

Handling Misbehavior in WLAN Systems

Navanit V. Arakeri
Department of Electrical Engineering
Stanford University
arakeri@stanford.edu

Abstract

The Wireless Medium Access Control (MAC) protocol in IEEE 802.11 uses a distributed contention resolution mechanisms for sharing the wireless channel. In this environment, self-optimized hosts that fail to adhere to the MAC protocol may obtain an unfair share of the channel bandwidth. The Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) scheme requires nodes competing for access to the channel to wait for a “backoff” interval randomly selected from a specified range, before initiating a transmission. Self-optimized nodes may wait for lower backoff intervals than well-behaved nodes, thereby obtaining an unfair advantage. An auction-based scheme is introduced that ensured that the Carrier Sense Multiple Access, Collision Avoidance (CSMA/CA) scheme specified in the IEEE 802.11 standard is the dominant strategy, while maintaining incentive compatibility and minimizing social cost.

Index terms

CSMA/CA, IEEE 802.11, self-optimized agents, auction, game theory, VCG mechanism

1. Introduction

The Wireless Medium Access Control (MAC) protocol in IEEE 802.11 [1] uses a distributed contention resolution mechanism for sharing the wireless channel. The contention resolution is based on cooperative mechanisms (random backoff before transmission) that ensure a reasonably fair share of the channel for all the participating nodes. In this environment, some *self-optimized*

hosts in the network may misbehave by failing to adhere to the network protocol, with the intent of obtaining an unfair share of the channel. The presence of *self-optimized nodes* that deviate from the contention resolution protocol can reduce the throughput share received by conforming nodes. Thus, development of mechanisms for preventing and handling misbehavior is essential.

Self-optimized nodes for the purpose of this paper are defined as rational agents that can conform to regular Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), but chose not to in order to gain an unfair advantage over conforming nodes. These agents are distinct from malfunctioning nodes with faulty implementations that do not have a choice in conforming to the protocol. Network performance in wireless networks with malfunctioning nodes is typically studied in the domain of coexistence rather than misbehavior. Malicious behavior such as RF-jamming and other methods are also not addressed here.

The IEEE 802.11 mechanism for resolving contention between nodes is based on CSMA/CA, which specifies that, each node with data to transmit over the channel selects a random backoff value from range $[0, CW]$ where CW is the Contention Window maintained by each node. While the channel is idle (i.e. the physical layer sensing mechanism does

not detect channel activity) the backoff value is decremented at each time slot. The user can access the channel when the backoff counter reaches zero. After the backoff counter is decremented to zero, the sender may reserve the channel for the duration of the data transfer by exchanging control packets on the channel (this is not necessary however). The sender first sends a RTS (Request to Send) packet to the receiver node. The receiver responds with a CTS (Clear to Send) packet and this exchange reserves the channel for the duration of data transmission, including all subsequent fragments (RTS-CTS exchange is optional). Other nodes that overhear either the RTS or the CTS (or both) are required to defer transmissions on the channel for the duration specified in RTS/CTS. The RTS/CTS mechanism also solves the hidden node problem in wireless networks. After a successful RTS/CTS exchange, the sender transmits a DATA packet. The receiver responds with an ACK packet to acknowledge a successful reception of the DATA packet.

The CW variable is modified as follows:

- Every successful transmission results in the CW being reset to a minimum value CW_{\min}
- An unsuccessful transmission or collision results in the CW being doubled subject to a maximum of CW_{\max}

Both CW_{\min} and CW_{\max} are initialized during network setup.

A self-optimized node may receive more than its fair share of bandwidth by selecting a backoff value from a different distribution with smaller average backoff value by failing to modify its CW size.

Such an agent may also pick a constant (possibly zero) backoff value irrespective of the status of the last transmission.

From the point of view of any self-optimized user, the *intention* of such a user is to minimize the probability of collision and force other users to pick higher backoff values in order to gain more bandwidth itself. Since the self-optimized users are considered rational, any behavior that does not accomplish the above and does not offer any other incidental advantage will not be a best response in the presence of strategies that offer even a marginally higher throughput to the self-optimized user.

The rest of the paper is organized as follows. A brief overview of the proposed scheme is outlined in Section 2 with details presented in Section 3. An evaluation of the scheme along with a discussion on efficiency is presented in Section 4, and the conclusion is presented in Section 5.

2. Terminology and Preliminaries

The proposed scheme deals with IEEE 802.11 networks in *infrastructure mode* with the presence of a single Access Point (AP) per service set. Each user (station, STA) is assumed to be capable of following the CSMA/CA protocol, but may not be doing so at any time in order to gain an advantage. In an infrastructure network, all transmission occurs through the AP even when stations are attempting to send data to each other on the same network. The MAC layer standard specifies an acknowledgement (ACK) for each data packet (DATA) successfully transmitted. An RTS/CTS exchange is optional before any transmissions.

2.1 Motivations and Structure

Given that the only strategies are evolutions of the CSMA/CA strategy and the self-optimized strategy, the proposed scheme is designed to ensure that if the channel access protocol is modeled as a game of perfect information, CSMA/CA is the dominant strategy for all nodes.

The proposed scheme is designed to make minimal modifications to the existing standard. The AP is assumed to be conforming to the standard and is also assumed to be trusted and well behaved. It is also assumed that there is no collusion between any AP and STA or between STAs.

2.2 Brief overview of the scheme

The scheme revolves around an auction that is invoked by a STA every time it is involved in a collision (i.e. when it does not receive an ACK). The auction is designed to be incentive compatible and minimize social cost.

The channel is reserved for the auction winner for the next time slot (immediately after the auction), and the winning STA has immediate first transmit privilege during that slot. The winner is then required to make verifiable, delay based payments to the AP. The payments are a function of the bids and the confidence interval specified beforehand for verifying that the STA is indeed making the delay based payments. Payments are done via the RTS/CTS mechanism, so that the AP may confirm any promised delays by a STA.

Consider a population of STAs that involve a mix of self-optimized users and naïve users (users that follow CSMA/CA)

that have identical CW values initially. Based on the intent of the self-optimized users to force larger backoff values by initially increasing collisions with naïve STAs, it is evident that a self-optimized user will be a participant in a higher number of collisions (or participate in any given collision with higher probability) than an average naïve STA (this follows immediately from noting that the probability of collisions in the network would drop in the absence of self-optimized users).

Hence in a repeated game of the proposed auction, there exists a high incentive for each STA to win the auction and capture the channel. In particular, since self-optimized users are principally involved (directly or indirectly through a naïve STA) in invoking an auction, it is in every self-optimized user's best interest to win every auction.

3. Proposed Scheme

The mechanics of the auction works as follows. On every collision, the STAs involved in the collision invoke an auction by transmitting a *bid* to the AP. The AP then solicits bids from all other STAs in the network. Each STA sets its bid value to its current CW value (deviating behavior will be addressed later). Once the AP receives all the bids, it declares the STA with the highest bid, and consequently the highest current CW value, to be the winner. The AP then informs all other STAs in the network with the identity of the winner by transmitting a control frame (other STAs are assumed not to have gathered all other bids).

The winning STA gets immediate first transmit privilege from the moment it

receives the winner notification frame. The winning STA makes this transmission using the RTS/CTS mechanism so all other STAs are able to identify and defer to the winner. Once the winner is identified and successfully completes the first channel access, the network goes back to CSMA/CA based contention.

The winning STA is required to make verifiable delay based payments to the AP for the next N transmissions. The winning STA makes the next N transmissions based on a CW value that is a function of the second highest bid.

$$CW_{win} = \alpha CW_2 \quad (1)$$

Where CW_2 is the 2nd highest bid (and consequently the second highest CW value).

The backoff value generated randomly from the range $[0, CW_{win}]$ is sent by the AP to the winning STA through the CTS messages preceded by each DATA transmission from the STA. The AP then counts the number of idle slots observed on the channel, during the interval between the sending of a CTS by the AP, and the reception of the next RTS from the STA. The STA is designated as deviating from the payments if the observed number of idle slots is smaller than a specified fraction of the assigned backoff.

A single deviation does not necessarily indicate a lower payment, since the channel conditions seen by the AP and STA may be different. Hence, the value N is chosen such that consecutive deviations can be stored by the AP. If a certain fraction of deviations (higher than a set threshold) are measured out of N transmissions, then the STA is considered

to be deviating from its payments. At this point the MAC layer may be set to refuse to accept packets from this STA.

This auction is played out on every collision that is detected by a naïve STA.

3.1 Strategy Space

Given the nature of the auction, each STA has a set of strategies to choose from while playing the repeated form game:

1. Play fair (regular CSMA/CA) and bid fair
2. Play greedy (self-optimized) and bid fair
3. Play greedy and overbid
4. Play greedy and underbid

A STA is considered to bid fair when it plays a strategy such that bid is equal to the current CW value (plays the correct protocol). There does not exist any incentive for a naïve STA to underbid or try to lose the auction in any way. The winner of the auction not only gets to transmit immediately without contention, but also (since there is low probability of collision) gets to set the CW value back to the minimum for future transmissions (after the payment round).

3.2 Strategy and Incentive compatibility

Once N has been set during network initialization, the value for α in (1) can be set such that the expected delay cost of playing and winning the auction in a *single* game is higher than the expected delay cost of playing CSMA/CA with a CW value equal to that which was used in the auction. Specifically,

$$\alpha > (N+1) CW_1/N CW_2 \quad (2)$$

Realizes this condition.

Where CW_1 and CW_2 are the winning bid and the second highest bid respectively.

Hence, given that in a repeated game, there exists an incentive for a self-optimized user to win an auction, the payoff after winning an auction is lower than for playing regular CSMA/CA on a per game basis. This means in the repeated game scenario, CSMA/CA is the dominant strategy and there does not exist an incentive for any STA to unilaterally shift from a naïve implementation to a self-optimized implementation.

The significance of making the payments a linear function of the 2nd highest bid becomes clear when compared to a Second-price Sealed-bid (SPSB) auction. The SPSB auction is known to incentive compatible and an instance of a Generalized Vickrey Auction. The SPSB auction works by making the winner (highest bid) pay an amount equal to the second highest bid in the sealed-bid auction for the object being auctioned. The VCG mechanism further generalizes that the payments be a linear (or quasi-linear) function of the 2nd highest bid in order to maintain incentive compatibility. Incentive compatibility implies that there is no incentive for any of the bidders to bid a value higher or lower than their true value for the object. Bidding their true value maximizes the bidders utility (Appendix A).

Hence, in the context of the proposed scheme, there exists an incentive for each STA to set their bid equal to their current CW. Hence underbidding or overbidding actually decreases each STAs expected payoff if they are following the regular CSMA/CA.

The social cost involved in playing the repeated game can be controlled by picking values of N and α such that the expected delay cost for playing the auction and the expected delay cost for playing CSMA/CA is only marginally different. This will still maintain CSMA/CA as a dominant strategy in the long run and minimize social cost. Hence even if a naïve user wins an auction, the winning STA would only make delay payments that are marginally higher than the expected delay if it played regular CSMA/CA with the new CW value.

If the network consists only of trusted STA, the social cost can actually be driven to zero, if appropriate α is chosen in (2). Additionally, if there is reason to expect a large number of self-optimized users, a draconian version of the auction can be implemented such that the value of α is dynamically varied such that it initially forces higher payments (at the risk of higher social cost) from newer STAs (those STAs that just joined the service set) and then reduces α until there is minimal social cost for that STA.

4. Evaluation of the scheme

The proposed scheme converts CSMA/CA to a dominant strategy while maintaining incentive compatibility and minimizing social cost. However, the overheads involved in any auction-based scheme may overcome any advantages gained by implementing this scheme, especially in friendly (no self-optimized agents) networks. One possible mechanism for decreasing overhead is to piggyback bids and notification messages on DATA and ACK from or other control frames such as beacons. This may however significantly reduce the

responsiveness of the scheme, so that a self-optimized user might employ bursts of packets before enough DATA and ACK frames are transmitted for an auction to be held.

A fundamental assumption in the mechanism design was that each STA could only play minor evolutions of CSMA/CA and the self-optimized strategy (evolutions such as underbidding and overbidding were obviously allowed). This scheme may not hold up well against intelligent agents that perform statistical learning over the network to determine the payment parameters, and *then* self-optimize to maximize its payoff.

Both the question of overheads and intelligent learning can be addressed through simulations, and will be fertile ground for future research.

4.1 Efficiency and malfunctioning users

As mentioned earlier in this paper, a very specific class of agents was modeled. These self-optimized agents were assumed to have been in a position to play either CSMA/CA or the self-optimized implementation. Agents that were mimicking self-optimized behavior due to malfunctioning implementations or due to playing a completely different protocol (say, Bluetooth or a microwave oven) were not modeled.

Hence each STA in this scenario was able to make an intelligent estimate of the payoffs and costs involved in playing the various strategies *before* joining the network (note this does not require that each STA be able to switch between implementations while already associated to a network).

However, a malfunctioning user has no such capability and will continue to play a strategy oblivious to the presence of strategies that may increase its payoff. If a malfunctioning STA joins a network configured to play the auction, it will continue to flood the channel with packets without ever attempting to win the auction (note the analogy to coexistence) or make verifiable payments. In this scenario, naïve users will invoke auctions at a very high rate as a result of collisions with the malfunctioning users. In every such auction, a naïve user will win and gain immediate first transmit privilege, but will soon invoke another auction because of a new collision. The malfunctioning STA does not receive transmit privileges at all in a repeated game scenario, and in fact can increase its expected payoff if it could, however it is oblivious to this and continues to attempt to transmit with the same backoff value (which violates the rationality assumption). The worst-case scenario in this environment will actually require an auction for every transmission by a naïve user. This creates extremely high overhead for every single successful transmission.

As suggested before, this scenario is best dealt with as a coexistence problem, and not as self-optimization by intelligent agents.

5. Conclusion

A game theoretic approach to discouraging self-optimized misbehavior in the IEEE 802.11 MAC layer was presented. The proposed scheme minimizes social cost (minimum bandwidth or delay cost for naïve users) while ensuring that playing CSMA/CA is the dominant strategy. The mechanism is also designed to be incentive compatible.

Future work involves studies of overhead and tweaking the mechanism to handle malfunctioning and coexistence scenarios.

References

- [1] IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specifications, P802.11 1999
- [2] Detection and Handling of MAC layer Misbehavior in Wireless Networks, P. Kyasanur, N. Vaidya
- [3] Multi Agent Systems, Yoav Shoham, Stanford University. Draft only, Stanford custom publishing
- [4] Multiple Access in Ad-hoc Wireless LANs with non-cooperative Stations, J. Konorksi

Appendix A: Delay costs

Choosing the correct value of α will increase the expected delay cost for the self-optimized strategy compared to the naïve implementation.

Given that in a repeated game of the auction, there exists an incentive to win an auction as opposed to lose it (this is trivially true for the self-optimized implementation) the value of α should be set such that the expected delay cost is higher for the self-optimized strategy.

Consider the highest possible expected delay cost for playing regular CSMA/CA after a collision followed by $N+1$ transmission attempts:

$$\text{Expected Delay cost} = (N+1) CW_1$$

Since the winning bid is the highest possible CW size in the network. In order for the self-optimized STA to make payments that are higher than the worst-

case scenario of the naïve strategy (so as to make the naïve strategy give a higher expected payoff) we set α such that:

$$(N+1) CW_1 < \alpha N CW_2$$

Equation (2) in the paper follows from this inequality.

Appendix B: Incentive compatibility

To show that the proposed auction mechanism is incentive compatible, consider the following argument.

Each user is considered to have uniform utility for access to the medium, and payments are dictated by the CSMA/CA protocol. The uniform utility is normalized in this proof, and we only consider the payments. The linear payment schemes acts a Quasi-linear welfare maximizing function over the network [3]. Since the payments are a linear function of the *social cost* (the difference between the declared social welfare of the remaining agents in the current situation, and the their declared welfare in the hypothetical situation in which the winning agent did not exist) which is essentially the 2nd highest bid, the scheme is identical to a Generalized Vickrey Auction and is therefore incentive compatible.

Appendix C: Evolutionary Stable

A strategy is considered to be evolutionary stable if in a population entirely consisting of agents playing that strategy, a small perturbation does not create an incentive for the agents to play a different strategy.

In the IEEE 802.11 CSMA/CA as specified in the standard, the self-

optimized strategy is an Evolutionary Stable Strategy (ESS). In a population of STAs with all of them playing a self-optimized strategy, introducing a naïve STA does not create an incentive for the other STAs to switch to a naïve or any different strategy (here, STAs are allowed to switch strategies even after association).

However, if the proposed auction mechanism is implemented the self-optimized strategy ceases to be an ESS. In a population of STAs with all of them playing the self-optimized strategy, introducing a naïve player will ensure that auctions are invoked often and that the naïve player will win the auctions every time if fair bidding is followed. Hence, the naïve STA will continue to transmit (although with low efficiency initially), while the self-optimized STAs do not receive any channel access slots since they lose every auction. Hence there exists an incentive for the self-optimized STAs to attempt to win the auction by switching to a naïve state (at least temporarily). Once such a STA wins an auction, it will be required to make payments with a CW value of the order of the naïve STA. Hence each STA has an incentive to switch to a naïve strategy.

Hence, under the proposed auction scheme, the self-optimized strategy is not an ESS.