Modeling and Performance Evaluation of Backoff Misbehaving Nodes in CSMA/CA Networks

Zhuo Lu, *Student Member, IEEE,* Wenye Wang, *Senior Member, IEEE,* and Cliff Wang

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, to assess the gain that misbehaving nodes can obtain, we define and study two general classes of backoff misbehavior: *continuous misbehavior*, which keeps manipulating the backoff time unless it is disabled by countermeasures, and *intermittent misbehavior*, which tends to evade the detection of countermeasures by performing misbehavior sporadically. Our approach is to introduce a new performance metric, namely *order gain*, to characterize the performance benefits of misbehaving nodes in comparison to legitimate nodes in CSMA/CA-based wireless networks. We derive the order gains of both continuous and intermittent misbehaviors and further investigate the relation between our metric, order gain, and the throughput gain for a misbehaving node. We show that in IEEE 802.11 networks, the throughput ratio of a backoff misbehaving node to a legitimate node is either *bounded above* or *proportional to the number of legitimate nodes*. We use both simulations and experiments to validate our theoretical analysis and to further demonstrate the impact of a wide range of backoff misbehaviors on network performance in CSMA/CA-based wireless networks.

Index Terms—CSMA/CA, random backoff, misbehaving nodes, performance gain, wireless networks.

1 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] based on a variety of misbehavior models. However, the behavior of a misbehaving node could be unpredictable in a wireless network. A misbehaving node can perform any type of misbehavior as long as it achieves sufficient benefits, which poses a challenging problem to the design of countermeasures. A recent work [9] indicates that it is not practical to design an omnipotent method to counter-attack all possible misbehaviors and further points out that countermeasures should focus on the misbehaving nodes with significant gains and at the same time neglect the misbehaving nodes with only marginal gains to save resources such as energy and bandwidth. Therefore, quantifying the performance gain of backoff misbehavior becomes a prerequisite to the design of countermeasures to backoff misbehavior.

To this end, a gain factor is proposed in [9] to indicate the impact of misbehavior. However, the gain factor is limited since it is assumed that there exists only one misbehaving node in the network and the backoff process of legitimate nodes is simplified to uniform backoff, which is inconsistent with the widely-used binary exponential backoff in CSMA/CA networks. Thus, a fundamental question remains unsolved: *how to quantify the gain of backoff misbehavior in CSMA/CA-based wireless networks?*

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, as shown in Fig. 1 (a). Specially, 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

- *Zhuo Lu is with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC. E-mail: zlu3@ncsu.edu.*
- *Wenye Wang is with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC. E-mail: wwang@ncsu.edu.*
- *Cliff Wang is with Army Research Office, Research Triangle Park, NC. Email: cliff.wang@us.army.mil.*

An earlier version of the work was published in the 29th IEEE Conference on Computer Communications (INFOCOM' 10).

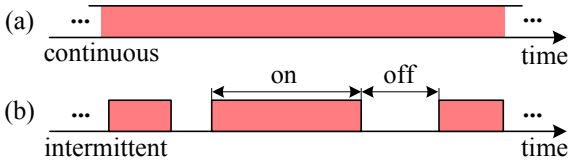

Fig. 1. Comparison between continuous backoff misbehavior and intermittent backoff misbehavior.

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 behaving legitimately in *off* periods, as shown in Fig. 1 (b). The goal of intermittent misbehavior is to obtain benefits over legitimate nodes and at the same time to evade misbehavior detection. Although existing literature has mainly dealt with continuous misbehavior and focused little attention on intermittent misbehavior, the work in [5] has indicated that an intermittently 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 on 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 the period that 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 three-fold.

1) 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.
2) We validate the impact of backoff misbehavior via simulations and experiments. We find that the number of users is a critical factor to the evaluation of countermeasures to backoff misbehaviors. Our analytical and experimental results show that both *double-window* and *fixed-window* backoff misbehaviors can achieve significant gains when the number of users is small. Compared with *fixed-window* backoff misbehavior, *double-window* backoff misbehavior only leads to negligible damage to a network with a large number of users. We also show that an intermittently misbehaving node can not achieve substantial gains when it only has a short *on* period.
3) Besides quantification of existing backoff misbehavior models, we further show that backoff misbehaviors in IEEE 802.11 networks can be categorized into two classes: *finite-gain* misbehavior and *scalable-gain* misbehavior, in terms of the throughput gain ratio that is the ratio of the throughput of a misbehaving node to that of a legitimate node. A finite-gain misbehaving node always has upper-bounded throughput gain ratio; while a scalable-gain misbehaving node has throughput gain ratio proportional to the number of legitimate nodes in a network, which indicates that scalable-gain misbehaving nodes are much more harmful than finite-gain misbehaving nodes in large-scale networks. In lights of analytical studies, simulations and experiments, we suggest that *countermeasures to backoff misbehavior should focus primarily on scalable-gain misbehavior*.

The rest of this paper is organized as follows. In Section 2, we introduce preliminaries and formulate the problem of quantifying the gain of backoff misbehavior. In Sections 3, we present our main results of the order gains for misbehaving nodes via analytical modeling and simulations. In Section 4, we show the throughput gains of misbehaving nodes in IEEE 802.11 networks and further categorize backoff misbehavior in terms of the throughput gain. In Section 5, we present experimental results to show the impact of misbehaving nodes on a practical WiFi network. Finally, we conclude in Section 6.

2 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.

2.1 CSMA/CA Backoff and Misbehaviors

In wireless networks, CSMA/CA features a distributed control algorithm for resolving packets collisions due to contending a shared channel 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 the *contention window*. At first w is set to be w_0, which is called the *minimum contention window*[2], and is

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.

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.

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.

Remark 1: Note that in practice, there are upper limits for the contention window as well as the number of retransmissions (e.g., 1024 and 7 in IEEE 802.11, respectively). In this paper, we assume in our theoretical model that there are no upper limits on both the number of retransmissions and the contention window to facilitate our subsequent analysis. In other words, we adopt an asymptotic approach to analyze the gain of backoff misbehavior in CSMA/CA networks. We will investigate the effects of the two limits via simulations and experiments in Section 5.3.

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]. Note that CSMA/CA suffers several other fairness problems. For example, the near-far effect due to physical diversity in wireless LANs [10] results in a node with a better channel condition having a higher chance to access the channel. In this paper, we assume that the unfairness in a wireless network is caused only by backoff misbehavior. It is also worth noting that the backoff behavior of several practical network cards has been shown to have some degree of violation of standard specifications [11], but we assume that all legitimate nodes use the same backoff scheme in Definition 1. 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. Therefore, backoff misbehaviors have been studied extensively because of their easy operation and potential catastrophic impact on network performance.

In the following, we describe two widely-studied 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. 2, 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 [12] as the backoff misbehavior model and was shown to achieve substantial performance gains over legitimate nodes. Thus, we can see from Fig. 2 that compared to the legitimate backoff scheme, which is shown as dashed lines, 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. 2, 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:

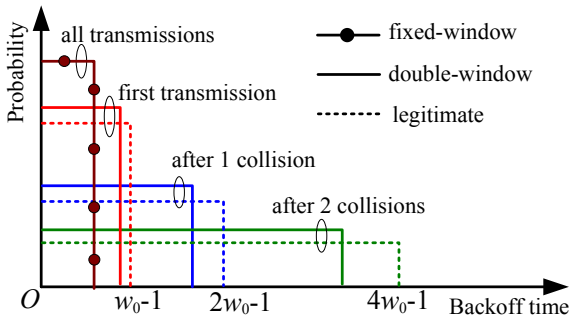

Fig. 2. Comparison between legitimate backoff, *double-window* misbehaving backoff and *fixed-window* misbehaving backoff.

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 2: 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 note 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 intermittently misbehaving node only performs misbehavior in the *on* state and returns to legitimate behavior 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. Such an intermittently misbehaving node can

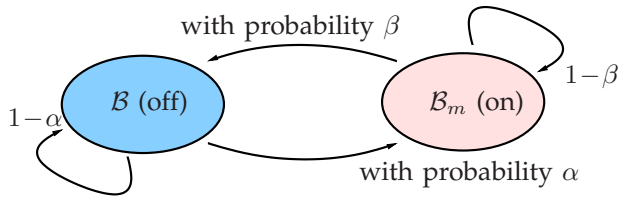

Fig. 3. The *on* and *off* states in intermittent backoff misbehavior.

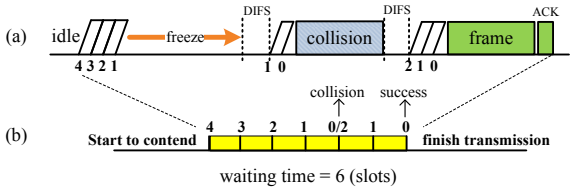

Fig. 4. A packet transmission process in IEEE 802.11.

choose its status by following various criteria. For example, it can switch (on/off) status memorylessly or based on history. In this paper, we assume that an intermittently misbehaving node chooses its next status based on the current status; i.e., we define intermittent misbehavior with a Markov chain with two states 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 3: As shown in Fig. 3, an intermittently 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.

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

2.2 Definition of Order Gain

The benefits of misbehavior 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 [13], [14]. 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 5.4.

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 the most commonly-used throughput and delay [15], [16]. However, the two performance metrics depend highly on protocol specifications. For example, Fig. 4(a) illustrates a simple transmission process in IEEE 802.11 DCF. During the transmission, we can see that the packet delay includes the idle slot time, freezing time, DCF Interframe Space (DIFS) interval, and the packet transmission time. If we consider the same transmission process under a different MAC protocol, such as ZigBee or even different 802.11 models, the packet delay will change because of distinct protocol specifications. However, we do not want our analysis to be limited to a particular MAC protocol as CSMA/CA is extensively adopted in wireless networks. Therefore, we attempt to extract the essential backoff part of CSMA/CA from a MAC protocol by deleting all protocol-related signals, as shown in Fig. 4(b).

We name the resultant process as the backbone process since it is protocol-independent and consists of a number of slots induced only by a random backoff mechanism. In the backbone process, we define the waiting time of a node as follows.

Definition 5 (Waiting time): The waiting time of a node, W, is the total number of counted slots induced by counter decrements 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 (counted by slots) after the i-th collision.

From Fig. 4(b), we see that the waiting time during the transmission is 6 slots, which is not dependent on protocol signals and the time duration of a slot, but is determined only by a backoff mechanism. Thus, it can be considered as a generic performance metric for CSMA/CA. Note that the waiting time has the limitation of measuring the real-time delay performance when dealing with a particular CSMA/CA protocol such as 802.11, since it neglects protocol specifications such as counting-down freezing and DIFS signals. However, it is still clear that a node's throughput (or delay) is in fact a consequence of its waiting time. For example, if a node's waiting time is zero (meaning that it never waits to transmit), its packet delay should be very small and its throughput is almost equal to the channel bandwidth. Thus, waiting time can immediately represent the performance of a node with a backoff mechanism: the shorter the waiting time, the better the performance (i.e., higher throughput and shorter delay).

On the other hand, although waiting time can charac-

terize 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:

1) This metric should not be 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 DIFS, ACK should not affect the interpretation of the *gain.* Hence, we choose the protocol-independent waiting time W as a basis for our performance metric. We use the tail distribution function $\mathbb{P}(W > t)$ to represent the waiting time since it is a random variable.
2) If nodes A and B have the same backoff scheme, the gain of node A over node B should be zero.
3) 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 the 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.

Keeping these requirements in mind, we introduce a new metric, namely *order gain* of waiting time[3] 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

$$G(t) \triangleq \log_t \frac{\mathbb{P}(W_B > t)}{\mathbb{P}(W_A > t)}, \ (t > 0) \tag{1}$$

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 4: As shown in (1), the order gain is defined as the logarithm of the ratio between two tail distribution functions to the base of t. Note that any base in fact satisfies the three requirements. Here, we choose the base of t since the operator of $\log_t(\cdot)$ can yield the slope values of widely-used power-law distributions in log-log scales for large t, which in turn means that for such distributions, the order gain has an approximate geometric interpretation, i.e., the slope difference between the tail distribution functions of misbehaving and legitimate nodes on log-log scales.

3 Order Gains of Misbehaving Backoff Schemes

In this section, we present our analytical results on quantifying the gain of backoff misbehavior. In particular, we first study the two continuous misbehaviors: *double-window* misbehavior and *fixed-window* misbehavior. Then, we move on to the intermittent misbehavior.

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

3.1 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.

Lemma 1: Let p be the collision probability[4] of a legitimate node. Based on Definition 1, the tail distribution function of waiting time of a legitimate node $\mathbb{P}(W > t)$ is lower and upper bounded by

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

for all t sufficiently large.

Proof : Please refer to the proof in [17]. □

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

$$G_D(t) = \log_2\left(\frac{p}{p_{_D}}\right) + \Theta\left(\frac{1}{\ln t}\right),^{5}$$

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

$$G_D(t) = \log_t \frac{\mathbb{P}(W > t)}{\mathbb{P}(W_{_D} > t)}, \tag{3}$$

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

$$\mathbb{P}(W > t) = \Theta\left((t/w_0+1)^{\log_2 p}\right). \tag{4}$$

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

$$\mathbb{P}(W_{_D} > t) = \Theta\left((t/w_{_D}+1)^{\log_2 p_{_D}}\right), \tag{5}$$

where $w_{_D}$ and $p_{_D}$ are the minimum contention window and collision probability of *double-window* misbehaving node, respectively. By substituting (4) and (5) into (3), we obtain

$$G_D(t) = \log_2\left(p/p_{_D}\right) + \Theta\left(1/\ln t\right).$$

□

Remark 5: According to Theorem 1, the order gain of

4. 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 sends a packet. We also assume that it always holds that a collision probability is in (0,1) for our analytical analysis.

5. 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 $x > x_0$.

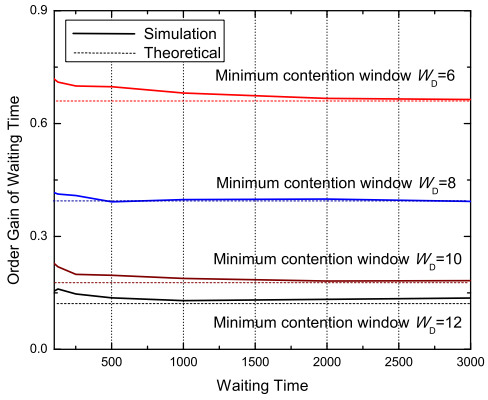

Fig. 5. Order gains of a *double-window* backoff misbehaving node with minimum contention window $w_D = 6$, 8, 10, and 12 in an 802.11 network in the presence of 5 legitimate nodes.

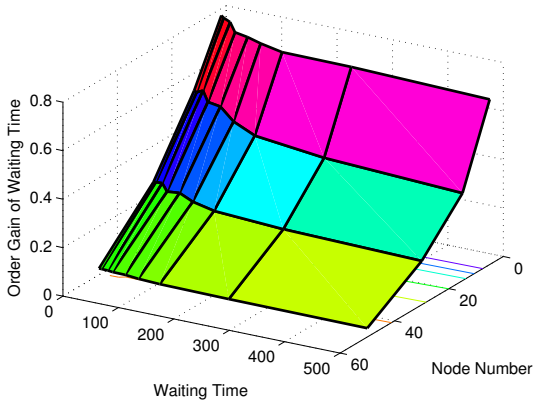

Fig. 6. Order gains of a *double-window* backoff misbehaving node with minimum contention window $w_D = 6$ in an 802.11 network with different numbers of legitimate nodes.

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 [18] that the ratio $p/p_D \to 1$ as the number of nodes goes to infinity. Therefore, the order gain of a *double-window* misbehaving node will approach zero when the number of nodes increases to infinity.

To attest our models and analytical results, we use the 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 and five legitimate nodes. In addition, we use the following setups for our simulations: we generate saturated traffic at all misbehaving and legitimate nodes. There is no upper limit for the contention window or the number of retransmissions for any node. The minimum contention window of legitimate nodes is $w_0 = 16$.

We first show in Fig. 5 the empirical order gains of the misbehaving node compared with theoretical results $\log(p/p_D)$ in Theorem 1 for different minimum contention windows $w_D = 6, 8, 10, 12$. Note that the collision probabilities p and p_D are measured during simulations. As [18] has shown that $\log(p/p_D)$ is a decreasing function of both w_D and the number of nodes, Fig. 5 illustrates that the order gain is indeed inversely proportional to w_D: the larger the minimum contention window w_D, the smaller the order gain. Fig. 5 also shows that with increasing waiting time t, the order gain converges monotonically to the constant $\log(p/p_D)$ as predicated in Theorem 1, even through the convergence rate is low. Then, in Fig. 6, we fix the minimum contention window of the misbehaving node to be $w_D = 6$ and show the order gain of the *double-window* misbehaving node for different numbers of legitimate nodes in the network. 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 is equal to 50, which validates our statement that the order gain of *double-window* misbehaving nodes approaches zero with increasing the number of nodes in Remark 5.

3.2 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 : Please refer to the proof in [17]. □

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

$$G_F(t) = \log_t \frac{\mathbb{P}(W > t)}{\mathbb{P}(W_F > t)}. \quad (6)$$

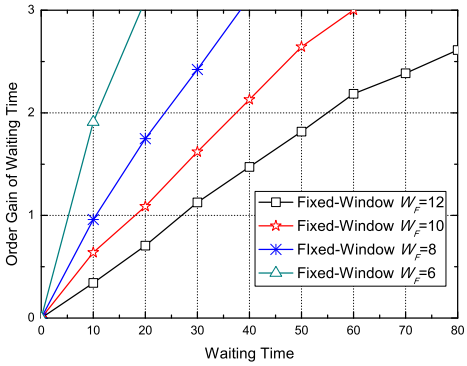

Fig. 7. Order gain of a *fixed-window* backoff misbehaving node with minimum contention window $w_{_F} = 6$, 8, 10, and 12 in an 802.11 network in the presence of 5 legitimate nodes.

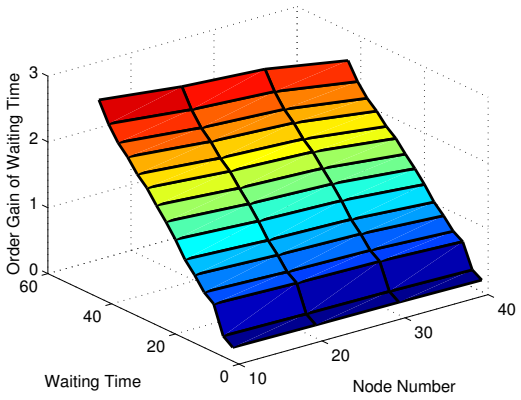

Fig. 8. Order gains of a fixed-window backoff misbehaving node with fixed contention window $w_{_F} = 8$ in an 802.11 network with different numbers of legitimate nodes.

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 simulation results regarding the order gain of *fixed-window* backoff misbehavior. We use the same network setups in Fig. 5. But the misbeahving node will perform *fixed-window* backoff misbehavior instead of *double-window* backoff misbehavior. The fixed contention window of the misbehaving node is set to be $w_{_F} = 6, 8, 10, 12$. Fig. 7 shows the order gain of the misbehaving node for different $w_{_F}$. It is observed from Fig. 7 that the order gain of the *fixed-window* backoff misbehaving node keeps increasing sub-linearly as t increases. This is because the order gain of fixed-window misbehavior is at the order of a sub-linear function $t/\log(t)$ as shown in Theorem 2. Note also that the increasing rate of the order gain of *fixed-window* misbehavior depends on $w_{_F}$. Thus, theoretically, *fixed-window* misbehavior with a small $w_{_F}$ can have very large values of order gain even when the waiting time t is small.

We also consider the impact of the number of legitimate nodes on the order gain of the misbehaving node, as shown in Fig. 8. It is noted from Fig. 8 that compared with the *double-window* backoff misbehaving node in Fig. 6, the number of legitimate nodes does not have a significant effect on the order gain of the *fixed-window* backoff misbehaving node. As shown in Fig. 8, the order gain always increases as the waiting time increases, regardless of the number of legitimate nodes, implying that in general, *fixed-window* backoff misbehavior can obtain larger gain than *double-window* backoff misbehavior.

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.

3.3 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 intermittently misbehaving node is defined as a Markov process with *on* and *off* states in Definition 4. With this definition, we have

Theorem 3: For an intermittently misbehaving node with on-state ratio θ, assume that when it changes its states, all nodes can immediately re-enter steady states. Then, its order gain 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 steady-state collision probabilities of legitimate nodes in *on* and *off* states, respectively.

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

$$G_I(t) = \log_t(\mathbb{P}(W > t)/\mathbb{P}(W_I > t)), \tag{7}$$

where $\mathbb{P}(W > t)$ and $\mathbb{P}(W_I > t)$ are the tail distribution functions of the waiting time for legitimate and intermittently misbehaving nodes, respectively. The probabilities of the intermittently 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 intermittently misbehaving node, therefore also have *on* and *off* states. Then, we have

$$\mathbb{P}(W>t) = \theta\mathbb{P}(W>t|\text{on}) + (1-\theta)\mathbb{P}(W>t|\text{off}) \quad (8)$$

and $$\mathbb{P}(W_I>t) = \theta\mathbb{P}(W_I>t|\text{on}) + (1-\theta)\mathbb{P}(W_I>t|\text{off}), \quad (9)$$

respectively. Substituting (9) and (8) into (7) yields

$$G_I(t) = \log_t\left(\frac{\theta+(1-\theta)t^{-G(t)}}{\theta t^{-G_{on}(t)}+(1-\theta)t^{-G(t)}}\right), \quad (10)$$

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. Since $G(t)$ can be regarded as the order gain of a double-window misbehaving node over a legitimate node with collision probabilities p_{on} and p_{off}, respectively. We reuse Theorem 1 and obtain that

$$G(t) = \log_2\frac{p_{on}}{p_{off}} + \Theta\left(\frac{1}{\ln t}\right). \quad (11)$$

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 (10), we have found the lower bound

$$\begin{aligned} G_I(t) &\ge \log_t\left(\frac{\theta+(1-\theta)t^{-G(t)}}{\theta t^{-G(t)}+(1-\theta)t^{-G(t)}}\right) \\ &\ge \log_t\left(\frac{\theta}{t^{-G(t)}}\right) = G(t) + \frac{\ln\theta}{\ln t}. \end{aligned} \quad (12)$$

On the other hand, it follows from (10) that

$$G_I(t) \le \log_t\left(\frac{\theta+(1-\theta)t^{-G(t)}}{(1-\theta)t^{-G(t)}}\right). \quad (13)$$

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 (13) can be upper bounded by

$$G_I(t) \le \log_t\left(\frac{\theta+(1-\theta)}{(1-\theta)t^{-G(t)}}\right) = G(t) - \frac{\ln(1-\theta)}{\ln t} \quad (14)$$

for all $t > t_0$. Combining (11), (12), and (14) yields

$$G_I(t) = \log_2\frac{p_{on}}{p_{off}} + \Theta\left(\frac{1}{\ln t}\right). \quad (15)$$

□

Theorem 3 shows that, perhaps surprisingly, the order gain of an intermittently misbehaving node $G_I(t)$ always converges to a constant that does not depend on θ. In the following, we use simulations to investigate the effect of θ on the order gain of intermittent misbehavior.

We consider an 802.11 network consisting of five legitimate nodes and one intermittently misbehaving node in simulations. The intermittently misbehaving node chooses a random backoff time uniformly from $[0, 7]$ when it is in on-state. Fig. 9 demonstrates the order gains of the intermittently misbehaving node for different on-state ratios θ. We see from Fig. 9 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. 9, t^* increases from 18 to 33 as θ goes from 50% to 99%.

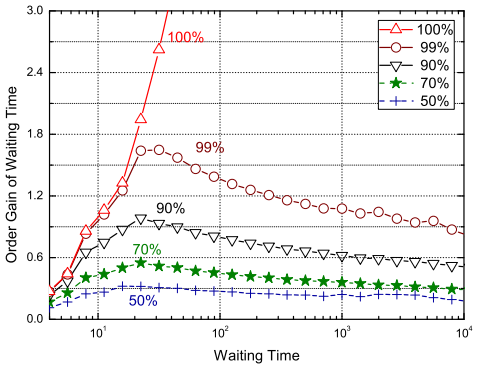

Fig. 9. Order gain of an intermittently misbehaving node in an 802.11 network with 5 legitimate nodes.

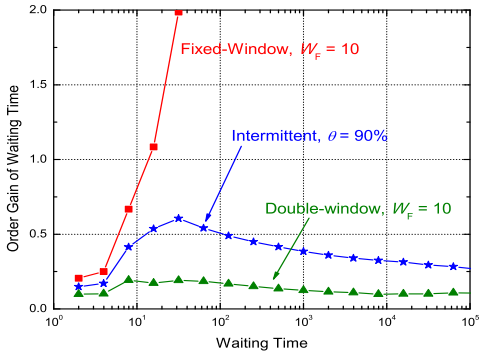

Fig. 10. Order gains of various misbehaving nodes in an 802.11 network with 5 legitimate nodes.

Fig. 9 also shows that the order gain of an intermittently 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 intermittently misbehaving node attempts to evade misbehavior detection by choosing a small θ, it cannot achieve large values of order 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 intermittently 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. 9 that when the intermittently misbehaving node has $\theta = 99\%$, its order gain is almost the same as $\theta = 100\%$ for small waiting time t. In this case, the intermittently misbehaving node has a higher risk to be detected.

We have provided ns2 simulation results for both continuous and intermittent misbehaviors. To further verify our analytical modeling and derivation, we consider a more heterogenous network with five legitimate nodes, one *fixed-window* misbehaving node, one *double-window* misbehaving node, and an intermittently misbehaving node with $\theta = 90\%$ that performs *fixed-window* misbehavior in its on-state. Fig. 10 shows the simulation results on the order gains for different misbehaving nodes in this scenario. As we can see from Fig. 10, the order gain of the *fixed-window* misbehaving node always increases as the waiting time increases; the order gain of the *double-window* misbehaving node is approximately a constant; and the order gain of the intermittently misbehaving node has a phase transition phenomenon and eventually converges as the waiting time increases.

Fig. 10 validates that our analytical results on assessing the order gains of misbehaving nodes are general and depend on neither the number of legitimate and misbehaving nodes nor the heterogeneity of a CSMA/CA-based wireless network.

4 From Order Gain to Throughput Gain in IEEE 802.11 Networks

We have so far investigated the performance gains of continuous and intermittently misbehaving nodes via the metric of order gain, which is a general metric to quantify backoff misbehavior in CSMA/CA-based wireless networks. For IEEE 802.11 DCF that becomes ubiquitous nowadays, the order gain-based analysis of previous misbehavior models is also applicable since the metric of order gain is based on the essential waiting time that is measured by the number of slots and does not depend on any specific protocol. However, the MAC layer throughput of a node is one of the most widely-used metrics in 802.11 DCF (e.g. [15], [19]–[21]). Moreover, the throughput, unlike the order gain, can directly reflect how much data a node has transmitted over a time period. Thus, it is of great interest to investigate how much throughput gain a misbehaving node can obtain from legitimate nodes in an 802.11 network.

In the following, we consider the basic access model in IEEE 802.11 DCF as our primary protocol model. We assume that the idle slot length and packet length are fixed to be σ and L (measured by μs), respectively. We also assume that all nodes are in saturated state. It has been shown in the literature (e.g., [15], [19]–[21]) that it is difficult to derive a closed-form throughput formula for a node working under IEEE 802.11 DCF. Therefore, our goal in this section is not to derive the exact throughput gain for a certain type of backoff misbehaving nodes, but to show the relation between the metric of order gain and throughput gain of a misbehaving node in an IEEE 802.11 network. Formally, we define a misbehaving node's throughput gain over legitimate nodes as follows.

Definition 7: Let the access delay of a node be the real-time interval (measured by μs) from the instant that the node begins to contend for the channel to the instant that the node finishes a successful transmission. Then, the saturated throughputs of a legitimate node and a misbehaving node are defined as

$$S = L/\mathbb{E}(D) \tag{16}$$

and

$$S_m = L/\mathbb{E}(D_m), \tag{17}$$

where D and D_m are the access delays of the legitimate node and the misbehaving node, respectively. The throughput gain ratio for the misbehaving node is defined as the ratio between the saturated throughputs of the misbehaving node and the legitimate node; i.e.,

$$R_m = S_m/S = \mathbb{E}(D)/\mathbb{E}(D_m). \tag{18}$$

Remark 8: From (18), we can see the throughput gain ratio is essentially the ratio between the mean access delays of the legitimate node and the misbehaving node. Therefore, in the following, we obtain the desirable throughput gain ratio by computing the ratio between mean access delays for legitimate and misbehaving nodes.

With Definition 7, we state our main results about the throughput gain of backoff misbehaving nodes as follows.

Theorem 4 (Throughput Gain Ratio): In an IEEE 802.11 network with n legitimate nodes and a backoff misbehaving node, assume that all nodes use the same physical layer parameters (e.g., modulation and error-correction coding). If the order gain of the misbehaving node $G_m(t)$ satisfies $\lim_{n,t\to\infty} G_m(t) = 0$, the throughput gain ratio of the misbehaving node is always upper-bounded, i.e.,

$$\lim_{n\to\infty} R_m(n) < \infty. \tag{19}$$

If $G_m(t)$ satisfies $\lim_{n,t\to\infty} G_m(t) > 0$, the throughput gain ratio of the misbehaving node goes to infinity as $n \to \infty$, i.e.,

$$\lim_{n\to\infty} R_m(n) = \infty. \tag{20}$$

Proof : The proof consists of two parts.

Part I. ($\lim_{n,t\to\infty} G_m(t) = 0 \Rightarrow \lim_{n\to\infty} R_m(n) < \infty$)

The access delay for 802.11 DCF has been well modeled and studied in the literature. Following the model of access delay for 802.11 DCF in [22], the mean access delays of a legitimate node and a misbehaving node can be represented as

$$\mathbb{E}(D) = ((1-p)\sigma + pL)\mathbb{E}(W) + \frac{L}{1-p} \tag{21}$$

and

$$\mathbb{E}(D_m) = ((1-p_m)\sigma + p_m L)\mathbb{E}(W_m) + \frac{L}{1-p_m}, \quad (22)$$

respectively, where p and p_m are the collision probabilities of the legitimate node and misbehaving node, respectively. As shown in [18], the collision probability p is an increasing function of n and converges to 0.5. Then, from Lemma 1, the mean waiting time of a legitimate node satisfies that $\lim_{n\to\infty} \mathbb{E}(W) = \infty$.

Since the order gain of the misbehaving node converges to 0; i.e.,

$$\lim_{n,t\to\infty} G_m(t) = \lim_{n,t\to\infty} \log_t \frac{P(W > t)}{P(W_m > t)} = 0, \quad (23)$$

From Lemma 1 and (23), we have

$$\lim_{n,t\to\infty} \left(\log_t \frac{p^2}{4} \left(\frac{t}{w_0} + 1 \right)^{\log_2 p} - \log_t P(W_m > t) \right) = 0,$$

and

$$\lim_{n,t\to\infty} \log_t P(W_m > t) = \lim_{n\to\infty} \log_2 p = -1, \quad (24)$$

which indicates that W_m also asymptotically follows the power-law distribution with the same parameter of $\lim_{n\to\infty} -\log_2 p = 1$ as W. Thus, $\lim_{n\to\infty} \mathbb{E}(W)/\mathbb{E}(W_m)$ is always upper bounded although $\mathbb{E}(W)$ and $\mathbb{E}(W_m)$ go to infinity, respectively. Therefore, the throughput gain ratio can be represented as

$$\begin{aligned} \lim_{n\to\infty} R_m(n) &= \lim_{n\to\infty} \frac{\mathbb{E}(D)}{\mathbb{E}(D_m)} \\ &= \lim_{n\to\infty} \frac{((1-p)\sigma + pL)\mathbb{E}(W) + \frac{L}{1-p}}{((1-p_m)\sigma + p_m L)\mathbb{E}(W_m) + \frac{L}{1-p_m}} \\ &= \lim_{n\to\infty} \frac{(1-p)\sigma + pL + \frac{L}{(1-p)\mathbb{E}(W)}}{((1-p_m)\sigma + p_m L)\frac{\mathbb{E}(W_m)}{\mathbb{E}(W)} + \frac{L}{(1-p)\mathbb{E}(W)}}. \end{aligned} \quad (25)$$

Since $\lim_{n\to\infty}(\mathbb{E}(W)/\mathbb{E}(W_m))$ is upper bounded and $\lim_{n\to\infty}((1-p_m)\sigma + p_m L) \neq 0$, we finally obtain from (25) that

$$\lim_{n\to\infty} R_m(n) < \infty. \quad (26)$$

Part II. ($\lim_{n,t\to\infty} G_m(t) > 0 \Rightarrow \lim_{n\to\infty} R_m(n) = \infty$) First, the order gain of the misbehaving node satisfies

$$\lim_{n,t\to\infty} G_m(t) = \lim_{n,t\to\infty} \log_t \frac{\mathbb{P}(W > t)}{\mathbb{P}(W_m > t)} = \epsilon > 0. \quad (27)$$

From Lemma 1 and (23), we have

$$\lim_{n,t\to\infty} \left(\log_t \frac{p^2}{4} \left(\frac{t}{w_0} + 1 \right)^{\log_2 p} - \log_t P(W_m > t) \right) \leq \epsilon, ,$$

and

$$\lim_{n,t\to\infty} \log_t P(W_m > t) \geq \lim_{n\to\infty} \log_2 p - \epsilon = -(\epsilon + 1), \quad (28)$$

which indicates that W_m asymptotically follows the power-law distribution with parameter $1 + \epsilon > 1$ and $\mathbb{E}(W_m)$ is always well-defined, i.e., $\lim_{n\to\infty} \mathbb{E}(W_m) < \infty$. Therefore, from (25), the throughput gain ratio is

$$\lim_{n\to\infty} R_m(n) = \infty. \quad (29)$$

Combining the two parts completes the proof. □

TABLE 1
Classifying backoff misbehaviors in terms of throughput gain.

Finite-Gain	Scalable-Gain
Double-window misbehavior, Intermittent misbehavior	Fixed-window misbehavior

Remark 9: Theorem 4 shows that any backoff misbehavior yields one of two consequences as the number of legitimate nodes increases: (i) the throughput gain ratio is bounded above, (ii) the throughput gain ratio goes to infinity. Theorem 4 further indicates that all backoff misbehavior models can be in fact categorized into two types in terms of harmfulness. The first type of misbehavior always has upper-bounded throughput gain ratio, regardless the number of users in a network. Thus, we refer this type of misbehavior as *finite-gain backoff misbehavior*. The second type of misbehavior can be more harmful and its throughput gain ratio goes to infinity as the number of users increases. We refer it *scalable-gain backoff misbehavior*, which implies the gain of this type of misbehavior is scalable: the larger the network scale, the more the gain of the misbehaving node.

In previous sections, based on the basic backoff structure of misbehaving nodes, we generalized misbehavior models into continuous misbehavior and intermittent misbehavior. From Theorem 4, we can categorize backoff misbehavior models into finite-gain misbehavior and scalable-gain misbehavior in terms of the throughput gain ratio. Thus, existing misbehaviors can be formally separated into the two types in terms of their throughout gains, as shown in Table 1. The throughout gain obtained by misbehaving nodes, on the other hand, indicates that there exists throughput degradation of all legitimate nodes. The larger the gain of a misbehaving node, the larger the throughput degradation of legitimate nodes. We show in the following that when the number of nodes increases in a network, finite-gain misbehavior has only negligible impact on the network.

Definition 8 (Throughput Degradation Ratio): Let S and S_m be the throughputs of a legitimate node and a backoff misbehaving node in a wireless network. Let S_l be the throughput of a legitimate node when all misbehaving nodes do not perform any misbehavior; i.e., S_l is the throughput that a legitimate node should have. Then, the throughput degradation ratio of a legitimate node due to backoff misbehavior is defined as

$$R_d = 1 - S/S_l. \quad (30)$$

Theorem 5 (Impact of finite-gain backoff misbehavior): In an IEEE 802.11 network in the presence of n legitimate nodes and n_m backoff misbehaving nodes with the same physical-layer parameters. If the misbehaving nodes are all finite-gain misbehaving and n_m is fixed, then the throughput degradation ratio of a legitimate node, R_d satisfies that

$$\lim_{n\to\infty} R_d = 0. \quad (31)$$

Proof : We assume that the channel bandwidth is normalized into 1 and is efficiently shared by legitimate nodes and misbehaving nodes, i.e.,

$$nS + n_m S_m = 1. \tag{32}$$

For the finite-gain misbehaving nodes, it always holds that

$$S_m/S \leq c, \tag{33}$$

where c is a sufficiently large constant. Thus, it follows from (32) and (33) that $1/n \geq S \geq 1/(cn_m + n)$. If all misbehaving nodes perform legitimately, we have

$$S_l = 1/(n + n_m).$$

Therefore, we can obtain

$$\lim_{n\to\infty} \frac{1/n}{1/(n+n_m)} \geq \lim_{n\to\infty} \frac{S}{S_l} \geq \lim_{n\to\infty} \frac{1/(cn_m+n)}{1/(n+n_m)},$$

and $\lim_{n\to\infty} S/S_l = 1$.

Finally, the throughput degradation ratio of a legitimate node is

$$\lim_{n\to\infty} R_d = 1 - \lim_{n\to\infty} S/S_l = 1 - 1 = 0.$$

□

Remark 10: In general, the deployment cost of a countermeasure increases as the number of nodes increases since the countermeasure needs to not only monitor states of all nodes, but also consistently perform computations based on their activities to detect any misbehavior (e.g. [23]). Existing work [9] has indicated that countermeasures to backoff misbehavior should be more concerned with misbehaving nodes that can significantly affect the network performance. Based on our analytical results, we suggest that *in large-scale networks, countermeasures to backoff misbehavior should focus primarily on scalable-gain misbehavior* since when the number of nodes is large, the effect of finite-gain misbehavior becomes marginal from a *damage perspective* as shown in Theorem 5.

5 Performance Evaluation and Discussions

In previous sections, we have investigated the performance gains of a variety of backoff misbehaviors in wireless networks. Based on analytical analysis and simulations, we used both the metric of order gain and the metric of throughput gain ratio to quantify how many benefits a backoff misbehaving node can obtain. 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 the Madwifi driver [24] to set up an experimental WiFi network in the presence of a misbehaving node. Note that Madwifi is an advanced WiFi driver for Atheros chipsets. It provides application-layer interfaces for users to modify WiFi physical-layer parameters, such as the minimum contention window and the retry limit.

5.1 Experiment Setup

5.1.1 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. There is no other access point working during our experiments. We place all devices inside a laboratory to ensure that they are under the same channel condition. The only difference between legitimate and misbehaving nodes is the backoff scheme. The other parameters, such as physical-layer rate and retry limit, are set up with the same values in all nodes. As it is difficult to find a completely interference-free environment, we perform all experiments at midnight to minimize the impact of interference on our experimental results.

5.1.2 Network Traffic

The commonly-used network testing tool, *Iperf* [25], 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.

5.1.3 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.

5.2 Experimental Results

Throughout our experiments, legitimate nodes always adopt the binary exponential backoff: the minimum and maximum contention windows are 32 and 65536, respectively. The retry limit for both legitimate and misbehaving nodes is set to be 16. Here, we set large values for the maximum contention window and the retry limit to validate our asymptotic analysis.

We first study the performance gain of *double-window* and *fixed-window* misbehaving schemes. Fig. 11 shows the throughput gain ratio of a *double-window* misbehaving node as a function of the minimum contention window of the misbehaving node and the number of legitimate nodes. We can see from Fig. 11 that the through gain ratio of the misbehaving node decreases as the minimum contention window increases and that the throughput gain ratio remains approximately the same when the number of legitimate nodes increases, which validates our analytical results in Section 4 showing that the throughput gain ratio is always upper bounded. According to Theorem 5, we can expect that when the number of legitimate nodes increases in the network, *double-window* misbehavior only causes negligible performance degradation of legitimate nodes.

Fig. 12 shows the throughput gain ratio of a *fixed-window* misbehaving node as a function of the minimum

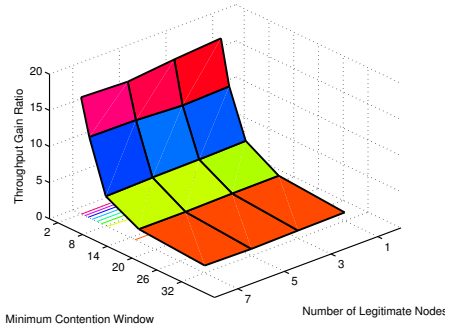

Fig. 11. Throughput ratio of a *double-window* backoff misbehaving node to a legitimate node for different backoff misbehaving schemes.

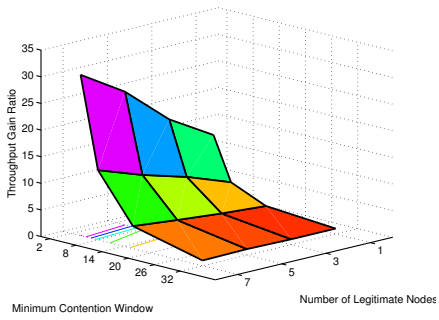

Fig. 12. Throughput ratio of a *fixed-window* backoff misbehaving node to a legitimate node.

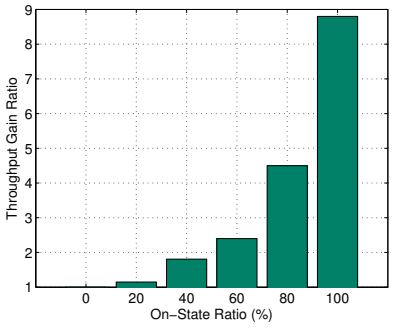

Fig. 13. Throughput ratio of the misbehaving node to a legitimate node for different on-state ratios θ.

contention window of the misbehaving node and the number of legitimate nodes. From Fig. 12, we observe that the throughput gain ratio of the *fixed-window* misbehaving node is proportional to the number of legitimate nodes: the more the number of legitimate nodes, the larger the throughput gain ratio of the misbehaving node. For example, when the contention window of the *fixed-window* misbehaving node is 4, the throughput gain ratio increases from 12.9 to 30.2 as the number of legitimate nodes goes from 1 to 7. Fig. 12 validates our results in Table 1, which shows that *fixed-window* backoff misbehavior belongs to scalable-gain misbehavior.

From Figs. 11 and 12, we see that if the number of legitimate nodes is small, *double-window* backoff misbehavior and *fixed-window* backoff misbehavior have similar throughput gain. If the number of legitimate nodes increases, *fixed-window* backoff misbehavior has much more gain than *double-window* backoff misbehavior. For example, when the misbehaving node has a minimum contention window of 8 and the number of legitimate nodes is 1, both *double-window* backoff misbehavior and *fixed-window* backoff misbehavior have approximate throughput gain ratio of 4.5. When the number of legitimate nodes becomes 7, the throughput gain ratio of *double-window* backoff misbehavior is still about 4.5 but that of *fixed-window* backoff misbehavior reaches 13. We can conclude that the number of users should be considered as a critical factor to the evaluation of providing countermeasures to a network. When the number 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 the gain of *double-window* misbehavior is always bounded and therefore it can only cause negligible performance degradation of legitimate nodes, as indicated in Theorem 5.

We then study the performance of intermittent misbehavior by considering a one-bad and five-good scenario. The intermittently misbehaving node chooses its random backoff time uniformly from $[0, 7]$ in the *on* state and performs legitimate backoff in the *off* state. Fig. 13 demonstrates the throughput ratio of the intermittently 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 the ratio is large only when θ is very large. The reason is that θ denotes the switching probability of misbehavior. For example, when $\theta = 50\%$, it switches between on and off states. From the time perspective, it in fact spends more time (large than 50%) on legitimate behavior since it has smaller access probability when behaving legitimately. Therefore, the overall throughput of the intermittently misbehaving node is less than 50% even when θ=50%. Thus, a node has to choose a large θ to obtain significant benefits from intermittent misbehavior.

5.3 Effects of Upper Limits on Retransmissions and Contention Window

As we have acknowledged, our theoretical models are based on the assumption that there is no upper limit on either the number of retransmissions or the contention window. As there always exist such upper limits in practice, we discuss via both simulations and experiments the impact of these upper limits on our theoretical results.

We first use ns2 simulations to evaluate the effect of the upper limits. We set up an IEEE 802.11 network with one misbehaving node and five legitimate nodes. The minimum contention windows for legitimate and misbehaving nodes are 32 and 8, respectively. For all nodes, the upper limit of the contention window is 1024 (the same as that in IEEE 802.11); and the upper limit of the number of transmissions of a single packet (denoted by N_R) varies from 3 to 7. All nodes are saturated.

Fig. 14 illustrates the order gain of the misbehaving node when it chooses double-window misbehavior. From Fig. 14, we can find that the finite value of N_R leads to a *finite region phenomenon* for the order gain: as waiting time t increases, the order gain dramatically increases to infinity. In other words, the order gain is

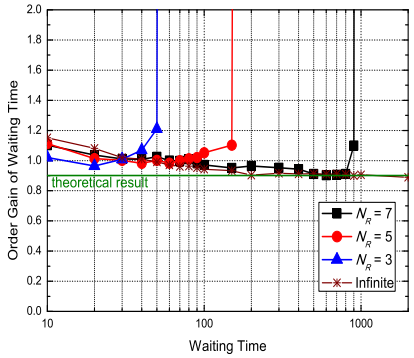

Fig. 14. Order gains of a double-window misbehaving node with finite retransmissions.

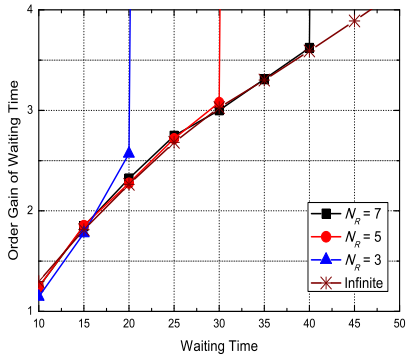

Fig. 15. Order gains of a fixed-window misbehaving node with finite retransmissions.

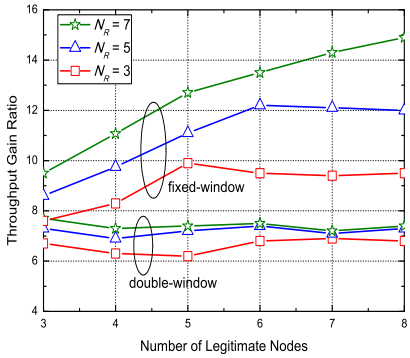

Fig. 16. Throughput gain of a misbehaving node with finite retransmissions.

finite only when t is sufficiently small. This is because the tail distribution of the waiting time for the misbehaving node $\mathbb{P}(W_D > t)$ will become zero when t is large enough. For example, when $N_R = 3$, the misbehaving node will attempt to transmit a packet 3 times before it drops the packet. Therefore the maximum possible waiting time is 8+16+32 = 56. Then, it is impossible that the waiting time W_D is larger than 56, leading to $\mathbb{P}(W_D > 56) = 0$. Accordingly, the order gain $G_D(t) = \log_t(P(W > t)/P(W_D > t))$ increases to infinity as t approaches 56.

Fig. 15 shows the order gain of the misbehaving node when it chooses fixed-window misbehavior. We can also see the *finite region phenomenon* in Fig. 15: the order gain of the fixed-window misbehavior dramatically increases to infinity when the waiting time t is large enough.

Figs. 14 and 15 indicate that we have to evaluate the order gain of a misbehaving node at its finite region (e.g., t is small) when considering a practical scenario; otherwise, the order gain will become infinity. We can see that the order gain with infinite retransmissions is still a good approximation of that with finite retransmissions, especially for fairly large N_R. For example, in Fig. 14, the order gain of $N_R = 7$ always has similar values to the order gain of $N_R = \infty$ when $t < 900$.

Next, we investigate via experiments how this *finite region phenomenon* of the order gain affects our theoretical results on throughput analysis. We consider an IEEE 802.11b network with one misbehaving node and a varying number of legitimate nodes. The setups are the same as those in Section 5.1, except that all nodes have the same upper limit for the number of transmissions for a single packet N_R. In addition, the maximum contention window for all nodes is set to be 1024. The minimum contention windows of legitimate and misbehaving nodes are 32 and 8, respectively.

Fig. 16 illustrates the throughput gain ratio of the misbehaving node as a function of the number of legitimate nodes. It can be found in Fig. 16 that the smaller the retry limit N_R, the smaller the throughput gain ratio of the misbehaving node. This is because when a legitimate node has a smaller N_R, it will more frequently start a new transmission by resetting its contention window to the minimum, thereby having more chance to access the channel. From Fig. 16, we can see that the throughput gain ratio of double-window misbehavior is approximately the same regardless of the number of legitimate nodes; while that of fixed-window misbehavior increases proportionally to the number of legitimate nodes. However, the finite value of N_R imposes an upper bound on the throughput gain ratio of fixed-window misbehavior. For example, the upper bound is 9.9 and 12.1 when $N_R = 3$ and 5, respectively.

Fig. 16 indicates that with upper limits of the contention window and the number of retransmissions, the finite-gain misbehavior (e.g., *double-window*) still has a finite throughput gain ratio; while scalable-gain misbehavior (e.g. *fixed-window*) has a throughput gain ratio that initially increases as the number of legitimate nodes increases, but also has an upper bound when the number of legitimate nodes is sufficiently large. We conclude from Fig. 16 that analytical results in Theorem 4 partially hold in practical scenarios and that such upper limits alleviate the damage caused by misbehaving nodes. However, scalable-gain misbehavior should still be a primary focus for countermeasures in that its throughput gain ratio remains scalable before approaching the upper bound that increases with the increasing of N_R.

5.4 Discussions

In previous sections, we studied the problem of quantifying the gain of backoff misbehavior and further presented experimental results to illustrate the impact of backoff misbehavior. Our findings can be summarized as: 1) *Double-window* misbehavior has an order gain converging to a constant. The performance loss of legitimate nodes due to *double-window* misbehavior is not significant in a network with a large number of users. 2) *Fixed-window* misbehavior has an order gain increasing to infinity nodes regardless of the number of users. Therefore, *fixed-window* misbehavior should

always be the primary target of countermeasures to backoff misbehavior. 3) An intermittently misbehaving node can not achieve significant gain when it chooses a small θ to evade misbehavior detection. 4) In IEEE 802.11 networks, backoff misbehavior can be categorized into two classes: finite-gain misbehavior and scalable-gain misbehavior. Scalable-gain misbehavior (e.g., *fixed-window* backoff misbehavior) has throughput gain ratio that increases as the number of legitimate nodes increases; while finite-gain misbehavior (e.g., *double-window* backoff misbehavior) always has upper-bounded throughput gain ratio.

Theoretically, the metric of order gain can be used to compare one type of misbehavior with another to show which one is more harmful. Practically, it can be used to classify misbehavior into either finite-gain or scalable-gain misbehavior, thereby providing a better understanding of how a type of misbehavior can affect the throughput in a wireless network. We pointed out that countermeasures should focus more on scalable-gain misbehaving nodes, whose throughput gain over legitimate nodes increases as the number of nodes increases. It is also worthy of mention that it may be difficult to clearly identify whether a misbehaving node is scalable-gain or finite-gain in a practical system. A possible approach is to develop a statistical detector for particular scalable-gain misbehavior, such as *fixed-window* misbehavior. Alternatively, a heuristic approach can be used in a network to intentionally add a testing node to generate additional traffic, if a node's throughput exhibits an increase, it can be detected as a scalable-gain misbehavior. Overall, an efficient and scalable detection approach is essential in a large-scale network.

6 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 formally categorize backoff misbehavior into finite-gain misbehavior and scalable-gain misbehavior. We show that *double-window* backoff misbehavior belongs to finite-gain misbehavior and has negligible impact on a network with a large number of users; *fixed-window* backoff behavior is much more harmful than others because it has scalable gain, which means its throughput gain ratio goes to infinity as the number of legitimate nodes increases to infinity.

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] S. Radosavac, J. S. Baras, and I. Koutsopoulos, "An analytic framework for modeling and detecting access layer misbehavior in wireless networks," *ACM Trans. Information and Systems Security*, vol. 11, no. 4, pp. 19:1–19:28, Jul. 2008.

[10] S. Choi, K. Park, and C. kwon Kim, "On the performance characteristics of WLANs: Revisited," in *Proc. of ACM SIGMETRICS '05*, 2005, pp. 97–108.

[11] G. Bianchi, A. D. Stefano, C. Giaconia, L. Scalia, G. Terrazzino, and I. Tinnirello, "Experimental assessment of the backoff behavior of commercial IEEE 802.11b network cards," in *Proc. of IEEE INFOCOM'07*, May 2007, pp. 1181–1189.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] Z. Lu, W. Wang, and C. Wang, "On order gain of backoff misbehaving nodes in CSMA/CA-based wireless networks," in *Proc. of IEEE Conference on Computer Communications (INFOCOM' 10)*, March 2010.

[18] 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.

[19] F. Cali, M. Conti, and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit," *IEEE/ACM Trans. Networking*, vol. 8, no. 6, pp. 785–799, Dec. 2000.

[20] J. Hui and M. Devetsikiotis, "A unified model for the performance analysis of IEEE 802.11e EDCA," *IEEE Trans. Commun.*, vol. 53, no. 9, pp. 1498–1510, Sept. 2005.

[21] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions," *IEEE/ACM Trans. Networking*, vol. 15, no. 1, pp. 159–172, Feb. 2007.

[22] T. Sakurai and H. L. Vu, "MAC access delay of IEEE 802.11 DCF," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1702–1710, May 2007.

[23] A. L. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE J. Sel. Areas in Commun.*, vol. 25, no. 6, pp. 1124–1134, Aug. 2007.

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

[25] Iperf, http://sourceforge.net/projects/iperf/.

Zhuo Lu received the B.S. degree and M.S. degree in communication engineering from Xidian University, China, in 2002 and 2005, respectively. He was a Research Assistant and Ph.D. student in Xidian University from 2005 to 2007. He is now a Ph.D. student in the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC. His research interests include communication and network systems, performance modeling, robust and fault tolerant computing.

Wenye Wang received the M.S.E.E. degree and Ph.D. degree in computer engineering from the Georgia Institute of Technology, Atlanta, in 1999 and 2002, respectively. She is an Associate Professor with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC. Her research interests include mobile and secure computing, modeling and analysis of wireless networks, network topology, and architecture design. Dr. Wang has been a Member of the Association for Computing Machinery (ACM) since 1998, and a Member of the Eta Kappa Nu and Gamma Beta Phi honorary societies since 2001. She is a recipient of the NSF CAREER Award 2006. She is the co-recipient of the 2006 IEEE GLOBECOM Best Student Paper Award - Communication Networks and the 2004 IEEE Conference on Computer Communications and Networks (ICCCN) Best Student Paper Award.

Cliff Wang graduated from North Carolina State University with a PhD degree in computer engineering in 1996. He is currently the program director for the Army Research Office's Information and Software Assurance program and manages a large portfolio of advanced information assurance research projects. He is also appointed as an associate faculty member of computer science in the College of Engineering at North Carolina State University. Dr. Wang has been carrying out research in the area of computer vision, medical imaging, high speed networks, and most recently information security.