On the Impact of Backoff Misbehaving Nodes in IEEE 802.11 Networks

Zhuo Lu† Cliff Wang* and Wenye Wang†
†Department of Electrical and Computer Engineering, NC State University, Raleigh NC 27606.
*Army Research Office, Research Triangle Park, NC 27709.
Emails: †{zlu3, wwang}@ncsu.edu, *cliff.wang@us.army.mil

***Abstract*—In this paper, we address the problem of quantifying the impact of backoff misbehaving nodes in IEEE 802.11 networks. We propose two performance metrics, *throughput gain ratio* and *throughput degradation ratio* to quantify the performance gain of misbehaving nodes over legitimate nodes and the performance loss of legitimate nodes due to backoff misbehavior, respectively. We use asymptotic analysis to derive both throughput gain ratio and throughput degradation ratio in an IEEE 802.11 network in the presence of multiple misbehaving nodes. We show that, in general, the throughput gain ratio increases linearly with the number of legitimate nodes, and the throughput degradation ratio increases linearly with the number of misbehaving nodes. Finally, we use ns-2 simulations to validate our analytical results.**

I. Introduction

IEEE 802.11 distributed coordination function (DCF) uses binary exponential backoff to coordinate all wireless nodes to access the shared wireless channel. However, it is not always guaranteed that a node can legitimately follow the binary exponential backoff as wireless devices become more programmable to support compatibility and flexibility of wireless protocols. It is possible that a node can deliberately manipulate its backoff time to gain unfair access to the channel, which is referred to as *backoff misbehavior* [1].

Backoff misbehavior can lead to severe problems, such as unfairness [1] and even denial-of-service [2]. In the literature, there are mainly two lines of work to deal with backoff misbehavior: backoff misbehavior detection [3], [4] and backoff misbehavior resilient protocol design [5], [6]. Besides providing these two types of counter-measures to backoff misbehavior, existing work focused little attention on quantifying the impact of backoff misbehavior. A recent work in [7] pointed out that counter-measures should focus on the backoff misbehaviors with significant gains and at the same time neglect backoff misbehaviors with marginal gains to save resources such as energy and bandwidth. Therefore, quantification of the gain of backoff misbehavior is a prerequisite to guiding the design of counter-measures. To this end, the authors in [7] proposed a metric, gain factor, to measure the gain of backoff misbehavior. However, the metric is limited since it is assumed in [7] that there exists only one misbehaving node in a network and that every legitimate node chooses its random backoff time uniformly from a fixed interval, which is inconsistent with the binary exponential backoff defined in DCF. Thus, it is still unclear how one or even multiple backoff misbehaving nodes affect the performance of an 802.11 network.

The work was supported by Army Research Office (ARO) under Grant Number 53435-CS-SR.

In this paper, *we address the problem of quantifying the impact of backoff misbehaving nodes*. We first define a backoff misbehavior model that is a generalized form of widely-used models in the literature [1], [2], [5], [6]. Then, we proposed two performance metrics, *throughput gain ratio* and *throughput degradation ratio*, to quantify the impact of a misbehaving node in an 802.11 network. The throughput gain ratio is defined as the ratio of throughput of a misbehaving node to that of a legitimate one, indicating how much gain the misbehaving node can obtain. The throughput degradation ratio is defined as the ratio of the throughput loss of a legitimate node to the throughput that the legitimate node should have if there were no misbehaving nodes, indicating how much loss the legitimate node suffers.

We show via both analytical results and ns-2 simulations that, in general, the throughput gain ratio of misbehaving nodes goes linearly with the number of legitimate nodes, while the throughput degradation ratio of legitimate nodes goes linearly with the number of misbehaving nodes. Therefore, besides the backoff schemes used by misbehaving nodes, both the number of legitimate nodes and the number of misbehaving nodes are critical factors to the impact of backoff misbehavior on a network.

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

II. Models and Problem Statements

A. Legitimate and Misbehaving Backoff Schemes

IEEE 802.11 DCF uses binary exponential backoff to resolve packet collisions due to uncoordinated nodes. 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*[1], and is doubled after each collision, up to $2^K w_0$, where K is the upper-limit of retransmissions. According to this procedure, we formally define the legitimate backoff scheme in 802.11 DCF as follows.

Definition 1 (Legitimate backoff scheme): The legitimate backoff scheme $\mathcal{B}$ is the backoff scheme in which the random backoff time $T(i)$ after the i-th collision is uniformly distributed on $[0, 2^i w_0)$, where w_0 is the minimum contention window of legitimate nodes.

Remark 1: As shown in [8], the transmission probability of a node that determines how frequently the node can access the channel is not sensitive to K when K is large, especially when $K \geq 15$, which motivates many works (e.g., [8], [9]) to assume $K = \infty$ to simplify the analysis of the backoff process of a node. Thus, we also assume $K = \infty$ in this paper.

Then, we formally define backoff misbehavior as follows.

Definition 2 (Backoff scheme for misbehaving nodes): The misbehaving backoff scheme $\mathcal{B}_m$ is the backoff scheme in which the random backoff time $T_m(i)$ after the i-th collision is uniformly distributed on $[0, \gamma^i w_m)$, where w_m and γ are the minimum contention window and backoff multiplier of misbehaving nodes, respectively. It holds that $\gamma^i w_m < 2^i w_0$ for $i = 0, 1, 2, ...$, where w_0 is the minimum contention window of legitimate nodes.

Remark 2: Fig. 1 illustrates the comparison of the legitimate backoff scheme and several misbehaving backoff schemes. As shown in Fig. 1, misbehaving backoff schemes always have smaller contention windows and thus can access the channel more frequently than legitimate nodes. It is difficult to develop a unified misbehavior model including all possible misbehaving schemes since the behavior of a misbehaving node can be arbitrary as long as it gains more access to the channel. Our backoff misbehavior model is a generalized form of widely-used models for backoff misbehavior in the literature. For example, $\gamma = 2$ means that the misbehaving node also adopts binary exponential backoff, which is the model used in [1], [4], and $\gamma = 1$ means that the misbehaving node always fixes its contention window, which is the model used in [2], [6].

B. Problem Formulations

Misbehaving nodes can have more chance to access the channel than legitimate nodes at the cost of performance loss of legitimate nodes. Thus, the impact of misbehaving nodes on a wireless network is two-fold. First, they induce an unfairness problem in the network. Second, they cause damage to a network in that they unfairly access the shared wireless medium, leading to performance degradation of legitimate nodes. Therefore, we introduce two performance metrics to quantify the impact of misbehaving nodes. The first is *throughput gain ratio* that measures the unfairness induced by backoff misbehavior. The second is *throughput degradation ratio* that measures the damage that backoff misbehavior causes to the network. Formally, we define the metrics as follows.

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

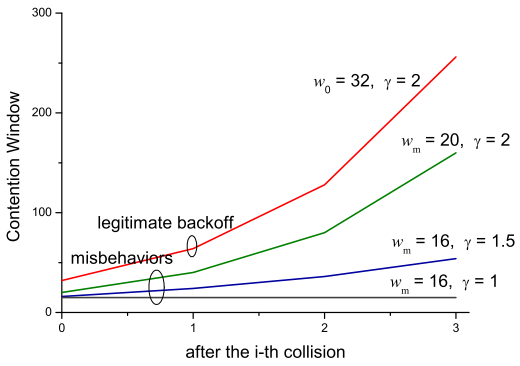

Fig. 1. The increasing of contention windows: legitimate backoff v.s. misbehaving backoff.

Definition 3: In an IEEE 802.11 network with n legitimate nodes and n_m misbehaving nodes. Throughput gain ratio is defined as

$$R_G = S_m / S, \tag{1}$$

where S_m and S are the throughputs of a misbehaving node and a legitimate node, respectively. Throughput degradation ratio is defined as

$$R_D = 1 - S / S_o, \tag{2}$$

where S is the throughput of a legitimate node, and S_o is the throughput of a legitimate node in the same network when there were $n + n_m$ legitimate nodes and no misbehaving nodes in the network.

Remark 3: Throughput gain ratio is an important metric that is already used in the literature [10], [11] to quantify the heterogeneous gains in IEEE 802.11e. The gain obtained by misbehaving nodes, on the other hand, indicates that there exists performance degradation of all legitimate nodes. Thus, it is also important to quantify the performance loss of legitimate nodes. For example, if a misbehaving node leads to 1% throughput degradation of a legitimate node, its impact can be considered to be negligible from a network perspective since it does not significantly disrupt the normal operation of a network. However, if it results in 99% throughput degradation of the legitimate node, it should be regarded as a harmful node. Hence, both throughput gain ratio and throughput degradation ratio are valid metrics for quantifying the impact of backoff misbehavior.

III. Impact of Backoff Misbehavior

A. Modeling Throughput Ratios

Our proposed metrics to evaluate the impact of backoff misbehavior are based on throughput ratios. Thus, it is essential to model the throughput of a node. We consider an 802.11 network with n legitimate nodes and n_m misbehaving nodes. All nodes work in the basic access model and are in saturated status, i.e., they always have packets ready to transmit. The only difference between legitimate nodes and

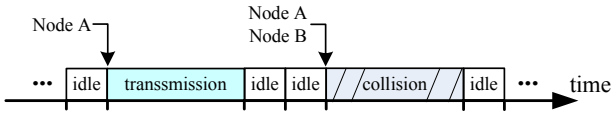

Fig. 2. Time slots in IEEE 802.11 DCF.

misbehaving nodes is the backoff scheme. The packet lengths of all nodes are equal. As shown in Fig. 2, the time in DCF is slotted, every transmission occupies a slot whose length is approximately the length of a packet. Every node can transmit a packet at a slot with a certain probability that depends on its backoff scheme. A node can successfully transmit a packet if it makes a transmission attempt and at the same time no collision happens.

Modeling the throughput for 802.11 DCF has been well studied in many papers (e.g., [10], [12]). Therefore, it follows from [12] that the throughput of a node can be modeled as $S_{\text{node}} = P_{\text{succ}} L_p / \mathbb{E}(L_s)$, where P_{succ} is the successful transmission probability of the node, L_p is the packet length, and $\mathbb{E}(L_s)$ is the average length of a slot and $\mathbb{E}(L_s) = P_{\text{idle}}\sigma + (1 - P_{\text{idle}})L_p \approx (1 - P_{\text{idle}})L_p$, where σ is the length of an idle slot and $\sigma \ll L_p$. P_{idle} is the probability that no node transmits at a slot. Then, the throughput gain ratio can be computed as

$$R_G = \frac{P_{\text{succ-mis}}}{P_{\text{succ-leg}}} = \frac{\beta_m(1-p_m)}{\beta(1-p)}, \tag{3}$$

where $P_{\text{succ-mis}}$ and $P_{\text{succ-leg}}$ are the successful transmission probabilities of a legitimate node and a misbehaving node, respectively. β and β_m are the transmission probabilities of the legitimate and misbehaving nodes, respectively; p and p_m are the collision probabilities of the legitimate and misbehaving nodes, respectively. In this paper, the transmission probability of a node is defined as the probability that the node transmits a packet at a slot, and the collision probability of a node is defined as the probability that there is at least one other node transmitting when the node transmits a packet. Thus, p and p_m can be represented by β and β_m as

$$\begin{cases} p_m = 1 - (1-\beta)^n (1-\beta_m)^{n_m - 1} & (4) \\ p = 1 - (1-\beta)^{n-1} (1-\beta_m)^{n_m}. & (5) \end{cases}$$

On the other hand, given the backoff schemes in Definitions 1 and 2, it follows from [11] that β and β_m can be represented as

$$\begin{cases} \beta_m = 2/(w_m(1-p_m)/(1-\gamma p_m) - 1) & (6) \\ \beta = 2/(w_0(1-p)/(1-2p) - 1). & (7) \end{cases}$$

From Definition 3, the throughput degradation ratio can be also computed as

$$R_D = 1 - \frac{\beta(1-p)}{\beta_o(1-p_o)} \frac{1-(1-p_o)(1-\beta_o)}{1-(1-p)(1-\beta)}, \tag{8}$$

where p_o and β_o are the collision and transmission probabilities of a legitimate node in a network where there are $n + n_m$ legitimate nodes and no misbehaving nodes. It holds for p_o and β_o that

$$\begin{cases} p_o = 1 - (1-\beta_o)^{n+n_m-1} & (9) \\ \beta_o = 2/(w_0(1-p_o)/(1-2p_o) - 1). & (10) \end{cases}$$

B. Main Results

In order to derive the throughput gain ratio (3) and the throughput degradation ratio (8), we have to solve the non-linear fixed-point equations (4)–(7), (9) and (10), which are in general mathematically intractable. Numerical methods to find the solutions of the non-linear equations are widely used in the literature (e.g., [12], [13]). In the following, we will use asymptotic analysis to derive the throughput gain and throughput degradation ratios.

Before we proceed to our main results, we first introduce two lemmas.

Lemma 1: The collision probabilities of legitimate and misbehaving nodes p and p_m are increasing functions of the number of legitimate node n, and the transmission probabilities of legitimate and misbehaving nodes β and β_m are decreasing functions of n. It holds that

$$\lim_{n\to\infty} p = 1/2, \quad \lim_{n\to\infty} \beta = 0, \tag{11}$$

$$\lim_{n\to\infty} p_m = c_1, \quad \lim_{n\to\infty} \beta_m = c_2, \tag{12}$$

where $c_1 = \frac{-3w_m+5\gamma+6+\sqrt{w_m^2-6\gamma w_m+4w_m+25\gamma^2-60\gamma+36}}{4(-w_m+3\gamma)}$ and $c_2 = 2/(w_m\frac{1-c_1}{1-\gamma c_1} - 1)$.

Proof: The proofs that p and p_m are increasing functions of n and that β and β_m are decreasing functions of n follow the same line in [11]. It has also been shown in [11] that $\lim_{n\to\infty} p = 1/2$ and $\lim_{n\to\infty} \beta = 0$. Thus, in the following, we prove that $\lim_{n\to\infty} p_m = c_1$ and $\lim_{n\to\infty} \beta_m = c_2$.

Consider the non-linear equations (4) and (5). The necessary condition for the equations holding is $(1-p)(1-\beta) = (1-p_m)(1-\beta_m)$. Thus $\lim_{n\to\infty}(1-p)(1-\beta) = \lim_{n\to\infty}(1-p_m)(1-\beta_m)$. Since $\lim_{n\to\infty} p = 1/2$ and $\lim_{n\to\infty} \beta = 0$, we get

$$(1 - \lim_{n\to\infty} p_m)(1 - \lim_{n\to\infty} \beta_m) = 1/2. \tag{13}$$

Substituting (6) into (13) and solving the equation, we finally have $\lim_{n\to\infty} p_m = c_1$, and $\lim_{n\to\infty} \beta_m = c_2$, where $c_1 = \frac{-3w_m+5\gamma+6+\sqrt{w_m^2-6\gamma w_m+4w_m+25\gamma^2-60\gamma+36}}{4(-w_m+3\gamma)}$ and $c_2 = 2/(w_m\frac{1-c_1}{1-\gamma c_1} - 1)$. □

Lemma 2: The transmission probabilities β, β_m and β_o, and the collision probabilities p, p_m, and p_o satisfy that $\beta = \Theta(1/n)$, $\beta_m = c_2 + \Theta(1/n)$, $\beta_o = \Theta(1/n)$, $p = 1/2 + \Theta(1/n)$, $p_m = c_1 + \Theta(1/n)$, $p_o = 1/2 + \Theta(1/n)$,[2] where c_1 and c_2 are constants defined in Lemma 1.

Proof: In the following, we only prove $\beta = \Theta(1/n)$. The others can be derived in a similar way and are omitted due to page limit. First, we rewrite (5) as

$$p = 1 - e^{(n-1)\ln(1-\beta)} (1-\beta_m)^{n_m}. \tag{14}$$

[2]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 $c_1|g(x)| \le |f(x)| \le c_2|g(x)|$ for all $x > x_0$.

From Lemma 1, p is an increasing function of n converging to 1/2. Therefore for any $0 < \epsilon_1 < 1/2$, the following always holds for n sufficiently large.

$$\epsilon_1 \leq 1 - e^{(n-1)\ln(1-\beta)}(1-\beta_m)^{n_m}. \quad (15)$$

From Lemma 1, β converges decreasingly to zero, which means there exist $\sigma_2 > \sigma_1 > 0$ such that $e^{-(n-1)\sigma_1\beta} \geq e^{(n-1)\ln(1-\beta)} \geq e^{-(n-1)\sigma_2\beta}$ for all sufficiently large n. Further, β_m is always upper bounded by $1/(w_m - 1)$. We then have

$$\epsilon_1 \leq 1 - e^{-\sigma_2(n-1)\beta}\epsilon_2, \quad (16)$$

where $\epsilon_2 = ((w_m - 2)/(w_m - 1))^{n_m}$. We get the lower bound

$$\beta \geq (\ln\epsilon_2 - \ln(1-\epsilon_1))/(\sigma_2(n-1)). \quad (17)$$

On the other hand, since p converges increasingly to 1/2, it holds that

$$1/2 \geq 1 - e^{(n-1)\ln(1-\beta)}(1-\beta_m)^{n_m} \geq 1 - e^{-\sigma_1(n-1)\beta}. \quad (18)$$

Therefore, we have

$$\beta \leq \ln 2/(\sigma_1(n-1)). \quad (19)$$

Combining (17) and (19) completes the proof. □

With Lemmas 1 and 2, we now state our main results.

Theorem 1 (Throughput Gain Ratio): In a network with n legitimate nodes and n_m misbehaving nodes, the throughput gain ratio of a misbehaving node is

$$R_G = \begin{cases} (w_0 - 4)/(w_m - 4) + \Theta(1/n) & \gamma = 2 \\ \Theta(n) & 1 \leq \gamma < 2 \end{cases}. \quad (20)$$

Proof: First, it can be obtained from Lemma 1 that $c_2 = 0$ if and only if $\gamma = 2$. The throughput gain ratio can be represented as

$$R_G = (\beta_m(1-p_m))/(\beta(1-p)). \quad (21)$$

From Lemma 2, we have

$$R_G = \frac{(c_2 + \Theta(1/n))(1 - c_1 - \Theta(1/n))}{\Theta(1/n)(1/2 - \Theta(1/n))}. \quad (22)$$

If $c_2 > 0$, we have $R_G = \Theta(n)$. If $c_2 = 0$, it holds that

$$R_G = \frac{\Theta(1/n)(1 - c_1 - \Theta(1/n))}{\Theta(1/n)(1/2 - \Theta(1/n))} = \Theta(1) + \Theta(1/n). \quad (23)$$

It has been shown in [11] that $\lim_{n\to\infty} R_G = (w_0 - 4)/(w_m - 4)$. Therefore, when $c_2 = 0$, $R_G = (w_0 - 4)/(w_m - 4) + \Theta(1/n)$. □

Theorem 2 (Throughput Degradation Ratio): In a network with n legitimate nodes and n_m misbehaving nodes, the throughput degradation ratio of a legitimate node $R_D \in [0, 1]$ satisfies

$$R_D = \begin{cases} \Theta(1/n) & \gamma = 2 \\ -n_m \log_2(1 - c_2) + \Theta(1/n) & 1 \leq \gamma < 2 \end{cases}. \quad (24)$$

where c_2 is a constant defined in Lemma 1.

Proof: From Lemma 2 and Equation (8), the throughput degradation ratio can be written as

$$\begin{aligned} R_D &= 1 - \frac{\Theta(\frac{1}{n})(\frac{1}{2} - \Theta(\frac{1}{n}))}{\Theta(\frac{1}{n})(\frac{1}{2} - \Theta(\frac{1}{n}))} \frac{(1 - (\frac{1}{2} - \Theta(\frac{1}{n})(1 - \Theta(\frac{1}{n}))))}{(1 - (\frac{1}{2} - \Theta(\frac{1}{n})(1 - \Theta(\frac{1}{n}))))} \\ &= \Theta(1) + \Theta(1/n). \end{aligned} \quad (25)$$

Then, it suffices to show $\lim_{n\to\infty} R_D = -n_m \log_2(1 - c_2)$ to finish the proof.

From Lemmas 1 and 2, β is a decreasing function of n and $\beta = \Theta(1/n)$. Therefore, $\lim_{n\to\infty} n\beta = b$ exists. Thus, it follows from (5) that

$$\lim_{n\to\infty}(1-p) = \lim_{n\to\infty}(1-\beta)^{n-1} \lim_{n\to\infty}(1-\beta_m)^{n_m}. \quad (26)$$

From Lemmas 1 and 2, Equation (26) can be written as

$$1/2 = e^{-b}(1 - c_2)^{n_m}. \quad (27)$$

Solving (27) for b yields

$$b = \lim_{n\to\infty} n\beta = \ln 2 + n_m \ln(1 - c_2). \quad (28)$$

The transmission probability β_o is the probability that a legitimate node makes a transmission at a slot when there exists no misbehavior in the network. It has been shown in [13] that $\lim_{n\to\infty} n\beta_o = \ln 2$ and $\lim_{n\to\infty} p_o = 1/2$. Thus, we have

$$\begin{aligned} \lim_{n\to\infty} R_D &= 1 - \lim_{n\to\infty} \frac{\beta}{\beta_o} \frac{1-p}{1-p_o} \frac{1 - (1-p_o)(1-\beta_o)}{1 - (1-p)(1-\beta)} \\ &= 1 - \frac{\ln 2 + n_m \ln(1 - c_2)}{\ln 2} \\ &= -n_m \log_2(1 - c_2). \end{aligned} \quad (29)$$

When $\gamma = 2$, we have $c_2 = 0$ and thus

$$\lim_{n\to\infty} R_D = -n_m \log_2(1 - 0) = 0 \quad \text{if } \gamma = 2. \quad (30)$$

Combining (25), (29), and (30) completes the proof. □

Remark 4: Theorems 1 and 2 show that if misbehaving nodes adopt binary exponential backoff ($\gamma = 2$), their gain R_G is always upper bounded and converges to $(w_0 - 4)/(w_m - 4)$ and, at the same time, their damage to the network R_D becomes negligible when the number of legitimate nodes n becomes large. When $1 \leq \gamma < 2$, we have $R_G = \Theta(n)$, showing that the gain of misbehaving nodes depends mainly on n and increases linearly with n. Thus, interestingly, the more the number of legitimate nodes, the more the gain of misbehaving nodes. On the other hand, the damage of misbehaving nodes to the network $R_D = -n_m \log(1 - c2) + \Theta(1/n)$, where c_2 depends only on the backoff scheme of misbehaving nodes, showing that R_D increases linearly with n_m when n is large.

IV. Simulation Results

We perform ns-2 simulations to validate our analysis and to further evaluate the impact of backoff misbehaving nodes. We use the following setups in our simulations: the IEEE 802.11 MAC module, the TwoRayGround propagation model, the WirelessChannel model. The legitimate nodes use binary exponential backoff with minimum contention window $w_0 = 32$. We use (γ, w_m) to denote a misbehaving backoff scheme since according to Definition 2, a misbehaving backoff scheme depends only on backoff multiplier γ and minimum contention window w_m. Figs. 3 and 4 illustrate the throughput gain and throughput degradation ratios in an IEEE 802.11 network with one misbehaving node, respectively. We consider three different misbehaving schemes: (1,16), (1.5,16), and (2,16). From Figs. 3 and 4, we see that the throughput gain ratio of

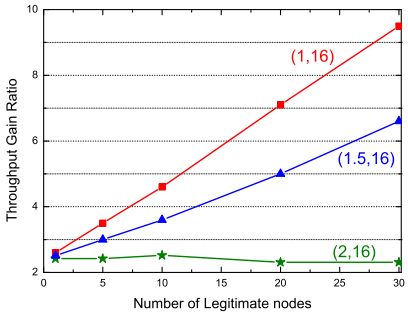

Fig. 3. Throughput gain ratios of misbehaving nodes versus the number of legitimate nodes.

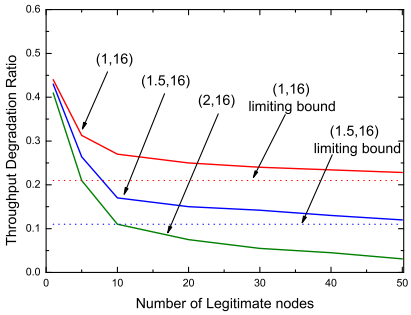

Fig. 4. Throughput degradation ratios of legitimate nodes nodes versus the number of legitimate nodes

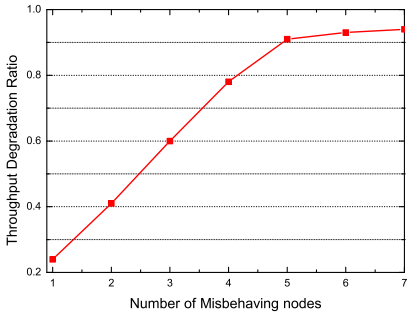

Fig. 5. Throughput degradation ratios of legitimate nodes versus the number of misbehaving nodes

a (2,16) misbehaving node is approximately a constant and at the same time the throughput degradation ratio converges to zero, which indicates that when a misbehaving node adopts binary exponential backoff ($\gamma = 2$), it can only achieve a constant gain and has negligible impact on a network when the number of legitimate nodes n is large. However, the throughput gain ratios of (1,16) and (1.5,16) misbehaving schemes go linearly with n and the throughput degradation ratios converge decreasingly to their limiting bounds that are calculated according to Equation (29). Figs. 3 and 4 further indicate that, interestingly, a misbehaving node in general achieves more gain in a large-scale network (i.e., a network with a large number of legitimate users) than it does in a small-scale network. On the contrary, its damage to a large-scale network is smaller than its damage to a small-scale network.

Fig. 5 shows the throughput degradation ratio of legitimate nodes in a network with 10 legitimate nodes and multiple misbehaving nodes, which adopt the (1,16) scheme. It is observed that throughput degradation ratio increases linearly with the number of misbehaving nodes n_m and finally converges to 1. It is worth noting that, according to our analytical analysis, the throughput degradation ratio R_D can have a value greater than 1 when n_m is sufficiently large. It is due to the multistability phenomenon pointed out in [11] that leads to multi-solutions of the fixed-point equations (4)-(7). In simulations, we found that when the analytical degradation ratio R_D is larger than 1, the simulated throughput degradation ratio is always near 1. As shown in Fig. 5, R_D starts to increase linearly as n_m increases, and eventually converges to 1, which indicates that our analytical result is only applicable to the linearly increasing part. However, it is reasonable to assume that only a small amount of misbehaving nodes exist in an 802.11 network; therefore, our result is still valid to assess the damage of misbehaving nodes to a network.

V. Conclusions

In this paper, we analyzed the impact of backoff misbehavior in IEEE 802.11 networks. We proposed two performance metrics, *throughput gain ratio* and *throughput degradation ratio* to quantify the performance gain of misbehaving nodes and the performance loss of legitimate nodes, respectively. We used asymptotic analysis to derive the throughput gain and degradation ratios and showed that, in general, a misbehaving node achieves more gain in a large-scale network than it does in a small-scale network. However, its damage to a large-scale network is smaller than its damage to a small-scale network. We further show that the damage that misbehaving nodes cause to a network increases linearly with the number of misbehaving nodes.

References

[1] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Trans. Mobile Computing*, vol. 4, no. 5, pp. 502–516, Sept. 2005.

[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] 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.

[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] 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.

[6] 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.

[7] 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.

[8] A. Kumar, E. Altman, D. Miorandi, and M. Goyal, "New insights from a fixed point analysis of single cell IEEE 802.11 wireless LANs," in *Proc. of IEEE INFOCOM '05*, vol. 3, Mar. 2005, pp. 1550– 1561.

[9] D. Xu, T. Sakurai, and H. L. Vu, "An access delay model for IEEE 802.11e EDCA," *IEEE Trans. Mobile Computing*, vol. 8, no. 2, pp. 261–275, Feb. 2009.

[10] 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.

[11] 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.

[12] 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.

[13] B.-J. Kwak, N.-O. Song, and L. E. Miller, "Performance analysis of exponential backoff," *IEEE/ACM Trans. Networking*, vol. 13, no. 2, pp. 343–355, Apr. 2005.