On Order Gain of Backoff Misbehaving Nodes in CSMA/CA-based Wireless Networks

Zhuo Lu Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh NC 27606
Emails: {zlu3, wwang}@ncsu.edu

Cliff Wang
Army Research Office
Research Triangle Park, NC 27709
Email: cliff.wang@us.army.mil

***Abstract*—Backoff misbehavior, in which a wireless node deliberately manipulates its backoff time, can induce significant network problems, such as severe unfairness and denial-of-service. Although great progress has been made towards the design of countermeasures to backoff misbehavior, little attention has been focused on *quantifying* the gain of backoff misbehaviors. In this paper, we define and study two general classes of backoff misbehavior to assess the gain that misbehaving nodes can obtain. The first class, called *continuous misbehavior*, keeps manipulating the backoff time unless it is disabled by countermeasures. The second class is referred to as *intermittent misbehavior*, which tends to evade the detection by countermeasures by performing misbehavior sporadically. Our approach is to introduce a new performance metric, namely *order gain*, which is to characterize the performance benefits of misbehaving nodes in comparison to legitimate nodes. Through analytical studies, simulations, and experiments, we demonstrate the impact of a wide range of backoff misbehaviors on network performance with respect to the number of users in CSMA/CA-based wireless networks.**

I. INTRODUCTION

The carrier-sense multiple-access with collision avoidance (CSMA/CA) protocol, which is widely used in wireless networks such as IEEE 802.11 and IEEE 802.15, relies on a distributed backoff mechanism for efficient use of the shared channel. However, backoff misbehavior [1], which manipulates the backoff time at the medium access control (MAC) layer, is one of the easiest ways to obtain network resources at the cost of performance degradation [1] or even denial-of-service of legitimate nodes [2]. Hence, many works have been done to provide countermeasures to backoff misbehavior [1], [3]–[8]. However, little attention has been focused on quantifying the gain of backoff misbehavior. Thus, a fundamental question remains unsolved: *how to quantify the gain of backoff misbehavior?*

In this paper, we address the problem of quantifying the gain of backoff misbehavior. Our methodology is to study the gain that a misbehaving node can obtain via two general classes of backoff misbehavior. The first class is called *continuous misbehavior*, which performs misbehavior persistently and does not stop until it is disabled by countermeasures. In particular, we consider two extensively-adopted models of continuous misbehavior [1], [4], [7], [8]: 1) *double-window* backoff misbehavior, which conforms to the exponential backoff that is used by legitimate nodes, but has a smaller average backoff time than legitimate nodes. For example, the work in [4] defined the misbehavior model as *double-window* misbehavior and proposed a sequential hypothesis testing algorithm to detect the misbehavior; 2) *fixed-window* backoff misbehavior, which chooses the random backoff time uniformly in a given range. For example, the work in [7] considered *fixed-window* misbehavior as the easiest model for misbehaving nodes and designed an incentive-based protocol to discourage *fixed-window* misbehaving nodes and to motivate all nodes to achieve a Nash equilibrium.

The second class is called *intermittent misbehavior*, which in contrast to continuous misbehavior, performs misbehavior in *on* periods and returns to be legitimate in *off* periods. The goal of intermittent misbehavior is to obtain benefits over legitimate nodes and at the same time to evade misbehavior detection. Although existing literature mainly dealt with continuous misbehavior and focused little attention on intermittent misbehavior, the work in [5] has indicated that an intermittent misbehaving node may evade the detection of misbehavior detectors if the *on* period in which it performs misbehavior is smaller than the monitoring period of misbehavior detectors. However, the gain of intermittent misbehavior, especially the impact of intermittent misbehavior to a wireless network remains unknown yet.

We consider the two classes of backoff misbehavior in slotted CSMA/CA-based wireless networks, in which the time is measured by the number of idle slots[1]. In order to quantify the gain of backoff misbehavior, we introduce a new performance metric, namely *order gain* $G(t)$, as a function of waiting time t that denotes the number of idle slots during a node contends for the channel. Then, we use the metric of order gain to analyze the benefits of the two classes of backoff misbehavior and further evaluate their impacts via simulations and experiments. Our contributions are two-fold.

First, a new metric, order gain, is defined to measure the performance benefits of misbehaving nodes over legitimate nodes, which is helpful in evaluating the gain and impact of a misbehaving node in a CSMA/CA-based wireless network. We find that the order gain of a *double-window* backoff misbehaving node always converges to $\log_2(p/p_{_D})$ as $t \to \infty$, where p and $p_{_D}$ are the collision probabilities of legitimate and misbehaving nodes, respectively. The ratio of collision

[1]The length of an idle slot varies upon different standards. For example, the durations of an idle slot is 20μs in IEEE 802.11b for direct sequence spread spectrum (DSSS), and is 9μs in IEEE 802.11g for orthogonal frequency-division multiplexing (OFDM) with 20MHz channel spacing.

probabilities p/p_D, as shown in [9], converges to 1 as the number of users goes to infinity, which indicates that double-window backoff misbehavior may have marginal gains in a network with a large number of users. While the order gain of a *fixed-window* backoff misbehaving node is an increasing function to infinity as $t \to \infty$, showing that it can always obtain performance gains from backoff misbehavior. We also find that although an intermittent misbehaving node can perform any backoff misbehavior when it is in the *on* state, the order gain of the intermittent misbehaving node always converges as $t \to \infty$, regardless the misbehaving scheme in the *on* state.

Second, we validate the impact of backoff misbehavior via simulations and experiments. Our simulation and experimental results show that both *double-window* and *fixed-window* backoff misbehaviors can achieve significant gains when the number of users is small. *Double-window* backoff misbehavior is more sensitive to the number of users and has marginal gains when the number of users is large. Thus, the number of users can be considered as an evaluating factor for the deployment of a counter-strategy to backoff misbehavior in a wireless network. Our experimental results also show that an intermittent misbehaving node can not achieve substantial gain by setting a short *on* period to perform misbehavior.

The rest of this paper is organized as follows. In Section II we introduce preliminaries and formulate the problem of quantifying the gain of backoff misbehavior. In Sections III, we present our main results via analytical modeling and simulations. In Section IV, we present experimental results to show the performance of misbehaving nodes. Finally, we conclude in Section V.

II. Preliminaries and Problem Statement

In this section, we first introduce the models of backoff misbehavior in CSMA/CA-based wireless networks, then define the order gain of backoff misbehaviors for later analysis.

A. CSMA/CA Backoff and Misbehaviors

In wireless networks, CSMA/CA features a distributed control algorithm for resolving packets collisions due to contending a shared channels by uncoordinated users. A widely-used collision resolution algorithm is *binary exponential backoff*, which has been adopted in many standards, such as Ethernet and 802.11 distributed coordination function (DCF). In binary exponential backoff, a node which has packets ready to transmit keeps sensing the channel until the channel is idle and then generates a random backoff time uniformly from $[0, w-1]$, where w is called *contention window*. At first w is set to be w_0, which is called *minimum contention window*[2], and is doubled after each collision. According to this procedure, we formally define legitimate CSMA/CA backoff as follows.

Definition 1 (Legitimate binary exponential backoff): The legitimate CSMA/CA backoff scheme $\mathcal{B}$ is defined as the backoff mechanism in which the random backoff time $T(i)$ is chosen uniformly from $[0, 2^i w_0 - 1]$ after the i-th collision of a packet, where w_0 is the minimum contention window.

Legitimate CSMA/CA backoff attempts to coordinate all nodes to efficiently share the same channel by assigning a node a longer backoff time with a higher probability after each collision, which in turn reduces the chance of the node to access the channel. Therefore, if one node intends to acquire the channel with a higher chance regardless of the others, the easiest solution is to reduce its backoff time, which is referred to as *backoff misbehavior* [1][3]. The objective of a backoff misbehaving node is to gain unfair access to the channel by manipulating its backoff time at the cost of performance deterioration of legitimate nodes, regardless whether they are malicious or selfish users. In fact, a misbehaving node can become a jamming node when its backoff time is set to be zero. Therefore, backoff misbehaviors have been studied extensively because of their easy operation and potential catastrophic impact on network performance.

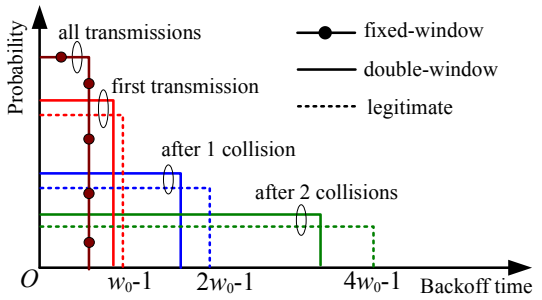

Fig. 1. Comparison between legitimate backoff, *double-window* misbehaving backoff and *fixed-window* misbehaving backoff.

In the following, we describe two widely-adopted backoff misbehavior schemes in the literature: *double-window* backoff misbehavior and *fixed-window* backoff misbehavior. In *double-window* backoff misbehavior, as shown in the solid line of Fig. 1, a misbehaving node conforms to the binary exponential backoff, but uses a smaller minimum contention window than w_0. For example, *double-window* backoff misbehavior was considered in both [1] and [11] as the backoff misbehavior model and was shown to achieve substantial performance gains over legitimate nodes. Thus, we can see from Fig. 1 that compared to legitimate backoff scheme, which is shown in dashed line, a *double-window* misbehaving node always has a higher chance to access the channel after each collision. For *fixed-window* backoff misbehavior which is shown by dotted solid lines in Fig. 1, a misbehaving node never increases its contention window and always chooses backoff time uniformly from a fixed interval. Thus, it has a much higher chance to access the channel than legitimate nodes. Formally, we have the definitions for these two types of backoff misbehavior as follows:

[2]The minimum contention window is the initial value of the contention window. For example, the minimum contention window is 32 in IEEE 802.11b for DSSS, and is 16 in IEEE 802.11g for OFDM.

[3]Here we do not consider the near-far effect due to physical diversity in wireless LANs [10]. In the near-far effect, a node with a good channel condition can have a higher chance to access the channel, thereby leading to a severe unfairness problem.

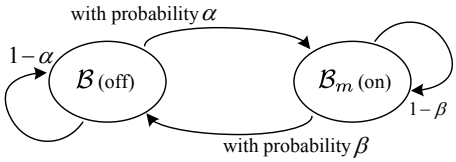

Fig. 2. The *on* and *off* states in intermittent backoff misbehavior.

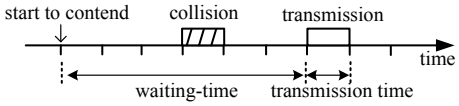

Fig. 3. A single transmission in a slotted CSMA/CA network.

*Definition 2 (*Double-window *backoff misbehavior):* A *double-window* misbehaving node uses backoff scheme $\mathcal{B}_D$ in which the random backoff time $T_D(i)$ is chosen uniformly from $[0, 2^i w_D - 1]$ after the i-th collision, where $w_D < w_0$.

*Definition 3 (*Fixed-window *backoff misbehavior):* A *fixed-window* misbehaving node uses backoff scheme $\mathcal{B}_F$ in which the random backoff time $T_F(i)$ is chosen uniformly from $[0, w_F - 1]$ after the i-th collision, where $w_F < w_0$.

Remark 1: Both *double-window* and *fixed-window* backoff misbehaviors share a common feature; that is, once they start to misbehave, they never stop unless they are disabled by countermeasures. Thus, we refer them also *continuous misbehavior* because such misbehaving nodes constantly manipulate their backoff time to obtain unfair access to the channel.

It is worthy of noting that a misbehaving node may not perform a particular backoff scheme all the time. For example, it is implied in [5] that a misbehaving node may evade misbehavior detection if it frequently changes backoff schemes. This type of misbehavior can be characterized as *intermittent misbehavior*, which performs misbehavior sporadically. Therefore, in this study, we further consider such type of misbehavior in order to thoroughly understand the impact of misbehaving nodes in CSMA/CA-based wireless networks.

In order to evade misbehavior detection, an intermittent misbehaving node only performs misbehavior in the *on* state and returns to be legitimate in the *off* state. Therefore, it has two backoff schemes: the misbehaving (on-state) and legitimate (off-state) backoff schemes, either of which can be used to transmit a packet. Thus, we define intermittent misbehavior with a Markov chain as follows.

Definition 4 (Intermittent backoff misbehavior): Given the legitimate backoff scheme $\mathcal{B}$ and a misbehaving backoff scheme $\mathcal{B}_m$, the backoff scheme of intermittent backoff misbehaving nodes is defined as a Markov process $\{\mathcal{B}_I(n);\ n = 0, 1, 2, ...\}$, where n denotes the n-th packet to be transmitted, $\mathcal{B}_I(n) \in \{\mathcal{B},\ \mathcal{B}_m\}$. Transition probabilities from $\mathcal{B}$ to $\mathcal{B}_m$ and from $\mathcal{B}_m$ to $\mathcal{B}$ are denoted by α and β, respectively. The on-state ratio $\theta \in (0, 1)$ is defined as the steady-state probability of $\mathcal{B}_I(n) = \mathcal{B}_m$, i.e., $\theta \triangleq \alpha/(\alpha + \beta)$.

Remark 2: As shown in Fig. 2, an intermittent misbehaving node can frequently switch its state between *on* and *off* with backoff schemes $\mathcal{B}_m$ or $\mathcal{B}$, respectively. Our definition of intermittent misbehavior is generic since the misbehaving scheme $\mathcal{B}_m$ in *on* state is not constrained to be a specific misbehaving backoff scheme.

By far, we have defined the models for both continuous and intermittent misbehaving nodes. In the next subsection, we will introduce a new metric to quantity the benefits of backoff misbehaving nodes.

B. Definition of Order Gain

The benefits of misbehaving nodes can be either gaining more resources for selfish nodes or to degrade network performance even without performance gain. In the former case, a selfish node attempts to have a higher chance to access the channel than legitimate nodes, and therefore performs backoff misbehavior as studied in [1], [4], [7], [8]. In the later case, the goal of malicious nodes is to disrupt normal network operation. Such nodes are often referred to as jammers [12], [13]. In this work, we focus on the former case in that it can also evolve into the later case, which will be discussed in Section IV-C.

In general, the benefits of misbehaving nodes are improving their occupancy of resources and achieving better performance. The network performance, on the other hand, can be evaluated by a number of metrics, such as throughput, which can be the data transmission rate of one user, or aggregated rate of a group of users, and so on. There have been many works on throughput analysis of CSMA/CA networks [14], [15]. By taking a close look, we can find that many analysis are based on the waiting time and transmission time. Fig. 3 illustrates a simple example of a transmission in a slotted CSMA/CA network. During the observation period, throughput can be computed as $\eta = \text{transmission time}/(\text{waiting time} + \text{transmission time}) = 1/7$. It is clear that throughput η is in fact a consequence of waiting time, which is the number of slots before a node captures the channel. Therefore, *waiting time* can immediately represent the performance of a node: the longer the waiting time, the worse the performance; the shorter the waiting time, the better performance or higher throughput and shorter delay. Here we define the waiting time as follows.

Definition 5 (Waiting time): The waiting time of a node, W, is the number of slots between the instant that the node starts to contend for the channel and the instant that the node successfully captures the channel, that is, $W \triangleq \sum_{i=0}^{N} T(i)$, where N is the number of collisions before the node makes a successful transmission and $T(i)$ is the random backoff time after the i-th collision.

Although waiting time is an essential metric to the performance of a node, our objective is *not* to evaluate the performance of a single node but to understand benefits of backoff misbehaving schemes, that is the *gain* of misbehaving nodes over legitimate nodes. To this end, we introduce a *new* performance metric by considering the following constraints: (i) This metric should not subject to a particular protocol because of the wide deployment of CSMA/CA networks, such as IEEE 802.11 and IEEE 802.15. Therefore, the definitions

of control messages, such as RTS/CTS, ACK should not affect the interpretation of the *gain*. (ii) If the gain of node A over node B is G_1 and the gain of node B over node C is G_2, then the gain of node A over node C follows additive rule, that is, $G_1 + G_2$. This property is very important because it enables us to quantitatively compare the impacts of two misbehaving nodes by directly comparing their metrics. Keep these requirements in mind, we introduce a new metric, namely *order gain* of waiting time[4] as follows.

Definition 6 (Order gain of waiting time): Let W_A and W_B be the waiting times of nodes A and B, respectively. The order gain of node A over node B is defined as

$$G(t) \triangleq \log_t \frac{\mathbb{P}(W_B > t)}{\mathbb{P}(W_A > t)}, \tag{1}$$

where $\mathbb{P}(W_A > t)$ and $\mathbb{P}(W_B > t)$ are the tail distribution functions (or complementary cumulative distribution functions, CCDFs) of W_A and W_B, respectively.

Remark 3: The definition of order gain is based on tail distribution functions of nodes A and B. The tail distribution function, for example, $\mathbb{P}(W_A > t)$ denotes the probability that the waiting time of node A is greater than a given t, showing that how often the waiting time of node A is longer than a given value. Thus, $\mathbb{P}(W_A > t)$ can in fact indicate the performance of node A since the longer the waiting time, the less the chance for the node to capture a channel.

III. Order Gains of Misbehaving Backoff Schemes

The most commonly-used misbehaving backoff schemes are *double-window* and *fixed-window* misbehaviors, which both belong to continuous misbehavior and have been extensively studied regarding detection schemes [1], [4] and incentive-based protocols [7], [8]. Therefore, in this section, we first study the two continuous misbehaviors: *double-window* misbehavior, which conforms to binary exponential backoff but chooses a smaller minimum contention window than legitimate nodes; and *fixed-window* misbehavior, which chooses random backoff time uniformly from a fixed range. Then, we move on to the intermittent backoff misbehavior in which a misbehaving node performs misbehavior and legitimate backoff in *on* state and *off* state, respectively.

A. Double-Window Backoff Misbehavior

A *double-window* misbehaving node, which is defined in Definition 2, adopts binary exponential backoff but uses a smaller minimum contention window than the legitimate nodes. In order to find the order gain of *double-window* misbehaving nodes, it is essential to obtain the tail distribution functions of waiting time for *double-window* misbehaving nodes and the legitimate nodes. We first derive the tail distribution function of the waiting time of legitimate nodes in the following lemma.

[4]The order gain of waiting time will be simplified as *order gain* thereafter; unless specified otherwise.

Lemma 1: The tail distribution function of waiting time of a legitimate node $\mathbb{P}(W > t)$ is lower and upper bounded by

$$\frac{p^2}{4}\left(\frac{t}{w_0}+1\right)^{\log_2 p} \le \mathbb{P}(W > t) \le \frac{1}{p}\left(\frac{t}{w_0}+1\right)^{\log_2 p} \tag{2}$$

for all t sufficiently large, where w_0 and p is the minimum contention window and collision probability[5] of the legitimate node, respectively.

Proof : From Definition 5, the waiting time of a legitimate node can be written as $W = \sum_{i=0}^{N} T(i)$, where N is the number of collisions before the node makes a successful transmission. Given collision probability p, $\mathbb{P}(N=j)=(1-p)p^j$. $T(i) \in [0, 2^i w_0 - 1]$ is the random backoff time after the i-th collision. Let $\{W > t\}$ be the event that waiting time W is larger than t, which means that there is no successful transmission of the node in $[0, t]$. Since $T(i)$ is upper bounded by $2^i w_0 - 1$, a necessary condition for holding $\{W > t\}$ is that there are at least ρ collisions, where $\rho = \min \mathcal{X}$ and $\mathcal{X} = \{x : \sum_{i=0}^{x}(2^i w_0 - 1) \ge t\}$. Since $\rho \in \mathcal{X}$, we have $\sum_{i=0}^{\rho}(2^i w_0 - 1) \ge t$ and have a lower bound of ρ

$$\rho \ge \log_2(\frac{t}{w_0}+1) - 1. \tag{3}$$

Meanwhile, ρ is the minimum in $\mathcal{X}$, which means $\rho - 1 \notin \mathcal{X}$ and $\sum_{i=0}^{\rho-1}(2^i w_0 - 1) < t$. Then, we have an upper bound of ρ

$$\rho \le \log_2(\frac{t}{w_0}+1) + 1. \tag{4}$$

Thus, the tail distribution function $\mathbb{P}(W > t)$ can be represented as

$$\begin{aligned}\mathbb{P}(W > t) &= \sum_{j=\rho}^{\infty} \mathbb{P}(N=j)\mathbb{P}\left(\sum_{i=0}^{N} T(i) > t | N = j\right) \\ &\le \sum_{j=\rho}^{\infty} \mathbb{P}(N=j) = p^\rho. \end{aligned} \tag{5}$$

It follows from (3) and (5) that

$$\mathbb{P}(W > t) \le \frac{1}{p}\left(\frac{t}{w_0}+1\right)^{\log_2 p}, \tag{6}$$

which completes the proof of the upper bound.

Now we derive the lower bound of $\mathbb{P}(W > t)$. We first separate $\{W > t\}$ into two disjoint events: $\{W > t\} = \{t < W \le \sum_{i=0}^{\rho}(2^i w_0 - 1)\} \bigcup \{W > \sum_{i=0}^{\rho}(2^i w_0 - 1)\}$; then,

$$\mathbb{P}(W > t) \ge \mathbb{P}\left(W > \sum_{i=0}^{\rho}(2^i w_0 - 1)\right) = \sum_{k=\rho+1}^{\infty} \mathbb{P}(N=k)\,\mathbb{P}(E_k) \tag{7}$$

where event $E_k = \left\{\sum_{i=0}^{N} T(i) > \sum_{i=0}^{\rho}(2^i w_0 - 1) | N = k\right\}$ for $k = \rho+1, \rho+2, \cdots$. We further have

$$\begin{aligned} E_{\rho+1} &= \left\{\sum_{i=0}^{\rho+1} T(i) > (2^{\rho+1}-1)w_0 - (\rho+1)\right\} \\ &\supset \left\{T(\rho+1) + T(\rho) > (2^{\rho+1}-1)w_0 - (\rho+1)\right\}, \end{aligned} \tag{8}$$

[5]Throughout this paper, we define the collision probability of a node as the probability that there is at least one other node transmitting when the node makes a transmission attempt.

where $T(\rho+1)$ and $T(\rho)$ are uniformly distributed on $[0, 2^{\rho+1}w_0-1]$ and $[0, 2^{\rho}w_0-1]$, respectively. Thus,

$$\mathbb{P}(E_{\rho+1}) \geq \mathbb{P}\left(T(\rho+1)+T(\rho) > (2^{\rho+1}-1)w_0-(\rho+1)\right) = \frac{(2^{\rho}w_0-1)/2+w_0+\rho}{2^{\rho+1}w_0} \geq \frac{1}{4}. \quad (9)$$

Similarly, we have

$$\mathbb{P}(E_k) \geq \frac{1}{4}, \quad \text{for } k=\rho+2, \rho+3, \cdots. \quad (10)$$

By substituting (4) and (10) into (7), we obtain the lower bound

$$\mathbb{P}(W > t) \geq \frac{p^2}{4}\left(\frac{t}{w_0}+1\right)^{\log_2 p}. \quad (11)$$

□

With Lemma 1, we state our main result on the order gain of *double-window* misbehavior as follows.

Theorem 1: The order gain of a *double-window* backoff misbehaving node over legitimate nodes is

$$G_D(t) = \log_2\left(\frac{p}{p_D}\right) + \Theta\left(\frac{1}{\ln t}\right),^{6}$$

where p and p_D are the collision probabilities of the legitimate and misbehaving nodes, respectively.

Proof : The order gain of the *double-window* misbehaving node over legitimate nodes is defined as

$$G_D(t) = \log_t \frac{\mathbb{P}(W > t)}{\mathbb{P}(W_D > t)}, \quad (12)$$

where $\mathbb{P}(W > t)$ and $\mathbb{P}(W_D > t)$ are the tail distribution functions of waiting time for legitimate nodes and the *double-window* misbehaving node, respectively. From Lemma 1, the tail distribution function of waiting time of legitimate nodes can be represented as

$$\mathbb{P}(W > t) = \Theta\left(\left(\frac{t}{w_0}+1\right)^{\log_2 p}\right). \quad (13)$$

Since a *double-window* misbehaving node also adopts binary exponential backoff, we can have

$$\mathbb{P}(W_D > t) = \Theta\left(\left(\frac{t}{w_D}+1\right)^{\log_2 p_D}\right), \quad (14)$$

where w_D and p_D are the minimum contention window and collision probability of *double-window* misbehaving node, respectively. By substituting (13) and (14) into (12), we finish the proof. □

Remark 4: According to Theorem 1, the order gain of *double-window* misbehaving nodes, $G_D(t)$, converges to $\log_2(p/p_D)$ as $t \to \infty$, showing that the order gain can be determined by collision probabilities of legitimate and misbehaving nodes. In this paper, we do not discuss how to calculate these collision probabilities, but it has been shown in [9] that the ratio $p/p_D \to 1$ as the number of nodes goes to infinity. Therefore, the performance gain of a *double-window* misbehaving node can become marginal because $G_D(t)$ approaches to zero as the number of nodes increases to infinity.

[6]We say function $f(x)$ is of the same order as function $g(x)$ and write $f(x) = \Theta(g(x))$ if and only if there exist two positive real numbers c_1 and c_2 and a real number x_0 such that $c_1|g(x)| \leq |f(x)| \leq c_2|g(x)|$ for all $x > x_0$.

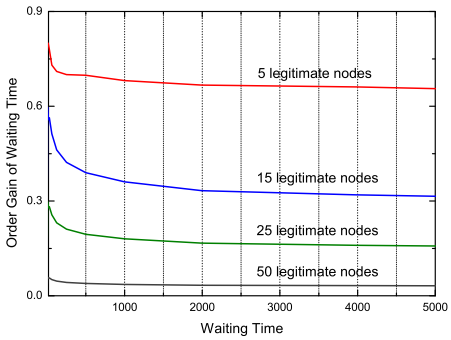

Fig. 4. Order gain of a *double-window* backoff misbehaving node in an 802.11 network with different numbers of legitimate nodes.

To attest our models and analytical results, we use ns2 simulator to evaluate the performance of *double-window* backoff misbehavior by considering an 802.11 network in the presence of one *double-window* backoff misbehaving node. The minimum contention window of legitimate nodes is $w_0 = 16$, while the minimum contention window of the misbehaving node is set to $w_D = 6$. Fig. 4 shows the order gain of the *double-window* misbehaving node for different numbers of legitimate nodes in the network. We see from Fig. 4 that the order gain of the misbehaving node converges decreasingly to a constant as t increases. We also observe that the order gain of the misbehaving node decreases as the number of legitimate nodes increases. For example, the order gain of the misbehaving node converges to 0.02 when the number of legitimate nodes equals to 50, which collectively validates our statement that the misbehaving node can only achieve marginal gains in a network with a large number of users in Remark 4.

Remark 5: The deployment cost of a countermeasure in general increases as the number of nodes increases since the countermeasure needs to monitor the activities of all nodes in the network. Thus. it is reasonable to suggest that when the number of nodes is sufficiently large, countermeasures can neglect *double-window* backoff misbehavior in order to save resources such as bandwidth and energy.

B. Fixed-Window Backoff Misbehavior

Another widely-adopted continuous misbehaving scheme is *fixed-window* backoff misbehavior. A *fixed-window* backoff misbehaving node, as defined in Definition 3, never increases its contention window in order to achieve frequent access to the channel. Next, we first derive the tail distribution function of its waiting time, followed by the analysis of its order gain, $G_F(t)$.

Lemma 2: For a *fixed-window* misbehaving node, the tail distribution function of its waiting time $\mathbb{P}(W_F > t)$ is lower and upper bounded by

$$\frac{1}{w_F} e^{\frac{t}{w_F-1}\ln(p_F/w_F)} \leq \mathbb{P}(W_F > t) \leq e^{\left(\frac{t}{w_F-1}-1\right)\ln p_F},$$

where w_F and p_F are the minimum contention window and collision probability of the misbehaving node, respectively.

Proof : The waiting time of the misbehaving node can be written as $W_F = \sum_{i=0}^{N_F} T_F(i)$, where N_F is the number of collisions before the misbehaving node makes a successful transmission. Given the collision probability p_F, $\mathbb{P}(N_F = j) = (1-p_F)p_F^j$. $T_F(i)$ is the backoff time of the *fixed-window* misbehaving node after the i-th collision, and is upper bounded by $(w_F - 1)$. Thus, a necessary condition for event $\{W_F > t\}$ holding is that there have been at least $\rho_F = \lfloor t/(w_F - 1) \rfloor$ collisions. The tail distribution function of waiting time of the misbehaving node can be written as

$$\mathbb{P}(W_F > t) = \sum_{j=\rho_F}^{\infty} \mathbb{P}(N_F = j)\mathbb{P}\left(\sum_{i=0}^{N_F} T_F(i) > t | N_F = j\right) \leq \sum_{j=\rho}^{\infty} \mathbb{P}(N_F = j) = p_F^{\rho_F} \leq e^{\left(\frac{t}{w_F - 1} - 1\right) \ln p_F}. \quad (15)$$

On the other hand, if $T_F(0), T_F(1), ..., T_F(\rho_F)$ are all equal to $w_F - 1$, we have

$$\sum_{i=0}^{N_F} T_F(i) \geq \sum_{i=0}^{\rho_F} T_F(i) = (\rho_F + 1)(w_F - 1) \geq t \quad (16)$$

since $N_F \geq \rho_F = \lfloor t/(w_F - 1) \rfloor$. Then

$$\mathbb{P}\left(\sum_{i=0}^{N_F} T_F(i) > t | N_F = j\right) \geq \mathbb{P}(T_F(0) = ... = T_F(\rho_F) = w_F - 1) = (1/w_F)^{\rho_F + 1}. \quad (17)$$

Consequently, we have

$$\mathbb{P}(W_F > t) = \mathbb{P}\left(\sum_{i=0}^{N_F} T_F(i) > t\right) \geq \sum_{j=\rho_F}^{\infty} \mathbb{P}(N_F = j)\left(\frac{1}{w_F}\right)^{\rho_F + 1} = \frac{1}{w_F}\left(\frac{p_F}{w_F}\right)^{\rho_F} \geq \frac{1}{w_F} e^{\frac{t}{w_F - 1} \ln(p_F / w_F)}, \quad (18)$$

which finishes the proof. □

With Lemma 2, we are ready to present the main result on the order gain of *fixed-window* backoff misbehavior.

Theorem 2: The order gain of a *fixed-window* backoff misbehaving node over legitimate nodes is

$$G_F(t) = \Theta\left(\frac{t}{\ln t}\right).$$

The proof is similar to Theorem 1. The order gain of a *fixed-window* backoff misbehaving node is represented by

$$G_F(t) = \log_t \frac{\mathbb{P}(W > t)}{\mathbb{P}(W_F > t)}. \quad (19)$$

Using the bounds of $\mathbb{P}(W > t)$ in Lemma 1 and the bounds of $\mathbb{P}(W_F > t)$ in Lemma 2 can finish the proof.

Remark 6: Theorem 2 tells that the order gain of *fixed-window* backoff misbehavior is an increasing function to infinity as $t \to \infty$ regardless of the number of nodes in the network. This implies that a misbehaving node can always obtain substantial benefits from *fixed-window* backoff misbehavior. Thus, any countermeasure to backoff misbehavior should consider *fixed-window* backoff misbehavior as its primary target.

Next we present the simulation results regarding the order gain of *fixed-window* backoff misbehavior. We consider an 802.11 network with 15 legitimate nodes and a misbehaving node that performs *fixed-window* backoff misbehavior with contention window $w_F = 6, 8, 12$. Fig. 5 shows the order gain of the misbehaving node for different w_F. It is observed from Fig. 5 that the order gain of the *fixed-window* backoff misbehaving node keeps increasing as t increases and that the increasing rate of the order gain of *fixed-window* misbehavior depends on w_F. Thus, *fixed-window* misbehavior with a small w_F can severely degrade the performance of legitimate nodes.

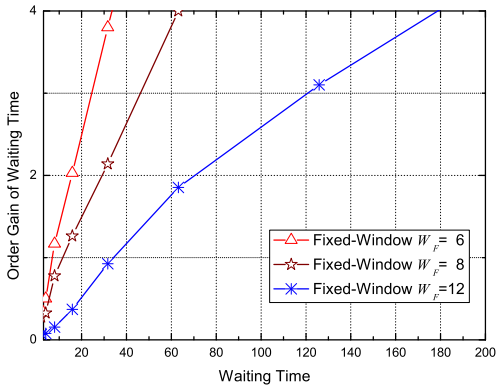

Fig. 5. Order gain of a *fixed-window* backoff misbehaving node in an 802.11 network with 15 legitimate nodes.

Remark 7: Compared with *double-window* backoff misbehavior, *fixed-window* backoff misbehavior can be much more harmful to a wireless network. Therefore, *fixed-window* backoff misbehavior should always be the primary target of countermeasures to backoff misbehavior.

C. Intermittent Backoff Misbehavior

We have studied the order gains of two widely-used backoff schemes for continuous misbehavior. However, a misbehaving scheme is not always guaranteed to be continuous, especially when there exists a counter-strategy in the network which aims to detect and disable misbehaviors. It has been shown in [5] that a node performing misbehavior intermittently may evade such misbehavior detection. Thus, it is important to understand the benefits of such an intermittent misbehaving in a wireless network. The backoff scheme of an intermittent misbehaving node is defined as a Markov process with *on* and *off* states in Definition 4. With this definition, we have

Theorem 3: The order gain of an intermittent misbehaving node over legitimate nodes satisfies

$$G_I(t) = \log_2 \frac{p_{on}}{p_{off}} + \Theta\left(\frac{1}{\ln t}\right),$$

where p_{on} and p_{off} are collision probabilities of legitimate nodes in *on* and *off* states, respectively.

Proof : The order gain of an intermittent misbehaving node is defined as

$$G_I(t) = \log_t(\mathbb{P}(W>t)/\mathbb{P}(W_I>t)), \quad (20)$$

where $\mathbb{P}(W > t)$ and $\mathbb{P}(W_I > t)$ are the tail distribution functions of the waiting time for legitimate and intermittent misbehaving nodes, respectively. The probabilities of the intermittent misbehaving node being in *on* and *off* states are $\mathbb{P}(\text{on}) = \theta$ and $\mathbb{P}(\text{off}) = 1-\theta$, respectively. Note that though legitimate nodes do not change their backoff scheme, they are affected by the change of status of the intermittent misbehaving node, therefore also have *on* and *off* states. Then, we have

$$\mathbb{P}(W>t) = \theta\mathbb{P}(W>t|\text{on}) + (1-\theta)\mathbb{P}(W>t|\text{off}), \quad (21)$$

$$\mathbb{P}(W_I>t) = \theta\mathbb{P}(W_I>t|\text{on}) + (1-\theta)\mathbb{P}(W_I>t|\text{off}). \quad (22)$$

Substituting (22) and (21) into (20) yields

$$G_I(t) = \log_t\left(\frac{\theta + (1-\theta)t^{-G(t)}}{\theta t^{-G_{on}(t)} + (1-\theta)t^{-G(t)}}\right), \quad (23)$$

where $G_{on}(t) = \log_t \frac{\mathbb{P}(W>t|\text{on})}{\mathbb{P}(W_I>t|\text{on})}$ is called *all-on* order gain, and $G(t) = \log_t \frac{\mathbb{P}(W>t|\text{on})}{\mathbb{P}(W>t|\text{off})}$ is called *on-off legitimate order gain*, which is due to the difference between the collision probabilities p_{on} and p_{off} of legitimate nodes in *on* and *off* states, respectively. It follows from Theorem 1 that

$$G(t) = \log_2\frac{p_{on}}{p_{off}} + \Theta\left(\frac{1}{\ln t}\right). \quad (24)$$

Since the misbehaving node can always obtain gains from its backoff misbehavior when it is *on*, it holds that $\mathbb{P}(W_I > t|\text{on}) \le \mathbb{P}(W > t|\text{off})$. Thus, $G_{on}(t) \ge G(t)$ and $\theta t^{-G_{on}(t)} \le \theta t^{-G(t)}$. Then, from (23), we have found the lower bound

$$G_I(t) \ge \log_t\left(\frac{\theta + (1-\theta)t^{-G(t)}}{\theta t^{-G(t)} + (1-\theta)t^{-G(t)}}\right) \ge \log_t\left(\frac{\theta}{t^{-G(t)}}\right) = G(t) + \frac{\ln\theta}{\ln t}. \quad (25)$$

On the other hand, it follows from (23) that

$$G_I(t) \le \log_t\left(\frac{\theta + (1-\theta)t^{-G(t)}}{(1-\theta)t^{-G(t)}}\right). \quad (26)$$

Because $G(t)$ converges to $\log_2(p_{on}/p_{off}) > 0$, there exists a constant t_0 such that $t^{-G(t)} \le 1$ for all $t > t_0$, and then (26) can be upper bounded by

$$G_I(t) \le \log_t\left(\frac{\theta + (1-\theta)}{(1-\theta)t^{-G(t)}}\right) = G(t) - \frac{\ln(1-\theta)}{\ln t} \quad (27)$$

for all $t > t_0$. Combining (24), (25), and (27) yields

$$G_I(t) = \log_2\frac{p_{on}}{p_{off}} + \Theta\left(\frac{1}{\ln t}\right). \quad (28)$$

□

Theorem 3 shows that, perhaps surprisingly, the order gain of an intermittent misbehaving node $G_I(t)$ always converges as $t \to \infty$ regardless of the misbehaving backoff scheme used in the *on* state.

The order gain of intermittent misbehavior is assessed by considering an 802.11 network consisting of five legitimate nodes and one intermittent misbehaving node in simulations.

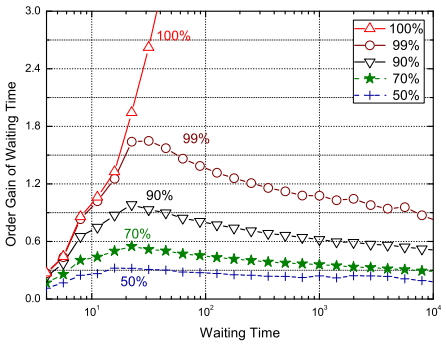

Fig. 6. Order gain of an intermittent misbehaving node in an 802.11 network with 5 legitimate nodes.

The intermittent misbehaving node chooses a random backoff time uniformly from $[0, 7]$ when it is in on-state. Fig. 6 demonstrates the order gains of the intermittent misbehaving node for different on-state ratios θ. We see from Fig. 6 that the order gain of the misbehaving node always exhibits an initial increasing phase, and after reaching a maximum, it starts to converge decreasingly. This reveals an interesting phenomena that there exists a *phase transition phenomenon* in the order gain of intermittent misbehavior. The phase transition phenomenon is more evident when θ becomes large. We denote by t^* the phase transition point, which is the value of waiting time corresponding to the maximum of the order gain. During simulations, we find that t^* increases as θ increases, but the increment is not significant. For example, in Fig. 6, t^* increases from 18 to 33 as θ goes from 50% to 99%.

Fig. 6 also shows that the order gain of an intermittent misbehaving node is not significant when θ is small. For example, when $\theta = 50\%$, the order gain is always smaller than 0.35 and the phase transition phenomenon is not evident. When $\theta = 70\%$, the order gain is also upper bounded by 0.6. Consequently, our simulation results indicate that if an intermittent misbehaving node attempts to evade misbehavior detection by choosing a small θ, it cannot achieve substantial gain. An extreme case is that when $\theta = 0$, there is no performance gain of intermittent nodes which cannot degrade network performance because it always follows the legitimate backoff scheme.

On the other hand, if an intermittent misbehaving node chooses a large θ to achieve substantial gains, it may not be able to evade misbehavior detection in that it appears similarly as a continuous misbehaving node. For example, we can see in Fig. 6 that when the intermittent misbehaving node has $\theta = 99\%$, its order gain is almost the same as $\theta = 100\%$ for small waiting time t. In this case, the intermittent misbehaving node has a higher risk to be detected.

IV. Performance Evaluation and Discussions

As we have explained earlier, manipulating backoff time is one of the easiest methods to gain more network resources at the cost of performance degradation of legitimate nodes. To

further evaluate the performance gain of misbehaving nodes and the impact of backoff misbehavior on a practical wireless network, we use off-the-shelf IEEE 802.11 products and Madwifi driver [16] to set up an experimental WiFi network in the presence of a misbehaving node.

A. Experiment Setup

1) Network Deployment: The experimental network consists of six laptops and two iPAQ pocket PCs with plug-in wireless cards. The laptops and pocket PCs are associated with a Cisco Access Point (Aironet 1200 series) working under IEEE 802.11b. We place all devices inside a laboratory to ensure that they are under the same channel condition and the only difference between legitimate and misbehaving nodes is the backoff scheme.

2) Network Traffic: The commonly-used network testing tool, $Iperf$, is used to generate traffic over the network. We use $Iperf$ to generate UDP streams at the rate of 10Mbps that can fill up the transmission queue at each device such that all devices are in saturated state.

3) Performance Metric: It is not easy to accurately measure the waiting time at the MAC layer, since commercial 802.11 adapters do not expose their internal parameters to higher layers. Therefore, in our experiments, throughput of each node is measured for performance evaluation.

B. Experimental Results

We first study the performance gain of *double-window* and *fixed-window* misbehaving schemes. We consider two scenarios: 1) one-bad node and one-good node scenario, which can straightforwardly show the gain of a misbehaving node and its impact on a legitimate node, and 2) one-bad (node) and seven-good (nodes) scenario, which illustrates the impact of the number of nodes on a misbehaving backoff scheme.

The throughput ratio of the misbehaving node to a legitimate node, as a function of the minimum contention window of the misbehaving node is shown in Fig. 7, from which we can observe the follows. In the one-bad and one-good case, the misbehaving node can obtain significant gains from both *double-window* and *fixed-window* misbehaviors when its minimum contention window is small. On the other hand, such great gains mean that the legitimate node encounters a denial-of-service attack. For example, we find during experiments that the legitimate node had a transmission rate below 30 Kbps when the misbehaving node performed *fixed-window* backoff misbehavior with minimum contention window equal to 2.

Fig. 7 also illustrates the performance of the misbehaving node in the one-bad and seven-good scenario. We see that the throughput ratio slightly decreases as more legitimate nodes contend for the channel for the *double-window* misbehavior; while the throughput ratio even increases for *fixed-window* misbehavior. Thus, if a node intends to misbehave in a network with many users, it may choose *fixed-window* misbehavior to achieve substantial gains. On the other hand, the number of users should be considered as a critical factor to the evaluation of providing countermeasures to a network. When the number

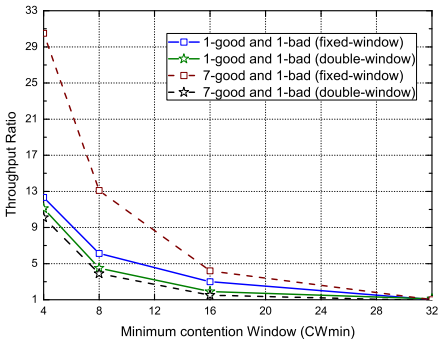

Fig. 7. Throughput ratio of the misbehaving node to a legitimate node for different backoff misbehaving schemes.

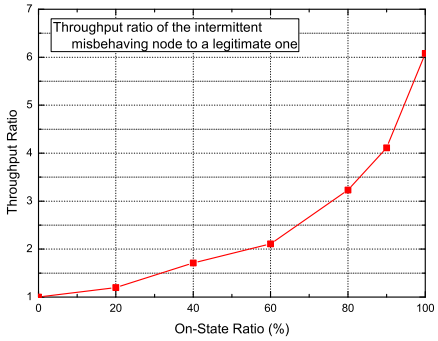

Fig. 8. Throughput ratio of the misbehaving node to a legitimate node for different on-state ratios θ.

of users is small, countermeasures can focus on both *double-window* and *fixed-window* misbehaviors. When the number of users is large, countermeasures can focus only on *fixed-window* misbehavior since *double-window* misbehavior benefits only marginal gains.

We then study the performance of intermittent misbehavior by considering a one-bad and five-good scenario. The intermittent misbehaving node chooses its random backoff time uniformly from $[0, 7]$ in the *on* state and performs legitimate backoff in the *off* state. Fig. 8 demonstrates the throughput ratio of the intermittent misbehaving node to a legitimate one, as a function of on-state ratio θ. We observe that the throughput ratio does not increase linearly with the increasing of θ and throughput ratio is not large when $\theta < 50\%$. Our experimental results further validate our simulation results, showing that an intermittent misbehaving node can not benefit much with a small θ and needs to choose a fairly large θ to achieve significant performance gains, which in turn is easy to be detected.

C. Discussions

In previous sections, we have studied the problem of quantifying the gain of backoff misbehavior and obtained the order gains for two continuous backoff misbehaving schemes and the intermittent misbehaving scheme, which are validated by simulation. We further present experimental results to

illustrate the impact of backoff misbehavior. Our findings can be summarized as: (i) *Double-window* misbehavior is more sensitive to the number of users than *fixed-window* misbehavior and can only achieve marginal gains when the number of user increases, which shows that, on the other hand, the performance loss of legitimate nodes due to *double-window* misbehavior is not significant in a network with a large number of users. (ii) *Fixed-window* misbehavior can always achieve substantial gains over legitimate nodes regardless of the number of users. Therefore, *fixed-window* misbehavior should always be the primary target of countermeasures to backoff misbehavior. (iii) An intermittent misbehaving node can not achieve significant gain when it chooses a small θ to evade misbehavior detection.

The above results are studied from a "gain" perspective. Note that the network resources are limited and finite, especially for a number of users sharing the same medium. In other words, when some users gain throughput or bandwidth benefits, others can potentially lose their transmission opportunity, resulting in zero user-throughput. A trivial example is that one user occupies the channel for the entire time period, regardless of transmitting useful data or not. which turns to be an extreme of misbehavior, *jamming* [12]. When this happens, the entire network appears to be dysfunctional, and even not accessible to legitimate nodes. It is interesting to use order gain to quantify a jammer, which can be regarded as a *fixed-window* misbehaving node with $w_{_F} = 1$ under saturated state. Therefore, the jammer's waiting time $W_J = 0$ and $\mathbb{P}(W_J > t) = 0$ for all $t > 0$. Then the jammer's order gain $G_J(t) = \infty$ for all $t > 0$, indicating that the jammer has "infinite gains" over legitimate nodes.

It is worthy of mention that our results have several limitations. For example, the upper limits of contention window and retransmissions for legitimate nodes, such as the 7 short-retry limit in the basic access model of 802.11 DCF, is not considered in our analytical model. Thus, the order gain may not fully reflect the performance gain of backoff misbehaving nodes in theory. Nevertheless, we believe our results are still applicable in practical scenarios. For instance, a legitimate node will start a new transmission after reaching the upper limit of retransmissions, which means that its chance to capture the channel becomes larger. Thus, our results in fact provide an upper bound on performance gain of misbehaving nodes for a practical network. Moreover, our experiments are limited in a small-scale, single-hop network with 8 *active* users for basic service set. Thus, our experimental results may not be able to reveal the performance and impact of misbehaving nodes in more complicated wireless environments, such as extended service sets.

V. Conclusions

In this paper, we provided an in-depth study on the benefits of backoff misbehaving nodes by analytical modeling, simulations and experiments. We introduced a new performance metric, *order gain*, to quantitatively investigate two widely-used continuous misbehavior models: *double-window* and *fixed-window* backoff misbehaviors, and intermittent misbehavior that performs misbehavior intermittently to evade misbehavior detection. Besides our theoretical quantification of the gains of continuous and intermittent misbehaviors, we find that the number of users is a critical factor to the evaluation of countermeasures to backoff misbehaviors. We find that *double-window* backoff misbehavior is more sensitive to the number of users and shows only marginal order gains in a network with a large number of users; *fixed-window* backoff behavior is much more harmful than others because it can always obtain performance gain; and finally an intermittent misbehaving node can not achieve substantial gains when its on-state ratio θ is small.

Note that as shown in our experiments, the throughput ratios for various backoff misbehaviors are quite different. It is of interest to investigate the relationship between the throughput ratio and the order gain of a misbehaving node, which will be included in the future work.

References

[1] P. Kyasanur and N. H. Vaidya, "Detection and handling of mac layer misbehavior in wireless networks," in *Proc. of IEEE DSN'03*, Jun. 2003, pp. 173–182.

[2] S. Szott, M. Natkaniec, R. Canonico, and A. R. Pach, "Impact of contention window cheating on single-hop IEEE 802.11e MANETs," in *Proc. of IEEE WCNC'08*, Apr. 2008, pp. 1356–1361.

[3] L. Guang, C. Assi, and A. Benslimane, "MAC layer misbehavior in wireless networks: challenges and solutions," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 6–14, Aug. 2008.

[4] Y. Rong, S.-K. Lee, and H.-A. Choi, "Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis," in *Proc. of IEEE INFOCOM'06*, Apr. 2005.

[5] M. Raya, I. Aad, J. Hubaux, and A. E. Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," *IEEE Trans. Mobile Computing*, vol. 5, no. 12, Dec. 2006.

[6] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Performance comparison of detection schemes for MAC layer misbehavior," in *Proc. of IEEE INFOCOM'07*, Apr. 2007, pp. 1496–1504.

[7] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. of IEEE INFOCOM'05*, vol. 4, Mar. 2005, pp. 2513–2524.

[8] J. Konorski, "A game-theoretic study of CSMA/CA under a backoff attack," *IEEE/ACM Trans. Networking*, vol. 14, no. 6, pp. 1167–1178, Dec. 2006.

[9] V. Ramaiyan, A. Kumar, and E. Altman, "Fixed point analysis of single cell IEEE 802.11e WLANs: uniqueness, multistability and throughput differentiation," in *Proc. of ACM SIGMETRICS '05*, 2005, pp. 109–120.

[10] S. Choi, K. Park, and C. kwon Kim, in *Proc. of ACM SIGMETRICS '05*, 2005, pp. 97–108.

[11] L. Guang, C. Assi, and A. Benslimane, "Enhancing IEEE 802.11 random backoff in selfish environments," *IEEE Trans. Vehicular Techn.*, vol. 57, no. 3, pp. 1806–1822, May 2008.

[12] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. of ACM MobiHoc'05*, 2005, pp. 46–57.

[13] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," in *Proc. of IEEE INFOCOM'08*, Apr. 2008, pp. 1265–1273.

[14] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas in Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[15] E. Ziouva and T. Antonakopoulos, "CSMA/CA performance under high traffic conditions: throughput and delay analysis," *Computer Communications*, vol. 25, pp. 313–321, 2002.

[16] Madwifi, http://madwifi.org.