Malicious or Selfish? Analysis of Carrier Sense Misbehavior in IEEE 802.11 WLAN

Kyung-Joon Park[1], Jihyuk Choi[2], Kyungtae Kang[1], and Yih-Chun Hu[2]

[1] Department of Computer Science,
University of Illinois at Urbana-Champaign, 201 N. Goodwin Avenue, Urbana, IL 61801 USA
{kjp,ktkang}@illinois.edu
[2] Department of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign, 1406 West Green Street, Urbana, IL 61801 USA
{jchoi43,yihchun}@illinois.edu

Abstract. The behavior of selfish users, which does not respect the backoff procedure of IEEE 802.11 WLAN, has been nicely studied in game-theoretic frameworks. However, in these studies, the effect of physical carrier sense has not been properly incorporated into the analysis. In this paper, we study the problem of how carrier sense misbehavior can affect network performance in addition to backoff misbehavior. Our analysis shows that a cheater can increase its throughput by ignoring the carrier sense mechanism while a well-behaved user significantly loses its throughput. Consequently, not only a malicious user, but also a selfish one is motivated to disregard the carrier sense mechanism, which will result in significant throughput degradation of well-behaved ones. Our analysis also shows that carrier sense misbehavior corresponds to the case of virtually increasing the channel access probability of the cheater in the backoff procedure. We provide our preliminary simulation results, which verify our analysis.

Keywords: IEEE 802.11 MAC, physical carrier sense, wireless network security, MAC-layer misbehavior.

1 Introduction

With the ubiquitous deployment of wireless networks such as IEEE 802.11 Wireless Local Area Network (WLAN), it becomes critical to protect the network from malicious and selfish users. In particular, the Medium Access Control (MAC) protocols in wireless networks typically adopt distributed contention resolution schemes for the shared wireless channel. Hence, a misbehaving user that does not respect MAC protocols can significantly degrade network performance by diminishing the bandwidth share of well-behaved users. For example, the IEEE 802.11 WLAN MAC adopts the Distributed Coordination Function (DCF), which basically consists of the CSMA/CA with the exponential backoff mechanism. Consequently, a malicious or selfish user, which disregards the IEEE 802.11 DCF, may cause significant performance degradation of well-behaved ones.

Recently, selfish or greedy behavior in IEEE 802.11 MAC has been substantially studied [1, 2, 3, 4, 5, 6]. In particular, the selfish behavior disregarding the exponential

N. Bartolini et al. (Eds.): QShine/AAA-IDEA 2009, LNICST 22, pp. 351–362, 2009.

backoff mechanism has been nicely formulated in game-theoretic frameworks [2, 3, 5]. These studies have shown that the selfish behavior of disregarding the exponential backoff mechanism can significantly increase the bandwidth share of a cheater at the expense of that of a normal user. In addition, several efficient detection mechanism for misbehavior of a cheater have been proposed [2, 4, 5]. However, in these studies, the effect of physical carrier sense has not been considered in the analysis.

In this paper, we study the problem of how carrier sense misbehavior affects network performance in IEEE 802.11 WLAN. Since the basic IEEE 802.11 MAC consists of physical carrier sense and the exponential backoff mechanism, carrier sense misbehavior provides another line of possibilities for a cheater in addition to disregarding the exponential backoff mechanism. We consider the case when a cheater does not respect the carrier sense mechanism with a certain cheating rate when it has a packet to send. We first derive the saturation throughput of a cheater and a well-behaved user as a function of the cheating rate, respectively. Then, we show that the throughput of a cheater increases while that of a normal user decreases as the cheating rate increases. Consequently, similarly as in the case of the backoff misbehavior, the cheater can increase its bandwidth share by sacrificing that of the normal user. Our analysis further shows that carrier sense misbehavior corresponds to the case of virtually increasing the channel access probability of the cheater in the exponential backoff mechanism. Our simulation results validate our analysis.

The remainder of the paper is organized as follows. We introduce recent studies on wireless network security in Section 2. Then, in Section 3, we introduce the IEEE 802.11 DCF and the Bianchi's model for the exponential backoff procedure, which will be used in our analysis in subsequent sections. In Section 4, we derive the saturation throughput of a cheater and a well-behaved user as a function of the cheating rate, respectively. Then, we show that the throughput of a cheater increases while that of a normal user decreases as the cheating rate increases. Simulation results that verify our analysis are given in Section 5. Finally, our conclusion follows in Section 6.

2 Related Work

The IEEE 802.11 standard has seen successful widespread deployment because of its unlicensed spectrum and low hardware cost. The original security protocol of IEEE 802.11, called Wired Equivalent Privacy (WEP), was designed to provide privacy and authenticity of data. However, it has been shown by Fluhrer et al. [7] that weakness in the encryption algorithm used by WEP can be exploited to allow the discovery of session keys. After this study, various related attacks have been demonstrated, for example, [8, 9].

Bellardo and Savage [10] have implemented and demonstrated an attack that targets the authentication/association scheme of IEEE 802.11. They showed that the deauthentication and disassociation messages are not encrypted in the scheme, and thus an attacker can easily forge these messages. The attacker can then send the deauthentication message to the access point before client's data is received, or the attacker can send the disassociation message to the client before the client's data is transmitted. They further showed in [10] that the 802.11 carrier sense mechanism can be easily exploited. For

example, in 802.11 networks, a node can only send data a certain time after the channel stops being busy. In particular, if not due to retransmission or fragmentation, a user can only transmit data DCF InterFrame Space (DIFS) after channel is available; otherwise the user can transmit data Short InterFrame Space (SIFS) after, where SIFS $<$ DIFS. Bellardo and Savage then presented a sophisticated scheme exploiting the virtual carrier sense mechanism. The 802.11 standard specifies that the MAC frame header of all packets should contain a *duration* field, which specifies how long others have to wait before transmission is allowed in order to avoid collision. Users update their Network Allocation Vector (NAV) with this duration information and keep quiet for the specified duration. Thus an attacker can repeatedly request long channel occupancy time, thereby starving normal clients of channel occupancy.

Another type of attack that disregards the backoff procedure in 802.11 MAC has been substantially studied [1,2,3]. In these studies, game-theoretic frameworks have often played a key role for analyzing the network behavior [2,3]. For example, it has been shown in [2] that the backoff misbehavior leads to a significant unfair share of bandwidth between the cheater and the well-behaved users. Then, an efficient game-theoretic framework has been proposed to drive the network operating point to a pareto-optimal one. More recently, Pelechrinis et al. [6] showed in their empirical studies that carrier sense misbehavior significantly degrades the performance of well-behaved users while the cheater can substantially increase its bandwidth share. Based on this observation, They proposed a scheme for detecting this misbehavior in IEEE 802.11 WLAN. Their key idea is as follows: Since the cheater will ignore low-power receptions as legitimate packets, by intelligently sending low-power probe packets, an AP can detect the cheater with high probability.

Our study here lies in the direction of these studies on carrier sense misbehavior. Our main focus is on investigating the performance of each user with carrier sense misbehavior, which has not been considered in the analysis of previous studies. Though the throughput performance with carrier sense misbehavior has been empirically shown in [6], there has been few analytical studies on this issue. Consequently, we look into this problem in an analytical manner, which we expect will be a building block for developing efficient detection and prevention mechanisms for carrier sense misbehavior in the future.

3 Preliminaries

3.1 IEEE 802.11 DCF Mechanism

The basic CSMA/CA mechanism in IEEE 802.11 DCF operates as follows. When a station has a frame to transmit, it senses the medium first, which is called *physical carrier sense*. After the medium is sensed idle for a time interval of Distributed InterFrame Space (DIFS), it starts to transmit the frame. Otherwise, the station defers its transmission according to a exponential backoff algorithm: It maintains a random backoff timer, whose value is uniformly distributed in $[0, CW]$, where CW stands for the contention window size. CW is always 1 less than a power of 2 (e.g, 15, 31, 63, ...). CW is initially set to its minimum value of CW_{min}, moves to the next greatest power of two, up to its maximum value of CW_{max}, after each time the frame incurs a collision. The backoff

timer is decremented by one for each physical slot time σ when the channel is idle, suspended whenever the channel is busy, and reactivated after the channel is sensed idle again for a DIFS. The node transmits when the backoff timer reaches zero. After transmitting frame except broadcasting message, the source node expects to receive a positive acknowledgement (ACK) frame from the destination node within an interval of Short InterFrame Space (SIFS). If an ACK is not received in SIFS, the sender assumes the frame has experienced a collision, and schedules a retransmission for this frame while updating CW according to the exponential backoff algorithm.

3.2 Markov Chain Model for the IEEE 802.11 Exponential Backoff Mechanism

Here, we briefly introduce the Markov chain model for the IEEE 802.11 exponential backoff mechanism in [11] for completeness, which will be used in our analysis in the next section. For a given node, each state is represented as (i, k) where i is the backoff stage and k is the current backoff counter. The backoff window size at stage i is denoted by W_i. Since the minimum backoff window size is W, W_i becomes $W_i = 2^i W$ with the binary exponential backoff.[1] The maximum backoff stage is m. Then, the one-step transition probabilities are as follows:

$$\begin{cases} P\{i,k \mid i,k+1\} = 1, & k \in (0, W_i - 2), i \in (0,m); \\ P\{0,k \mid i,0\} = \frac{(1-p)}{W_0}, & k \in (0, W_0 - 1), i \in (0,m); \\ P\{i,k \mid i-1,0\} = \frac{p}{W_i}, & k \in (0, W_i - 1), i \in (i,m); \\ P\{m,k \mid m,0\} = \frac{p}{W_m}, & k \in (0, W_m - 1). \end{cases}$$

Now, let $b_{i,k}$ denote the stationary probability of state (i, k). Then, we have the following relation.

$$\begin{cases} b_{i,0} = p^i b_{0,0}, & 0 < i < m; \\ b_{m,0} = \frac{p^m b_{0,0}}{(1-p)}. \end{cases}$$

Then, we have

$$b_{i,k} = \frac{W_i - k}{W_i} b_{i,0},\ i \in (0,m), k \in (1, W_i - 1).$$

Finally, $b_{i,k}$ can be expressed as a function of $b_{0,0}$ as follows:

$$\begin{cases} b_{i,k} = \frac{p^i (W_i - k)}{W_i} b_{0,0}, & i \in (0, m-1), k \in (1, W_i - 1); \\ b_{m,k} = \frac{p^m (W_m - k)}{(1-p) W_m} b_{0,0}, & k \in (1, W_i). \end{cases} \tag{1}$$

Now, $b_{0,0}$ can be obtained by applying the normalization condition of the Markov chain as follows:

$$1 = \sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} b_{i,k} = \sum_{i=0}^{m} b_{i,0} + \sum_{i=0}^{m} \sum_{k=1}^{W_i - 1} b_{i,k}. \tag{2}$$

[1] In fact, W_i and W correspond to $CW + 1$ at stage i and $CW_{min} + 1$ in the previous section, respectively.

By using (1), (2) gives

$$b_{0,0} = \frac{2(1-2p)(1-p)}{(1-2p)(W+1)+pW(1-(2p)^m)}. \quad (3)$$

From (3), the channel access probability τ can be obtained as follows.

$$\tau = \sum_{i=0}^{m} b_{i,0} = \frac{2(1-2p)}{(1-2p)(W+1)+pW(1-(2p)^m)}. \quad (4)$$

4 Performance Analysis with Carrier Sense Misbehavior

In this section, we present an analytical framework for modeling a heterogeneous IEEE 802.11 WLAN, where a cheater and a well-behaved user coexist. In our analysis, we assume that there exist one misbehaving user and one normal user in the network. A more general analysis will be an issue of future work.

4.1 System Descriptions and Assumptions

There are basically two ways for a cheater to disregard the carrier sense mechanism. First, it can intentionally ignore the ongoing transmission of a well-behaved user during the exponential backoff procedure and attempt to transmit by decrementing its backoff counter without freezing. In this case, if the transmission of a frame takes longer than a usual backoff window, it is clear that both of the transmissions will fail because of the collision, which is apparently malicious to both the cheater and the well-behaved user. Another way is to disregard the carrier sense mechanism at the beginning, and starts to transmit without entering into the exponential backoff mechanism. Here, we consider the latter case, under which the cheater may benefit from its misbehavior.

Without loss of generality, let User 1 denote the cheater and User 2 the well-behaved one. The conditional collision probability and the channel access probability of each user are denoted by p_i and τ_i, $i = 1, 2$, respectively. In addition, the cheater ignores the carrier sense mechanism with a cheating rate of q, i.e., with a probability of q, the cheater accesses the channel without carrier sense (which also results in bypassing the exponential backoff mechanism). Consequently, the cheater can affect the throughput performance of both users by adjusting the value of q. Our analysis has the following two goals; to derive the throughput of each user as a function of the cheating rate q and to identify the effect of q on the throughput of each user based on the derived model.

Note that it is not a simple task to discover the analytical relation between the throughput of each user and the cheating rate because of the exponential backoff procedure. In addition, it should be noted that the channel access probability of the cheater, τ_1, is defined as the conditional channel access probability when the cheater has decided not to cheat (which occurs with a probability of $(1-q)$). The actual channel access probability of the cheater seen by the well-behaved one is different from τ_1. We will discuss this issue in the subsequent section.

4.2 Markov Chain Model for the Exponential Backoff Mechanism with Carrier Sense Misbehavior

Here, by using (4), we derive the systems of equations for the exponential backoff mechanism with carrier sense misbehavior. Note that our analysis is different from the homogeneous case in [11] in the sense that we consider the heterogeneous situation where τ_i's and p_i's are different, respectively, because of the introduction of the carrier sense cheating rate q.

As already introduced in the previous sections, let p_i and τ_i, $i = 1, 2$ denote the collision probability and the channel access probability of the cheater and the well-behaved user, respectively. Since the event of cheating is independent of the well-behaved user's channel access, the conditional collision probability of the cheater, p_1, becomes

$$p_1 = 1 - (1 - \tau_2) = \tau_2. \tag{5}$$

In the meantime, the channel access of the well-behaved user will succeed if the cheater has decided not to cheat and further decided not to transmit according to the exponential backoff mechanism. Hence, p_2 becomes

$$p_2 = 1 - (1 - q)(1 - \tau_1) = 1 - [1 - \{(1 - q)\tau_1 + q\}] = \tau_1', \tag{6}$$

where $\tau_1' = (1 - q)\tau_1 + q$. In addition, from (4), we have

$$\tau_i = \frac{2(1 - 2p_i)}{(1 - 2p_i)(W + 1) + p_i W(1 - (2p_i)^m)}, i = 1, 2. \tag{7}$$

Hence, from (5), (6), and (7), we have

$$\tau_1 = F(\tau_2) = \frac{2(1 - 2\tau_2)}{(1 - 2\tau_2)(W + 1) + \tau_2 W(1 - (2\tau_2)^m)}, \tag{8}$$

and

$$\tau_2 = G(\tau_1, q) = \frac{2(1 - 2\tau_1')}{(1 - 2\tau_1')(W + 1) + \tau_1' W(1 - (2\tau_1')^m)}, \tag{9}$$

where $\tau_1' = (1 - q)\tau_1 + q$. Similarly as in the homogeneous case in [11], (8) and (9) constitutes a nonlinear system of equations for τ_1 and τ_2. It should be noted in (9) that the access probability of the well-behaved user, τ_2, is determined by the exponential backoff procedure in (4) as if the cheater accesses the channel with $\tau_1' = (1 - q)\tau_1 + q$. We have the following relation for F in (8):

Lemma 1. *$F(\tau_2)$ in (8) is a decreasing function of τ_2.*

Proof. From (8), we can easily show that $dF(\tau_2)/d\tau_2 < 0$. □

In addition, we have the following result for G in (9):

Lemma 2. *For a given value of τ_1, $G(\tau_1, q)$ is a decreasing function of q.*

Proof. It is straightforward from (9) that $\partial G(\tau_1, q)/\partial q < 0$. □

From Lemma 1 and Lemma 2, the solution to the systems of equations in (8) and (9) has the following property:

Theorem 1. *Let* (τ_1^*, τ_2^*) *denote the solution to the system of* (8) *and* (9)*. Then,* (τ_1^*, τ_2^*) *is unique. Furthermore,* τ_1^* *increases with* q *while* τ_2^* *decreases with* q*.*

Proof. From (8), $F(0) = 2/(W+1)$ and $F(1) = 2/(2^m W + 1)$. Similarly, from (9), we have $G(0,q) = 2(1-2q)/\left[(1-2q)(W+1) + qW(1-(2q)^m)\right] = F(q)$ and $G(1,q) = 2/(2^m W + 1) = F(1)$. Since $0 \le q \le 1$ and F is a decreasing function from Lemma 1, we have $F(q) \ge F(1)$. Hence, it can be concluded that (τ_1^*, τ_2^*) is unique. Furthermore, since G is a decreasing function of q from Lemma 2, τ_1^* is an increasing function of q while τ_2^* is a decreasing function of q. □

From Theorem 1, we have the following corollary:

Corollary 1. *The virtual access probability of the cheater, denoted by* $\tau_1' = (1-q)\tau_1 + q$*, is an increasing function of* q*.*

Proof. By differentiating τ_1' with respect to q, we have

$$\frac{\partial \tau_1'}{\partial q} = (1-\tau_1) + (1-q)\frac{\partial \tau_1}{\partial q}.$$

Since $0 \le q, \tau_1 \le 1$ and $\partial\tau_1/\partial q > 0$ from Theorem 1, we have $\partial\tau_1'/\partial q > 0$. □

Remark 1. *Our analysis shows that the effect of carrier sense misbehavior is to virtually increase the channel access probability of the cheater seen by the normal user from* τ_1 *to* $\tau_1' = (1-q)\tau_1 + q$*. From Corollary 1, the virtual channel access probability of the cheater increases as the cheating rate* q *increases. It should be noted that* τ_1 *is still determined according to the ordinary exponential backoff mechanism as given in* (8)*.*

4.3 Saturation Throughput of Heterogeneous IEEE 802.11 WLAN with Carrier Sense Misbehavior

Let v_i, $i = 1, 2$ denote the virtual slot time, which is the average time for each event of User i. Then, we have

$$\begin{aligned} v_1 = v_2 =& (1-q)\left[(1-\tau_1)(1-\tau_2)\sigma + \left\{\tau_1(1-\tau_2) + \tau_2(1-\tau_1)\right\} T_s + \tau_1\tau_2 T_c\right] \\ &+ q\left\{(1-\tau_2)T_s + \tau_2 T_c\right\} \\ =& (1-\tau_1')(1-\tau_2)\sigma + \left\{\tau_1'(1-\tau_2) + \tau_2(1-\tau_1')\right\} T_s + \tau_1'\tau_2 T_c, \end{aligned} \tag{10}$$

where σ, T_s, and T_c denote the slot time, the time for successful transmission, and that for collision, respectively.

Let S_i, $i = 1, 2$ denote the saturation throughput of User i. Then, from (5), we have

$$S_1 = \frac{\left((1-q)\tau_1 + q\right)(1-p_1)}{v_1} = \frac{\tau_1'(1-\tau_2)}{v_1},$$

where $\tau_1' = (1-q)\tau_1 + q$ and v_1 is given in (10). We have the following relation between S_1 and q:

Theorem 2. *The saturation throughput of the cheater is an increasing function of the cheating rate q.*

Proof. By applying the chain rule,

$$\begin{aligned}\frac{\partial S_1}{\partial q} =& \frac{\partial S_1}{\partial \tau_1'}\frac{\partial \tau_1'}{\partial q} + \frac{\partial S_1}{\partial \tau_2}\frac{\partial \tau_2}{\partial q} + \frac{\partial S_1}{\partial v_1}\frac{\partial v_1}{\partial q} \\ =& \frac{(1-\tau_2)}{v_1}\frac{\partial \tau_1'}{\partial q} - \frac{\tau_1'}{v_1}\frac{\partial \tau_2}{\partial q} - \frac{\tau_1'(1-\tau_2)}{v_1^2}\frac{\partial v_1}{\partial q}. \end{aligned} \tag{11}$$

In the meantime, from (10),

$$\frac{\partial v_1}{\partial q} = \frac{\partial v_1}{\partial \tau_1'}\frac{\partial \tau_1'}{\partial q} + \frac{\partial v_1}{\partial \tau_2}\frac{\partial \tau_2}{\partial q}. \tag{12}$$

By plugging (12) into (11), we have

$$\frac{\partial S_1}{\partial q} = \frac{(1-\tau_2)}{v_1}\left[1 - \frac{\tau_1'}{v_1}\frac{\partial v_1}{\partial \tau_1'}\right]\frac{\partial \tau_1'}{\partial q} - \frac{\tau_1'}{v_1}\left[1 + \frac{(1-\tau_2)}{v_1}\frac{\partial v_1}{\partial \tau_2}\right]\frac{\partial \tau_2}{\partial q}. \tag{13}$$

Let $v_1 = A(\tau_2)\tau_1' + B(\tau_2)$. Then, from (10), we have

$$A(\tau_2) = \frac{\partial v_1}{\partial \tau_1'} = (1-\tau_2)(T_s - \sigma) + \tau_1'(T_s - T_c) > 0. \tag{14}$$

Furthermore, $B(\tau_2) = v_1|_{\tau_1'=0} = (1-\tau_2)T_s + \tau_2 T_c > 0$. Hence, we have

$$\frac{\tau_1'}{v_1}\frac{\partial v_1}{\partial \tau_1'} = \frac{A(\tau_2)\tau_1'}{A(\tau_2)\tau_1' + B(\tau_2)} < 1. \tag{15}$$

In a similar manner, let $v_1 = C(\tau_1')\tau_2 + D(\tau_1')$. Then, for positive $C(\tau_1')$, by (15), Theorem 1, and Corollary 1, the right-hand side of (13) becomes positive. When $C(\tau_1') < 0$, we have

$$\left|\frac{(1-\tau_2)}{v_1}\frac{\partial v_1}{\partial \tau_2}\right| = \left|\frac{C(\tau_1')(1-\tau_2)}{C(\tau_1')\tau_2 + D(\tau_1')}\right| \le \left|\frac{C(\tau_1')}{D(\tau_1')}\right| < 1,$$

because $D(\tau_1') > |C(\tau_1')|$. Consequently, we have $\partial S_1/\partial q > 0$ for all cases. □

In a similar manner, from (6), we have

$$S_2 = \frac{\tau_2(1-\tau_1')}{v_2}.$$

Then, we have the following result for the relation between S_2 and q.

Theorem 3. *The saturation throughput of the well-behaved user, S_2, is a decreasing function of the cheating rate q.*

Proof. By symmetry, from (13),

$$\frac{\partial S_2}{\partial q} = \frac{(1-\tau_1')}{v_2}\left[1 - \frac{\tau_2}{v_2}\frac{\partial v_2}{\partial \tau_2}\right]\frac{\partial \tau_2}{\partial q} - \frac{\tau_2}{v_2}\left[1 + \frac{(1-\tau_1')}{v_2}\frac{\partial v_2}{\partial \tau_1'}\right]\frac{\partial \tau_1'}{\partial q}. \quad (16)$$

Let $v_2 = A'(\tau_1')\tau_2 + B'(\tau_1')$. When $A'(\tau_1')$ is positive, we have

$$\frac{\tau_2}{v_2}\frac{\partial v_2}{\partial \tau_2} = \frac{A'(\tau_1')\tau_2}{A'(\tau_1')\tau_2 + B'(\tau_1')} < 1.$$

Hence, in all cases, the right-hand side of (16) is negative by virtue of Theorem 1 and Corollary 1. □

5 Simulation Study

In this section, we perform a simulation study to verify our analysis. We use ns-2.34 with the MAC model in [12]. For saturation condition, we generate downlink UDP traffic of 6 Mb/s from the AP to each user. The default parameters used in our simulation is given in Table 1. For each given value of q, simulation run of 100 seconds has been performed for 20 times. Each point in figures is shown with a confidence level of 95%.

Table 1. Default parameters used in ns-2 simulations

802.11a modulation	BPSK (6Mbps)	Data rate	6 Mb/s
CW_{min}	15	CW_{max}	1023
RTS/CTS	Disabled	Thermal noise	-96 dBm
SINR threshould	10 dB	Rx threshould	-82 dBm

First, we consider the case when both of the users adopt the exponential backoff mechanism in Fig. 1. When the cheating rate q is zero, both users show the same throughput performance. However, as q increases, the throughput of the cheater increases while that of the normal user decreases, which agrees with our analysis. As q reaches one, the cheater takes most of the bandwidth share, and the throughput of the well-behaved user becomes almost zero.

Now, we take look into the case when both of the users use a fixed value of 15 for the contention window size in Fig. 2. Similarly as in Fig. 1, both users evenly share the bandwidth when q is zero. In addition, as q increases, the throughput of the cheater increases while that of the well-behaved user decreases in a similar manner. However, if we compare Fig. 2 with Fig. 1 carefully, it can be noticed that the rate of change in the throughput is smaller in Fig. 2. This difference results from the fact that the well-behaved user does not back off as q increases, but accesses the channel with a fixed contention window sizes (CW) of 15.

In Fig. 3, we consider the case when the cheater uses a fixed CW of 15 while the well-behaved user adopts the ordinary exponential backoff mechanism. As one can easily expect, the cheater accesses the channel in the most aggressive manner in this case

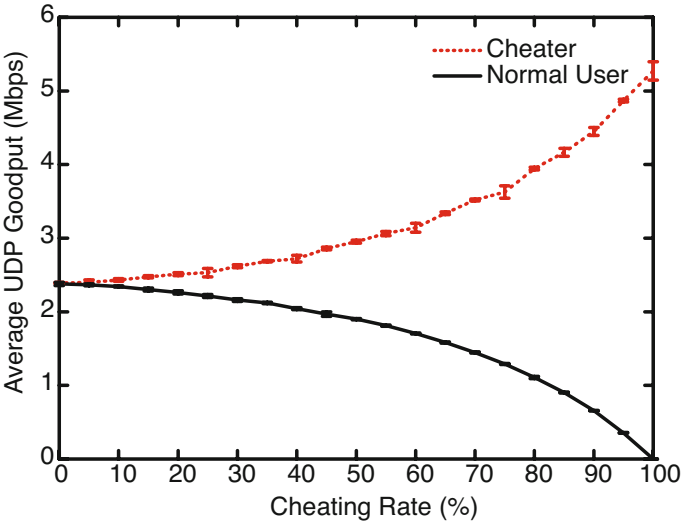

Fig. 1. Throughput performance vs. cheating rate when both users adopt the exponential backoff mechanism

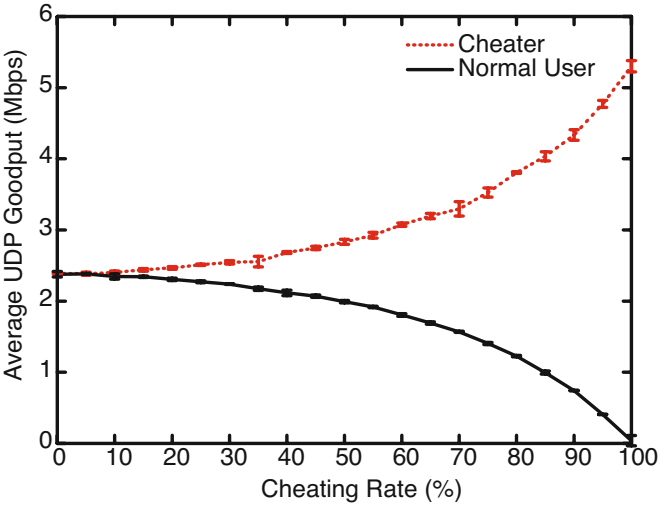

Fig. 2. Throughput performance vs. cheating rate when both users use a fixed CW of 15

among all three ones. Even when q is zero, there is a difference between the throughput of the cheater and that of the normal user. Since the cheater uses a fixed CW of 15, which is the minimum possible value for the normal user, the cheater can take more bandwidth than the well-behaved one in this case. As q increases, similarly as in the aforementioned cases, the cheater has more bandwidth share while the normal user loses its share.

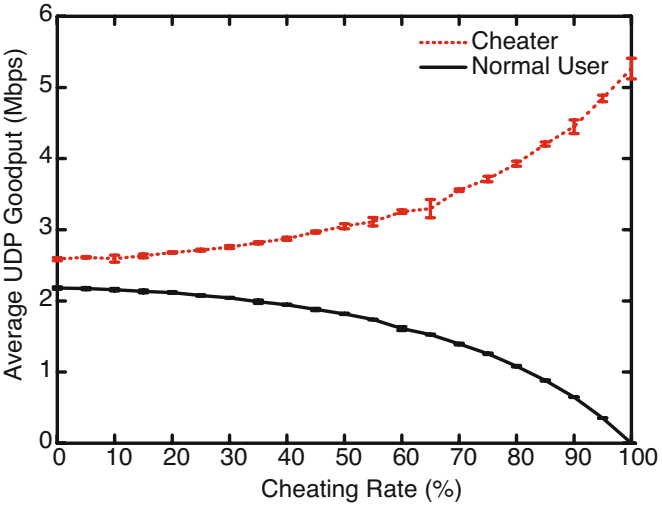

Fig. 3. Throughput performance vs. cheating rate when the cheater uses a fixed CW of 15 while the normal user adopts the exponential backoff mechanism

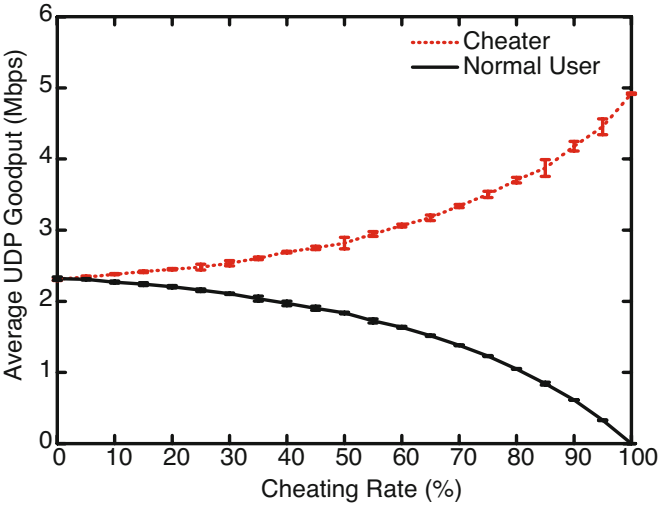

Fig. 4. Throughput performance vs. cheating rate when both users adopt the exponential backoff with RTS/CTS enabled

Finally, in Fig. 4, we consider the case when both users adopt the exponential backoff mechanism with Request to Send (RTS)/Clear to Send (CTS) enabled. Even though we have not considered RTS/CTS in our analysis, Fig. 4 shows that the trends are quite similar with those in the previous figures. Consequently, we can conclude that our

analysis is valid with the RTS/CTS procedure. A more detailed analysis of the network performance with the RTS/CTS mechanism will be an issue of future research.

6 Conclusion and Future Work

We have shown that a cheater can significantly increase its throughput by ignoring the carrier sense mechanism in IEEE 802.11 WLAN while a normal user will lose its throughput. In fact, our analysis shows that the carrier sense misbehavior corresponds to the case of virtually increasing the channel access probability of a cheater. Consequently, not only a malicious user, but also a selfish one are motivated to disregard the carrier sense procedure, which will result in significant degradation in throughput performance of well-behaved users. One important issue in future research is how to efficiently detect and penalize the carrier sense misbehavior of a selfish user to protect well-behaved ones from significant performance degradation.

References

1. Kyasanur, P., Vaidya, N.H.: Selfish MAC layer misbehavior in wireless networks. IEEE Transactions on Mobile Computing 4(5), 502–516 (2005)
2. Čagalj, M., Ganeriwal, S., Aad, I., Hubaux, J.P.: On selfish behavior in CSMA/CA networks. In: Proc. the 24th IEEE Conference on Computer Communications (INFOCOM 2005), Miami, FL, March 2005, pp. 2513–2524 (2005)
3. Konorski, J.: A game-theoretic study of CSMA/CA under a backoff attack. IEEE/ACM Transactions on Networking 14(6), 1167–1178 (2006)
4. Toledo, A., Wang, X.: Robust detection of selfish misbehavior in wireless networks. IEEE Journal on Selected Areas in Communications 25(6), 1124–1134 (2007)
5. Buttyán, L., Hubaux, J.P.: Security and Cooperation in Wireless Networks. Cambridge University Press, Cambridge (2007)
6. Pelechrinis, K., Yan, G., Eidenbenz, S., Krishnamurthy, S.: Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks. In: Proc. the 28th IEEE Conference on Computer Communications (INFOCOM 2009), Rio de Janiero, Brazil (April 2009)
7. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4. In: Vaudenay, S., Youssef, A.M. (eds.) SAC 2001. LNCS, vol. 2259, pp. 1–24. Springer, Heidelberg (2001)
8. Stubblefield, A., Ioannidis, J., Rubin, A.D.: A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Transactions on Information and System Security 7(2), 319–332 (2004)
9. Bittau, A., Handley, M., Lackey, J.: The final nail in WEP's coffin. In: Proc. the 27th IEEE Symposium on Security and Privacy, Oakland, CA, May 2006, pp. 386–400 (2006)
10. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proc. the 12th USENIX Security Symposium, Washington, DC, August 2003, pp. 15–27 (2003)
11. Bianchi, G.: Performance analysis of the IEEE 802.11 distributed coordination function. IEEE Journal on Selected Areas in Communications 18(3), 535–547 (2000)
12. Chen, Q., Schmidt-Eisenlohr, F., Jiang, D., Torrent-Moreno, M., Delgrossi, L., Hartenstein, H.: Overhaul of ieee 802.11 modeling and simulation in ns-2. In: Proc. the 10th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems (MSWiM 2007), Chania, Crete Island, Greece, October 2007, pp. 159–168 (2007)