Computer Networks 55 (2011) 2259–2270

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Fight jamming with jamming – A game theoretic analysis of jamming attack in wireless networks and defense strategy

Lin Chen [a,*], Jean Leneutre [b]

[a] Laboratoire de Recherche en Informatique (LRI), CNRS, University of Paris-Sud XI and INRIA, 91405 Orsay, France
[b] Department of Computer Science and Networking, TELECOM ParisTech – LTCI CNRS 5141, 46 Rue Barrault, Paris 75013, France

ARTICLE INFO

Article history:
Received 22 June 2010
Received in revised form 7 March 2011
Accepted 13 March 2011
Available online 23 March 2011
Responsible Editor: P. Dowd

Keywords:
Jamming
Security game
Wireless network
Game theory

ABSTRACT

In wireless networks, jamming is an easily mountable attack with detrimental effects on the victim network. Existing defense strategies mainly consist of retreating from the jammer or rerouting traffic around the jammed area. In this paper, we tackle the problem from a different angle. Motivated by the high energy-consuming nature of jamming, we propose our defense strategy to defeat the jammer by draining its energy as fast as possible. To gain an in-depth insight on jamming and to evaluate the proposed defense strategy, we model the interaction between the jammer and the victim network as a non-cooperative game which is proven to admit two equilibria. We demonstrate analytically that the proposed defense strategy can eliminate the undesirable equilibrium from the network's perspective and increase the jammer's energy consumption at the remaining equilibrium without degrading the performance of the victim network. We also investigate the game dynamics by developing the update mechanism for the players to adjust their strategies based on only observable channel information. Numerical study is then conducted to evaluate the performance of the proposed strategy. Results demonstrate its effectiveness in defeating jamming, especially when the jammer is aggressive.

1. Introduction

1.1. Background and motivation

It is widely recognized that the broadcast nature of the shared wireless medium makes wireless networks extremely vulnerable to various attacks ranging from the passive eavesdropping to the sophisticated manipulation of routing information, among which an easily mountable one with detrimental effects on the victim network is jamming, a malicious attack whose objective is to disrupt the communication of the victim network by intentionally causing interference or collision at the receiver side. Usually launched at the PHY and MAC layers, jamming requires no special hardware and can virtually paralyze any wireless networks. [14] provides a taxonomy of different types of jamming in wireless networks. The detrimental degradation on throughput caused by the jamming attack in IEEE 802.11 WLANs is demonstrated in [2], in which the authors show that even the memoryless jamming attack can reduce the network throughput by up to 90%.

Besides traditional spread spectrum techniques at the physical layer (cf. [3,4]), the defense strategies in existing literature mainly consist of retreating from the jammer after detecting jamming or rerouting traffic around the jammed area. In [1], Xu et al. propose two strategies to evade jamming. The first strategy, channel surfing, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. The second strategy, spatial retreats, is a form of spatial evasion where legitimate devices move away from the jammer. In [5], Wood et al. present a distributed protocol

* Corresponding author. Tel.: +33 169153940.
E-mail addresses: Lin.Chen@lri.fr (L. Chen), Jean.leneutre@telecom-paristech.fr (J. Leneutre).

1389-1286/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2011.03.006

to map the jammed region so that the network can avoid routing traffic through it. The solution proposed by Cagalj et al. [6] uses different wormholes (wired wormholes, frequency-hopping pairs, and uncoordinated channel hopping) that lead out of the jammed region to report the alarm to the network operator. In [7], Wood et al. investigate how to deliberately avoid jamming in IEEE 802.15.4-based wireless networks. A recently proposed strategy consists of constructing a low-rate timing channel in the physical layer in spite of the presence of the jammer [11]. In [12], Awerbuch et al. propose a jamming-resistant MAC protocol for single-hop wireless networks with provable robustness against adversarial jammers. The authors of [20] and [21] study the effect of adversarial jamming in 802.11 networks.

Despite the different techniques used in existing solutions, they usually require frequency hopping capability or sufficient node mobility to avoid confronting the jammer. Such requirements might be too expensive to implement or even impractical in some scenarios, e.g., single-channel WLANs. Moreover, their effectiveness may be significantly reduced if the jammer is strategic, e.g., mapping the jammed area becomes more difficult if the jammer keeps moving in an unpredictable fashion.

1.2. Paper overview

In this paper, we tackle the problem of defeating jamming from a different angle. Our work is motivated by the observation that although a jamming packet of a few bits suffices to disrupt a transmitted packet, as argued in [8], yet continuously transmitting the jamming packets is energy-consuming and may quickly drain the energy of the jammer with limited battery supply. In other words, a jammer with limited energy resource can never succeed jamming the victim network for any extended period of time. This is especially the case where the jammer is restricted to a configuration similar to that of ordinary network nodes with limited energy resource such as laptops, e.g., an attacker with a mobile device aiming at jamming the WiFi-based hotspots in an airport. Given the above argument, an alternative defense strategy against jamming besides passively retreating, especially when it is impossible to move away from the jammer, is to actively fight the jammer face-to-face by draining its energy as fast as possible.

Following the above line of defense, we proceed our analysis as follows. Firstly, we formulate jamming as an optimization problem for the jammer whose goal is to block the communication of the victim network as long time as possible under its energy constraint. To this end, it controls the probability of transmitting jamming packets to strike a balance between keeping a high jamming probability and limiting the energy consumption. On the network side, each node adapts its channel access probability to maximize its utility under the jamming attack. We model the interaction between the jammer and the network as a non-cooperative game G. We show that G has two Nash equilibria (NE) and at one of them, the jammer can paralyze the network with little energy consumption. To avoid this inefficient NE for the network, we propose our defense strategy by introducing the anti-jammer, a special node dedicated to draining the jammer's energy. To achieve its goal, the anti-jammer configures the probability of transmitting bait packets to attract the jammer to transmit. We then formulate the new jamming game G' with the anti-jammer and show that G' admits a unique NE where if the anti-jammer chooses its strategy wisely, the network utility remains the same as that in G, but the jammer's energy consumption increases significantly. Next, we extend our efforts to investigate the dynamics of G' by developing an update mechanism in which the anti-jammer and network nodes adjust their transmission strategies based on only observable channel information.

1.3. Related work on game theoretical analysis on jamming

Recently, applying game theory [18] in different areas of wireless communication has attracted considerable research attention. Concerning jamming, Mallik et al. [13] model the problem of a victim node and a jammer transmitting to a common receiver in an on–off mode as a two-person zero-sum noncooperative dynamic game. Structures of steady-state solutions to the game are then investigated. Sagduyu et al. [15] model the denyof-service (DoS) attacks as stochastic games among non-cooperative selfish nodes that randomly transmit packets to a common receiver and malicious nodes with the dual objectives of blocking the packet transmissions of the other selfish nodes as well as optimizing their individual performance. The NEs are analyzed and the network performance is compared with the cooperative equilibrium. In [16], Li et al. formulate the jamming attack as optimization problem as well as max–min problem and derive the optimal attacking strategy for the jammer to maximize the duration before being detected and the optimal defense strategy for the defender to alleviate the attack damage. Altman et al. study the jamming game in wireless networks with transmission cost [9] and with partially available information [10].

1.4. Summary of contribution and paper organization

Compared with existing work, the focus of our work is not only to alleviate the damage caused by the jammer, but also to fight the jammer actively by draining its energy as quickly as possible. The main contributions of our work can be summarized as follows:

- *Game theoretic framework:* we establish a game theoretic model between the victim network and the energy-limited jammer and derive the NE.
- *Active defense strategy:* we propose an active defense strategy against jamming and demonstrate its benefits via both mathematical analysis and numerical experiment.
- *Distributed strategy update mechanism:* we derive a distributed update mechanism in which the anti-jammer and network nodes adjust their strategies based on observable channel information.

The rest of this paper is organized as follows. Section 2 introduces the network model with related assumptions. Section 3 formulates the jamming game and derives the resulting NEs. Section 4 presents and analyzes our defense strategy. Section 5 and 6 focus on the distributed update mechanism and the implementation issues. Section 7 presents numerical results to evaluate the performance of the proposed defense strategy. Finally, the paper is concluded by Section 8.

2. Network model and problem formulation

We consider a single-hop wireless network consisting of a set $\mathcal{N}$ of n nodes operating on the following generalized version of the slotted-Aloha protocol to access the shared wireless medium: Time is divided into synchronized slots. Each node can send one packet in a slot. If a node has a packet to send, it transmits during the next slot with probability p called channel access probability. Since the above generalized slotted-Aloha scheme is the root of various medium access control protocols widely used nowadays, basing our analysis on it makes our results a generic framework easily extensible to other protocols.

In our study, we focus on the extreme case where all network nodes are continuously backlogged, i.e., they always have packets to transmit. The transmission is successful if there is no collision with other transmissions.

As discussed in Introduction, jamming is a DoS attack whose goal is to disable the communication of the victim network by intentionally causing collisions. To mount such attack, the jammer senses the wireless channel and transmits a jamming packet colliding with legitimately transmitted packets if the channel is not free. In this paper, we focus on energy-limited strategic jammer aiming at keeping the communication of the victim network blocked as long time as possible under its energy budget. To this end, it configures the probability of transmitting jamming packets to strike a balance between keeping a high jamming probability and limiting the energy consumption. Mathematically, the jammer's strategy is modeled by the following optimization problem $\mathbf{P_J}$

$$\mathbf{P_J}: \max_{0\leqslant\theta\leqslant 1} \; T_J \quad \text{s.t.} \quad S \leqslant S_0,$$

where θ denotes the jammer's strategy, i.e., the probability of transmitting jamming packets, T_J denotes the expected time during which the communication of the victim network is blocked by the jammer, S denotes the throughput of the victim network, S_0 denotes the threshold of effective jamming from the jammer's perspective, i.e., to block the communication of the victim network, it has to limit S not to exceed S_0.

Let p denote the channel access probability of the network nodes, the network throughput can be expressed as $S = np(1-p)^{n-1}(1-\theta)$. $\mathbf{P_J}$ can thus be translated to the following optimization problem $\mathbf{P_J'}$:

$$\min_{0\leqslant\theta\leqslant 1} \; U_J = [1-(1-p)^n]\theta$$
$$\text{s.t.} \quad np(1-p)^{n-1}(1-\theta) \leqslant S_0.$$

U_J can be seen as the expected energy consumption of the jammer per slot, given that the energy of transmitting one jamming packet is normalized to 1. As mathematically characterized by $\mathbf{P_J'}$, a strategic jammer searches to block the victim network while minimizing its energy consumption.

At the victim network side, it reacts strategically to operate the most efficiently possible under jamming. Specifically, the network nodes adapt their channel access probability p to maximize the utility function U_N that reflects the difference between the throughput reward and the transmission cost, i.e.,

$$U_N = np(1-p)^{n-1}(1-\theta) - npc,$$

where the throughput reward is normalized to 1 and $c \leqslant 1$ denotes the transmission cost. To simplify our study, we assume that the transmission cost is the same for all packets. Moreover, throughout this paper, to avoid the trivial case where the jammer has no incentive to launch jamming attack, we impose the following assumption on S_0:

$$S_0 < n\hat{p}(1-\hat{p})^{n-1}, \tag{1}$$

where $\hat{p} = \arg\max_{0\leqslant p\leqslant 1} np(1-p)^{n-1} - npc$. Generally, for the jamming to be effective, S_0 should be sufficiently small. The smaller S_0 is, the more effective the jamming is (also the more aggressive the jammer is). In this paper, we are especially interested in the aggressive case with small S_0.

To concentrate on the essential properties of jamming and the proposed defense strategy, we limit our study to jamming at PHY/MAC layers. The jammer does not interpret the semantics of the packets to determine which packet to jam. Interested readers are referred to [8] for such intelligent jamming attacks in IEEE 802.11 DCF, which are out of the scope of this paper. Despite some simplifications made in our model, the analysis of the jamming attacks and the derived defense strategy are far from trivial and indeed provide valuable insight on the topic, as shown in the reminder of the paper.

3. Jamming game analysis

We model the interactions between the jammer and the victim network as a non-cooperative jamming game G, defined as follows:

Definition 1. The non-cooperative jamming game G is a 3-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{U})$, where $\mathcal{P} = \{\mathcal{J}, \mathcal{N}\}$ denotes the player set consisting of the jammer $\mathcal{J}$ and the victim network $\mathcal{N}$, $\mathcal{A} = [0,1] \times [0,1]$ denotes the strategy space, $\mathcal{U} = \{U_N, U_J\}$ denotes the utility function set. The player $\mathcal{J}(\mathcal{N})$ selects its strategy $\theta(p)$ to minimize (maximize) its utility U_J (U_N).

The solution of the jamming game G is characterized by Nash equilibrium (NE) [18], a strategy profile from which no player has incentive to deviate unilaterally. Our focus in this section is to derive and analyze the NE(s) of G.

Theorem 1. *Let $k \triangleq \frac{S_0}{c}$ and $A(k) \triangleq \sqrt{(1+k)^2 - \frac{4}{n}k}$, G admits two NEs: $p_1^* = 0, \theta_1^* = 1$ and $p_2^* = \frac{1+k-A(k)}{2}, \theta_2^* = 1 - \frac{2^n S_0}{n(1+k-A(k))(1-k+A(k))^{n-1}}$.*

Proof. We proceed by distinguishing two cases of NE:

Case 1: the NE is on the border of the strategy space. In this case, it is easy to check that only $p^* = 0$, $\theta^* = 1$ satisfies the NE definition.

Case 2: the NE is the non-border point of the strategy space: $0 < p^*$, $\theta^* < 1$. In this case, for the network, the global maximum of its utility function is achieved at inner point where $\frac{\partial U_N}{\partial p} = 0$, or

$$(1-p^*)^{n-2}(1-np^*)(1-\theta) = c. \tag{2}$$

On the other hand, at the NE it holds that

$$S = np^*(1-p^*)^{n-1}(1-\theta^*) = S_0. \tag{3}$$

Otherwise, if $S > S_0$, the jammer has incentive to unilaterally decrease θ^*, which contradicts with the definition of NE. □

Combining (2) and (3), we can solve p^* and θ^* as

$$\begin{cases} p^* = \frac{1}{2}\left[1+k-\sqrt{(1+k)^2-\frac{4}{n}k}\right] = \frac{1+k-A(k)}{2}, \\ \theta^* = 1 - \frac{2^n S_0}{n(1+k-A(k))(1-k+A(k))^{n-1}}. \end{cases} \tag{4}$$

The following two lemmas guarantee that the derived solution (p^*, θ^*) in (4) is a NE. Lemma 1 proves that it is an inner point of the strategy space. Lemma 2 shows that $U_N(p^*, \theta^*) > 0$.

Lemma 1. *It holds that* $\frac{k}{n(1+k)} < p^* < \min\{\frac{1}{n}, \frac{k}{n}\}$ *and* $0 < \theta^* < 1$.

Proof. To prove $\frac{k}{n(1+k)} < p^* < \min\{\frac{1}{n}, \frac{k}{n}\}$, we rewrite p^* in (4) as

$$p^* = \frac{1}{2}\,\frac{\frac{4k}{n}}{1+k+\sqrt{(1+k)^2-\frac{4}{n}k}}.$$

On the other hand, we have:

$$\begin{cases} \sqrt{(1+k)^2-\frac{4}{n}k} < 1+k, \\ \sqrt{(1+k)^2-\frac{4}{n}k} = \sqrt{(1-k)^2+4(1-\frac{1}{n})k} > |1-k|. \end{cases}$$

It follows that $\frac{k}{n(1+k)} < p^* < \min\{\frac{1}{n}, \frac{k}{n}\}$. We next prove $0 < \theta^* < 1$. It is obvious that $\theta^* < 1$. Suppose, by contradiction, that $\theta^* \leqslant 0$, it follows from (1) and (2) that

$$np^*(1-p^*)^{n-1} \geqslant n\hat{p}(1-\hat{p})^{n-1} > S_0 \geqslant \frac{S_0}{1-\theta^*},$$

which contradicts with (3). □

Lemma 2. *It holds that* $U_N(p^*, \theta^*) > 0$.

Proof. Noticing (3), we have

$$U_N(p^*, \theta^*) = np^*(1-p^*)^{n-1}(1-\theta^*) - np^*c = np^*\frac{S_0}{np^*} - np^*c = np^*c\left(\frac{k}{np^*} - 1\right).$$

It follows from Lemma 1 that $U_N(p^*, \theta^*) > 0$. Combining the above analysis in Case 1 and Case 2, we conclude our proof of Theorem 1. □

As an important implication of Theorem 1, the network is paralyzed ($S = 0$) at the border NE where the jammer adopts the most aggressive strategy by setting θ^* to 1 and the network nodes keep silent.

In contrast to the common sense that the jamming attack is usually very energy consuming, Theorem 1 shows that the jamming attack is very cost-effective at the border NE. This is due to the fact that any rational node in the victim network, aware of the existence of the jammer, will not attempt to send any packet, which brings no gain but a waste of energy. Take the IEEE 802.11 WLAN as an example, the rationality of nodes leads to doubling the value of the contention window (CW) after each collision. In such context, the jammer makes the network node repeatedly double the CW value until finally the transmission attempt is given up, which corresponds to the border NE in Theorem 1. Consequently, the jammer can disrupt the communication of the victim network with little energy consumption.

4. Proposed jamming defense strategy

Motivated by the analytical results of previous section, especially the detrimental damage caused by the jammer at the border NE, we propose our jamming defense strategy in this section. Different form existing solutions that retreat from the jammed area or switch to other channels to avoid being jammed, our approach tackles the problem from a new angle, which is inspired from the following philosophy:

The best defense is an offense.

Applying the above philosophy in our context, we propose our jamming defense strategy consisting of actively fighting the jammer face-to-face by draining its energy as fast as possible. The task of fighting against the jammer is designated to a special network entity referred to as *anti-jammer*. Several practical implementations are possible: e.g., the anti-jammer can be a network node disposing a large amount of energy; or, the role of the anti-jammer can be assigned to all network participants in a distributed way, i.e., each node serves as the anti-jammer for a certain period of time for the interests of the whole network. With the goal of draining the jammer's energy, the anti-jammer transmits a bait packet indistinguishable from legitimate packets at probability q at each slot to attract the jammer to emit the jamming packet.

In the sequel, we formulate the new jamming game G' with the anti-jammer and characterize the resulting NE. The central questions we pose in order to study the performance of the proposed defense strategy are: (1) Does G' have NE? (2) If so, is it unique and can players converge

to the NE? (3) How does the NE compare with the NEs in Theorem 1? Is it more desirable for the network?

4.1. Jamming game with anti-jammer

In this subsection, we study the jamming game G' consisting of the victim network of n nodes, a jammer and an anti-jammer, based on the same network model as in G. The only difference is that the anti-jammer is introduced operating on q to fight against the jammer. In this new context, the network throughput becomes $S = np(1-p)^{n-1}(1-q)(1-\theta)$. The utility function of the network can be written as:

$$U_N = np(1-p)^{n-1}(1-q)(1-\theta) - npc.$$

The jammer's optimization problem $\mathbf{P}'_{\mathbf{J}}$ becomes

$$\min_{0\leqslant\theta\leqslant 1} \; U_J = [1-(1-p)^n(1-q)]\theta$$
$$\text{s.t.} \quad np(1-p)^{n-1}(1-q)(1-\theta) \leqslant S_0.$$

The following theorem establishes the NE of G'.

Theorem 2. *If $q > 0$, G' admits a unique NE (p^*, θ^*).*

1. If the following condition holds

$$n(1-q)(1+k-A(k))(1-k+A(k))^{n-1} > 2^n S_0, \quad (5)$$

$$\begin{cases} p^* = \frac{1+k-A(k)}{2}, \\ \theta^* = 1 - \frac{2^n S_0}{n(1-q)(1+k-A(k))(1-k+A(k))^{n-1}}. \end{cases} \quad (6)$$

2. If the condition (5) does not hold,

$$\begin{cases} p^* = \arg\max_p \quad (1-q)p(1-p)^{n-1} - cp, \\ \theta^* = 0. \end{cases} \quad (7)$$

Proof. We distinguish two cases: (1) The NE is the inner point of the strategy space and (2) The NE is at the border. We start by examine the inner NE. Let $c' \triangleq \frac{c}{(1-q)}, S'_0 \triangleq \frac{S_0}{(1-q)}$, the non-border NE (p^*, θ^*) can be derived following exactly the same way as case 2 in the proof of Theorem 1. The condition of the derived solution to be the non-border NE is $0 < p^*, \theta^* < 1$, which is satisfied if and only if (5) holds. It can be further shown that in this case, there is no border NE.

On the other hand, if (5) does not hold, G' does not have non-border NE. In this case, by checking the border of the strategy space, we can show that the only NE is $p^* = \arg\max_p (1-q)p(1-p)^{n-1} - cp$ and $\theta^* = 0$. □

Theorem 2 establishes the existence and uniqueness of the NE and quantifies the relation between different parameters (S_0, c and q) and the resulting NE. Theorem 2 implies that by properly setting q, the border NE in Theorem 1 where the jammer can paralyze the network with little energy consumption can be eliminated in G' and the game reaches a more desirable NE (6) from the network's perspective. In this regard, the anti-jammer plays the role of refining NE by eliminating the undesirable equilibrium.

In the following corollary, we provide a simplified necessary condition on q to ensure that the unique NE is the non-border NE derived in (6).

Corollary 1. G' admits a unique non-border NE (p^*, θ^*) given by (6) if the following sufficient condition holds:

$$\frac{(1-q)k}{1+k}\left[1 - \frac{k}{n(1+k)}\right]^{n-1} > S_0.$$

Proof. Following Lemma 1, we have

$$(1-q)np^*(1-p^*)^{n-1} > \frac{(1-q)k}{1+k}\left(1 - \frac{k}{n(1+k)}\right)^{n-1}.$$

Hence, if $\frac{(1-q)k}{1+k}\left(1 - \frac{k}{n(1+k)}\right)^{n-1} > S_0$, it holds that $(1-q)np^*(1-p^*)^{n-1} > S_0$. From Theorem 2, G' admits a unique non-border NE (6). □

Corollary 1 provides a guideline for the anti-jammer to choose its strategy q to avoid the less desirable NE. In the asymptotic scenario where $n \gg 1$, noticing that $k = S_0/c$, after some mathematical arrangement, the sufficient condition in Corollary 1 can be further simplified to $q < 1 - (S_0 + c)e^{\frac{k}{1+k}}$.

4.2. NE analysis: comparison with G

After solving the NE of G', it is natural and interesting to compare the non-border NE of G' given in (6) with the non-border NE of G derived in (4). As can be seen from (4) and (6), the network utility U_N is the same at the two non-border NEs. In the following theorem, we investigate the jammer's utility U_J at the non-border NE of G and G'.

Theorem 3. *By wisely choosing q, the anti-jammer can increase the jammer's energy consumption at the non-border NE under the following condition:*

$$S_0 < np^*(1-p^*)^{2n-1}, \quad (8)$$

where $p^* = \frac{1+k-A(k)}{2}$.

Proof. Let U_J^G and $U_J^{G'}$ denote the jammer's utility at the non-border NE of G and G', we have

$$U_J^G = [1-(1-p^*)^n]\left[1 - \frac{S_0}{np^*(1-p^*)^{n-1}}\right],$$

$$U_J^{G'} = [1-(1-p^*)^n(1-q)]\left[1 - \frac{S_0}{np^*(1-p^*)^{n-1}(1-q)}\right],$$

where $p^* = \frac{1+k-A(k)}{2}$. After some straightforward mathematic manipulations, we get

$$U_J^{G'} - U_J^G = (1-p^*)^n q\left[1 - \frac{S_0}{np^*(1-p^*)^{2n-1}(1-q)}\right].$$

Under the condition (8), if $0 < q < 1 - \frac{S_0}{np^*(1-p^*)^{2n-1}}$, we have $U_J^{G'} > U_J^G$, i.e., the existence of the anti-jammer actually can increase the jammer's energy consumption at the non-border NE.

On the contrary, if $S_0 \geqslant np^*(1-p^*)^{2n-1}$, then it follows that:

$$1-\frac{S_0}{np^*(1-p^*)^{2n-1}(1-q)} \leqslant 1-\frac{S_0}{np^*(1-p^*)^{2n-1}} \leqslant 0,$$

i.e., $U_J^2 \leqslant U_J^1$. In this case, regardless of the value of q, the anti-jammer cannot increase the jammer's energy consumption. □

In the following corollary, we provide a simplified sufficient condition under which the result of Theorem 3 holds.

Corollary 2. If $S_0 + c < \left(1-\frac{1}{n}\right)^{2n-1}$, or if $S_0 + c < 1/e^2$ when $n \gg 1$, the anti-jammer can increase the jammer's utility at the NE by wisely choosing q.

Proof. Recall Lemma 1, we have:

$$S_0 + c < \left(1-\frac{1}{n}\right)^{2n-1} \rightarrow S_0\frac{1+k}{k} < \left(1-\frac{1}{n}\right)^{2n-1} \rightarrow S_0 < np^*(1-p^*)^{2n-1}.$$

From Theorem 2, this indicates that by choosing proper q, the anti-jammer can increase the jammer's utility at the non-border NE. When $n \gg 1$, the above sufficient condition becomes $S_0 + c < 1/e^2$. □

As a summary of previous analysis, we have demonstrated via Theorem 2 and 3 the following benefits of the proposed defense strategy. Theorem 2 states that if q is properly chosen, the jamming game admits a unique non-border NE given in (6). Compared with the non-border NE in G without anti-jammer, the network gets the same payoff at the non-border NE in G'. Theorem 3 further shows that under the condition (8), the jammer consumes more energy. In this perspective, our solution not only can eliminate the undesirable NE (the border NE in G), but also can increase the jammer's energy consumption at the remaining NE. As a result, under the condition of (8) which is especially true for aggressive jammer, our solution can force the jammer to spend its energy more quickly without degrading the network performance.

Theorem 3 quantifies the condition under which $U_J^G \geqslant U_J^{G'}$. Next we provide a qualitative explication on the implication behind. The goal of introducing the anti-jammer is to increase the jammer's energy consumption without degrading the network performance. From another angle, the anti-jammer can be regarded as a jammer that jams the traffic of both the network and the jammer, the latter being our objective while the former the side effect. When the condition (8) is met, i.e., $S_0 + c$ is sufficiently small, the cost of jamming the network traffic is less than the gain of jamming the jammer. In contrast, if the condition is not met, the benefit of introducing the anti-jammer is counter-balanced by its side effect, i.e., the anti-jammer actually helps the jammer jam the network. In this sense, introducing the anti-jammer to counter jamming is like using a "double-bladed sword" which brings both benefit and side effect. Therefore, the strategy of the anti-jammer q should be carefully chosen so as to strike a balance between maximizing the benefit and limiting the side effect.

4.3. Choosing optimal value of q

In this subsection, we seek the optimal value of q that achieves the above balance, i.e., we solve the optimal value of q that maximizes the jammer's energy consumption at the non-border NE under the condition (8).

Theorem 4. *Under the condition (8), the optimal strategy for the anti-jammer is* $q^* = 1-\sqrt{\frac{S_0}{np^*(1-p^*)^{2n-1}}}$.

Proof. From (6), at the non-border NE, we have

$$U_J^{G'} = [1-(1-p^*)^n(1-q)]\left[1-\frac{S_0}{np^*(1-p^*)^{n-1}(1-q)}\right].$$

By imposing $\frac{\partial U_J^{G'}}{\partial q} = 0$, the optimal value of q can be solved as

$$q^* = 1-\sqrt{\frac{S_0}{np^*(1-p^*)^{2n-1}}}. \tag{9}$$

A necessary condition that q^* given by (9) is the optimal value is that G' has a unique non-border NE and $0 < q^* < 1$. From Theorem 2, this can be translated to check whether the condition (5) holds or not. We proceed our analysis as follows:

$$n(1-q^*)(1+k-A(k))(1-k+A(k))^{n-1} > 2^nS_0$$
$$\leftarrow np^*(1-p^*)^{n-1}(1-q^*) > S_0 \quad \text{From (9)}$$
$$\leftarrow \sqrt{\frac{nS_0p^*}{(1-p^*)}} > S_0 \quad \text{Noticing } p^* < 1$$
$$\leftarrow np^*(1-p^*)^{2n-1} > S_0 \quad \text{From (8)}$$

The above shows that (5) holds, q^* is the optimal strategy to drain the jammer's energy, which concludes our proof. □

4.4. Further discussion and limitation of proposed strategy

It is insightful to note that the interactions among the network, the jammer and the anti-jammer can be modeled by a Stackelberg game [18], in which the anti-jammer is the leader, the network and the jammer are the followers. The followers choose their strategies p and θ to maximize and minimize their utility function U_N and U_J based on the leader's strategy q. The leader chooses its strategy q to maximize its utility function (i.e., the jammer's energy consumption), taking into account that the followers will subsequently choose their strategy to greedily maximize/minimize their own payoff. Apply our analysis in this section, the Stackelberg game admits a unique NE (q^*, p^*, θ^*) under the condition (8).

We conclude this section by discussing the limitations of the proposed defense strategy. Firstly, our solution aims at draining the jammer's energy rather than coping with jamming. As a result, although the jammer consumes more energy to mount the jamming attack, yet the communication of the victim network is disrupted as long as the jammer does not use up its battery. Secondly, as discussed in the beginning of Section 4, the role of anti-jammer can be designated to the network node disposing a large

amount of energy or to all network participants in a distributed way, e.g., network participants can form a defense ring in which each member on the ring assures for one time period the task of the anti-jammer. In this regard, the altruism of the anti-jammer is implicitly assumed. However, this assumption is not always valid, especially in open environments where network participants are selfish and have no incentive to spend their own energy for the interests of the common, including themselves. In such cases, incentive mechanisms [19] are needed to avoid the above common dilemma. Thirdly, as shown in Theorems 2 and 3 as well as the numerical experiments presented later, the proposed solution is less effective when the jammer acts more mildly by operating on large S_0. It is insightful to note that in such cases, the attack is no more a jamming attack in the strict sense in that the jammer's goal is not to block the network communication as that of pure jamming with S_0 sufficiently small, but rather to limit the network throughput with a mild threshold S_0.

5. Game dynamics and distributed strategy update

In the previous section, we have studied some structural properties of the NE in the jamming game with the anti-jammer and demonstrated the benefits of the proposed defense strategy. In this section, we extend our efforts to study the game dynamics. More specifically, we develop distributed strategy update mechanisms for players to adjust their strategies to converge to the equilibrium based on only observable channel information.

We start with the victim network. The core idea is to adjust the strategy (i.e., channel access probability) based on local channel information to gradually converge to the system optimum. Noticing that the objective of the network nodes is to maximize the global network utility under jamming, we propose the following distributed update mechanism of the channel access probability:

$$p_i(t+1) = \left[p_i(t) + \lambda\left((1-q)(1-\theta)(1-np_i(t)) \times \prod_{j\in\mathcal{N}, j\neq i}(1-p_j(t)) - (1-p_i(t))c\right)\right]_0^{p_{max}}, \quad (10)$$

where t is the iteration index, $[x]_a^b$ denotes $\max\{a,\min\{b,x\}\}$, λ is the step size, $p_{max}\in(0,1)$ is the system parameter.

Theorem 5. *Under the condition (8), if* $\frac{(1-q)(1-\theta)(1-np_{max})}{1-p_{max}} < c < (1-q)(1-\theta)(1-p_{max})^{n-1}$, *the update scheme (10) has a unique fixed point, which is also the optimal point where the global network utility is maximized.*

Proof. The proof, detailed in Appendix, consists of two steps: we first show that any border point cannot be a fixed point of (10); we then focus on the non-border fixed point and prove that $\{\tilde{p}\}$ is the only non-border fixed point of (10), where $\tilde{p}$ is the root of $(1-q)(1-\theta)(1-p)^{n-2}(1-np)=c$. It is easy to see that $\{\tilde{p}\}$ is also the optimal point where the global network utility is maximized. □

Remark. (10) can be seen as a subgradient strategy update scheme that gradually approaches the fixed point, which corresponds to the global optima.

We then analyze the jammer's strategy. Noticing that the jammer's utility is to minimize its energy consumption while limiting the network throughput $S \leqslant S_0$, for the iteration $t+1$, its best strategy $\theta(t+1)$ can be derived by

$$S_0 = [1-\theta(t+1)](1-q)\sum_{i\in\mathcal{N}} p_i(t)\prod_{j\in\mathcal{N}, j\neq i}(1-p_j(t)).$$

However, in practice, since the jammer cannot distinguish the traffic of the anti-jammer and that of an ordinary node, it is impossible to compute $\theta(t+1)$ from the above equation. We thus consider in our study a more practical update scheme for the jammer in which it chooses the smallest θ such that the aggregated throughput including the anti-jammer's traffic is no more than αS_0, where $\alpha \geqslant 1$ is a tolerant factor, i.e.,

$$[1-\theta(t+1)]\left[(1-q)\sum_{i\in\mathcal{N}} p_i(t)\prod_{j\in\mathcal{N}, j\neq i}(1-p_j(t)) + q\prod_{j\in\mathcal{N}}(1-p_j(t))\right] \leqslant \alpha S_0.$$

$\alpha = 1$ corresponds to the scenario in which the jammer is not aware of the existence of the anti-jammer or it wants to limit the network throughput regardless of the anti-jammer's strategy q. This update scheme can be formally expressed as:

$$\theta(t+1) = \left[1 - \frac{\alpha S_0}{(1-q)\sum_{i\in\mathcal{N}} p_i(t)\prod_{j\in\mathcal{N}, j\neq i}(1-p_j(t)) + q\prod_{j\in\mathcal{N}}(1-p_j(t))}\right]_0^1. \quad (11)$$

In the following theorem, we analyze the equilibrium of G' under the update scheme (10) for the network nodes and (11) for the jammer.

Theorem 6. *The strategy update scheme in which the network nodes follow (10) and the jammer follows (11) admits a unique fixed point under the following condition:*

$$\begin{cases} \frac{\alpha S_0}{(1-p_{max})^n} < q \leqslant \frac{n}{n+1}, \\ \frac{(n-1)p_{max}}{1-p_{max}} + \frac{q}{1-q} < \frac{\alpha S_0}{c} < \frac{p_{max}(1-p_{max})}{1-np_{max}} + \frac{(1-p_{max})^2}{1-np_{max}}\frac{q}{1-q}. \end{cases} \quad (12)$$

Specifically, the fixed point coincides with the non-border NE (p^*,θ^*) derived in (6) if $\alpha\ S_0 = (1-\theta^*)[q(1-p^*)^n + n(1-q)p^*(1-p^*)^{n-1}]$.

Proof. Please refer to Appendix for detailed proof. □

Theorem 6 states that G' has a unique NE under the update scheme (10) and (11). In Section 7, the game dynamics of G' (i.e., the convergence to the unique equilibrium) is further studied via simulation under the above update scheme.

We conclude this section by analyzing the anti-jammer's strategy q, which should be carefully tuned in order to achieve a balance between maximizing the benefit and limiting the side effect, as discussed in the end of Section 4.2. Noticing that calculating the optimal value of q requires the knowledge of α which is not available to the anti-jammer, we propose the following adaptive recursive

search method to find the locally optimal value of q. We evaluate the proposed method via simulation in Section 7.

1. Set Δq, ε to some small values, T a sufficient long time for convergence. Initialize $q(0) = 0$. Set $m = 0$.
2. Set $m = m + 1$, wait time T for the players to converge, then estimate the jammer's utility $U_J(m)$.[1]
   (a) If $U_J(m) > U_J(m-1)$, set $q(m+1) = q(m) + \Delta q$.
   (b) If $U_J(m) < U_J(m-1)$, set $q(m+1) = q(m) - \Delta q$.
3. Stop until $|U_J(m) - U_J(m-1)| < \varepsilon U_J(m)$.

6. Implementation issue

Previously, we have investigated the dynamics of G' and the distributed strategy update scheme for players to converge to the unique operating point. However, for the network nodes and anti-jammer, since they usually do not have access to the access probability of others, they cannot directly implement the discussed update scheme. In this section, we address this implementation issue, more specifically, how to estimate $(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j)$ for node i to compute $p_i(t)$ based on (10) and how to estimate U_J for the anti-jammer to update q.

Our solution is based on the *Idle Sense* approach (see [17] for a detailed description) allowing a player to estimate the channel condition by observing the average number of consecutive idle slots between two transmission attempts. As a desirable property, our solution is based on only observable information and does not generate any additional message.

We start with the network nodes. Let $P_{idle} = (1-q)(1-\theta)\prod_{j\in\mathcal{N}}(1-p_j)$ be the probability of an idle slot and n_{idle} be the number of average consecutive idle slots between two transmission attempts, it holds that $n_{idle} = \frac{P_{idle}}{1-P_{idle}}$. It follows that:

$$(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j) = \frac{n_{idle}}{n_{idle}+1}\cdot\frac{1}{1-p_i}.$$

Since node i knows its own strategy $p_i(t)$ and can observe $n_{idle}(t)$, it can compute $p(t+1)$ based on (10).

We then turn to the anti-jammer who needs to estimate $U_J = [1-(1-p)^n(1-q)]\theta$, where p and θ is the converged value of $p_i(t), \forall i \in \mathcal{N}$ and $\theta(t)$. To this end, it estimates the network throughput as $S = \frac{N_s}{N_t}$, where N_s is the number of successful transmission on the channel within N_t, the measuring period. It then can establish the equation

$$n(1-q)(1-\theta)p(1-p)^{n-1} = \frac{N_s}{N_t}. \tag{13}$$

On the other hand, apply the Idle Sense approach, we have

$$(1-q)(1-\theta)(1-p)^n = P_{idle} = \frac{n_{idle}}{n_{idle}+1}, \tag{14}$$

which is observable to the anti-jammer. By (13) and (14), the anti-jammer can solve p and θ to further estimate U_J.

At the end of this section, we take $(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j)$ as an example to investigate the accuracy of the estimation of our solution. Based on the central limit theory, given m samples of n_{idle}, we have

$$\lim_{m\to\infty} P\left(\left|\frac{\overline{n_{idle}} - \frac{P_{idle}}{1-P_{idle}}}{\sigma/\sqrt{m}}\right| \leqslant z\right) = \frac{1}{\sqrt{2\pi}}\int_{-z}^{z} e^{-r^2/2}dr,$$

where σ is the variance of n_{idle}.

Hence, $(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j)$ can be precisely estimated if sufficient samples on n_{idle} is collected. However, this requires long periods of observation and may lead to slower convergence rate. Therefore, there is a trade-off between the accuracy of the observation and the delay of convergence. Based on the experiments we conduct, $m = 10 \sim 25$ achieves fairly good estimation with a reasonable convergence delay.

7. Numerical results

In previous study, we establish a game theoretic model on jamming with the proposed defense strategy and perform mathematical analysis on the existence, uniqueness of the NE and the game dynamics. In this section, we conduct numerical study to gain more in-depth insight on the NE and the performance of the defense strategy, which cannot be derived directly from analytical results.

7.1. NE analysis of G and G′

We start with the numerical analysis of the NE of the jamming game formulated previously, both with and without anti-jammer. We simulate a single-hop wireless network of 10 nodes. The transmission cost c is set to 0.01. Fig. 1 plots the non-border NE of G derived in Theorem 1 as a function of S_0. Fig. 2 plots the optimal strategy of the anti-jammer q^* and the NE of G' as a function of S_0 when the anti-jammer operates on q^*. As shown in the results for both cases, when the jammer becomes more aggressive, i.e., S_0 becomes smaller, it tends to increase the jamming probability at the NE. Consequently, the victim network reacts by decreasing their transmission probability at the NE. The optimal strategy of the anti-jammer also becomes more aggressive. Moreover, it can be checked that when $q \to 0^+$, the condition (5) equals to $S_0 < 0.14$. This is confirmed by the numerical results in Fig. 2 that $q^* > 0$ when

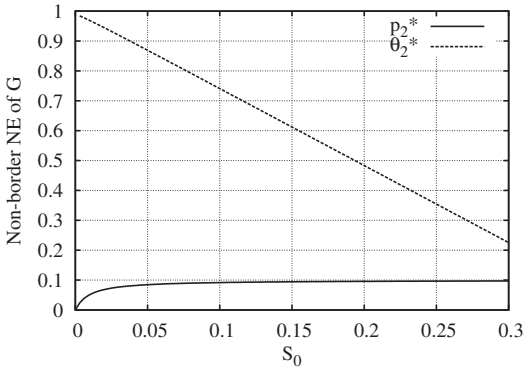

Fig. 1. Non-border NE of G.

[1] How to estimate U_J is addressed in Section 6.

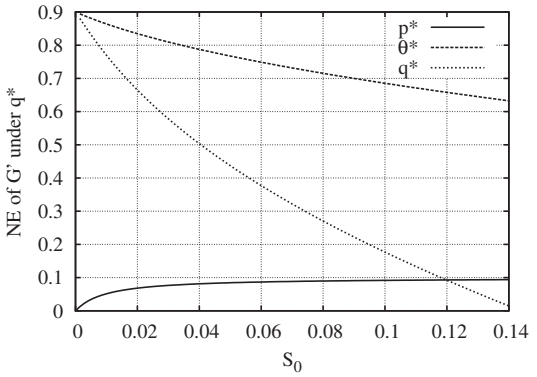

Fig. 2. NE of G' under q^*.

approximately $S_0 < 0.14$. As q^* tends to 0, the NE of G' coincides with the non-border NE of G, as shown in Fig. 1 and 2.

7.2. Performance evaluation of proposed defense strategy

We then evaluate the performance of the proposed defense strategy by comparing the jammer's utility U_J at the non-border NE of G and the unique NE of G', as plotted in Fig. 3. It is insightful to notice that the jammer's energy consumption at the non-border NE of G first increases sharply w.r.t. S_0 and then decreases mildly when S_0 is large. In fact, with the increase of S_0, p^* increases and θ^* decreases. Noticing that U_J is increasing in p^* and θ^*, the results in Fig. 3 indicates that U_J is much more sensible to p^* than to θ^* with small S_0 and less sensible to p^* with large S_0. This observation shows that the more aggressive jamming is also more cost-effective in terms of energy. In this sense, the border NE in G can be regarded as an extreme scenario where the jammer paralyzes the network with little energy consumption, as discussed in Section 3.

In contrast, when the proposed defense strategy is implemented, U_J decreases monotonously in S_0 at the NE, as shown in Fig. 3. As observed from Fig. 2, the anti-jammer acts more aggressively when the jammer is more aggressive, i.e., S_0 is small. Noticing that U_J is increasing in q, the interesting observation in Fig. 3 indicates that the influence of q on U_J outweighs that of p on U_J when S_0 is small, thus U_J increases when S_0 decreases in G'. From Fig. 3, we can also see that the jammer consumes more energy at the NE of G' regardless the value of S_0, which clearly demonstrates the benefits of the proposed defense strategy, especially with the aggressive jammer. We also observe that the network utility U_N is almost the same in G as in G'.

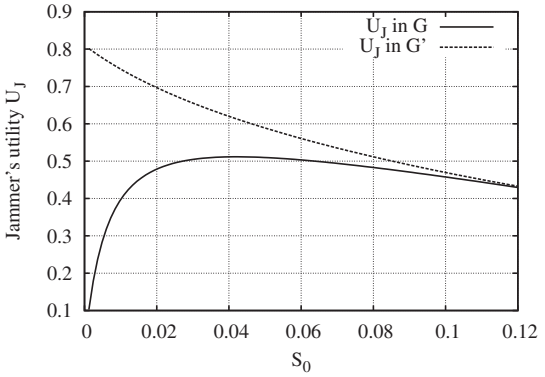

Fig. 3. Comparison of U_J in G and G'.

We also study the impact of the anti-jammer's strategy on the jammer's utility at the NE by plotting U_J at the NE of G' as a function of q with different value of S_0. As illustrated in Fig. 4, U_J is almost the same if q is slightly smaller than the optimal strategy q^*, but chutes sharply after q reaches q^*, especially under the aggressive jammer with small S_0. An important guideline that can be drawn from the results is that a conservative strategy at the anti-jammer yields better performance than a too aggressive one.

We then compare the energy consumption of the jammer and the anti-jammer at the NE when the anti-jammer operates on q^*. The result is shown in Fig. 5, where E_J denotes the total energy consumption of the jammer, e_J denotes the energy consumption of emitting a jamming packet, E_A denotes the total energy consumption of the anti-jammer, e_A denotes the energy consumption of emitting a bait packet. From the anti-jammer's perspective, Fig. 5 shows the upper-bound of the energy consumption to fight against the jammer since the anti-jammer will never emit bait packets with probability larger than q^*.

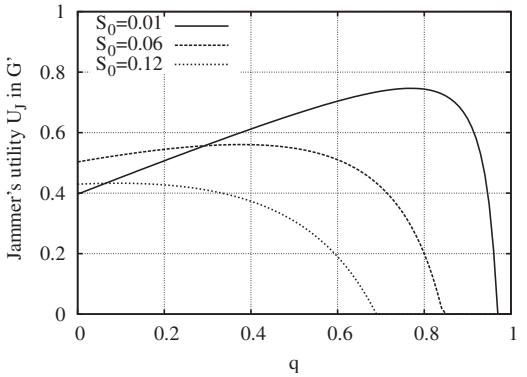

Fig. 4. U_J in G' as a function of q.

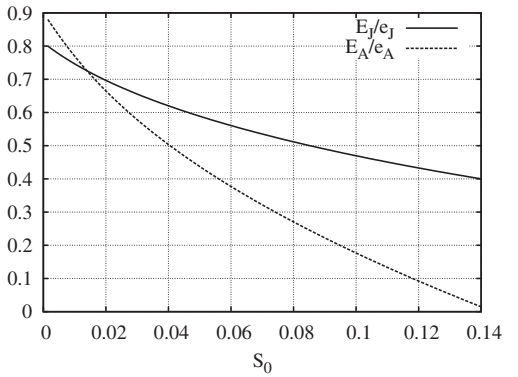

Fig. 5. Energy consumption comparison between the jammer and the anti-jammer.

Note that Fig. 4 shows that even the anti-jammer operates on a conservative strategy with q significantly less than q^*, (i.e., the energy consumption of anti-jammer is significantly less than that in Fig. 5), we can still achieve a reasonably effective result of eliminating the inefficient NE in Section 3 and forcing the jammer to maintain its energy consumption at a high level. For example, even if the anti-jammer operates on $q^*/2$, i.e., its energy consumption is half of the upper bound in Fig. 5, we can observe from Fig. 4 that the jammer's energy consumption is still maintained at 80%, 96% and 99% as that in Fig. 5 in the cases where $S_0 = 0.01$, 0.06 and 0.12. This simulation result, combined with the fact that the role of anti-jammer can be assigned to all network participants in a distributed way (cf. Section 4), demonstrate that the proposed strategy is also energy-efficient and that the anti-jammer can configure its strategy to keep a balance between the intensity of fighting the jammer and its energy consumption.

7.3. Game dynamics

Finally, we study the dynamics of G' by investigating the strategy update mechanisms proposed in Section 5. Figs. 6 and 7 plot the trajectory of the players' strategies under the update mechanism (10) for the network nodes and (11) for the jammer. The step size λ is set to 0.1. S_0 is set to 0.05.

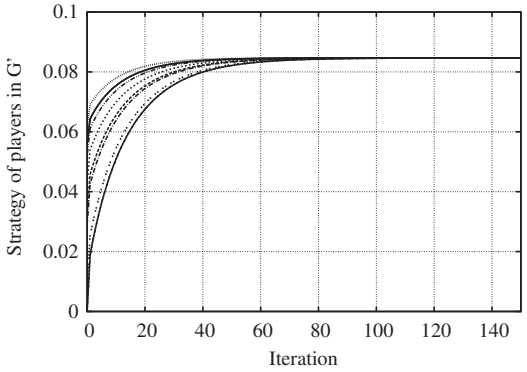

Fig. 6. Strategy trajectory of network nodes under (10).

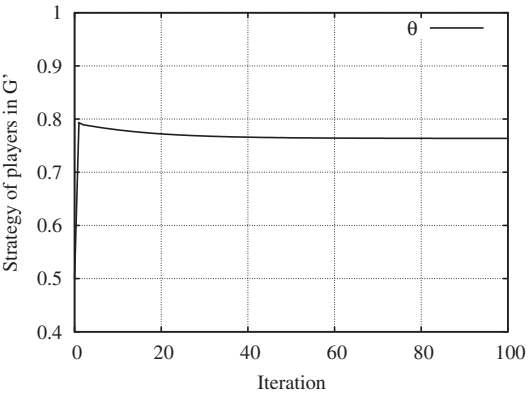

Fig. 7. Strategy trajectory of jammer under (11)

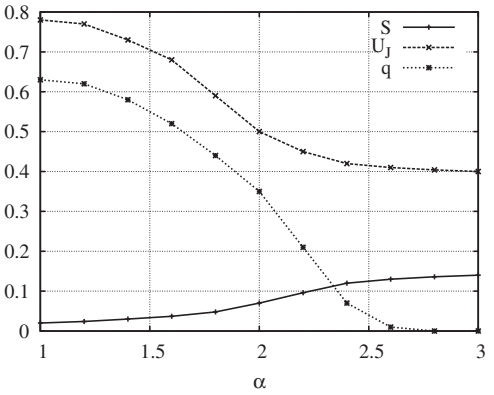

Fig. 8. Performance evaluation of the adaptive recursive search.

p_{max} is set to 0.1. The anti-jammer's strategy is set to the optimal value $q^* = 0.44$, as can be observed in Fig. 2. α is set to 1.87. With this parameter setting, it can be checked from Theorem 6 that the unique fixed point of the strategy update scheme (10) and (11) is the NE where $p^* = 0.084$ and $\theta^* = 0.76$, as can be estimated from Fig. 2. As shown in Fig. 6 and 7, if the network nodes follow (10) and the jammer follows (11), the game converges to the unique NE.

We conclude this section by evaluating the performance of the adaptive recursive research method for the anti-jammer to adjust its strategy q. For the parameters: $S_0 = 0.05$, $\Delta q = 0.005$, $\varepsilon = 0.01$. Fig. 8 plots the converged value of the network throughput S, the jammer's utility U_J and the anti-jammer's strategy q as functions of α. As illustrated in Fig. 8, if the jammer operates on large α, the network throughput exceeds the threshold S_0. Thus in order to effectively disrupt the network traffic, the jammer has to act aggressively by choosing a small α. As shown in Fig. 8, this leads to aggressive strategy of the anti-jammer and the increase of the energy consumption for the jammer, where the goal of our proposed defense strategy is achieved.

8. Conclusion

We have investigated jamming attack in wireless networks under a game theoretic framework. Based on the analysis of the jamming game, we proposed a defense strategy consisting of actively fighting the jammer face-to-face by draining its energy. We demonstrated that the proposed defense strategy can eliminate the undesirable equilibrium and increase the energy consumption of the jammer at the remaining equilibrium without degrading the network performance. Despite the limitations discussed in Section 4.4, we believe that the proposed defense strategy provides an alternative and active line of defense whose effectiveness is well demonstrated both analytically and numerically in the paper.

As future work, an interesting direction is to combine the proposed solution and the channel hopping approach. The idea in this paper can be extended in the way that the anti-jammer transmits on the bait channel(s) to decrease the probability that the channel with legitimate

transmission is attacked by the jammer. In this regard, draining the jammers energy and limiting the jamming damage can be achieved simultaneously, which opens a new dimension to the jamming defense strategy.

Appendix A

This section of Appendix completes the detailed proofs omitted from the main text.

A.1. Proof of Theorem 5

Step 1: We show that any border point cannot be a fixed point of (10). Assume, by contradiction, that at the fixed point $\tilde{\mathbf{p}}, \widetilde{p}_i = 0$ or $\widetilde{p}_i = p_{max}$.

- If $\widetilde{p}_i = 0$, then it follows from (10) that

$$(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p}_j) - c \leqslant 0,$$

which, noticing that $\widetilde{p}_j \leqslant p_{max}$, contradicts with $c < (1-q)(1-\theta)(1-p_{max})^{n-1}$.
- If $\widetilde{p}_i = p_{max}$, we have

$$(1-q)(1-\theta)(1-np_{max})\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p}_j) - (1-p_{max})c \geqslant 0,$$

which obviously contradicts with $c > \frac{(1-q)(1-\theta)(1-np_{max})}{1-p_{max}}$.

Combining the above analysis shows that any border point cannot be a fixed point of (10).*Step 2: We show that (10) admits a non-border fixed point which maximizes the network utility.*By imposing $p_i(t) = p_i(t+1) = \widetilde{p}_i, \forall i \in \mathcal{N}$, we obtain n equations

$$(1-q)(1-\theta)\left[1-\frac{(n-1)\widetilde{p}_i}{1-\widetilde{p}_i}\right]\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p}_j) = c \quad \forall i \in \mathcal{N},$$

which can be further transformed into

$$(1-q)(1-\theta)\left(\prod_{j\in\mathcal{N}}(1-\widetilde{p}_j)\right)\left[\frac{1}{1-\widetilde{p}_i} - \frac{(n-1)\widetilde{p}_i}{(1-\widetilde{p}_i)^2}\right] = c \quad \forall i \in \mathcal{N}. \tag{15}$$

Hence, $\forall i_1, i_2 \in \mathcal{N}$, we have

$$\frac{1}{1-\tilde{p}_{i_1}} - \frac{(n-1)\tilde{p}_{i_1}}{(1-\tilde{p}_{i_1})^2} = \frac{1}{1-\tilde{p}_{i_2}} - \frac{(n-1)\tilde{p}_{i_2}}{(1-\tilde{p}_{i_2})^2}.$$

Let $g(x) \triangleq \frac{1}{1-x} - \frac{(n-1)x}{(1-x)^2}$, we have

$$g'(x) = \frac{1}{(1-x)^2}\left[1-\frac{(n-1)(1+x)}{(1-x)}\right].$$

It holds that $g'(x) < 0, \forall x \in (0,1)$ and $g'(x) = 0$ at 0. It follows immediately from (15) that $\tilde{p}_{i_1} = \tilde{p}_{i_2}$. Therefore, at the non-border fixed point, we have $\tilde{p}_i = \tilde{p}, \forall i \in \mathcal{N}$, where $\tilde{p}$ is the root of

$$(1-q)(1-\theta)(1-p)^{n-2}(1-np) = c.$$

We now show that the above equation admits a unique solution in $(0, p_{max})$. To this end, let $Q(p) \triangleq (1-p)^{n-2}(1-np)(1-q)(1-\theta) - c$. We have

$$Q'(p) = [-n(n-1)(1-p)^{n-2} + (n-1)(n-2)(1-p)^{n-3}](1-q)(1-\theta).$$

It can be checked that $Q(p)$ is monotonously decreasing in p in $(0, \frac{2}{n})$ and monotonously increasing in $(\frac{2}{n}, 1)$. Noticing that $Q(0) = 1-c > 0$, $Q(1) = -c < 0$ and following the condition in the theorem,

$$Q(p_{max}) = (1-q)(1-\theta)(1-p_{max})^{n-2}(1-np_{max}) - c < 0.$$

We can show that $Q(p) = 0$ admits a unique solution $\tilde{p} \in (0, p_{max})$. It is further easy to notice that the network utility $n(1-q)(1-\theta)p(1-p)^n - npc$ is maximized at $\tilde{p}$.

A.2. Proof of Theorem 6

Step 1: We show that any border point cannot be a fixed point of (10) and (11). Assume, by contradiction, that $(\tilde{\mathbf{p}}, \tilde{\theta})$ is a border fixed point. It follows straightforwardly from the condition (12) that $0 < \tilde{\theta} < 1$. Hence there exists i such that $\widetilde{p}_i = 0$ or $\widetilde{p}_i = p_{max}$.

- If $\widetilde{p}_i = 0$, then it follows from (10) that

$$(1-q)(1-\tilde{\theta})\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p}_j) \leqslant c.$$

Injecting (11) into the above inequality leads to

$$\frac{\alpha S_0}{\sum_{j\in\mathcal{N}}\frac{\widetilde{p}_j}{1-\widetilde{p}_j} + \frac{q}{1-q}} \leqslant c,$$

which, noticing that $\widetilde{p}_j \leqslant p_{max}$, contradicts with $\frac{(n-1)p_{max}}{1-p_{max}} + \frac{q}{1-q} < \frac{\alpha S_0}{c}$.
- If $\widetilde{p}_i = p_{max}$, we have

$$(1-q)(1-\theta)(1-np_{max})\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p}_j) - (1-p_{max})c \geqslant 0.$$

Injecting (11) into the above inequality leads to

$$\frac{\alpha S_0}{\sum_{j\in\mathcal{N}}\frac{\widetilde{p}_j}{1-\widetilde{p}_j} + \frac{q}{1-q}} \geqslant \frac{(1-p_{max})^2}{(1-np_{max})}c,$$

which contradicts with $\frac{\alpha S_0}{c} < \frac{p_{max}(1-p_{max})}{1-np_{max}} + \frac{(1-p_{max})^2}{1-np_{max}}\frac{q}{1-q}$.

Combining the above analysis shows that any border point cannot be a fixed point.*Step 2: We show that (10) and (11) admits a unique non-border fixed point.* At the non-border fixed point, combining (10) and (11), we obtain n equations:

$$\frac{\alpha S_0}{\sum_{j\in\mathcal{N}}\frac{\widetilde{p}_j}{1-\widetilde{p}_j} + \frac{q}{1-q}} = \frac{(1-\widetilde{p}_i)^2}{1-n\widetilde{p}_i}c \quad \forall i \in \mathcal{N}.$$

Noticing that under the condition (12), $1-n\widetilde{p}_i > 0$, $\frac{(1-\widetilde{p}_i)^2}{1-n\widetilde{p}_i}$ is monotonously increasing in $\widetilde{p}_i$, following the same analysis

as that in Step 2 of the proof of Theorem 5, we have $\tilde{p}_i = \tilde{p} \forall i \in \mathcal{N}$, where $\tilde{p}$ is the root of

$$\frac{\alpha S_0}{\frac{n\tilde{p}}{1-\tilde{p}} + \frac{q}{1-q}} = \frac{(1-\tilde{p})^2}{1-n\tilde{p}} c, \tag{16}$$

which can be further arranged as

$$\frac{\alpha S_0}{c} = \frac{1-\tilde{p}}{1-n\tilde{p}} \left[\left(n - \frac{q}{1-q} \right) \tilde{p} + \frac{q}{1-q} \right].$$

Let $f(\tilde{p}) = \frac{1-\tilde{p}}{1-n\tilde{p}} \left[\left(n - \frac{q}{1-q} \right) \tilde{p} + \frac{q}{1-q} \right]$. $f(\tilde{p})$ is monotonously increasing in $\tilde{p}$ when $q \leqslant \frac{n}{n+1}$. Moreover, noticing (12), we have

$$\begin{cases} f(0) = \frac{q}{1-q} < \frac{\alpha S_0}{c}, \\ f(p_{max}) = \frac{np_{max}(1-p_{max})}{1-np_{max}} + \frac{(1-p_{max})^2}{1-np_{max}} \frac{q}{1-q} > \frac{\alpha S_0}{c}. \end{cases}$$

Therefore, (16) has a unique solution $\tilde{p}$. Noticing that at the non border fixed point, $\tilde{\theta}$ is uniquely determined by $\tilde{p}$, it holds that the update scheme (10) and (11) admits a unique non-border fixed point.

Specifically, if $\theta^* \leqslant \theta_{max}$ and $\alpha\ S_0 = (1-\theta^*)[q(1-p^*)^n + n(1-q)p^*(1-p^*)^{n-1}]$, it is easy to see that (p^*, θ^*) satisfies (10) and (11), thereby is the unique fixed point.

References

[1] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: defenses against wireless denial of service, ACM WiSe, Philadelphia, USA, 2004.

[2] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, B. Thapa, On the Performance of IEEE 802.11 under Jamming, IEEE INFOCOM, Phoenix, AZ, 2008.

[3] X. Liu, G. Noubir, R. Sundaram, S. Tan, Spread: Foiling smart jammers using multi-layer agility, in: IEEE INFOCOM, Anchorage, USA, 2007.

[4] V. Navda, A. Bohra, S. Ganguly, D. Rubenstein, Using channel hopping to increase 802.11 resilience to jamming attacks, in: IEEE INFOCOM 2007, Anchorage, USA, 2007.

[5] A.D. Wood, J.A. Stankovic, S.H. Son, JAM: a jammed-area mapping service for sensor networks, RTSS, Cancun, Mexico, 2003.

[6] M. Cagalj, S. Capkun, J.-P. Hubaux, Wormhole-based antijamming techniques in sensor networks, IEEE Trans. Mob. Comput. 6 (1) (2007) 100–114.

[7] A. D. Wood, J. A. Stankovic, G. Zhou, DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based Wireless Networks, in: IEEE SECON, San Diego, USA, 2007.

[8] G. Lin, G. Noubir, On link-layer denial of service in data wireless LANs, Wireless Comm. Mob. Comput. 5 (3) (2005) 273–284.

[9] E. Altman, K. Avrachenkov, A. Garnaev, A jamming game in wireless networks with transmission cost, NET-COOP 2007, Lecture Notes in Computer Science 4465, 2007, pp. 1–12.

[10] E. Altman, K. Avrachenkov, A. Garnaev, Jamming in wireless networks under uncertainty. WiOpt, Seoul, Korea, 2009.

[11] W. Xu, W. Trappe, Y. Zhang, Anti-jamming timing channels for wireless networks, in: ACM Conference on Wireless Security (WiSec), Alexandria, USA, March–April 2008.

[12] B. Awerbuch, A. Richa, C. Scheideler, A jamming-resistant mac protocol for single-hop wireless networks, in: ACM PODC, Toronto, Canada, 2008.

[13] R. Mallik, R. Scholtz, G. Papavassilopoulos, Analysis of an on–off jamming situation as a dynamic game, IEEE Trans. Commun. 48 (8) (2000) 1360–1373.

[14] W. Xu, W. Trappe, Y. Zhang, T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks, ACM MobiHoc, Urbana-Champaign, USA (2005).

[15] Y.E. Sagduyu, A. Ephremides, A game-theoretic analysis of denial of service attacks in wireless random access, WiOpt, Limassol, Cyprus (2007).

[16] M. Li, I. Koutsopoulos, R. Poovendran, Optimal jamming attack and network defense policies in wireless sensor networks, in: IEEE INFOCOM, Anchorage, USA, 2007

[17] M. Heusse, F. Rousseau, R. Guillier, A. Dula, Idle sense: an optimal access method for high throughput and fairness in rate diverse wireless LANS, in: ACM Sigcomm, Philadelphia, USA, 2005.

[18] R.B. Myerson, Game Theory: Analysis of Conflict, Harvard University Press, Cambridge, MA, 1991.

[19] L. Buttyan, J.-P. Hubaux, Security and Cooperation in Wireless Networks, Cambridge University Press, 2008.

[20] S.-G.H. Michael Hall, Aki Silvennoinen, Effect of pulse jamming on IEEE 802.11 wireless LAN performance, IEEE Milcom (2005).

[21] D. Thuente, M. Acharya, Intelligent jamming in wireless networks with applications to 802.11b and other networks, IEEE Milcom (2006).

Lin Chen currently works as assistant professor in the department of computer science of the University of Paris-Sud XI. He received his B.E. degree in Radio Engineering from Southeast University, China in 2002 and the Engineer Diploma from Telecom ParisTech, Paris in 2005. He also holds a M.S. degree of Networking from the University of Paris 6. His main research interests include security and cooperation enforcement in wireless networks, modeling and control for wireless networks and game theory.

Jean Leneutre is an associate professor at the department of Computer Science and Networks at Telecom ParisTech (French National School of Telecommunications), CNRS LTCI-UMR 5141 laboratory. He received his Ph.D. in Computer Science from Telecom ParisTech in 1998. His main research interests include security models and mechanisms for mobile *ad hoc* networks.