regular users to play a more efficient equilibrium. Hence, we first assume that regular users' strategies are fixed and investigate how an intervention user can mitigate the malicious jamming and how much performance gain for the regular users can be achieved by using intervention. In Section 3.2, we will discuss how the intervention user can enforce the regular users to comply with certain desirable target strategies.

Since we assume that all the regular users' transmission strategies are fixed as $\mathbf{p}_{-N} = \{p_1,p_2,\ldots,p_{N-1}\}$, we have the malicious user's utility (when there is no intervention) as

$$u_N(p_N) = U_N(q(\mathbf{p}_{-N})(1-p_N)) - c_N p_N \quad (12)$$

with $q(\mathbf{p}_{-N}) = \sum_{n=1}^{N-1} p_n\prod_{m=1,m\neq n}^{N-1}(1-p_m)$. For simplicity, we will use from now on q instead of $q(\mathbf{p}_{-N})$ when there is no ambiguity, and we also let $y_q(p_N) = U_N(q(\mathbf{p}_{-N})(1-p_N))$. Hence, the utility function can be rewritten as $u_N(p_N) = y_q(p_N) - c_N p_N$.

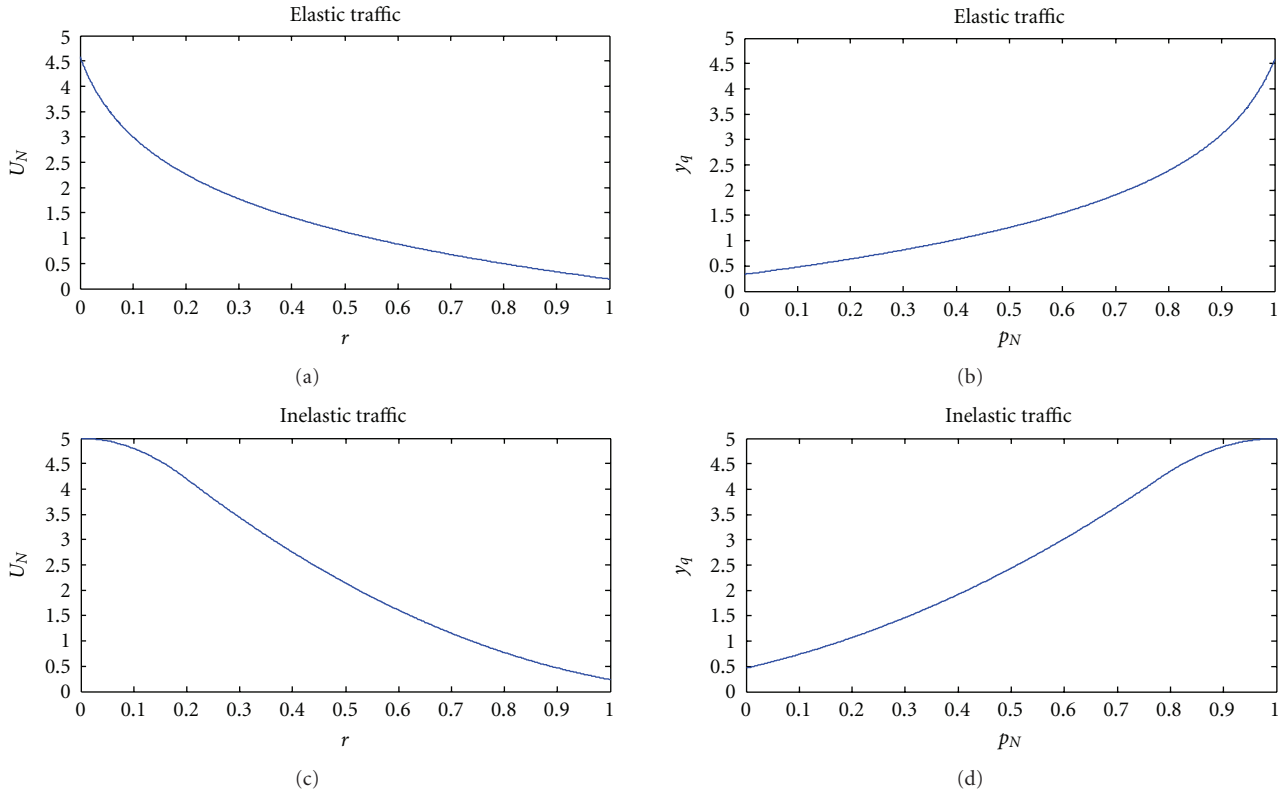


Figure 1: Two examples of $U_N(r)$ and $y_q(p_N)$.

From the properties of U_N, we can easily verify that given q, $y_q(p_N)$ should satisfy the following properties over its domain in its domain $[0,1]$:

(1) $y_q(p_N)$ is continuous and differentiable;

(2) $y_q(p_N)$ is increasing in p_N and $U_N(q) \le y_q(p_N) \le U_N(0)$ for any $p_N \in [0,1]$;

(3) $y_q(p_N)$ is concave (convex) if $U_N(r)$ is concave (convex).

In Figure 1, we give two examples of $U_N(r)$ and its corresponding $y_q(p_N)$. (We let $q = 0.9$ in both examples.) If the malicious user models the regular users' traffic as elastic traffic, both $U_N(r)$ and $y_q(p_N)$ will be convex functions (Figures 1(a) and 1(b)); if it models regular users' traffic as inelastic, both $U_N(r)$ and $y_q(p_N)$ are non-convex (Figures 1(c) and 1(d)).

Hence, given q, the malicious user's optimal jamming strategy when there is no intervention can be obtained by solving the following optimization problem:

$$p_N^* = \arg\max_{p_N} y_q(p_N) - cp_N \quad \text{s.t.} \quad 0 \le p_N \le 1. \tag{13}$$

Generally, this optimization problem is not convex because we do not make any assumption about the concavity of $U_N(r)$ and hence $y_q(p_N)$ can be nonconcave. Therefore, an explicit solution to (13) may not always exist. Fortunately, our following results only require $y_q(p_N)$ to be monotonically increasing, and hence they can be applied to networks with either elastic or inelastic traffic.

Since the regular users' transmission strategies are fixed, the intervention function reduces to a function of p_N, that is, $p_0 = g(p_N)$ with $g : [0,1] \to [0,1]$. The malicious user's utility will be

$$\tilde{u}_N(p_N, g) = \tilde{y}_q(p_N, g) - c_N p_N \tag{14}$$

with

$$\tilde{y}_q(p_N, g) = U_N(q(1-p_N)(1-g(p_N))). \tag{15}$$

We note that the properties (3)–(5) $y_q(p_N)$ are not necessarily satisfied for $\tilde{y}_q(p_N, g)$. For example, $\tilde{y}_q(p_N, g)$ may not be monotonically increasing in p_N.

The optimal strategy of the malicious user with intervention function g is

$$\tilde{p}_N^*(g) = \arg\max_{p_N} \tilde{y}_q(p_N, g) - cp_N \quad \text{s.t.} \quad 0 \le p_N \le 1. \tag{16}$$

We can have the following lemma which shows that given the same q and p_N, the malicious user's utility will not decrease if an intervention function g is applied.

Lemma 1. *For any fixed q and $p_N, q, p_N \in [0,1]$, and any intervention function g, $y_q(p_N) \le \tilde{y}_q(p_N, g) \le y_q(1)$.*

Conversely, for any function $f(p_N)$ that satisfies $y_q(p_N) \le f(p_N) \le y_q(1)$ for any $0 \le p_N \le 1$, there exists an intervention function g such that $\tilde{y}_q(p_N, g) = f(p_N)$.

Proof. Since U_N is decreasing and $q(1-1) \le q(1-p_N)(1-g(p_N)) \le q(1-p_N)$, we have $y_q(p_N) \le \tilde{y}_q(p_N, g) \le y_q(1)$.

For a function $f(p_N)$ that satisfies $y_q(p_N) \le f(p_N) \le y_q(1)$ for any $0 \le p_N \le 1$, since $y_q(p_N)$ is monotonically increasing in p_N, we can have $p_N \le y_q^{-1}(f(p_N)) \le 1$. Let the intervention function be

$$g(p_N) = 1 - \frac{1 - y_q^{-1}(f(p_N))}{1 - p_N}. \tag{17}$$

We can verify that $\tilde{y}_q(p_N, g) = f(p_N)$. □

From Lemma 1 we can see that the intervention function can reshape the utility of the malicious user, and if properly designed, the intervention can suppress the level of attack from the malicious user, that is, we can have $\tilde{p}_N^*(g) < p_N^*$. However, we note that at the same time the intervention user will also decrease the throughput of the regular user due to its own transmission. Hence, a problem that needs to be answered is whether the intervention function can really improve the regular users' utility by suppressing the malicious user?

Theorem 1. *For any given q, c and U_N, and any $\hat{p}_N < p_N^*$ there exists an intervention function $g(p_N)$ which satisfies*

(1) $\tilde{p}_N^*(g) = \hat{p}_N$;

(2) $(1 - g(\tilde{p}_N^*(g)))(1 - \tilde{p}_N^*(g)) > (1 - p_N^*)$.

Proof. We let $f(p_N)$ be the following function:

$$f(p_N) = \begin{cases} \dfrac{z - y_q(0)}{\hat{p}_N} p_N + y_q(0), & 0 \le p_N \le \hat{p}_N, \\ \dfrac{y_q(p_N^*) - z}{p_N^* - \hat{p}_N}(p_N - \hat{p}_N) + z, & \hat{p}_N < p_N \le p_N^*, \\ y_q(p_N), & p_N > p_N^*, \end{cases} \tag{18}$$

in which $z = y_q(p_N^*) - c(p_N^* - \hat{p}_N) + \varepsilon$ and ε is an arbitrarily small positive number. It is easy to verify that for any $0 \le p_N \le 1$, $y_q(p_N) \le f(p_N) \le y_q(1)$. Hence, from Lemma 1 we know there exists an intervention function g such that $\tilde{y}_q(p_N, g) = f(p_N)$. As shown in Figure 2 (the X-axis is malicious user's strategy p_N and Y-axis is its utility U_N), $\tilde{y}_q(p_N, g)$ designed by (18) is a piecewise linear function. The intervention is applied when the malicious user jams the channel with a probability lower than its optimal jamming probability without intervention, which is p_N^*.

Now we check the utility function $\tilde{u}_N(p_N, g) = \tilde{y}_q(p_N, g) - c_N p_N$ to verify that with intervention function g, the malicious user's optimal strategy will be $\tilde{p}_N^*(g) = \hat{p}_N$. First, since

$$\begin{aligned} \frac{z - y_q(0)}{\hat{p}_N} &> \frac{y_q(p_N^*) - c(p_N^* - \hat{p}_N) - y_q(0)}{\hat{p}_N} \\ &> \frac{y_q(\hat{p}_N) - y_q(0)}{\hat{p}_N} > c, \end{aligned} \tag{19}$$

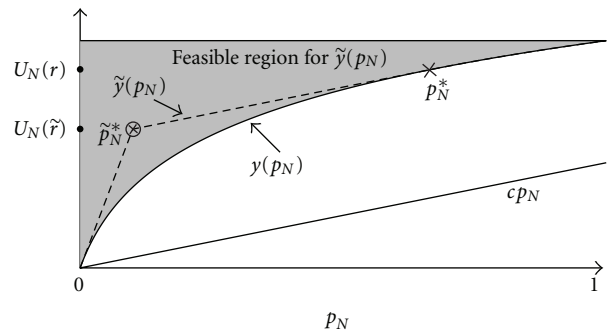


Figure 2: An illustrative example of using intervention to suppress malicious attacks.

we have $\tilde{u}_N(p_N, g) < \tilde{u}_N(\hat{p}_N, g)$ for any $0 \le p_N \le \hat{p}_N$. Similarly, since $(y_q(p_N^*) - z)/(p_N^* - \hat{p}_N) < c$, we have $\tilde{u}_N(p_N, g) < \tilde{u}_N(\hat{p}_N, g)$ for any $\hat{p}_N < p_N \le p_N^*$. For $p_N > p_N^*$, we also have

$$\begin{aligned} \tilde{u}_N(p_N, g) &= u_N(p_N, g) < u_N(p_N^*, g) \\ &= \tilde{u}_N(p_N^*, g) < \tilde{u}_N(p_N, g) < \tilde{u}_N(\hat{p}_N, g). \end{aligned} \tag{20}$$

Therefore, the optimal jamming strategy for the malicious user is $\tilde{p}_N^*(g) = \hat{p}_N$.

Since $\tilde{y}_q(\tilde{p}_N^*(g), g) < y_q(p_N^*)$, based on the monotonic decreasing property of U_N, we have $(1 - g(\tilde{p}_N^*(g)))(1 - \tilde{p}_N^*(g)) > (1 - p_N^*)$. □

The first part of Theorem 1 guarantees that for any $\hat{p}_N < p_N^*$, there always exists an intervention function which makes $\hat{p}_N$ the optimal jamming strategy of the malicious user. The second part of the theorem shows that any such intervention functions would enable the regular users to experience a higher throughput than the case without intervention, given that the malicious user always takes its optimal jamming strategy. If the malicious user does not take its optimal strategy, it gets lower utility for itself. In Figure 2, we give an illustrative example in which the intervention function is constructed as in Theorem 1 to reshape the malicious user's utility function from $y(p_N)$ to $\tilde{y}(p_N)$, and its optimal strategy is changed from p_N^* to $\tilde{p}_N^*$. The second part of Theorem 1 can also be interpreted as the following: if we let $r = q(1 - p_N^*)$ and $\tilde{r} = q(1 - g(\tilde{p}_N^*(g)))(1 - \tilde{p}_N^*(g))$, we can find that $U_N(r) > U_N(\tilde{r})$, hence $r < \tilde{r}$.

From Theorem 1, we know that there always exists an intervention function that can increase the regular users' sum throughput (and also individual regular user's utility) by suppressing the malicious user's attack level to $\tilde{p}_N^*(g)$. However, we are more interested in how the intervention function should be designed such that the regular users' utilities can be most improved. If we define the optimal intervention function as

$$\begin{aligned} g_{\text{opt}} &= \arg\max_g((1 - g(\tilde{p}_N^*(g)))(1 - \tilde{p}_N^*(g))) \\ \text{s.t.} \quad \tilde{p}_N^*(g) &= \arg\max_{p_N} \tilde{u}_N(p_N, g), \end{aligned} \tag{21}$$

then we can further have the following theorem.

Theorem 2. *Under the optimal intervention function g_{opt}:*

(1) *the malicious user's optimal jamming strategy will be* $\widetilde{p}_N^*(g_{\text{opt}}) = 0$;

(2) *the regular users' sum throughput is upper-bounded by* $U_N^{-1}[U_N(q(1-p_N^*)) - cp_N^*]$.

If we let $r^*(\widetilde{p}_N^*) = \arg\max_g(1-g(\widetilde{p}_N^*))(1-\widetilde{p}_N^*)$, *then* $\arg\max_{\widetilde{p}_N^*} r^*(\widetilde{p}_N^*) = 0$.

Proof. Since $\widetilde{p}_N^*(g)$ is the optimal jamming strategy with intervention function g, we have

$$\widetilde{u}_N(\widetilde{p}_N^*(g), g) \geq \widetilde{u}_N(p_N^*, g). \tag{22}$$

Substituting (14) and (15) into (22), we have

$$\begin{aligned} &U_N(q(1-g(\widetilde{p}_N^*(g)))(1-\widetilde{p}_N^*(g))) - c\widetilde{p}_N^*(g) \\ &\quad \geq U_N(q(1-p_N^*)) - cp_N^*. \end{aligned} \tag{23}$$

Hence, if we let $\widetilde{r}(g)$ be the regular users' sum throughput under intervention function g, that is, $\widetilde{r}(g) = q(1-g(\widetilde{p}_N^*))(1-\widetilde{p}_N^*)$, then

$$\begin{aligned} U_N(\widetilde{r}(g)) &\geq U_N(q(1-p_N^*)) - c(p_N^* - \widetilde{p}_N^*(g)) \\ &\geq U_N(q(1-p_N^*)) - cp_N^*. \end{aligned} \tag{24}$$

Noting that U_N is a monotonically decreasing function, we prove that $\widetilde{r}(g)$ is upper-bounded by $U_N^{-1}[U_N(q(1-p_N^*)) - cp_N^*]$, where U_N^{-1} is the inverse function of U_N. Moreover, $\widetilde{p}_N^*(g) = 0$ is a necessary condition to achieve the upper-bound. Hence, we must have $\widetilde{p}_N^*(g_{\text{opt}}) = 0$. □

From the proof of Theorem 2, we can also know that one of the methods to construct the optimal intervention function is to follow (18), and set $\widehat{p}_N = 0$. With such an intervention function, the regular users' sum throughput can approach arbitrarily close to its upper-bound, which is $U_N^{-1}[U_N(q(1-p_N^*)) - cp_N^*]$ as shown in Theorem 2.

In Figure 3, we give a numerical example to show the improvement of the sum throughput of the regular users by using the optimal intervention function to mitigate jamming from the malicious user, under different values of the malicious user's cost c. We can see that in the low-cost region, the network will be unavailable (zero throughput) to any regular user when there is no intervention. However, the regular user can still successfully access the channel when an intervention user exists. Similar improvements can also be observed as the cost of the malicious user increases.

3.2. Nash Equilibrium of the Game Augmented by an Intervention User. In the previous subsection, we assumed that all the regular users' transmission strategies are fixed. However, in many networking scenarios, users are self-interested, and they choose their strategies in order to maximize their own utilities. Many research works have shown that the selfish behavior may result in extremely poor performance for individual users. For example, as shown in [9], if each regular user selfishly maximizes its own utility, then either every user has 0 throughput, or only one user has nonzero throughput. Similar results for CSMA/CA networks are also shown in [16].

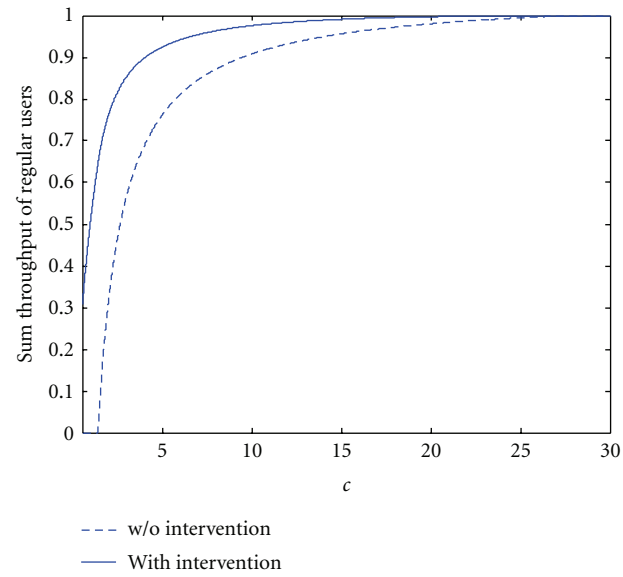


Figure 3: Sum throughput of the regular users without and with intervention.

In this subsection, each regular user is considered to be self-interested and chooses its transmission strategy to maximize its own utility. Hence we can use the non-cooperative game $\Gamma = \langle \mathcal{N}, (\mathcal{P}_n), (u_n) \rangle$ in Section 2.2 to model this scenario. The Nash equilibriums of game Γ must satisfy the following property.

Proposition 1. *If* $\mathbf{p} = (p_1, \ldots, p_N)$ *is an NE of game* Γ, *then at least one of the following two properties holds for* $\mathbf{p}$:

(1) *the malicious user has* $p_N = 1$ *as its optimal jamming strategy, that is,*

$$p_N = \arg\max_{p'_N} u_N(p_{-N}, p'_N) = 1; \tag{25}$$

(2) $p_N = \arg\max_{p'_N} u_N(p_{-N}, p'_N) < 1$, *and at least one regular user* n *has* $p_n = 1$.

Proof. If $p_N = 1$, then any transmission strategy p_n gives 0 utility for regular user n, hence $\mathbf{p} = (p_1, \ldots, p_N)$ is an NE as long as $p_N = \arg\max_{p'_N} u_N(p_{-N}, p'_N) = 1$.

If $p_N = \arg\max_{p'_N} u_N(p_{-N}, p'_N) < 1$, suppose $p_n < 1$ for any $1 \leq n \leq N-1$, then user 1's optimal strategy should be $p_1^* = \arg\max_{p_1} p_1 \prod_{n=2}^{N}(1-p_n) = 1$, which contradicts with the assumption that $p_n < 1$ for any $1 \leq n \leq N-1$. Hence, if $p_N = \arg\max_{p'_N} u_N(p_{-N}, p'_N) < 1$, there must be at least one regular user n which has $p_n = 1$. □

Proposition 1 shows that, for regular users an NE of the game Γ is either inefficient or unfair. If an NE satisfies property 1, then every regular user gets zero utility because the malicious user jams the channel with probability 1; if an NE satisfies property 2, at most one regular user can get

nonzero utility, and it still suffers from a certain level of jamming from the malicious user.

To avoid these undesirable properties of Nash equilibrium, we can use an intervention user with its intervention function g to transform the game Γ to an augmented game Γ_g. Unlike the reduced form intervention function in the previous subsection, now we need an intervention function which reacts to all the regular and malicious users' transmission strategies, that is, $p_0 = g(p_1, p_2, \ldots, p_N)$.

The following theorem establishes the main result of this section, which shows that for any strategy profile $\widetilde{\mathbf{p}} = (\widetilde{p}_1, \ldots, \widetilde{p}_{N-1}, 0)$ with $\widetilde{p}_n > 0$ for any $1 \le n \le N-1$, we can design an intervention function g such that $\widetilde{\mathbf{p}}$ is a Nash equilibrium of the augmented game Γ_g.

Theorem 3. *For any strategy profile $\widetilde{\mathbf{p}} = (\widetilde{p}_1, \ldots, \widetilde{p}_{N-1}, 0)$ with $\widetilde{p}_n > 0$ for any $1 \le n \le N-1$, we can design an intervention function $g(p_1, p_2, .., p_N) = 1 - \prod_{n=1}^{N}(1 - g_n(p_n))$, in which $g_n(p_n) = [1 - p_n/\widetilde{p}_n]_0^1 ([x]_0^1 = \min(1, \max(x, 0)))$ for $1 \le n \le N-1$, and $g_N(p_N)$ is constructed as in Theorem 1 with $\widetilde{p}_N = 0$ as its target strategy, such that $\widetilde{\mathbf{p}}$ is a Nash equilibrium of game Γ_g, which is the augmented game with intervention function g.*

Proof. To prove that $\widetilde{\mathbf{p}}$ is a Nash equilibrium of Γ_g, we just need to check the optimal transmission strategy of each user under intervention function g, if all the other users take actions according to $\{\widetilde{p}_n\}_{1 \le n \le N}$. For any regular user $1 \le n \le N-1$, its optimal transmission strategy will be

$$\begin{aligned} p_n^* &= \arg\max_{p_n} p_n \prod_{m \ne n} (1 - \widetilde{p}_m)(1 - g(\widetilde{p}_1, \ldots, p_n, \widetilde{p}_N)) \\ &= \arg\max_{p_n} p_n \left[2 - \frac{p_n}{\widetilde{p}_n}\right]_0^1 \prod_{m \ne n} (1 - \widetilde{p}_m) \\ &= \widetilde{p}_n. \end{aligned} \tag{26}$$

By using $[x]_0^1 = \min(1, \max(x, 0))$, we can finally reach that

$$p_n^* = \widetilde{p}_n. \tag{27}$$

When $p_n = \widetilde{p}_n$ for any $1 \le n \le N-1$, $g(p_1, p_2, \ldots, p_N) = 1 - \prod_{n=1}^{N}(1 - g_n(p_n)) = g(p_N)$. Hence the malicious user's optimal strategy will be $\widetilde{p}_N$, as proved in Theorem 1. □

Remark 1. In the above, we only consider a strategy profile $\widetilde{\mathbf{p}} = (\widetilde{p}_1, \ldots, \widetilde{p}_{N-1}, 0)$ as the target strategy of the intervention user. In fact, for $\widetilde{\mathbf{p}}' = (\widetilde{p}_1', \ldots, \widetilde{p}_{N-1}', \widetilde{p}_N')$ with $\widetilde{p}_N' \ne 0$, there still exists an intervention g such that $\widetilde{\mathbf{p}}'$ is a Nash equilibrium of Γ_g. However, as proved in Theorem 2, to maximize the regular users' utilities, the optimal intervention function should have $\widetilde{p}_N = 0$ as its target. Therefore, we only consider these Nash equilibriums with $\widetilde{p}_N = 0$.

Remark 2. $\widetilde{p}_n$ is actually a dominant strategy for any regular user n in game Γ_g (A transmission strategy p_n is a dominant strategy for user n in the game Γ_g if and only if $\widetilde{u}_n(p_n, p_{-n}, g) \ge \widetilde{u}_n(p_n', p_{-n}, g)$, for any feasible p_n' and p_{-n}. By checking this definition with the intervention function in Theorem 3, we can verify that $\widetilde{p}_n$ is a dominant strategy for any regular user n). (However, $\widetilde{p}_N = 0$ is not necessarily a dominant strategy for the malicious user N.) Hence, $\widetilde{\mathbf{p}} = (\widetilde{p}_1, \ldots, \widetilde{p}_{N-1}, 0)$ is the only NE of the game Γ_g. Moreover, if all the regular and malicious users start with an arbitrary strategy profile $\mathbf{p}^{(0)}$ at the beginning of the game (called round 0) and the intervention function is also given at this time, and each user takes its best-response strategy in the next round, then the unique Nash equilibrium will be reached in round 2. This is because any regular user n will take its dominant strategy $\widetilde{p}_n$ in round 1, and in round 2 the malicious user will take $\widetilde{p}_N = 0$ as its best-response to all the regular users' joint strategies $\{\widetilde{p}_1, \ldots, \widetilde{p}_{N-1}\}$.

Remark 3. In [9], the intervention user does not need to intervene when its target strategies are fulfilled by all the other users. However, in our setting with a malicious user, the intervention user needs to implement its intervention even when its target strategies are fulfilled, as shown in Theorem 3.

Note that we did not discuss the case of multiple malicious users in a single channel. This is because: first, we do not have a complete analysis of the scenario in which there are multiple malicious users that are *non-cooperative* with each other, because it requires an elaborate model of how the non-cooperative malicious users decide to interact in the presence of other malicious users; secondly, if these malicious users are *cooperative*, that is, they have a common objective to degrade the regular users' throughput, this will be equivalent to having a single malicious user. For instance, even if these malicious users have a higher combined power budget, this is analogous to the case of a single malicious user, because there is only one channel. However, when there is more than one channel, multiple malicious users have the ability to jam multiple channels simultaneously. This is also why we will consider multiple malicious users in a multi-channel case.

4. The Multichannel Case

4.1. Single Malicious User. We still first assume that the regular users have agreed on choosing their transmission strategies according to a certain transmission profile. We also assume there is only one malicious user. The malicious and intervention users have their power budgets as $P^0 = P^N = 1$, and we assume that either of them can access at most one channel in a certain time slot. We also assume that all the channels are sorted such that $q_1 \ge q_2 \ge \cdots \ge q_K$, where $q_k = \sum_{n=1}^{N-1} p_{n,k} \prod_{m=1, m \ne n}^{N-1} (1 - p_{m,k})$ is the sum throughput of all the regular users over channel k when there is no malicious or intervention user.

The optimal jamming strategy of the malicious user when there is no intervention is given by

$$\mathbf{p}_N^* = \arg\max_{p_N} U_N\left(\sum_{k=1}^{K} q_k(1 - p_{N,k})\right) - c_N\left(\sum_{k=1}^{K} p_{n,k}\right). \tag{28}$$

From this, it can be easily verified that the optimal jamming strategy will only jam the channel with the highest throughput, that is, $\mathbf{p}_N^* = (p_{N,1}^*, 0, \ldots, 0)$.

Similar to the single channel case, we define $y_{\mathbf{q}}(\mathbf{p}_N) = U_N(\sum_{k=1}^{K} q_k(1-p_{N,k}))$ and $\widetilde{y}_{\mathbf{q}}(\mathbf{p}_N, g_N) = U_N(\sum_{k=1}^{K} q_k(1-p_{N,k})(1-g_N^k(\mathbf{p}_N)))$, where $\mathbf{q} = (q_1,\ldots,q_K)$ and $g_N(\mathbf{p}_N) = (g_N^1(\mathbf{p}_N),\ldots,g_N^K(\mathbf{p}_N))$. We have the following lemma to determine the achievable region of the modified utility function $\widetilde{y}_{\mathbf{q}}(\mathbf{p}_N, g_N)$.

Lemma 2. *For any feasible $\mathbf{p}_N$ and intervention function g, $y_{\mathbf{q}}(\mathbf{p}_N) \le \widetilde{y}_{\mathbf{q}}(\mathbf{p}_N, g) \le y_{\mathbf{q}}(\mathbf{p}_N^1)$; conversely, if a function $f(\mathbf{p}_N)$ satisfies $y_{\mathbf{q}}(\mathbf{p}_N) \le f(\mathbf{p}_N) \le y_{\mathbf{q}}(\mathbf{p}_N^1)$, there exists a feasible intervention function g such that $\widetilde{y}_{\mathbf{q}}(\mathbf{p}_N, g) = f(\mathbf{p}_N)$.*

(An intervention function is feasible, if $\prod_{k=1}^{K} g_N^k(\mathbf{p}_N) \le P^N$ for any $\mathbf{p}_N \in \mathcal{P}_N$.)

Theorem 4. *For any given $\mathbf{q} = (q_1,\ldots,q_K)$, c and U_N, and any $0 \le \hat{p}_N < p_{N,1}^*$, there exists an intervention function $g_N(\mathbf{p}_N)$ with $g_N(\mathbf{p}_N) = (g_N^1(\mathbf{p}_N),\ldots,g_N^K(\mathbf{p}_N))$, which satisfies*

(1) $\sum_{k=1}^{K} \widetilde{p}_{N,k}^* = \hat{p}_N$,

(2) $\sum_{k=1}^{K} q_k((1-g_N^k(\widetilde{\mathbf{p}}_N^*))(1-\widetilde{p}_{N,k}^*)) > \sum_{k=1}^{K} q_k(1-p_{N,k}^*)$.

Proof. For simplicity, we let $\mathcal{P}_N^1 = \{\mathbf{p}_N \mid p_{N,k} = 0,\ k = 2,\ldots,K\}$ and denote any jamming strategy $(\alpha, 0, 0, \ldots, 0)$ as $\mathbf{p}_N^1(\alpha)$. For example, we can write $\mathbf{p}_N^*$ as $\mathbf{p}_N^1(p_{N,1}^*)$.

We first construct $f(\mathbf{p}_N)$ for any $\mathbf{p}_N \in \mathcal{P}_N^1$:

$$f(\mathbf{p}_N \in \mathcal{P}_N^1) = \begin{cases} \dfrac{z - y_{\mathbf{q}}(\mathbf{p}_N^1(0))}{\hat{p}_N} p_{N,1} + y_{\mathbf{q}}(\mathbf{p}_N^1(0)), & 0 \le p_{N,1} \le \hat{p}_N, \\ \dfrac{y_{\mathbf{q}}(\mathbf{p}_N^1(p_N^*)) - z}{p_{N,1}^* - \hat{p}_N}(p_{N,1} - \hat{p}_N) + z, & \hat{p}_N < p_{N,1} \le p_{N,1}^*, \\ y_{\mathbf{q}}(\mathbf{p}_N^1(p_{N,1})), & p_{N,1} > \hat{p}_N, \end{cases} \tag{29}$$

where $z = u_N(\mathbf{p}_N^1(p_{N,1}^*)) + c\hat{p}_N = y_{\mathbf{q}}(\mathbf{p}_N^1(p_{N,1}^*)) - c(p_{N,1}^* - \hat{p}_N)$. For any $\mathbf{p}_N \notin \mathcal{P}_N^1$, we let

$$f(\mathbf{p}_N \notin \mathcal{P}_N^1) = f\left(\mathbf{p}_N^1\left(\sum_{k=1}^{K} p_{N,k}\right)\right). \tag{30}$$

Similar to the proof of Theorem 1 and also based on Lemma 2, we can verify that there exists an intervention function $g_N(\mathbf{p}_N)$ such that $\widetilde{y}_{\mathbf{q}}(\mathbf{p}_N, g_N) = f(\mathbf{p}_N)$, and under this intervention function any jamming strategy $\mathbf{p}_N$ with $\sum_{k=1}^{K} p_{N,k} = \hat{p}_N$ is an optimal strategy for the malicious user.

Similar to the single channel case, we can show in the following corollary that the optimal intervention function should have $\widetilde{\mathbf{p}}_N^* = (0, 0, \ldots, 0)$. □

Corollary 1. *If we let the optimal intervention be*

$$g^* = \arg\max_{g} \sum_{k=1}^{K} q_k\left(\left(1 - g\left(\widetilde{p}_{N,k}^*\right)\right)\left(1 - \widetilde{p}_{N,k}^*\right)\right) \quad \text{s.t. } \widetilde{\mathbf{p}}_N^* = \arg\max_{\mathbf{p}_N} \widetilde{u}_N(\mathbf{p}_N, g), \tag{31}$$

then we have $\widetilde{\mathbf{p}}_N^* = \arg\max_{\mathbf{p}_N} \widetilde{u}_N(\mathbf{p}_N, g^*) = (0,\ldots,0)$.

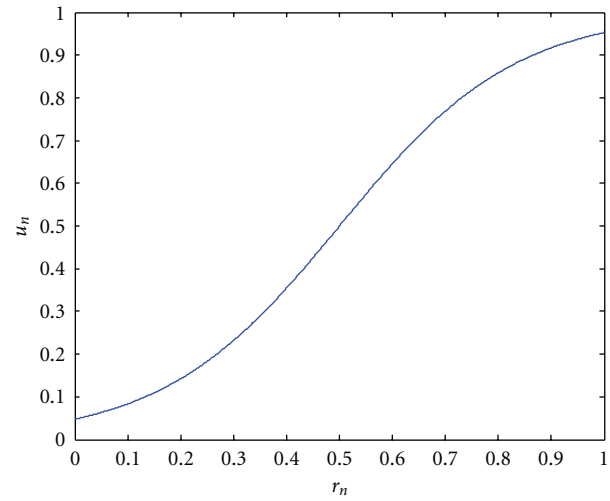


Figure 4: A sigmoid utility function.

The proof is similar to the proof of Theorem 2 and is omitted here.

We note that the intervention function designed in Theorem 4 requires that the intervention user monitors all the channels and responds to the malicious user's jamming strategy (i.e., its jamming probabilities) over all the channels. An alternative approach would be to deploy the intervention function which we designed for the single channel case over each channel. In this case, each intervention function only monitors its own channel and also only intervenes in this channel. Interestingly, by comparing these two approaches, we can find that the former one requires a smaller power budget for the intervention user, but the intervention user needs to be capable of monitoring and intervening in all the channels.

4.2. Multiple Malicious Users. We now consider a scenario when there exist N_m malicious users, who are cooperative with each other to maximize their system utility, which is defined the same as (3). Since all the malicious users are cooperative, we can consider them as a *fictitious* malicious user (still denoted as user N) but let its power budget be $P^N = N_m$, and $\mathbf{p}_N$ will be the joint effect of all the malicious users. Hence, user N's optimal jamming strategy will be

$$\mathbf{p}_N^* = \arg\max_{\mathbf{p}_N} u_N(\mathbf{p}_N) = U_N\left(\sum_{k=1}^{K} q_k(1-p_{N,k})\right) - c_N\left(\sum_{k=1}^{K} p_{N,k}\right), \quad \text{s.t.} = \sum_{k=1}^{K} p_{N,k} \le P^N = N_m \tag{32}$$

In this scenario, unlike in the single malicious user case described in the previous subsection, an intervention user with unit power budget, that is, $P^0 = 1$ may not be able to enforce the malicious users to have $\widetilde{\mathbf{p}}_N^* = (0, 0, \ldots, 0)$ as their optimal jamming strategy. Hence, in order to find

the most energy-efficient intervention function, we need to determine how large P^0 (this corresponds to the number of intervention users if each of them has unit power budget) should be in order to have an optimal intervention function which enforces $\widetilde{\mathbf{p}}_N^* = (0, 0, \ldots, 0)$.

First we note that the optimal jamming strategy without intervention will be in the form of $\mathbf{p}_N^* = (1, \ldots, 1, p_{N,l}, 0, \ldots, 0)$, with $l - 1 + p_{N,l} < P^N$ and $0 \le p_{N,l} \le 1$. The following theorem gives the minimum value of P^0 which can fully suppress the malicious users' jamming, that is, to have $\widetilde{\mathbf{p}}_N^* = (0, \ldots, 0)$.

Theorem 5. *For given* $\mathbf{q} = (q_1, \ldots, q_K)$, *c, and* U_N, *if the optimal jamming strategy without intervention is* $\mathbf{p}_N^* = (1, \ldots, 1, p_{N,l}, 0, .., 0)$ *for a certain* $P^N > 1$, *then the minimum* P^0 *that is required to have* $\widetilde{\mathbf{p}}_N^* = (0, .., 0)$ *can be determined by* $P^0_{\min} = j + ((\Delta r - \sum_{k=1}^{j} q_k)/q_{j+1})$, *where*

$$\Delta r = \sum_{k=1}^{K} q_k - U_N^{-1} \times \left(U_N\left(\sum_{k=l+1}^{K} q_k + q_l(1 - p_{N,l}) \right) - c_N(l - 1 + p_{N,l}) \right),$$
$$j = \max j', \text{ s.t. } \sum_{k=1}^{j'} q_k < \Delta r. \tag{33}$$

Proof. Since

$$U_N\left(\sum_{k=1}^{K} q_k\left(1 - p_{0,k}^*\right) \right) \ge U_N\left(\sum_{k=l+1}^{K} q_k + q_l(1 - p_{N,l}) \right) - c_N(l - 1 + p_{N,l}), \tag{34}$$

where $\mathbf{p}_0^* = (p_{0,1}^*, \ldots, p_{0,K}^*) = g(\mathbf{p}_N^*)$, from the monotonic property of U_N, we know that

$$\sum_{k=1}^{K} q_k p_{0,k}^* \ge \sum_{k=1}^{K} q_k - U_N^{-1}\left[U_N\left(\sum_{k=l+1}^{K} q_k + q_l(1 - p_{N,l}) \right) - c_N(l - 1 + p_{N,l}) \right] = \Delta r. \tag{35}$$

We note that $q_1 \ge q_2 \ge \cdots \ge q_K$, hence

$$P^0_{\min} \ge \sum_{k=1}^{K} p_{0,k}^* \ge j + \frac{\left(\Delta r - \sum_{k=1}^{j} q_k\right)}{q_{j+1}} \tag{36}$$

with $j = \max j'$, s.t. $\sum_{k=1}^{j'} q_k < \Delta r$. The minimum is achieved when

$$p_{0,k}^* = 0, \quad \text{for } k \le j,\ p_{0,j+1}^* = \frac{\left(\Delta r - \sum_{k=1}^{j} q_k\right)}{q_{j+1}}, \quad p_{0,k}^* = 0, \quad \text{for } k > j + 1. \tag{37}$$

□

4.3. Nash Equilibrium of the Augmented Game. Similar to the main result (Theorem 3) we get in the single channel case, we can also design an intervention function to mitigate jamming attack and at the same time enforce self-interested regular users to choose certain target strategies. The following theorem is an extension of Theorem 3 to the multi-channel case.

Theorem 6. *Let* $\widetilde{\mathbf{p}}_n = (\widetilde{p}_i^1, \ldots, \widetilde{p}_n^K)$ *be the target strategy for the regular user n, and* $\widetilde{\mathbf{p}}_N = (0, \ldots, 0)$ *the target strategy for the malicious user N. If the intervention function* $g(\mathbf{p}_1, \ldots, \mathbf{p}_N) = (g_1(\mathbf{p}_1, \ldots, \mathbf{p}_N), \ldots, g_K(\mathbf{p}_1, \ldots, \mathbf{p}_N))$ *is designed as follows:*

$$g_k(\mathbf{p}_1, \ldots, \mathbf{p}_N) = 1 - \left(1 - g_N^k(\mathbf{p}_N)\right) \prod_{n=1}^{N-1} \left(\left[1 - \frac{p_n^k}{\widetilde{p}_n^k} \right]_0^1 \right), \quad \forall 1 \le k \le K, \tag{38}$$

where $g_N^k(\mathbf{p}_N)$ *is designed as in Theorem 4, then* $(\widetilde{\mathbf{p}}_1, \ldots, \widetilde{\mathbf{p}}_N)$ *is a Nash equilibrium of the augmented game with intervention g.*

The proof is similar to Theorem 3, but we combine the result from Theorem 4 and the complete proof is omitted here. We note that when all the regular users fulfilled their target strategies, then the intervention function reduces to the one we designed in Theorem 4.

5. Information Requirements for Playing the Game

When a user tries to maximize its own utility, it needs to observe some information about all the other users before making its decision. We will discuss different information requirements for different users (regular, malicious and intervention user), in both the game without and with intervention. We first note that from user n's point of view, the channel observed at a certain time slot must be in one of the following four states: *idle* (no user transmits); *busy* (at least one other user transmits); *success* (only user n transmits); *fail* (user n and at least one other user transmit). We let $p_{n,k}^{idle}$, $p_{n,k}^{succ}$ be the probabilities that user n observes the channel k in idle and success states, respectively.

In the non-cooperative game Γ, a regular or malicious user $n \in \mathcal{N}$ only needs to know $\prod_{m \ne n}(1 - p_{m,k})$ for every channel $k \in \mathcal{K}_n$ in order to compute its best-response strategy as in (4) or (5). For a certain channel k, similar to [15], an estimation of $\prod_{m \ne n}(1 - p_{m,k})$ can be obtained by computing $p_{n,k}^{idle}/1 - p_{n,k}$ or $p_{n,k}^{succ}/p_{n,k}$, because $p_{n,k}^{idle} = (1 - p_{n,k})\prod_{m \ne n}(1 - p_{m,k})$ and $p_{n,k}^{succ} = p_{n,k}\prod_{m \ne n}(1 - p_{m,k})$.

In the augmented game Γ_g with intervention function g, the regular and malicious users need to know the intervention function explicitly or implicitly in order to make their best decisions. The intervention function can be explicitly known by the users if it is part of the network protocol or announced to them by the intervention user. If there is no explicit knowledge of the intervention function at the user side, it can still learn the intervention through repeated

interactions with the intervention user [9]. However, if the intervention function has a structure as $g(p_1, p_2, \ldots, p_N) = 1 - \prod_{n=1}^{N}(1 - g_n(p_n))$ in Theorem 3, each user only needs to know part of the intervention, that is, $g_n(p_n)$ for user n, and the communication overhead for announcing the intervention function or the time required to learn it can be greatly reduced. We also note that there is no need for explicit information exchange among regular users. This also helps to reduce the communication overhead in the network, and eliminates the possibility of any information exchange getting jammed.

The intervention user also needs to know some information about the regular and malicious users in order to compute the optimal intervention function and implement it when other users take their transmission strategies. To compute the optimal intervention function, the intervention user needs to know the utility function of the malicious user; to implement its intervention, it needs to know each user's transmission strategy $\mathbf{p}_n$. We assume that the utility function of the malicious user is already available to the intervention user from some previous modeling about the malicious user's behavior. To know the transmission strategy $\mathbf{p}_n$, as in [15], the intervention user can decode the successfully transmitted packet when there is only one regular or malicious user transmitting, and identify the sender. We let $p_{0,k}^{idle}$ be the probability that the intervention user finds channel k is idle, and $q_k(n)$ is the probability that user n has a successful transmission over channel k. We can have $p_{0,k}^{idle} = (1 - p_{0,k})\prod_{m\in\mathcal{N}}(1 - p_{m,k})$ and $q_k(n) = p_{n,k}(1 - p_{0,k})\prod_{m\neq n}(1 - p_{m,k})$, hence $p_{n,k}$ can be computed by $p_{n,k} = q_k(n)/q_k(n) + p_{0,k}^{idle}$, and $\mathbf{p}_n$ can be obtained by combining all the $p_{n,k}$ over different channels. Therefore, the transmission strategy $\mathbf{p}_n$ can be obtained by the intervention user without any explicit message exchange.

6. Illustrative Results

We will give several illustrative results to show how much the intervention user can help the regular users to improve throughputs when there is one or multiple malicious jamming users. The numerical results are computed based on our previous analysis.

6.1. General Setting. To numerically show the rate regions in different cases, we assume the regular users have sigmoid utility functions as in Figure 4, that is, $u_n(r_n) = 1/(1 + e^{-\alpha(r_n-\theta)})$ for $1 \leq n < N$ where r_n is the throughput of user n.

This is a widely used utility function to model the quality of service at different rates, as in [13, 17]. Hence, the malicious user's utility function can be defined by $u_N(p_N) = u_n(1) - (1/(1 + e^{-\alpha(q(1-p_N)-\theta)})) - cp_N$ in which q is the sum throughput of the regular users, and c is the transmission cost.

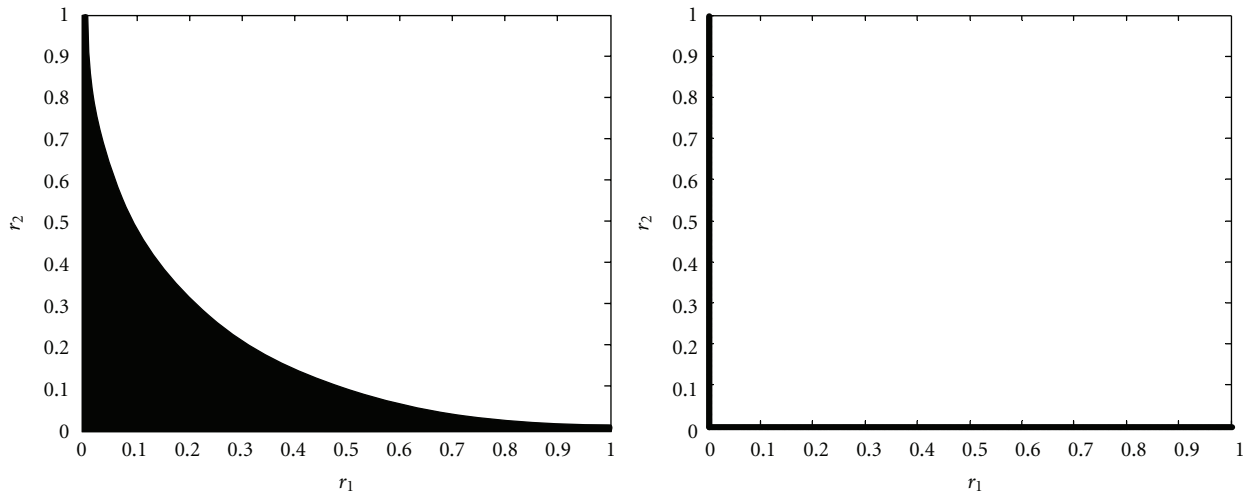
6.2. Achievable Rate-Region for Two-User Single-Channel Case, with or without Intervention. We first use a two-user single-channel case to compare the achievable rate regions of two regular users under different network settings. The three cases being compared in Figure 5 are: (a) no malicious user or intervention user; (b) one malicious user with optimal jamming strategy; (c) the intervention user adopts its optimal intervention function and the malicious user acts with its optimal jamming strategy given the intervention function.

In Figure 5, r_1 and r_2 are the rates (throughputs) of the two regular users, respectively, and we set $\alpha = 6$, $\theta = 0.5$, and $c = 0.5$. In the first two cases (Figures 5(a) and 5(b)), we give both the rate region achieved by independent random access (left), and the rate region of all the Nash equilibriums (right). The independent access rate region in Figure 5(a) is also shown by the dotted line in Figures 5(b) and 5(c) for comparison. We can see from Figure 5(c) that the optimal intervention can help the regular users achieve a larger rate region compared to Figure 5(b). In [4], it was shown that any point in the feasible region of Figure 5(a) can be achieved by a properly designed intervention function. This result can be extended to the case when there exists a malicious jamming user. Based on Theorem 3 in Section 3.2, we can also design an intervention function to enforce the transmission strategies of both regular and malicious users, hence any point in the rate region of Figure 5(c) can be achieved at a Nash equilibrium of an augmented game with a certain intervention function.

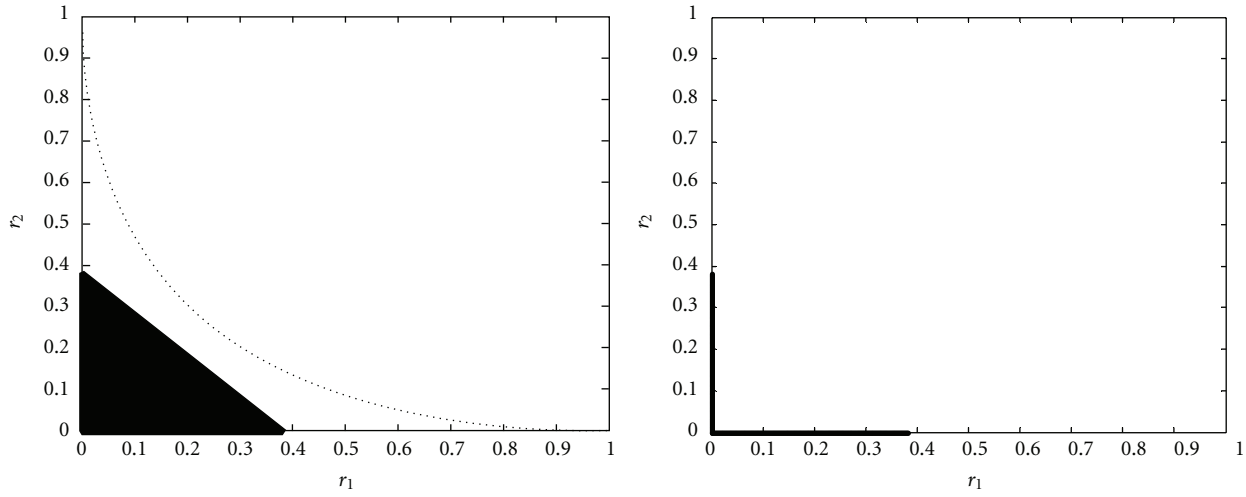
6.3. Sum Throughput of $(N-1)$ Regular Users Transmitting with Probability $1/N-1$. Next, we compare the sum throughput of all the $(N-1)$ regular users when each of them takes transmission strategy $1/(N-1)$, that is, $p_n = 1/(N-1)$ for any $1 \leq n \leq (N-1)$. It is well known that such a strategy profile achieves maximum sum throughput for $(N-1)$ users when there is no malicious jamming to the channel. In Figure 6, we compare the sum throughputs between two cases: when there is a malicious user but no intervention, and when there are both malicious and intervention users.

We consider both convex and non-convex $U_N(r)$ for the malicious user. When modeling the regular users' traffic as elastic traffic, the malicious user will have a convex $U_N(r)$; it will have non-convex $U_N(r)$ when modeling regular users' traffic as inelastic. We also have two different numbers of regular users, with $N-1 = 3$ and $N-1 = 30$, respectively. We can see that when the cost c is low, the regular users cannot get any successful transmission if there is no intervention.

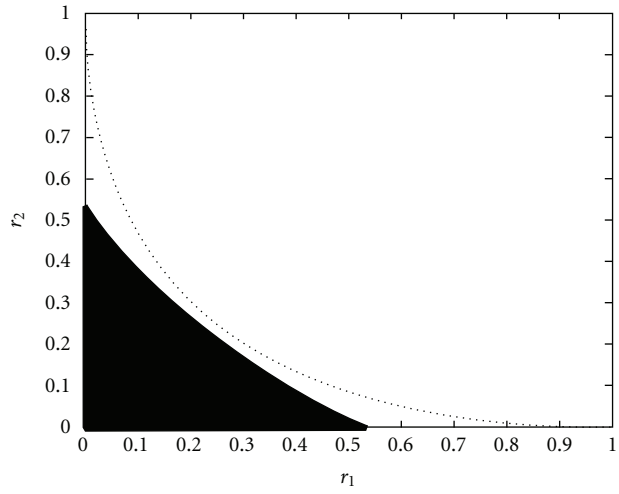
We also note that when $U_N(r)$ is convex, there is a threshold phenomenon: when the cost is below this threshold, the jammer will jam the channel with probability 1, and if the cost is beyond the threshold, it will not jam at all. This is because when $U_N(r)$ is convex, the problem in (13) becomes a maximization problem on a convex function, which can only have its optimal solution at two extreme points, that is, $p_N^* = 1$ or $p_N^* = 0$. However, with the intervention user, the regular users' sum throughput increases as the malicious user's cost increases, even in the low-cost region where they cannot access the channel at all without intervention user. When the cost becomes larger, the sum throughput will eventually approach $(1 - 1/(N-1))^{N-1}$, because the malicious user becomes less likely to attack due to the high cost.



(a) No malicious user or intervention user

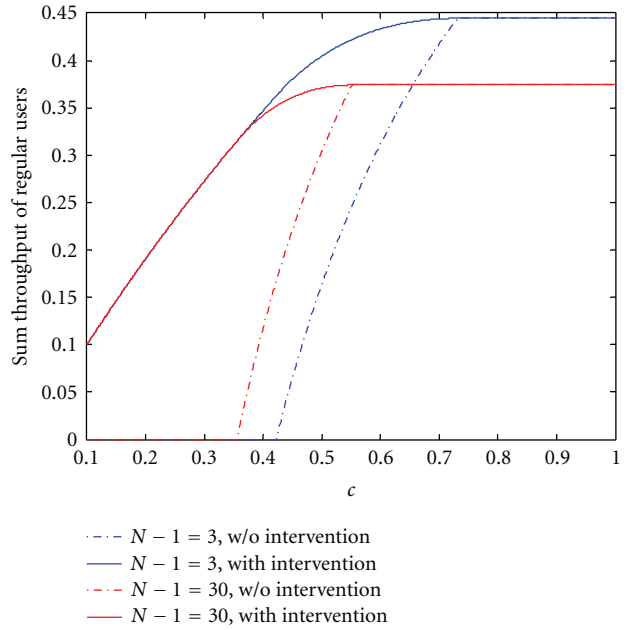


(b) One malicious user and no intervention

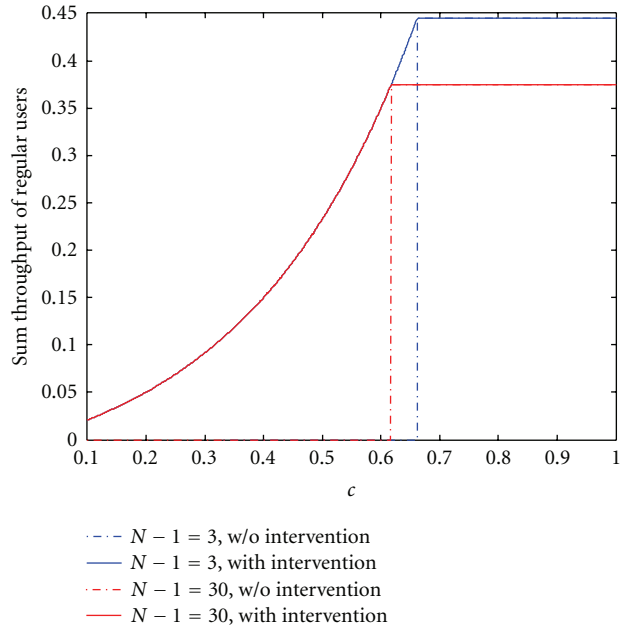


(c) One malicious user and optimal intervention

Figure 5: The rate region of the two regular users.



(a) with a non-convex $U_N(r)$



(b) with a convex $U_N(r)$

FIGURE 6: Sum throughput of all the regular users under different cost c.

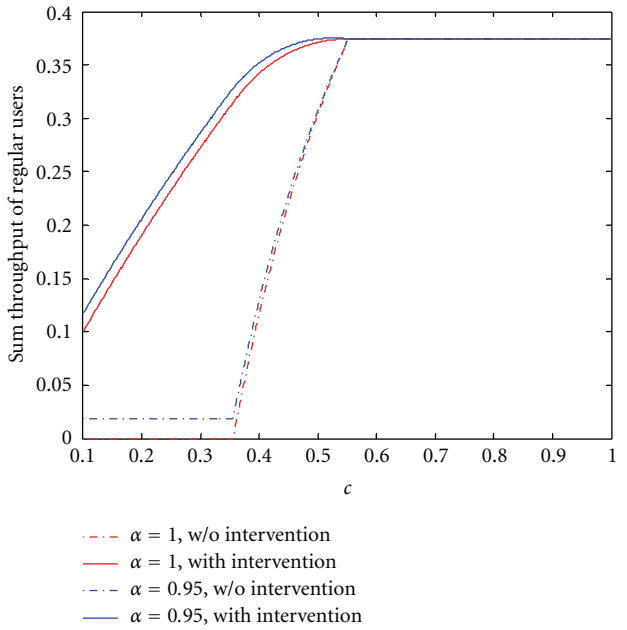


FIGURE 7: Sum throughput of all the regular users under "imperfect" jammer.

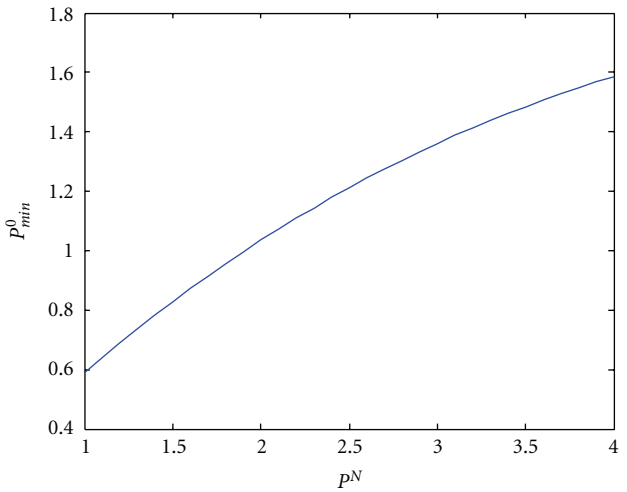


FIGURE 8: The minimum required $P^0_{\min}$ to have optimal intervention.

6.4. An "Imperfect" Jammer—Considering Range Effect. In Figure 7, we investigate the range effect in our setting. Particularly, we consider the case when the jammer is further away from the access point than the regular users. Due to the signal strength degradation along the transmission path, there is a small probability that its transmission cannot jam the regular users. We let α be the probability a packet transmitted by the malicious user can reach the access point, and simulate with $N-1 = 30$ regular users. Each regular user takes transmission strategy $1/(N-1)$, that is, $p_n = 1/(N-1)$, as in our previous setting. We compare an "imperfect" jammer with $\alpha = 0.95$ and a perfect jammer with $\alpha = 1$, as shown in Figure 7. We note that in either the case with an intervention user or without an intervention user, the regular users have higher sum throughput under an imperfect jammer. Particularly, even when the cost is very low, the jammer cannot totally block the regular users because α is smaller than 1. However, when the cost becomes higher, the jammer will become less likely to jam the regular users, hence the regular users throughput becomes independent on α at the high cost region.

6.5. Power Budget Requirement for the Intervention User. We also compute the power budget requirement for the intervention user when there are multiple malicious users in a multi-channel network. We assume there are 4 channels and 5 regular users. Each regular user has the same transmission strategy as $(1/5, 1/5, 1/5, 1/5)$. The malicious user's utility is again assumed to be $u_N(p_N) = u_n(1) - 1/(1 + e^{-\alpha(q(1-p_N)-\theta)}) - cp_N$, with transmission cost $c = 0.1$. According to Theorem 5, we compute the minimum power budget of the intervention user in order to have optimal intervention, that is, enforce the malicious users to not attack at all. In Figure 8 we illustrate the minimum required $P^0_{\min}$ for different $P^N \in [1, 4]$ (P^N corresponds to the number of malicious users, or more generally the total power budget of the malicious users. A P^N larger than 4 is not necessary because there are only 4 channels).

7. Conclusion

We investigated the problem of efficient channel access when there is a malicious jammer who tries to intentionally decrease all the regular users' throughputs. Using a non-cooperative game model, we showed that the regular users have very poor performance at the Nash equilibriums because of the jamming attacks and also their own selfish transmissions. To better utilize the channel and mitigate jamming attacks, we introduce an intervention user to transform the original game into an augmented game with an intervention function. The intervention function compels the selfish regular users to behave cooperatively by punishing their excessive access to the channel, and at the same time suppresses the jammer by providing additional incentives when it lowers its attacking level. It is shown that any point in the feasible rate region can be achieved as a Nash equilibrium of the augmented game with properly designed intervention function. Future extensions of this work may include the investigation of nonlinear cost for the malicious user and also the effect of network topology on the design of intervention function.

References

[1] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 1307–1315, Anchorage, Alaska, USA, May 2007.

[2] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *Proceedings of the 1st EuroFGI International Conference on Network Control and Optimization*, vol. 4465 of *Lecture Notes in Computer Science*, pp. 1–12, Avignon, France, June 2007.

[3] B. Awerbuch, A. Richa, and C. Scheideler, "A jamming-resistant MAC protocol for single-hop wireless networks," in *Proceedings of the 27th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC '08)*, pp. 45–54, August 2008.

[4] YI. Xie and S. Z. Yu, "Monitoring the application-layer DDoS sttacks for popular websites," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 15–25, 2009.

[5] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," in *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08)*, pp. 1265–1273, April 2008.

[6] I. Aad, J. P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 791–802, 2008.

[7] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: foiling smart jammers using multi-layer agility," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 2536–2540, Anchorage, Alaska, USA, May 2007.

[8] S. Khattab, D. Mosse, and R. Melhem, "Jamming mitigation in multi-radio wireless networks: reactive or proactive?" in *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureComm '08)*, September 2008.

[9] J. Park and M. van der Schaar, "Stackelberg contention games in multiuser networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, Article ID 305978, 15 pages, 2009.

[10] I. E. Pountourakis, "Throughput evaluation of multichannel slotted Aloha-type protocols with receiver collisions," *Telecommunication Systems*, vol. 5, no. 4, pp. 413–419, 1996.

[11] D. Bertsekas and R. Gallager, *Data Networks*, Prentice Hall, Englewood Cliffs, NJ, USA, 1987.

[12] E. Altman, R. El Azouzi, and T. Jiménez, "Slotted Aloha as a game with partial information," *Computer Networks*, vol. 45, no. 6, pp. 701–713, 2004.

[13] S. Shenker, "Fundamental design issues for the future Internet," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 7, pp. 1176–1188, 1995.

[14] M. Chiang, "Nonconvex optimization of communication systems," in *Advances in Mechanics and Mathematics, Special Volumn on Strang's 70th Birthday*, D. Gao and H. Sherali, Eds., Springer, Berlin, Germany, 2008.

[15] A. H. M. Rad, J. Huang, M. Chiang, and V. W. S. Wong, "Utility-optimal random access without message passing," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1073–1079, 2009.

[16] M. Čagalj, S. Ganeriwal, I. Aad, and J. P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05)*, pp. 2513–2524, Miami, Fla, USA, March 2005.

[17] G. D. Stamoulis, D. Kalopsikakis, A. Kyrikoglou, and C. Courcoubetis, "Efficient agent-based negotiation for telecommunications services," in *Proceedings of the IEEE Global Telecommunication Conference (GLOBECOM '99)*, vol. 3, pp. 1989–1996, December 1999.