Enhancements of the IEEE 802.11,
a MAC Protocol for Ad Hoc Network with History of Power Adjustment

Sylwia Van den Heuvel - Romaszko, Chris Blondia
University of Antwerp, PATS Research Group,
Middelheimlaan 1, B-2020 Antwerpen
E-mail: sylwia.romaszko,chris.blondia@ua.ac.be

Abstract

We propose a MAC protocol which improves disadvantages of the IEEE 802.11 DCF standard, like the blocking problem, scheduling concurrent transmissions (the hidden and exposed problem). Our protocol also achieves better spatial reuse of the spectrum thanks to the power control taking into consideration the number of neighbors in the one-hop neighborhood and the history of power changes. Through many simulations we show that our algorithm outperforms the IEEE 802.11 standard both in the static and dynamic network and also in high interference environments.

1. Introduction

The standard for Wireless LAN’s IEEE 802.11 specifies two medium access control mechanisms, DCF (Distributed Coordination Function), and PCF (Point Coordination Function). The DCF scheme has been developed to use within both IBSS (Independent Basic Service Set) and infrastructure network configurations. The DCF is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The CS (Carrier Sense) is performed through physical (by air interface, PHY - Physical Layer) and virtual mechanisms (VCS). Both sensing mechanisms are used to determine the state of the medium. The VCS is referred to Network Allocation Vector which contains the remaining time of the on-going transmission exchange of data. The VCS employs RTS/CTS packets exchange for channel reservation. The sender transmits a Request-To-Send frame to its receiver. The receiver sends a Clear-To-Send frame if the NAV at the receiver indicates idle channel. Then the sender transmits the DATA frame and waits for acknowledgement ACK. IEEE 802.11 defines four kinds of interframe space (IFS) periods of time between frames: SIFS (Short IFS), PIFS (PCF IFS), DIFS (DCF IFS) and EIFS (Extended IFS). They determine the priority level for accessing the channel. The SIFS is used for a CTS frame and ACK frame, or subsequent frame in fragment burst. It is the shortest period for the response with a corresponding frame in 4-handshake exchange. The PIFS is used under the PCF mechanism in order to gain a priority access to the medium at the beginning of the Contention Free Period. The DIFS duration is used by a station operating under the DCF mechanism. During this period stations sense the medium and start the frame exchange if the channel has been sensed as idle and its backoff time has expired. The EIFS begins following the indication that the medium is idle after detection of the erroneous frame, thus after a message has not successfully been received.

However the IEEE 802.11 DCF standard cannot handle many problems arising in the multihop wireless network and it also assumes that the network is homogeneous. In this work we have improved some limitations of the 802.11 standard and we have adjusted the transmission power in order to gain a better throughput and packets loss.

The remainder of the paper is organized as follows. In Section II the related work is described. We have presented the enhancements of the 802.11 standard and the power adjustment mechanism of our proposed protocol in Section III. Details of the simulations are presented in Section VI. Concluding remarks are formulated in section VI.

2. Related work

2.1. Blocking problem

Important issues in ad hoc networks are: the blocking problem (congestion), the false blocking problem and the pseudo-deadlock [2] that are induced by the current implementation of the RTS/CTS mechanism and the NAV duration of the standard [1]. Nodes that overheard an RTS or a
CTS defer their transmission, they are blocked for the NAV duration. When a neighbor’s free node of the blocked node sends an RTS to a blocked node and receives no answer, it interprets this as a channel contention and enters backoff (a blocking node creates a false blocking node). Thus in consequence, the neighbor’s free node of the false blocked node can also become the false blocked node causing a pseudo-deadlock.

2.2. Concurrent transmissions

The Hidden Terminal problem (HTP) and the Exposed Terminal Problem (ETP) are the most known problems in wireless ad hoc networks. The ETP refers to IEEE 802.11, which does not support any parallel transmission if nodes are either neighbors or have common neighboring nodes. Many studies, [3], [4], [5] have shown that when one-hop neighbors are either both transmitters (Fig. 1.A) and both receivers (Fig. 1.B) simultaneous transmissions are possible without causing any collision. The standard [1] does not allow for such transmission, because nodes revert between a transmitter and receiver role multiple times during the whole transmission without saying explicitly when this role shift takes place, thus neighbors cannot guess the role of the sender until 4-handshake is completed.

![Figure 1. Concurrent transmissions](image)

2.3. Power Control Approaches

The CSMA/CA mechanism assumes that each node uses a certain fixed (or maximum) transmission power for the transmission of each packet. One way to conserve energy supported by the standard [1] is the power saving mechanism. A second approach is the use of a power control scheme, that allows to vary transmit power in order to reduce energy consumption. Many studies have shown that in a real-life network power control protocols can achieve better power conservation and higher system throughput through better spatial reuse of the spectrum [10] [3] [6] [7]. A simple basic power control scheme is based on the assumption that RTS/CTS packets can be transmitted with the highest power level and DATA/ACK packets with a minimum power level [10]. It should be taken into consideration that different power levels among different nodes cause asymmetric links. In the basic scheme, a transmission power level for DATA/ACK packets is determined using two different methods: by calculating the desired power level by the receiver or by the transmitter (bases on received power level \( p_r \), transmitted power level \( p_{max} \) and an equation \( p_{desired} = p_{max} / p_r * R_{thresh} * c \), where \( R_{thresh} \) is the minimal necessary received signal strength and \( c \) is a constant). In order to solve the problem with nodes in the CSR (Carrier Sense Range) a solution is proposed in [7], where the sender periodically transmits DATA at the maximal power level, \( p_{max} \), just for enough time so that nodes in the CSR can sense it. Nodes in the CSR defer their transmission only for the EIFS (Extended InterFrame Space [1]) duration, so the transmit power for DATA is increased once every EIFS duration and also the interval using \( p_{max} \) should be larger than the time required for physical carrier sensing. Another interesting solution has been proposed in [6]. The protocol achieves energy conservation by dynamically adjusting the transmission range on the fly at each node and thus increasing spatial reuse of the spectrum. The algorithm derives the minimum power from the power strengths \( P_{ij} \) (taking into account: minimum SIR threshold \( SIR_{thresh} \), the background noise power \( (N_0) \), receiver power \( (P_{re}) \) at node \( j \), transmission power \( (P_{tr}) \) of node \( i \) of the received packets, and record it in a local table. Each node uses local information to determine the minimum required transmission power: \( P_{ij} = P_{tr} = SIR_{thresh} * N_0 / P_{re} \). In [3] an adaptive solution is proposed, where RTS/CTS packets are transmitted with the minimal power level on the first \( t \) attempts \( (t \) is a dynamically tunable parameter). If all \( t \) attempts fail then the power level of RTS/CTS is incremented by \( \omega (P_{max} - P_{ij}) \) for every additional failure (\( \omega \) is a tunable coefficient). In [8] load-sensitive algorithms are proposed that adapt the transmission range based on traffic load conditions.

3. Proposed power control solution

3.1. Blocking problem

In order to manage with the blocking problem we applied an idea from [2] study, but with different assumptions. As we have already mentioned, the congestion is induced by the current implementation of the RTS/CTS mechanism and the NAV duration of the standard [1]. In [2] the NAV duration was divided for RTS Defer Time and Additional Defer Time if the channel has been assessed to be busy during the CCA (Clear Channel Assessment [1]) time, otherwise the node concludes that the channel is idle and it can contend for it. However, because we have applied the power ad-
justment algorithm in our protocol, we have also analyzed and simulated the network with a shorter first NAV duration - RTS Defer Time. In the first approach our RTS Defer Time is equal to \((2 \times \text{SIFS Time}) + (\text{CTS Time}) + (2 \times \text{Slot Time}) + (\text{CCA Time}) + (4 \times \text{Propagation Delay})\), so continuing deferring during \text{CCA Time} and additionally we have added \(8\mu s\) of the propagation delay. In the second approach our RTS Defer Time is equal to \((2 \times \text{SIFS Time}) + (\text{CTS Time}) + (2 \times \text{Slot Time}) + (2 \times \text{Propagation Delay})\). We have noticed that this approach (we have called it the "shorter blocking timing") works better with the power control algorithm, especially in the mobility scenario. The first approach, which we have called the "longer blocking timing", has a better throughput performance without using the power control mechanism. In both approaches, if the channel has been assessed to be idle the node can contend for it at once, so it does not enter into the exponential backoff mode.

### 3.2. Concurrent transmissions

We have already mentioned that the standard does not allow for any parallel transmission but in the high interference environment the parallel transmission can be still successful even if it is not a transmission of the parallel sender (Fig. 1.A) or the parallel receiver (Fig. 1.B). In our protocol, each exposed parallel sender (Fig. 1.C) attempts to transmit under conditions. We modify the CTS packet, like in [11] and [12], so our new CTS packet contains informations about the power level of the \text{RTS of primary sender} and \text{SINR} (Signal-to-Interference-and-Noise-Ratio) of the primary receiver. The parallel sender estimates how much its transmission could affect the reception of the primary receiver. We have calculated it in the same way like in [11] study, namely:

\[
p^\text{RTS} \cdot \text{Primary receiver} \cdot \text{SINR} \cdot \text{Primary receiver} - p^\text{RTS} \cdot \text{Primary receiver} + p^\text{CTS} \cdot \text{Parallel sender} \cdot \text{SINR} \cdot \text{Primary receiver}
\]

If this equation is below the \(\gamma\) threshold, \(\gamma = \text{Threshold}_\text{Capture} + \varphi\) (in dB), where \text{Capture Threshold} usually is equal to 10dB or 6dB in our protocol, and \(\varphi\) is equal to 6.4dB (or smaller). In [12] study the \(\gamma\) is equal to 3.6dB (not specified how it is estimated) and in [11] study \(\gamma\) is equal to \(CE + 6dB\), where \(CE\) is the constant value of the \text{Capture Effect}. In [12] studies the physical CS is deactivated by setting a high value of the capture power, so each node recognizes the channel as busy only if highly overloaded. Although we have applied the algorithm from [11] study, we have not exploited the capture power. Even in that case, the possibility of destroying the ongoing transmission is less, because we adjust the transmission power, taking into consideration the number of neighbors.

### 3.3. Power adjustment algorithm

Actually the most moderate part of our protocol is the power control mechanism. But the two enhancements of the standard, presented above, also carry an important weight. In [14] we have discussed our power control mechanism with the fixed desired number of neighbors added to the IEEE 802.11 DCF standard in static networks. In this work in the simulation section we have compared our power control algorithm both with the enhancements and without the enhancements in the static and mobile scenarios.

The basic idea of our protocol is to adjust power if the number of neighbors increases in order to achieve a better spatial reuse, a better throughput and packet loss. Each node can estimate how many neighbors it has in its one-hop neighborhood, based on successfully detected signals or using the table that is built by the routing mechanism. If the number of neighbors is different from our desired number of neighbors, \text{number of NeighMAX}, then we adjust the power. If the number of neighbors increases we decrease our power and if the number of neighbors decreases we increase our power. In each increase or decrease (\(P_t^{\text{diff}}\)) in the desired transmission power \(P_t^{\text{TR}}\) (equation 3) we take into account the transmission power history \(P_t^{\text{HIST}}\) (equation 2). The transmission power history is the old calculated value \(P_t^{\text{TR}}\). Different values of \text{nr of NeighMAX}. 3, 4, 5, 6, have been discussed in the simulation section. The pseudocode of the algorithm is presented below:

\[
\text{IF} \ (\text{nr of NeighCURR} <= \text{nr of NeighMAX}) \quad P_t^{\text{TR}} = P_t^{\text{MAX}}; \\
\text{IF} \ (\text{nr of NeighCURR} > \text{nr of NeighMAX}) \quad P_t^{\text{DIFF}} = \varepsilon \times \log_{10}(\frac{\text{nr of NeighCURR}}{\text{nr of NeighMAX}}) \times P_t^{\text{HIST}}; \\
\text{IF} \ (\text{nr of NeighN} < \text{nr of NeighN-1}) \quad \text{OR IF} \ (\text{nr of NeighN} > \text{nr of NeighN-1}) \quad P_t^{\text{TR}} = P_t^{\text{MAX}} - P_t^{\text{DIFF}}; 
\]

where \text{nr of NeighCURR} is the current number of neighbors, \text{nr of NeighMAX} is the desired number of neighbors, \(\varepsilon\) is equal to \(\frac{1}{\text{nr of NeighMAX}}\) and \(P_t^{\text{MAX}}\) is the maximal transmission power. An alternative approach is to change the power when the number of neighbors decreases:

\[
\text{IF} \ (\text{nr of NeighN} < \text{nr of NeighN-1})
\]

Take the corresponding power from the \text{ListNP},

where the list \text{ListNP} maintains consecutive numbers of neighbors and corresponding transmission powers. However we have noticed in our simulations that the first
approach (equation 3) is better than the second (equation 4), because every time when the number of neighbors increases and then decreases the algorithm corrects the value of the transmission power. This correction always takes into account the power history from all ‘rounds’. The first approach is better not only because it achieves a better performance but also because the nodes do not need to store the list $List_{NP}$ with the numbers of neighbors and corresponding powers. Figure 2 shows the change of the power for $nr_{of\ Neigh_{MAX}}$ equal to 3, 4, 5, 6, respectively. In order to see this small correction of values a zoom of the plot is shown. The increase and decrease ($Pt_{DIFF}$) in the desired transmission power $Pt_{TR}$ is limited by the maximum and minimum power specified by the transceiver used by the nodes.

Figure 2. Power scheme

4. Performance parameters and metrics

The two enhancements of the IEEE 802.11 DCF standard and the proposed power control algorithm have been implemented in the ns-2.27 network simulator [13]. The simulations have been carried out for various topologies, scenarios and traffic. The following performance metrics are used:

- Total data packets received
- Average aggregate data throughput $\frac{Total_{recv}}{Trans_{time} \times Sim_{time}}$ [Mbps]
- Packets Loss $\frac{Total_{drop}}{Total_{sent}}$

The following parameters are used for the simulation: number of nodes: (4, 8, 25, 50, 100), simulation area: (500mx500m, 1000mx1000m), topology: (ring, string, random), capture threshold: (10dB), $\gamma$ threshold: (6.4dB), radio propagation model: (Shadowing), traffic: (CBR, TCP), packet size: (512, random), simulation time: (50s, 100s, 200s), bandwidth: (2Mbps), movement: (random and constant). We have used the Shadowing Propagation Model [13] with different parameters in order to analyze performance of our protocols and the standard IEEE 802.11 DCF in different interference environments, so with different fading effects e.g Outdoor - Shadowed urban area, Office hard or soft partition, Factory, line-of-sight or obstructed.

5. Performance results

5.1. Blocking solution

We have simulated a ring topology with 8 nodes (Figure 3) with TCP traffic and 512 bytes packet size.

In Table 1. we have shown results where the blocking solution was applied compared to the IEEE 802.11 DCF standard. The network has been simulated with the shadowing propagation model for the outdoor, shadowed urban area environment. Since we only were interested in the performance improvement of the fairness we have analyzed the total reception of packets on particular receivers. We can notice that our first enhancement leads to a higher degree of fairness than the 802.11 standard.

<table>
<thead>
<tr>
<th>Scene</th>
<th>Nodes</th>
<th>Standard</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>412</td>
<td>1891</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1974</td>
<td>1998</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>1918</td>
<td>1586</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>2224</td>
<td>1220</td>
</tr>
<tr>
<td>1 Total</td>
<td>6528</td>
<td>6695</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1372</td>
<td>1722</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2009</td>
<td>1959</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1387</td>
<td>1656</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>2118</td>
<td>1586</td>
</tr>
<tr>
<td>2 Total</td>
<td>6886</td>
<td>6923</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3. Topology: ring (a), string (b)
5.2. Concurrent transmission solution

We have simulated the a string topology (Figure 3) with TCP traffic with a random packet size, where the first and second improvement (the solution for concurrent transmission) have been applied.

![Image of string topology](image)

Figure 4. Total packet received: 802.11 (up) the enhancement (down)

The network has been simulated with the shadowing propagation model for the outdoor environment. Figure 4 depicts the total packets received by the nodes 1, 2. We can notice that our enhancements achieve a better fairness compared to the 802.11 standard.

5.3. Two enhancements plus power adjustment solution

We have carried out simulations with different scenarios for the CBR, TCP and mixed traffic for 25, 50, 100 nodes, in the static and mobile network in the 1000mx1000m area and the 500mx500m area. We have also applied two different blocking timings, a longer and a shorter one (in all descriptions to the Figures below it has been said which blocking timing had been used but usually we have applied the shorter one, because it seems to be better). In all Figures below PScx means Power Control Scheme with the desired number of neighbors equal to x and /Ex means that shorter blocking timing has been used (PScx without /Ex means that longer blocking timing has been used). In the first two Figures, 5 and 6, we have used different labels (Ex means the protocol with two enhancements but with the first blocking timing -longer and Ex* with the second blocking timing -shorter) in order to differentiate particular cases of the protocols in the comparison below.

![Image of throughput comparison](image)

Figure 5. Throughput: 25 nodes, static

First we have compared the proposed MAC protocol with our two enhancements of the 802.11 DCF standard, our MAC protocol with these enhancements plus the power control mechanism (with numberOfMaxNeighbors equal to 3) with the 802.11 standard plus our power control algorithm and with the pure 802.11 standard. The network of 25 nodes and 11 flows is static and it consists of CBR traffic.

In Figure 5 we have compared the throughput. The throughput performance of the 802.11 standard is the worst. The enhancements have already improved the performance of the network (Ex not shown -0.023696 Mbps). When our power control mechanism is added to the standard the throughput performance improves a lot. The power control scheme with the enhancements with shorter blocking timing outperforms other protocols, where the solution with longer blocking timing has the second best performance. Figure

![Image of packet loss comparison](image)

Figure 6. Packet Loss: 25 nodes, static

6 shows the packet loss for all these protocols. Above on the plot we can see the packet loss for the standard, the enhancements with longer (Ex) and shorter (Ex*) blocking timing. We can easily notice that the packet loss of the
standard is the worst (0.320969) and the packet loss of the enhancements with the shorter blocking timing is the best (0.294363) among approaches without the power control. Below the packet loss of the standard with our power control scheme added and the enhancements with our power control mechanism are shown. The smallest packet loss (0.026165) achieves our power adjustment mechanism with applied two enhancements with shorter blocking timing.

We have analyzed our power control algorithm with different values of the \( nr_{of \text{ Neigh}_{\text{MAX}}} \), namely, 3, 4, 5 and 6 in the static and mobile network. For the static network we ran 4 different scenarios for 25 nodes with 15 CBR flows (512 bytes packet size). In the static network the power control with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 3 seems to have the best throughput performance. The second best throughput performance achieves the power control with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 4. Figure 7 shows the throughput performance of four power control schemes for one of the scenarios. In case of the packet loss, the situation is not so clear, because in two scenarios the smallest packet loss had the power control algorithm with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 3 and in two other the power control algorithm with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 4, where the second the smallest packet loss achieved the power control algorithm with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 5 and 6.

We ran 12 different scenarios for the mobile vehicle network, where 10 \((m/s) \leq \text{Speed}_{\text{Maximal}} \leq 120 \,(m/s)\). In the slower scenarios (10 \((m/s) \leq \text{Speed}_{\text{Maximal}} \leq 60 \,(m/s)\) the best throughput performance has the power control scheme with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 3 and then 4. In faster scenarios (70 \((m/s) \leq \text{Speed}_{\text{Maximal}} \leq 120 \,(m/s)\) the best throughput performance achieves the power control scheme with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 5 and then 4. The smallest packet loss in the slower and faster scenarios has the power control scheme with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 4 and then 5.

We also ran 2 scenarios for the mobile pedestrian network (with maximal speed 1.5 \((m/s)\) and 2.5 \((m/s)\)) for the different power schemes and compared to the 802.11 standard. The best throughput performance achieves the power control scheme with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 4 and then 5, where the worst has the 802.11 standard. The smallest packet loss (Figure 8), like in the mobile vehicle network, has the power control scheme with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 4 and then 5, where the worst packet loss achieves the 802.11 standard.

We have analyzed the performance of the mobile network with 50 nodes and 23 CBR flows. In the first scenario we have simulated the static network and in the second, mobile. The movement of the nodes is random and the nodes move all the time in the 1000mx1000m area. In both cases the performance of our protocol is much better than the standard. In Figure 9 the throughput performance is presented in the static network for the power control protocol with \( nr_{of \text{ Neigh}_{\text{MAX}}} \) equal to 5 and the shorter timing compared to the 802.11 standard. In Figure 10 the packet loss is presented both for the static and mobile network of our protocol with respect to the standard. The packet loss of the 802.11 standard for the static network (0.377322) is much smaller than for the mobile network (0.801431). In case of our protocol we cannot see such a big divergence, namely, packet loss in the static network is equal to 0.04379, so in the static case it seems to be a little better.

We have simulated the mobile network with 100 nodes and 50 CBR flows. The movement of the nodes is random and the nodes move all the time in 1000mx1000m area. The
Figure 10. Packet loss, 50 nodes, static and mobile

maximum speed is equal \(10 \text{ (m/s)}\). Figure 11 depicts the packet loss for the standard compared to the all power control schemes. The power control schemes strongly outperform the 802.11 standard.

Figure 11. Packet loss: 100 nodes, mobile

Summarizing, the power control algorithm with \(nr_{of\, Neigh_{MAX}}\) equal to 3 achieves the best throughput performance in static networks and mobile networks with the maximum speed of the nodes from 10 to 60 \( (m/s) \). The power control algorithm with \(nr_{of\, Neigh_{MAX}}\) equal to 4 has the best performance in mobile pedestrian networks, where maximal speed is between 0 and 2.5 \( (m/s) \). It also strongly outperforms other schemes and the 802.11 standard in the mobile network with 100 nodes, placed in the 500mx500m area. In all scenarios, mentioned above, it achieves the best packet loss as well.

6. Conclusion

In this paper we have presented the performance of a MAC protocol for ad hoc networks, first, which is an enhancement of the IEEE 802.11 DCF standard, second, it applies a novel power control scheme. We have shown that the multihop wireless network (static and mobile) can be controlled using different values of the transmission power containing the history of power changes. In our future work we will try to find optimal values of the transmission power for the maximum throughput and the minimum consumed energy with different fading effects.

References


