Selfish Behaviours and Counteractions in CSMA/CA Wireless Protocol

31960073

Abstract

Carrier sensing multiple access with collision avoidance (CSMA/CA) protocol is a medium access control (MAC) protocol used by IEEE 802.11 stations to arbitrate the access of the shared wireless medium. With the increasing programmability of network adapter, malicious users can modify the wireless interface easily in order to gain some unfair shares of bandwidth. In particular, we consider the selfish behaviour of reducing the contention window size in order to get a higher throughput. Three counteractions proposed in [4], [5], [6] were studied and compared. The validity of their problem formulations and solution approaches were commented.

I. Introduction

In wireless ad hoc networks, the medium access control (MAC) protocols are important in orchestrating the access of the shared wireless medium. They are designed for a fully cooperative setting that each node exactly follows the operations of the protocol. However, with the increasing programmability of network adapter, users can modify the wireless interface easily. Selfish users can gain a larger share of the network resources at the expense of the reduction in bandwidth of the other users. Also, malicious users can disrupt the normal operations of the networks.

Game theory has shown to be a useful tool in analyzing the interaction of independent nodes in a wireless ad hoc network. It has been used to study wireless communication scenarios in different layers on the network protocol stack, including physical, medium access control, networking, transport and application layers [2], [3]. Normally, players in a game are the nodes in the network. The strategies of the players are the actions related to the functionalities being studied. The utility functions are often related to the performance metrics (e.g., bandwidth, delay) of the system [2].

In this paper, we focus on a particular selfish behaviour in CSMA/CA protocol that some users reduce the contention window size parameters in order to enjoy a larger bandwidth share. We then study the problem formulations and counteractions proposed in [4], [5], [6]. We will comment on these works based on the validity of the assumptions, problem formulations, and the appropriateness of the solution approaches.

Then, we will discuss the possibility of extending these previous works to IEEE 802.11e wireless network. In this new standard, some IEEE 802.11e nodes may enjoy higher priority services through the choice of some more favourable transmission parameters. Though they are “legitimate” to do so, these actions closely resembles the selfish behaviours in CSMA/CA protocol.

The rest of the paper is organized as follows: Section II describes the basic operations of CSMA/CA. Section III describes the possible selfish behaviours in CSMA/CA protocol. Then we survey on the literature about the selfish behaviour of having smaller contention window size. The basic game theoretic formulation of the CSMA/CA game is presented in Section IV, and the three counteractions shown in the literature are discussed from Sections V to VII. The comments of the three counteractions are given in Section VIII. A discussion on the similarities between IEEE 802.11e nodes and selfish nodes are explained in Section IX. Section X concludes the paper.

II. Operations of CSMA/CA

The general operation of the CSMA/CA is as follows: In CSMA/CA, a node always monitors the wireless medium to determine if it is idle or busy. If the medium is busy, it will not transmit as it will

TABLE I

BASIC OPERATION OF THE COUNTER IN THE CSMA/CA PROTOCOL

Counter Operations	**Descriptions**
Count value cnt	$cnt \in [0, CW)$, where $CW \in [CW_{min}, CW_{max}]$.
Start	Counting starts after waiting for a DIFS, at the end of the defer access as shown in Fig. 1.
Countdown	cnt is reduced by one after every time slot as shown in the "contention window" in Fig. 1.
Stop	When $cnt = 0$, the packet will be transmitted immediately at that time slot.

cause a collision. As shown in Figure 1, once the channel is idle, a node first waits for a distributed coordination function inferframe space (DIFS) period. Then the contention backoff algorithm is triggered and the counter would obtain a count value of cnt by taking a random integer from [0, CW). The count value is decremented by one after the transpiration of every idle contention slot. When the medium is sensed to be busy again, the countdown is frozen. It will be resumed after another DIFS. Then, the counting proceeds as above and eventually stops when $cnt = 0$. The packet will then be sent.

It should be noted that the size of the contention window CW would change throughout the operation of the protocol, which $CW \in [CW_{min}, CW_{max}]$. Initially, $CW = CW_{min}$. If the nodes receives an acknowledgement (ACK), CW will be set to CW_{min}. If a node cannot receive an ACK for the transmitted packet, indicating the transmission is unsuccessful, CW will be doubled for every iteration. It will keep doubling until it reaches CW_{max}. At this point, the transmission will abort when consecutive collisions beyond a retry limit is reached.

The purpose of the interframe space (IFS) (e.g. SIFS, PIFS and DIFS shown in Fig. 1) is to assign priorities for different types of network operations (e.g., control information, packet acknowledgement). The purpose for different nodes in waiting for different random amount of time instead of transmitting immediately is to prevent simultaneous transmissions by all the nodes after waiting for DIFS.

The basic operations of the counter in CSMA/CA protocol that are relevant to this work are summarized in table I.

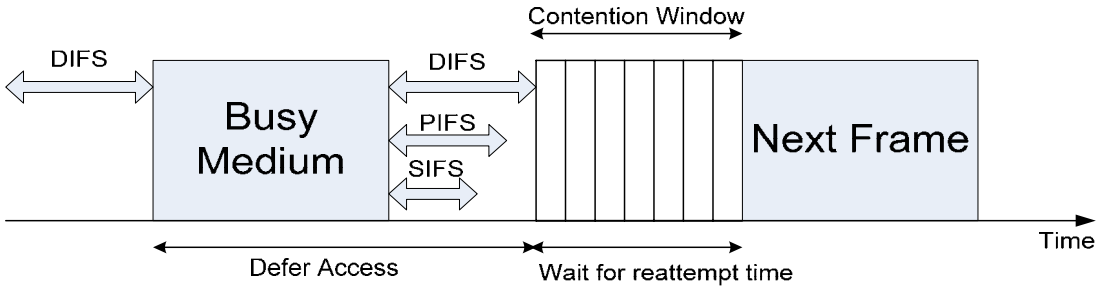

Fig. 1. Basic CSMA/CA operation.

III. SELFISH BEHAVIOURS

Based on the descriptions of the operations of backoff algorithm of the CSMA/CA described above, we see that there are some possible ways that a selfish user can manipulate the algorithm in order to gain an unfair share of bandwidth. Some of possible selfish behaviours are:

1) Smaller contention window sizes: By having smaller CW_{min} and CW_{max}, a higher probability in transmission would be resulted.
2) Slower increase in CW after collision: The value of CW is not doubled after every unacknowledged transmission. The range of possible value of cnt remains small and thus results in a higher probability in transmission.

3) Smaller interframe space (IFS): The counter starts counting earlier than the others and thus increases the probability in capturing the channel.
4) Faster counting: When the counting is resumed after DIFS, cnt does not take the unfinished value before the freezing of the counter. Instead, it takes this value decremented by one. Since the counter is resumed earlier, there is a higher chance in accessing the wireless medium.

In particular, selfish behaviour 1 has been studied in [4], [5], [6], and selfish behaviour 2 has been studied in [7]. In this work, we will only focus on selfish behaviour 1 in the following discussion.

IV. Game theoretic formulation of selfish behaviour 1

The operation of CSMA/CA can be formulated using game theory as normal-form game or repeated game. The normal-form game provides insights on the basic interactions among players, and the repeated game is a more realistic and accurate formulation of the operations of backoff algorithm in CSMA/CA protocol.

A. Normal-form CSMA/CA game

Firstly, we will discuss the normal-form CSMA/CA game which can be formulated game theoretically as follows:

1) Game: A finite n-person game (N, A, u).
2) Players: N is a finite set of n players indexed by i. They are all IEEE 802.11 stations.
3) Actions: $A = A_1 \times A_2 \times \dots A_n$ is a tuple of action sets for each player i, where $A_i = (CW_{min,i}, CW_{max,i})$ is the choice of contention window size parameters by player i.
4) Utility: $u = (u_1, u_2, \dots, u_n)$, where u_i is the bandwidth share (or throughput) obtained by player i.

In particular, we want to define some actions that we will discuss further.

Definition 1. *An action A_i is said to be **honest** if it follows the configuration prescribed by the IEEE 802.11 standard that $A_i = w_h$. A_i is said to be **selfish** if $A_i = (2, 2) = w_s$. A_i is said to be **greedy** if $A_i = (1, 1) = w_g$.*

The configuration of w_g implies that the count value cnt is always equal to zero, because cnt is an integer and $cnt \in [0, 1)$ all the time.

The work in [4] was the first work to formulate the operation of CSMA/CA using game theory. It has shown that:

Proposition 1. *For any strategy profile A that constitutes a Nash equilibrium (NE) [1], there exists i s.t. $A_i = (1, 1) = w_g$.*

Moreover, it has also shown that:

Proposition 2. *If there is only one greedy node i in the network, then node i has utility $u_i > 0$ and other nodes j get utilities $u_j = 0$ for $j \neq i$.*

Proposition 3. *If there is more than one greedy node, all the nodes get zero utilities (i.e. $u_j = 0$ for all j).*

The intuition behind the above two propositions is that when there is only one greedy player, he will get the entire bandwidth share while the others get zero bandwidth. However, if there is more than one greedy player, then packet transmissions collide all the time. As a result, no players can gain any positive throughput.

Following the work of [4], [5] has shown that:

Proposition 4. *Any strategy profile A with at least one station playing w_g is a non-strict NE.*

Proposition 5. *If w_g is not allowed to use, then w_s is a strictly dominant strategy for all the players. As a result, the strategy profile of $(w_s, w_s, \ldots, w_s)$ is a unique and strict NE.*

Proposition 6. *The unique NE strategy profile of $(w_s, w_s, \ldots, w_s)$ is Pareto dominated by $(w_h, w_h, \ldots, w_h)$, which is the only fair and Pareto optimal [1] strategy profile.*

In the above proposition, a strategy profile is fair if all the players obtain the same utility.

From the above two propositions, we see that the game has run into a multiplayer Prisoners' dilemma: If w_g is not allowed, the players will choose w_s due to their self-interest, which constitutes a strict NE. However, it is better for all the players to choose w_h instead to enjoy some higher utilities.

B. Repeated CSMA/CA game

We saw that normal-form CSMA/CA game run into a multiplayer Prisoner' dilemma that the NE achieved is neither fair nor Pareto-efficient. However, from the result in game theory, repeated game can offer a more realistic formulation and a more satisfying solution. In the following sections, we will discuss three counteractions to the selfish behaviour of smaller contention window sizes, based on the formulations of the infinitely repeated CSMA/CA. In this game, there is a finite set of n players indexed by i that are all IEEE 802.11 stations. However, the information obtained by players, the actions or strategies available to players and utilities are different in the three counteractions.

We will study the three counteractions to the selfish behaviour of smaller contention window sizes. For each counteraction, we will study their infinitely repeated game setting, detection of deviation techniques, punishment techniques and their overall algorithms.

V. COUNTERACTION 1 [4]

The work in [4] was the first to systematically study the selfish behaviours in CSMA/CA protocol. The main idea of the counteraction in this work is to identify and punish the deviating player individually.

A. Repeated CSMA/CA game

The infinitely repeated game was formulated as follows:

1) Information: The bandwidth of every player obtained in the previous stage games.
2) Actions: Player i can adjust the size of the contention window.
3) Utility: For each stage game, the utility for player i is $j_i = u_i - p_i$, where u_i is the bandwidth obtained by player i. p_i is the punishment imposed on player i. It is defined as $p_i = k_i(\tau_i - \tau_0)$, where $k_i \geq 0$ and $\tau_0 \in (0, 1)$ are the system parameters. τ_i is the access probability to the channel by player i. Average reward [1] is used to calculate the overall payoff in the whole game.

B. Deviation detection

In [4], it was assumed that all the players can measure the bandwidth obtained by other players in every stage game, due to the broadcast nature of wireless communications. If a player is measured with a bandwidth obtained different from the other players, this player is identified as deviating.

C. Punishment

In this work, a simple punishment scheme was proposed which will only bring a bandwidth reduction for the players who are punished, but not to the punishers. Basically, the idea is to use selective jamming that penalizes the non-cooperative players by jamming their packets for a short amount of time. When the non-cooperative players are transmitting, players who have listened to these transmissions will switch to transmission modes and jam the packets.

D. Distributed coordination protocol

The access probability τ_i for each player under different conditions in order to optimize his utility in each stage game is shown in the lemma 1 in [4]. Moreover, by the choice of certain system parameters k_i, choosing $\tau_i = \tau_0$ for all players can be made the unique NE.

Under the infinitely repeated game setting, with the use of the above detection and punishment techniques, a distributed coordination protocol was proposed which guides the players from a NE to a Pareto-optimal NE.

VI. Counteraction 2 [5]

Following the work in [4], [5] make some more reasonable assumptions on the deviation detection technique. To counteract the selfish behaviour, a strategy called CRISP (Cooperation via Randomized Inclination to Selfish/Greedy Play) was proposed. The main idea of CRISP strategy is to use a limited punishment technique that leads the equilibrium to a subgame perfect NE (SPNE).

A. Repeated CSMA/CA game

In the work of [5], the repeated CSMA/CA game was formulated as follows:

1) Information: "Coarse profile observability" (please refer to the next section).
2) Strategies: Player i can chooses a strategy s_i^k in the kth stage game, where s_i^k can be any mixed strategy in the set $\{w_h, w_s, w_g\}$.
3) Utility: $u = (u_1, u_2, \ldots, u_n)$, which u_i is the bandwidth of station i obtained using average reward [1].

B. Deviation detection

We need to detect whether there is any deviation from the cooperating strategy in order to punish the players. Based on some experiments in [5], the idea of "coarse profile observability" was proposed. It stated that the number of selfish or greedy players in the network can be inferred with certain granularity even though the exact strategies of other player cannot be guessed.

Let N, x and y be the total number of stations, selfish stations and greedy stations in the network respectively. Let $S(N, x)$ be the total successful transmission probability in the network when there are N stations in the network, which x of them are selfish users. Moreover, x^* is defined as a threshold such that the relative difference between $S(N, x)$ and $S(N', x+1)$ is "significant" for all N, N' and $x \leq x^*$. The result of coarse profile observability is as follows:

- Each station can distinguish among the cases of $y = 0$, $y = 1$ and $y > 1$.
- If $y = 0$ and $A_i = w_s$, agent i can distinguish the case between $x \leq x^*$ and $x > x^*$.
- If $y = 0$ and $A_i = w_h$, agent i can distinguish the case between $x = 0$ and $x > 0$.

C. Punishment

The idea is similar to enforcing cooperating strategy in the Prisoner's dilemma: Every player will start off playing using the non-punishing mode, which the player will play the honest strategy w_h. Punishing mode starts when any deviations from the honest strategy is detected: If it is detected that some players play w_s, CRISP strategy will toggle between w_h and w_s. Furthermore, if greedy play w_g is detected, CRISP strategy will toggle between w_s and w_g.

In this way, it is better for the invader to use the CRISP and cooperate in order to get a higher payoff, because a SPNE is achieved when all the players play CRISP.

TABLE II

CRISP STRATEGY

CRISP States	Descriptions	CRISP Strategy
H	No selfish player and x does not increase	Play pure strategy w_h
S/H	$x > 0$ but x remains the same	Play mixed strategy $[w_h : p_1; w_s : 1 - p_1]$, where $p_1 \geq 0$
S/H & Phase-up	$x > 0$ and it is increasing	Play mixed strategy $[w_h : p_2; w_s : 1 - p_2]$, where $p_2 \geq 0$
G/S	$y > 0$ and x remains the same	Play mixed strategy $[w_s : p_1; w_g : 1 - p_1]$, where $p_1 \geq 0$
G/S & Phase-up	$y > 0$ and x is increasing	Play mixed strategy $[w_s : p_2; w_g : 1 - p_2]$, where $p_2 \geq 0$

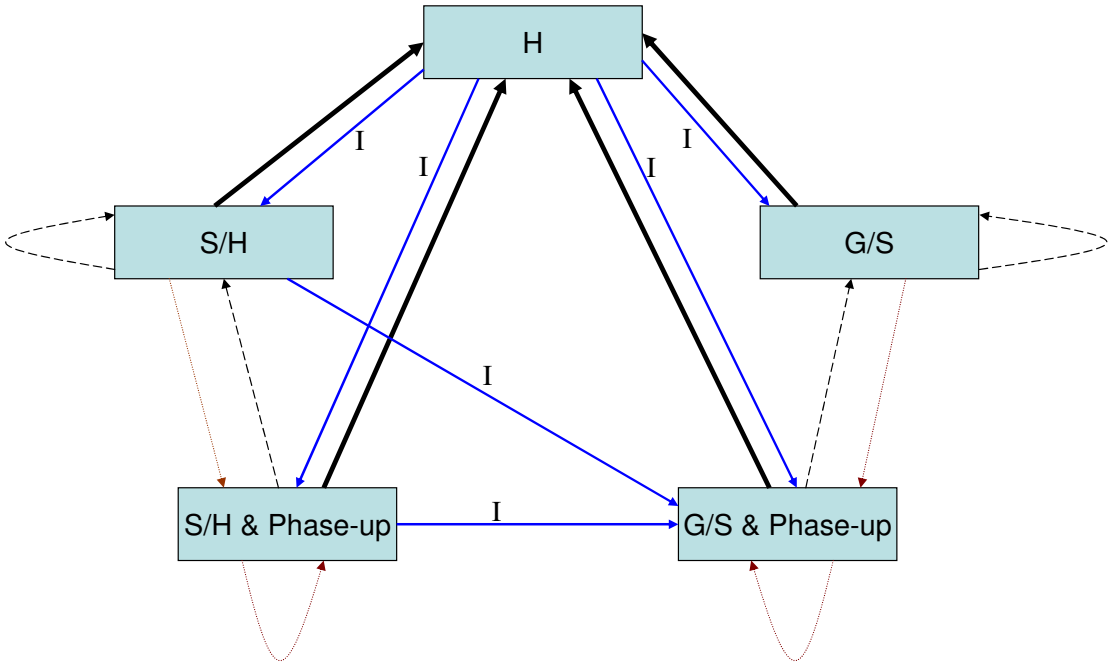

Fig. 2. CRISP state transition: the dark solid lines, dashed lines and dotted lines represent the state transitions when there is a decrease, no change and an increase in the number of selfish players in the system respectively. The solid lines marked with "I" represent the state transitions when deviating players not following CRISP are detected.

D. CRISP Strategy

As before, let x and y be the number of detected selfish and greedy players in the system respectively. In CRISP strategy, a state machine with five states is used. The CRISP states and strategies are shown in table II, and the state transitions are shown in Figure 2.

Moreover, the following proposition was proved in [5].

Proposition 7. *When all the players use the CRISP strategies, the equilibrium achieved is both fair and Pareto optimal.*

VII. COUNTERACTION 3 [6]

The work in [6] was not mainly intended to deal with the selfish behaviours of the IEEE 802.11 network stations. It optimized the throughput of each station by adjusting the contention window size, based on the Bayesian estimation of the number of competing stations in the network. Additionally, it has shown that there exists a SPNE that prevents the stations from choosing selfish or greedy settings.

A. Repeated CSMA/CA game

In [6], similar infinitely repeated game was considered but with some differences:

1) Information: A rough estimate on whether there is some malicious (i.e. not honest) players present in the network.
2) Actions: Player i can adjust the size of the contention window.
3) Utility: $u = (u_1, u_2, \ldots, u_n)$, which u_i is the bandwidth of station i obtained using discounted reward [1], which is different from that in counteractions 1 and 2.

B. Deviation detection

It was argued that all stations should have an equal share of bandwidth in the wireless channel when they are all honest. However, if some players are misbehaving and play dishonest strategies, the bandwidth share of the honest players will decrease. In this way, the existence of malicious players can be identified.

C. Punishment

Let S_r and S_c be the payoff vector (throughput) of malicious players and honest players that are cheated by malicious players. Also, let S_o be the payoff vector when all the nodes are honest and S_a be the payoff vectors when all the nodes implements the punishing strategy. Let W_k^{opt} be the optimal contention window at the stage game k derived in [6]. The following proposition gives a SPNE of the infinitely repeated CSMA/CA game:

Proposition 8. *If $S_r > S_o > S_a > S_c$, then the following punishment strategy W^* at each stage game k is a SPNE for the infinitely repeated CSMA/CA game:*

1) *Select $W^* = W_k^{opt}$ if all other nodes selects W_k^{opt} (i.e. when there are no malicious nodes detected).*
2) *Otherwise, choose the punishment strategy $W^* = w_g$ (i.e. the greedy strategy) forever.*

VIII. Comments

From the previous sections, we have discussed the selfish behaviours that the contention window size configurations are changed by some nodes so that they can gain some unfair shares of bandwidth. It was first formulated as a normal-form CSMA/CA game that provides a lot of insights to the interactions among the players. Then, three counteractions were studied which all of them used the infinitely repeated CSMA/CA game as their bases. However, the assumptions, detection of deviation techniques, punishment techniques and overall algorithms are different. In this section, we would like to study the soundness of the above settings.

Firstly, we would look at the assumption of infinitely repeated game. Because we are not certain when the game will end, infinitely repeated game is a good formulation to analyze this situation. However, consider the actual wireless network in reality, the network nodes can leave a network anytime by turning off the networking connection. We cannot put punishments on malicious nodes in succeeding stage games because it is difficult to force all the players to stay in a game. So the infinitely repeated game assumption may not be completely valid.

Next, we would like to compare the information obtained by players in the three interactions and their detection of deviation techniques:

1) In counteraction 1, it was assumed that the bandwidth share of individual player was known by all players due to the broadcast nature of wireless communications. However, it is difficult to achieve in great precision, so this assumption is not valid.
2) In counteraction 2, it was assumed that the number of selfish and greedy players can be estimated with certain granularity. It is a more reasonable assumption than the previous one, but the precision needs to be further investigated

3) In counteraction 3, it was assumed that the existence of malicious (i.e. not honest) players can be identified with non-zero probability. This assumption is not as strong as that in counteraction 2, and it can be justified. But the precision of the deviation detection is questionable.

For the punishment of deviating players, the three counteractions use different approaches:

1) In counteraction 1, selective jamming was used which punished the deviating players by selectively jamming their transmissions for a short amount of time. However, as shown in [8], this approach is not effective. Firstly, it takes some time to detect whether a player is misbehaving or not, and deviation detection is no easy task. Moreover, because of a phenomenon called "capture effect" in wireless communications, a subset of packets can be received even though packet collisions or jamming occur. As a result, the effect of punishment to the misbehaving players is limited.
2) In counteraction 2, when some players were found to be misbehaving, other players will switch to punishing mode for some time. Once the number of selfish or greedy players is declining, players will switch from punishing mode back to non-punishing mode. These strategies achieve a SPNE. With this kind of limited punishment, the benefits of players gain by deviation are offset by the punishment. The deviating players are encouraged to play back the CRISP or they will continue to receive a lower payoff. This technique is the most efficient punishment technique among the three counteractions.
3) In counteraction 3, when some players were found to be misbehaving, other players will switch to punishing mode forever. Though these strategies achieve a SPNE, the punishment is unnecessary strong. As the misbehaving players just gain a finite amount of benefit from deviation, it is not necessary to punish them forever. Moreover, the players who punish the misbehaving players also hurt themselves to the same extent.

Finally, it should be noted that counteraction 1 required the adjustment of some system parameters in order to achieve some equilibrium points. However, it is not desirable because it involves a change in the system settings, which is generally not allowed and is too complicated.

IX. Discussion: "Selfish" behaviours in IEEE 802.11e

The relevance of the selfish behaviours becomes higher with the emergence of new IEEE 802.11e standard [10] that allows users take control of the MAC parameters. To support quality of service (QoS) for different classes of traffic IEEE 802.11e, the traffic is classified into four access categories (ACs) and is put into four queues. Differentiation in priorities among the four access categories is achieved through the use of different parameters:

- The use of arbitration interframe space (AIFS), which is a type of IFS with different values for different ACs.
- Different values of CW_{min} and CW_{max}.
- Different transmission opportunity limit: the maximum duration for which a node can transmit after gaining the access to the wireless medium.

A "virtual" contention is performed among the four queues using the predefined parameters. The winner in this "virtual" contention will then compete with other nodes in "actual" contention.

As a result, when IEEE 802.11 and IEEE 802.11e nodes coexist, some IEEE 802.11e nodes may gain advantage over the IEEE 802.11 nodes under some settings as shown below. Though they are legitimate, they closely resemble the selfish behaviours that we have discussed in section III.

- Smaller contention window sizes by having smaller CW_{min} and CW_{max} (Selfish behaviour 1 described in Section III).
- Smaller interframe space (IFS) (Selfish behaviour 3).
- Different backoff counting rules (Selfish behaviour 4).

Based on some previous work on selfish behaviours in CSMA/CA protocol, we plan to investigate the ways that IEEE 802.11 nodes can respond to these "selfish" behaviours of IEEE 802.11e nodes.

X. Conclusions

In this project, we summarize some recent schemes ([4], [5], [6]) that use game theory to study the selfish behaviour of reducing contention window size in CSMA/CA protocol. We comment on the validity of the assumptions and problem formulations, and the effectiveness of the solution approaches. Finally, we discuss the possibility of extending these works to the new standard of IEEE 802.11e, which the network nodes closely resemble the selfish players in CSMA/CA protocol.

References

[1] Y. Shoham and K. Leyton-Brown, Multi Agent Systems: Algorithmic, Game-Theoretic, and Logical Foundations, Cambridge University Press, 2008.

[2] V. Srivastava, J. Neel, A. B. MacKenzie, R. Menon, L. A. DaSilva, J. E. Hicks, J. H. Reed, and R. P. Gilles, "Using game theory to analyze wireless ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 46 – 56, 2005.

[3] M. Felegyhazi and J. - P. Hubaux, "Game theory in wireless networks: a tutorial", *EPFL Infoscience*, 2006.

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

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

[6] A. L. Toledo, T. Vercauteren, and X. Wang, "Adaptive optimization of IEEE 802.11 DCF based on Bayesian estimation of the number of competing terminals," *IEEE Transactions on Mobile Computing*, vol. 5, no. 9, pp. 1283 – 1296, Sep. 2006.

[7] Y. Jin and G. Kesidis, "Distributed contention window control for selfish users in IEEE 802.11 wireless LANs," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 6, pp. 1113 – 1123, Aug. 2007.

[8] O. Queseth, "The effect of selfish behavior in mobile networks using CSMA/CA," *IEEE VTC Spring*, 2005, pp. 2157 – 2161.

[9] A. Leon-Garcia and I. Widjaja, *Communication Networks: fundamental concepts and key architectures*, 2nd edition, New York, NY, Mc-Graw Hill, 2004.

[10] IEEE 802.11 WG, IEEE Std 802.11, "International Standard for Information Technology. Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks. Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," 2005. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11e-2005.pdf