Simulation of a Backward Compatible IEEE 802.11g Network: Access Delay and Throughput Performance Degradation

Malisa Vucinic, Bernard Tourancheau, Andrzej Duda

Simulation of a Backward Compatible IEEE 802.11g Network: Access Delay and Throughput Performance Degradation

Mališa Vučinić*, Bernard Tourancheau† and Andrzej Duda*
†UJF - Grenoble 1, *Grenoble Institute of Technology
CNRS Grenoble Informatics Laboratory UMR 5217
Grenoble, France
Email: {Malisa.Vucinic, Bernard.Tourancheau, Andrzej.Duda}@imag.fr

***Abstract*—Performance degradation of an IEEE 802.11g network is studied in case legacy stations are associated with the AP. Custom event-driven simulator was developed for the purpose. We demonstrate its consistency by comparing the outputs with a widely accepted network simulator and with results of an analytical study. Performance degradation is analyzed in terms of access delay and throughput. We study the effect of an associated legacy node on access delay as a function of number of nodes in the network. Additionally, we focus on a fixed size network and examine the effect of the bit rate used for transmission of protection mechanisms' control frames. Significant performance drop is observed both in terms of access delay and throughput.**

***Keywords*—IEEE 802.11 Standards, performance analysis, access delay, throughput.**

I. Introduction

With the emergence of Fiber to the X (FTTx) last-mile technologies, the capacity of access links has been significantly increased. A common scenario in Home, Enterprise or Public environments is a Wireless Local Area Network using such a link as the backhaul. Although devices compliant with the latest IEEE 802.11n standard extension for WLANs have been deployed, there is still a substantial number of Access Points (AP) using IEEE 802.11g [1] that provides a maximum transmission rate of 54 Mb/s. In scenarios where an 802.11g compliant AP uses a high capacity link as the backhaul, the wireless link may become a bottleneck and the wireless stations may not be using the full capacity available. At the time of first deployment of 802.11g compliant devices, the dominating standard was IEEE 802.11b [2], providing maximal transmission rate of 11 Mb/s. In order to become commercially viable, IEEE 802.11g had to support presence of legacy 802.11b nodes in the network. Nowadays, 802.11b stations have been ruled out by the market but their presence is not uncommon. Hence, protection mechanisms developed in order to support backward compatibility in 802.11g networks are still widely used to allow support for association of legacy nodes.

This paper investigates the performance degradation of an 802.11g network in scenarios where at least one legacy station is associated with the AP. For that purpose a custom event-driven simulator was developed in C programming language. Consistency of the simulator was checked by comparative studies with analytical and simulation results from [3]. These results are presented in Section V.

Contribution of our work is twofold. Firstly, we present the access delay performance degradation of an 802.11g network for different number of nodes due to backwards compatibility. The BSSBasicRateSet is a set of transmission rates, communicated within the network (BSS), from which each rate must be supported by all nodes wanting to associate with an AP. Thus, if the AP supports legacy stations, it includes some or all of the 802.11b transmission rates in the advertised BSSBasicRateSet. Hence, the impact evaluation of the minimal rate in BSSBasicRateSet on this delay is detailed. Secondly, in order to extend [4], we evaluate channel throughput in saturation conditions in g-only, as well as backward compatible network scenarios using different protection mechanisms. These results are presented as a function of minimal transmission rate in BSSBasicRateSet.

The rest of the paper is organized as follows. Related work on the topic is presented in Section II. Section III summarizes IEEE 802.11 MAC layer specifications that are implemented in the developed simulator and are related to the performance analysis discussed in the paper. Interoperability issues of the standard extensions and the two protection mechanisms are reviewed in Section IV. Simulation studies performed and the results obtained are presented in Section VI. Finally, Section VII provides concluding remarks, observations and perspectives.

II. Related Work

The research community has given considerable interest to performance studies of IEEE 802.11 standards and high data rate extensions over the years. [5] evaluates the performance of the Distributed Coordination Function by means of an analytical model and simulation verifications. [6] noted a performance anomaly in a multi rate system due to low data rate stations. [4] gives an overview of the 802.11g standard extension and evaluates throughput degradation for backward compatible scenarios as a function of data transmission rate. [7] proposes a modification to Bianchi's model in order to evaluate the throughput degradation in hybrid networks. [8] studies a performance impact of an un-coordinated 802.11b

station in the network and presents the throughput degradation as a function of the station's data rate. However, neither [4] nor [8] specifies which rate was used in order to transmit protection mechanisms' control frames. This aspect should be taken into account because it affects the range of the network, as discussed in [9]. Therefore, a high minimal rate in this set prevents some legacy stations from associating with the AP. A model for access delay of 802.11 DCF is proposed in [3] and is used in our paper for consistency check of the developed simulator.

III. IEEE 802.11 STANDARD SPECIFICATIONS AND THE MAC PROTOCOL - DISTRIBUTED COORDINATION FUNCTION

The mandatory contention-based channel access function in the IEEE 802.11 MAC is called Distributed Coordination Function (DCF). DCF is based on carrier-sense multiple access with collision avoidance (CSMA/CA) which uses exponential backoff procedure. Unicast traffic uses immediate positive acknowledgment frames (ACK) for confirmation of a valid reception and when an ACK is not received after a certain timeout, the sender schedules a retransmission.

On the contrary with wired networks, in wireless networks it is not possible to detect an ongoing collision on the channel. Receiving signal level is much lower than the level of the signal that is being transmitted and thus it is hard to determine if a collision is taking place. Another important factor is the need for two transceivers, which adds significantly to the final cost of the wireless card, as a device needs to listen while transmitting. Thus, the only way to detect if collision happened is the lack of ACK control frame, which takes place after the complete data frame has already been transmitted. CSMA/CA addresses this problem with exponential backoff procedure. Each station extracts a random number of time slots to wait, distributed uniformly in the interval [0, CW], where CW denotes the Contention Window. At the first attempt CW is set to CWmin and for each retransmission the value is doubled, until it reaches CWmax. Once the CW has reached the maximum value, which is specified by different standard extensions, it holds it until the retransmission counter of the frame has reached Retry_Limit_Counter. In this case, the frame is discarded and the station pulls out the next frame in the queue.

Duration of a time slot is defined by standard extensions. 802.11g uses 9 μs in g-only mode while 802.11b uses 20 μs. A station senses the channel for a specified amount of time called DIFS, and if the channel is idle, starts decrementing the backoff counter. If the channel state changes, the decrement procedure is frozen and the station waits until the channel is idle again before continuing. The first station that reaches zero backoff counter value starts the transmission immediately. All stations are synchronized with the Access Point and can start transmitting only at the beginning of a time slot.

Channel sensing can be performed both at the physical and the MAC layers. A duration field in each 802.11 frame denotes the time needed for a given frame and its acknowledgment to be transmitted. Each station hearing the frame sets its Network Allocation Vector (NAV) to this value and defers access to the channel for this time. Channel is declared idle in terms of the MAC layer if the value of the NAV counter is zero, otherwise it is busy. This way, a significant amount of energy is saved as the station can turn off the radio during the busy channel state. The physical channel sensing is based on a received power threshold.

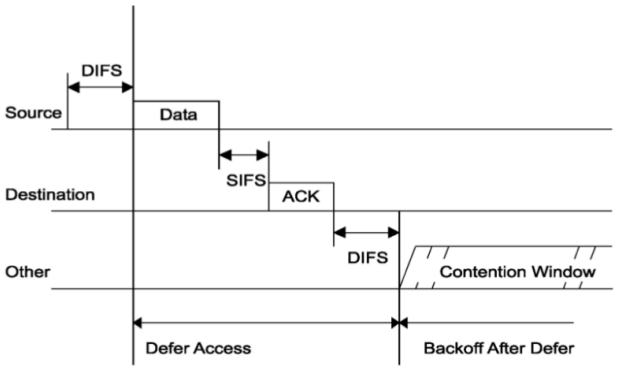

Fig. 1. DCF Basic Access Method [10].

After the receiving station has checked if the data frame was received well (by computing CRC), it sends back the ACK frame. A failure to receive the ACK frame at the transmitting node after a given timeout means that the frame needs to be retransmitted.

A. DCF Access Methods

DCF defines two access methods: basic access method and access with handshake. A decision which access method is going to be used is performed on a frame basis. For each station, parameter RTS_THRESHOLD specifies the size of a frame above which the access method with handshake should be used. The default value of this parameter is set to MAX_MPDU which is the maximum size of a frame in 802.11. Thus, by default, stations use the basic access method for each frame.

1) Basic Access Method: Before a station can declare the channel as idle, it needs to continuously sense for a time interval equal to DIFS. If the channel becomes busy, the station performs the backoff procedure. While the channel is busy the backoff counter is frozen. After the station has sensed the channel as idle for DIFS, it starts decrementing the backoff counter. As soon as the counter reaches zero, the station starts transmitting. At the destination end, the station starts receiving the frame, and, if there is no collision, transmits an ACK frame after a time interval called SIFS. As soon as the ACK is received at the data originating station, a new backoff value is being extracted and the station performs the backoff procedure. Fig. 1 summarizes the DCF Basic Access Method.

2) Access Method with Handshake: For frames of significant size a station can send a short control frame called RTS – Ready To Send. With this frame the station reserves the channel and notifies all nodes of the duration of the

upcoming conversation. The destination of the RTS, if there was no collision, sends the Clear To Send (CTS) control frame (after SIFS). Upon reception of CTS, originating station starts transmitting the data frame. This way, the channel is reserved before the actual transmission of a large frame takes place, and in the case of a collision not much time is wasted. The main advantage of this method is that all nodes within range of the source or of the destination will hear transmissions of RTS and CTS and thus will defer access for the time value set in the NAV field of the frames. This method solves the problem of hidden terminals but introduces large overhead in the transmission and affects the throughput performance. In order for the farthest nodes to be able to demodulate the frames and set their NAV accordingly, it is recommended that both RTS and CTS are sent at the lowest rate from BSSBasicRateSet. Section IV discusses how this method is used in an 802.11g network in order to support legacy stations compliant to the 802.11b [2] standard extension.

IV. Protection Mechanisms for Support of Legacy 802.11b Stations

The IEEE 802.11g standard extension [1] specifies an OFDM-based PHY layer - ERP-OFDM - in order to increase the throughput of the network. Furthermore, in order to support legacy devices, the 802.11g standard also specifies three additional PHY layers - ERP-DSSS, ERP-PBCC and DSSS-OFDM. The problem of interoperability arises as legacy devices cannot demodulate OFDM frames and furthermore are not able to properly sense the channel during an ongoing OFDM transmission, due to different power levels. The direct consequence is a significant performance degradation due to the collisions caused by the un-coordinated legacy station, as discussed in [8]. For this reason, the standard specifies as optional the DSSS-OFDM PHY layer that transmits the PLCP preamble and header with DSSS modulation, supported by legacy stations, and the payload with OFDM. Thus, the legacy stations hearing the DSSS transmission would refrain from transmitting, even if they cannot detect the OFDM frame [4]. However, as the DSSS-OFDM PHY layer is specified as optional, most manufacturers do not implement it in order to reduce the cost of the individual device. The only remaining way of supporting legacy stations in the network is to transmit complete frames with ERP-DSSS PHY layer. If this was done for all frames in the network, 802.11g stations would not see any performance benefit in comparison to legacy nodes. In order to overcome the interoperability issue, the standard defines two different protection mechanisms with the idea of sending a short control frame with ERP-DSSS PHY layer, that will be understood by legacy stations, and following a data frame with ERP-OFDM layer:

- **RTC/CTS protection mechanism** - equivalent to the access method with handshake discussed in Section III. Both control frames (RTS and CTS) are transmitted with ERP-DSSS PHY layer so the legacy nodes can decode them. However, this protection mechanism introduces significant overhead but is very robust in scenarios where hidden nodes are present.
- **CTS-to-self protection mechanism** - a node ready to transmit a data frame first transmits a CTS control frame with destination MAC address equal to its own by using ERP-DSSS PHY layer. The surrounding legacy stations can decode the frame and set their NAV counter. By omitting transmission of the RTS frame the protocol overhead is lowered at the cost of worse performance in presence of hidden nodes.

Legacy stations present in the network can demodulate the control frames, set the NAV counter and turn off the radio, as discussed in Section III. This way, the interoperability issue is solved at the MAC layer.

The Access Point signals to 802.11g stations in the network that a legacy station has associated by disabling the ERP network attribute (a flag) in beacon frames. The 802.11g stations are then required to use a protection mechanism preceding their transmissions. Furthermore, the state of the ERP network attribute signals the change in the slot time of network, used for backoff decrement procedure. In the case when the ERP network attribute is enabled (corresponds to g-only case) stations use 9 μs slot time, while in case 802.11b stations are present, 20 μs slot time is used. Additionally, the value of initial Contention Window also depends on the presence of legacy stations. In g-only case, stations use CWmin of 15, while in backward compatible mode, stations use value of 31. It is important to note that the performance degradation examined in Section VI is seen by an 802.11g station and is a consequence of a legacy station that is associated with the AP, but is not generating any traffic.

The standard does not precisely specify the transmission rate from the BSSBasicRateSet at which the control information in protection mechanisms should be transmitted. Clearly, the available rates are those of ERP-DSSS PHY layer (1, 2, 5.5 and 11 Mb/s). Although some implementations use the maximum rate - 11 Mb/s - in order to minimize the performance degradation, this can prevent access to nodes that are farther away from the AP, as discussed in [9]. Studies in Section VI analyze the channel access delay and throughput performance degradation due to a legacy station associated with the AP for different control frame transmission rates.

V. 802.11g simulator - Consistency Check

The simulator was implemented as discrete-event driven and was coded in C. A spatial model also had to be implemented as the transmission rate depends on the distance between the two stations. Results presented in [9] are used to determine the rate at which the station is going to transmit the frame. However, note that measurements presented in this paper all assume maximum bit rate of 54 Mb/s.

Consistency of the simulator has been checked through detailed examinations of generated traces as well as by comparison of results on collision probability and access delay with analytical and simulation results of Sakurai and Vu in [3]. Their study analyzes an 802.11b network and uses

the maximum transmission rate of 11 Mbps so parameter adjustments had to be made in order for the comparison to be fair. For results presented in this section, rate used has been set to 11 Mbps and the ACK transmission rate has been set to the minimal Basic Rate - i.e. 1 Mb/s, as in [3]. The 802.11 standard defines that an ACK may be sent at a rate not greater than the rate used for the transmission of the preceding data frame and this fact is exploited in our studies, resulting in smaller delay. Fig. 2 shows analytical and experimental analysis on collision probability as a function of number of nodes from [3], together with results obtained with our simulator.

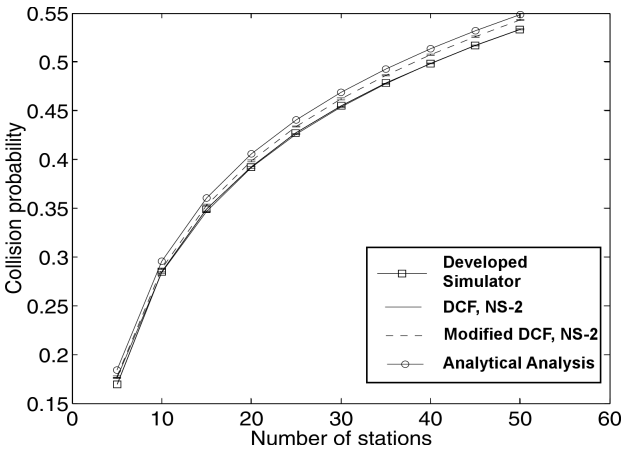

Fig. 2. Consistency check for collision probability of the developed simulator with results from [3].

We can see that there is a perfect match of results of DCF simulations in NS-2 with our simulator concerning collision probability. Modified DCF and the analytical approach for analysis of collision probability is discussed in [3]. It is worth noting that collision probability in our simulator is calculated as the ratio of total number of frames that collided and the sum of total frames transmitted and frames discarded.

Next step in the consistency check is access delay. Channel access delay is defined as the time interval between the instant when the packet reaches the head of the transmission queue and begins contending for the channel, and the time when the packet is successfully received at the destination station [3]. Thus, part of this delay is the transmission delay, so setting the common ground with [3] is essential in successful comparison of results. Apart from the fixed rate of 11 Mbps, we also had to set a deterministic UDP packet size of 1000 and 33 bytes (corresponds to the frame sizes of 1068 and 101 bytes, respectively). In all simulations performed, channel conditions have been assumed as perfect, allowing us to focus on the performance of the MAC protocol. The network is operating in saturation conditions - same as in the case of the collision probability study, and all the following measurement procedures.

Fig. 3 depicts average channel access delay as a function of number of nodes in the network. We can see that the results obtained for the two simulators match very well. Thus, we concluded that the developed simulator is consistent.

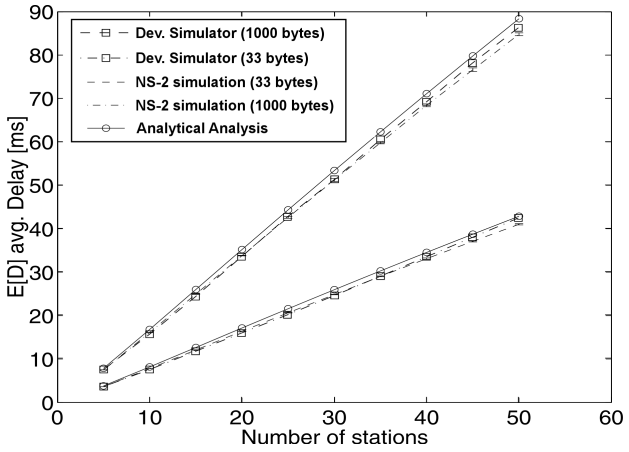

Fig. 3. Consistency check for access delay of the developed simulator with NS-2 and analytical results from [3].

VI. Performance Evaluation

As discussed in Section IV, in order to support 802.11b nodes in the network the AP disables the ERP network attribute in the beacon frame [4].This signals to the nodes the presence of one or more legacy stations and the necessary use of a protection mechanism as well as the network parameter setup, consisting of initial Contention Window value and the slot time. Another very important aspect that affects the performance is the PLCP (Physical Layer Convergence Protocol) preamble (synchronization purposes) and header (signalization of frame length, rate to be used, etc.) delay. This delay is PHY layer dependent and for ERP-DSSS equals to 192 or 96 μs, depending on the duration of the preamble (short or long) [4]. In our studies, we assume the worst case scenario, i.e. a PLCP delay of 192 μs. On the other hand, ERP-OFDM PHY layer delay is only 20 μs. It is important to stress that this delay is preceding each frame to be transmitted over the channel. Thus, in a scenario where RTS/CTS protection mechanism is used, two ERP-DSSS (one for RTS and one for CTS) and two ERP-OFDM (one for the data frame and one for the ACK) PLCP delays are added to the transmission time of MAC layer frames.

A. Collision Probability

Before proceeding with analysis of overall channel access delay, we present collision probability measurements obtained for g-only and backward compatible network scenario (see Fig. 4). As the simulation assumes perfect channel conditions and no hidden nodes in the network, the single factor that affects the collision probability is the initial Contention Window value. It is set to 15 and 31 for g-only and backward compatible scenarios, respectively. In the remaining part of the paper, channel access delay and throughput performance degradation is studied in g-only and backward compatible network scenarios.

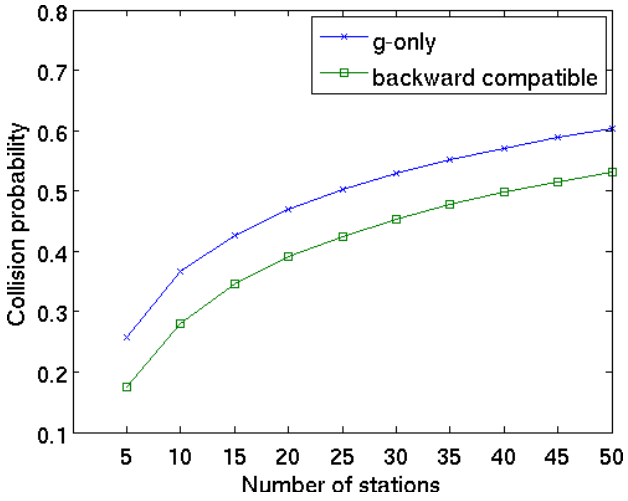

Fig. 4. Collision probability for g-only and backward compatible mode of an 802.11g network.

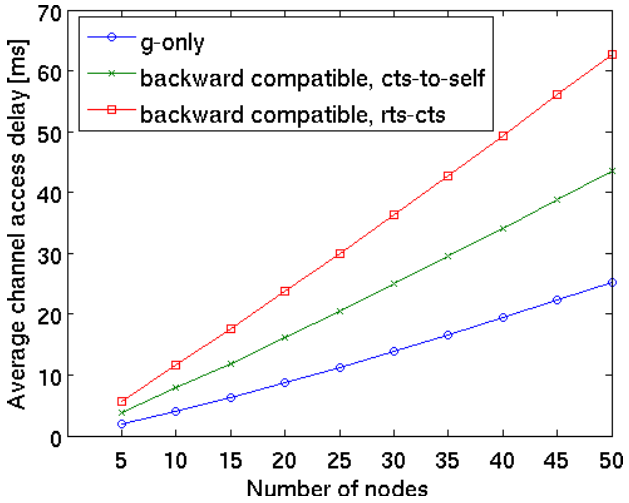

Fig. 5. Channel Access Delay [ms] for g-only and two backward compatible network scenarios.

B. Channel Access Delay

In order to evaluate the channel access delay performance of the network for different scenarios, we fixed the data frame size to 1534 bytes, as it is the most common MPDU size in 802.11 networks with Ethernet backbone. In the first study, we use 1 Mb/s rate for transmission of control frames of the two protection mechanisms, maximal 54 Mb/s rate for data and ACK frames and vary the number of nodes in the network. The control frame transmission rate of 1 Mb/s was chosen in order to support the largest spatial range of the network and to give an insight about latency values in the worst backward compatible scenario. In order to protect each frame in backward compatible scenarios, the RTS_THRESHOLD parameter is set to 0 bytes. In g-only scenario, basic access method of DCF is used. PHY delay parameters were set as discussed in the opening paragraph of this section. Initial Contention Window values and the slot time duration were set as discussed in Section IV. Results obtained are presented in Fig. 5. Notice that the shorter slot time duration and lack of control frame overhead of g-only supersede the higher collision probability, plotted in Fig. 4, resulting in better performance in terms of delay. Latency degradation increases with the number of stations present in the network, due to the increasing collision probability and protection mechanism overhead.

The second simulation scenario studied the effect of protection mechanism transmission rate on channel access delay. The number of nodes in the network was fixed to 10, while all other parameters were kept the same. As previously noted, data and ACK frames are transmitted at the maximal rate of 802.11g exploiting the standard specification. The minimal transmission rate in g-only scenario only affects the calculation of ACK timeout, as worst case is assumed (the receiving station can transmit ACK at any rate lower or equal than the one used for transmission of a data frame). In this way, the simulation setup emulates the case when a legacy node is associated with the AP, but remains inactive. We can notice

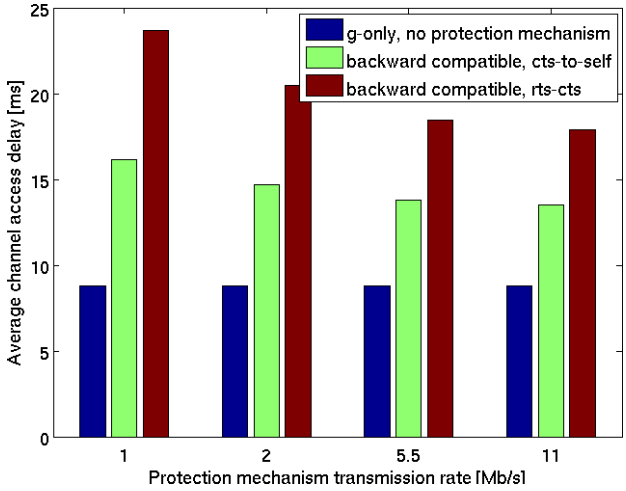

Fig. 6. Channel Access Delay [ms] as a function of protection mechanism control rate.

in Fig. 6 that the effect of slightly shorter ACK timeout (with increasing minimal transmission rate) does not play an important role in g-only scenario, as the delay is constant. Increase in protection mechanism transmission rate (minimal rate in BSSBasicRateSet) from 1 Mb/s to 11 Mb/s reduced the delay for CTS-to-self and RTS/CTS protection mechanisms by 2.64 and 5.79 miliseconds, respectively. Naturally, this comes at the price of lower radio coverage, as discussed in [9].

C. Channel Throughput

The goal of this third study was to analyze the useful channel throughput at the MAC layer of an 802.11g network in g-only and backward compatible scenarios. Perfect channel conditions were assumed and all the nodes transmit data and ACK frames at the maximal transmission rate of 54 Mb/s. All PHY and MAC layer parameters were set according to the discussions in previous sections, the number of nodes in

the network was fixed to 10 and the frame size was fixed to 1534 bytes. Similarly to the study of channel access delay, throughput is examined as a function of protection mechanism transmission rate. Again, g-only network scenario is barely affected by this change as it only changes the value of the ACK timeout, due to the worst case calculation. Results obtained are presented in Fig. 7. We can notice that the maximal obtainable

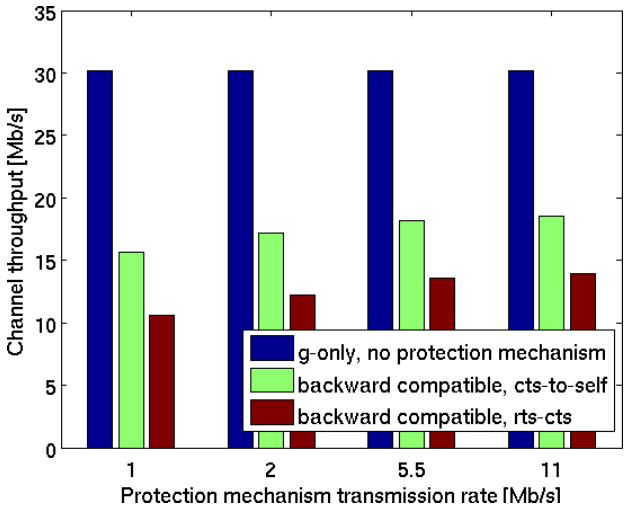

Fig. 7. Channel Throughput [Mb/s] as a function of protection mechanism control rate.

channel throughput in perfect channel conditions, 1534 byte frame size and g-only network scenario is around 30 Mb/s, due to the MAC protocol overhead. However, the performance drop due to the backwards compatibility is significant! In a scenario where backward compatibility is supported and the use of a long preamble is required, by employing CTS-to-self protection mechanism, channel throughput ranges from 15.6 to 18.5 Mb/s with increasing legacy data rate. An even larger performance drop is obtained with the RTS/CTS protection mechanism where the channel throughput varies from 10.6 to 13.9 Mb/s. Presented results imply MAC layer throughput so any applications running on top would experience additional overhead due to Network and Transport layer protocols.

VII. Conclusion

This paper presents results of our IEEE 802.11g simulator and a discussion regarding performance degradation in 802.11g networks supporting legacy 802.11b stations. Consistency check of the simulator was performed by comparative analysis with analytical and simulation results in [3] showing high conformance level. Studies of channel access delay in Section VI-B showed that the latency degradation, due to a legacy station associated with the AP, increases with the number of nodes in the network. The increase of the minimal transmission rate in BSSBasicRateSet from 1 to 11 Mb/s, used in order to transmit the protection mechanism control frames, reduces the delay by 2.64 and 5.79 miliseconds for CTS-to-self and RTS/CTS mechanisms, respectively. Significant performance degradation is observed in terms of channel throughput, as discussed in Section VI-C. Our simulation studies assume fixed frame size of 1534 bytes, saturation conditions and 802.11b nodes requiring the use of a long PLCP preamble. We could notice that the channel throughput drops from 30.1 Mb/s in case of g-only network scenario to 18.5 Mb/s in case the minimum overhead CTS-to-self protection mechanism is used by 802.11g stations (with 11 Mb/s control frame transmission rate). Performance drop is even higher for the RTS/CTS mechanism.

Depending on the frequency of occurrence of legacy nodes, by taking these results into account, it would be understandable to instruct the AP to decline association requests from legacy nodes for performance reasons.

References

[1] *Further Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz Band*, IEEE Std. 802.11g Std., 2003.

[2] *Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz Band*, IEEE Std. 802.11b Std., 2001.

[3] T. Sakurai and H. Vu, "MAC access delay of IEEE 802.11 DCF," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 5, pp. 1702 –1710, may 2007.

[4] D. Vassis, G. Kormentzas, A. Rouskas, and I. Maglogiannis, "The IEEE 802.11g standard for high data rate WLANs," *Network, IEEE*, vol. 19, no. 3, pp. 21 – 26, may-june 2005.

[5] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 3, pp. 535 –547, mar 2000.

[6] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance anomaly of 802.11b," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2, March 2003, pp. 836 – 843.

[7] S.-C. Wang, Y.-M. Chen, T.-H. Lee, and A. Helmy, "Performance evaluations for hybrid IEEE 802.11b and 802.11g wireless networks," in *Performance, Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International*, april 2005, pp. 111 – 118.

[8] M.-J. Ho, J. Wang, K. Shelby, and H. Haisch, "IEEE 802.11g OFDM WLAN throughput performance," in *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, vol. 4, oct. 2003, pp. 2252 – 2256 Vol.4.

[9] C. Heegard, "Range versus rate in IEEE 802.11g wireless local area networks," in *September meeting of IEEE 802.11 Task Group G*, 2001, available: http://www.nativei.com/ heegard/papers/RvR.pdf.

[10] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11 Std., 2007.

[11] Y. Kim, S. Choi, K. Jang, and H. Hwang, "Throughput enhancement of ieee 802.11 wlan via frame aggregation," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 4, sept. 2004, pp. 3030 – 3034 Vol. 4.

[12] R. Sharma, "Simulator to analyze QoS for IEEE 802.11b/a/g standards," *International Journal of Computer Science and Technology*, vol. 1, pp. 91 – 96, 2010.

[13] Y. Xiao, "Performance analysis of priority schemes for IEEE 802.11 and IEEE 802.11e wireless LANs," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 4, pp. 1506 – 1515, july 2005.