

Performance Analysis of IEEE 802.11 Ad hoc Networks with Cooperative ARQ in the Presence of Hidden and Exposed Terminals

G. Kormentzas*, J. Alonso-Zárate†, L. Alonso‡, and C. Verikoukis†

*University of the Aegean
gkorm@aegean.gr

†Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Castelldefels, Barcelona, Spain
{jesus.alonso, cveri}@cttc.es

‡Dept. of Signal Theory and Communications
Universitat Politècnica de Catalunya (UPC-EPSC), Castelldefels, Barcelona, Spain
luisg@tsc.upc.edu

Abstract—We present in this paper the analysis of an IEEE 802.11 network in the presence of hidden and exposed terminals when a Cooperative ARQ (C-ARQ) scheme is executed at the MAC layer. When spontaneous helpers transmit to assist in a failed transmission, the area exposed to the original transmission increases in comparison to non-cooperative ARQ schemes. In this paper we quantify this effect and we evaluate the relevance of designing efficient protocols to combat the exposed terminal problem.

I. INTRODUCTION

Cooperative communications have gained a lot of interest over the last years [1]. In this paper we focus on a particular kind of cooperation wherein feedback from the receiver is exploited: Cooperative Automatic Retransmission Request (C-ARQ) schemes. In C-ARQ cooperation is only executed when needed and thus the efficiency of the communications can be improved. Within the context of C-ARQ communication takes place in four slots whenever a data packet is received with errors at destination:

- 1) In the first slot, the source transmits a data packet to the destination.
- 2) In the second slot, the destination broadcasts a Call for Cooperation (CFC) packet. This packet invites all the potential helpers, i.e., those users which overheard to original transmission from the source, to assist in the transmission. Some of them become active relays (helpers) and a cooperation phase is initiated.
- 3) In the third slot, all the active relays attempt to assist the receiver by transmitting copies of the original transmission. These copies might be exact, recoded, compressed, or simply amplified versions of the original transmission. The relays or helpers might transmit orthogonally in time, frequency, or code.

This work has been supported by NEWCOM++ (ICT-216715), PASSENGER (PIEF-219561), LOOP (FIT-330215), CENTENO (TEC2008-06817-C02-02), and HURRICANE (ICT-216006).

- 4) In the fourth and last slot, the destination acknowledges, either positively or negatively, the reception or reconstruction of the original packet. The cooperation phase is finished.

Several works in the literature evaluate this kind of schemes from a fundamental point of view [2]–[4]. These works focus on the analysis at the PHY layer and usually assume simplified topologies with just one relay or in isolated conditions.

However, less work has been done on studying C-ARQ from upper layers of the protocol stack. An exception to that can be found in [5]. In that work, a MAC protocol based on the IEEE 802.11 Standard [6] is presented to operate within the context of a C-ARQ scheme. The analysis presented in that paper was in clear channel conditions, wherein all the users are in the transmission range of each other. Therefore, we want to contribute to the field by analyzing in this paper how the execution of a C-ARQ scheme at the MAC layer modifies the effects of the hidden and exposed terminals in the performance of an IEEE 802.11 network. Therefore the main contributions of the paper are:

- 1) Discussion on how the execution of a C-ARQ scheme at the MAC layer modifies the hidden and exposed terminal problems in an 802.11-based network.
- 2) Theoretical analysis of the channel utilization factor of an 802.11-based network in the presence of hidden and exposed terminals when a C-ARQ scheme is executed at the MAC layer.
- 3) Evaluation of a practical case study wherein the relays of a C-ARQ scheme transmit orthogonally in time.

The rest of the paper is organized as follows. In Section II, we review the hidden and exposed terminal problems and we discuss on how the use of C-ARQ schemes can modify their effects. In Section III, we analyze the throughput of a network executing a C-ARQ scheme at the MAC layer and taking into account both the hidden and the terminal problems. In Section IV we conduct numerical evaluation

to assess the performance of a network in the presence of hidden and exposed terminals, and considering the execution of C-ARQ scheme. Finally, Section V concludes the paper by summarizing and highlighting the most relevant results.

II. PROBLEM STATEMENT AND DISCUSSION

It is well known that the presence of hidden and exposed terminals in 802.11-based wireless networks has a great impact on the performance of the communications. We briefly define these two problems as follows.

A *hidden terminal* lies in the transmission range of a receiving station, but it is out of the range of the transmitting station. Therefore, the hidden terminal is oblivious of the ongoing transmission and can initiate a new transmission that will cause a collision at the receiver. The occurrence of these collisions reduces the overall performance of the network.

On the other hand, an *exposed terminal* lies in the transmission range of the transmitter but out of the transmission range of the receiver. Therefore, a transmission initiated by this terminal would not cause a collision at the receiver. However, it remains silent due to the busy channel detection. This effect reduces the overall throughput by stopping some stations from transmitting despite the fact that they would not cause a collision.

We evaluate in this paper how the execution of a C-ARQ scheme at the MAC layer modifies these two problems.

The first observation is that the vulnerability period of a transmission is extended if cooperation is required. If a cooperation phase is initiated, then the channel has to be reserved for enough time as to ensure that the cooperation phase can be completed. For this time, collisions can occur due to the hidden terminal problem and the exposed terminal problem is exacerbated.

However, the essence of the hidden terminal problem remains unaltered. By definition, a hidden terminal lies in the transmission range of the destination. However, in a C-ARQ scheme, the destination of a message does not change and, in addition, the helpers do not expect any ACK for their retransmissions (they are not receivers). Therefore, the hidden terminal problem is not altered by the execution of a C-ARQ scheme at the MAC layer, except for the fact that the vulnerability period is longer.

On the other hand, a C-ARQ scheme does modify the exposed terminal problem. Whenever a destination station calls for cooperation, new transmitters appear in its surrounding area, changing the otherwise simple scenario formed by a transmitter and a receiver. The fact that some neighbors become active transmitters, and thus occupy the channel, extends the area exposed to the original transmission from the source to the destination.

In the next section we provide a comprehensive insight and analysis of the problem, and we compute the throughput of a network considering the hidden and terminal problems within the context of a C-ARQ scheme. We first consider the operation of the network without C-ARQ and then we

discuss on how the execution of C-ARQ scheme with relays transmitting orthogonally in time modifies the analysis.

III. THROUGHPUT ANALYSIS

We consider an ad hoc network formed by an arbitrary number of mobile stations spread out uniformly in a given network area. All the stations contribute equally to the total offered traffic load, which we assume to be generally distributed and to have a mean value of g packets per second where g includes originally generated packets and retransmissions. The size of the data packets is also generally distributed and has a mean value of P bits per packet. The network operates in finite load conditions. Therefore, we can define the throughput or utilization factor of the network as

$$U(g) = U_{LOS}(g)e_2(g), \quad (1)$$

where U_{LOS} is the throughput of a network wherein all the stations are in the transmission range of each other (Line Of Sight) and e_2 is the throughput reduction factor due to the collisions caused by hidden terminals. For convenience and to clarify the notation, we drop henceforth the dependence of these terms with g in the notation. The term U_{LOS} can be computed as

$$U_{LOS} = \frac{S}{B+I}. \quad (2)$$

S is the average effective data packet transmission time, B is the average duration of a busy period (including the transmission of data and control as well as collisions), and I is the average duration of an idle period wherein the channel remains idle.

We focus on a network executing the Distributed Coordination Function (DCF) of the IEEE 802.11 Standard. Therefore, in order to evaluate these parameters, we define τ as the duration of the IEEE 802.11 time slot, as defined at the PHY layer of the standard [6]. On the other hand, we consider a discrete time reference where events occur at the end of each slot. We define p as the probability that no packet arrives in a given time slot. Consequently, packet arrivals can be modeled as a Bernoulli process with probability of success $(1-p)$. Therefore, the number of consecutive idle slots until a packet arrival occurs follows a geometric distribution $(1-p)p^{(n-1)}$, where n is the number of consecutive idle slots. Accordingly, the expected duration of an idle period can be expressed as

$$I = \tau \sum_{n=1}^{\infty} np_n = \tau \sum_{n=1}^{\infty} n(1-p)p^{n-1} = \frac{\tau}{1-p}. \quad (3)$$

For the computation of the average busy period (B), we define p_s as the conditioned probability that a successful transmission occurs in a given slot, given that at least one arrival occurs in that slot. Let define p_1 as the probability that a single arrival occurs in a slot. Since the probability that at least one arrival occurs in a slot is given by $(1-p)$, the probability that a packet is successfully transmitted is given by

$$p_s = \frac{p_1}{1-p}. \quad (4)$$

Subsequently, the average number of slots for which at least one packet arrives is denoted by t_B and computed as

$$t_B = \sum_{n=1}^{\infty} np(1-p)^{n-1} = \frac{1}{p}. \quad (5)$$

According to these definitions, $t_B p_s$ is the average number of successful slots within a busy period, and $t_B(1-p_s)$ is the average number of collided slots within a busy period. Therefore, the expected duration of a busy period is given as

$$B = T_s t_B p_s + T_c t_B (1-p_s) = \frac{T_c + p_s(T_s - T_c)}{p}, \quad (6)$$

with T_s and T_c the duration of a successful and collided slots, respectively. The values for these two parameters are given in [7].

Lastly, we have to compute the value of S . To do so, we assume that data packets of length P bits are transmitted at a certain rate R . The transmission time of these packets is $T_p = P/R$, and the average time for which payload information is transmitted in the channel is given by

$$S = T_p t_B p_s = \frac{P p_1}{R p (1-p)}. \quad (7)$$

Using (3), (6), and (7) into (2), a closed-form expression for the average throughput can be obtained in LOS conditions.

Following the terms in (1), we now consider the hidden terminal problem to compute the value of e_2 . In this case, the probability of success of a transmission depends on the probability that no node within the transmission range of the intended receiver initiates a transmission. This probability is derived in [8] within the context of a CSMA-based protocol and can be expressed as

$$e_2 = \left[\frac{I}{B+I} p^{T_s/\tau} \right]^{N-1}, \quad (8)$$

where N is the quotient of stations that are in LOS with a specific station to the stations that can affect the transmission of this station. The stations that can affect the current transmission are those that are at a maximum distance r from the receiver, and at farther distance than r from the transmitter and thus can be within the transmission range of the receiver but not the transmitter. Therefore, if ρ is the nodes' density and r is the transmission range of each station, then

$$N = \rho \pi (2r)^2 / \rho \pi r^2 = 4. \quad (9)$$

We now turn the focus to the analysis of the exposed terminal problem. It is important to note that this problem does not reduce the throughput as computed with (1), but it prevents it from becoming higher. In fact, it is possible to express the ideal throughput that would be achievable in the case that exposed stations could know when to transmit and

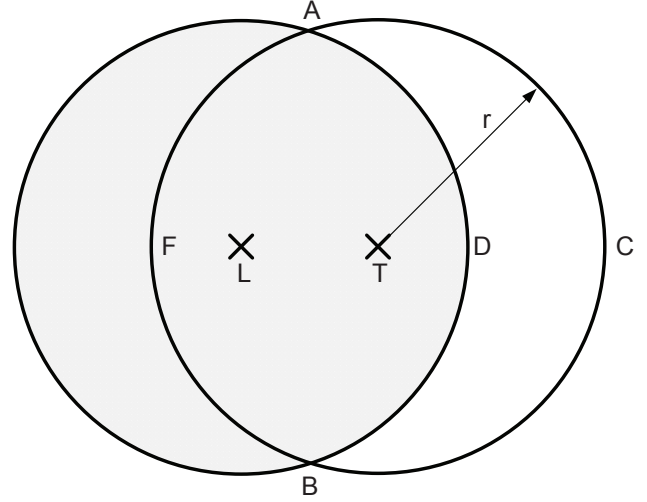


Fig. 1. Exposed Terminal Problem

when to defer the transmissions to avoid either misused or waste of resources as

$$U = U(g) + U(g_e). \quad (10)$$

In this expression, g_e represents the additional data traffic rate (packets per second) that could be transmitted in the network if the exposed terminal problem could be solved. In order to analyze this parameter, let now take a look at Figure 1. T is transmitting at a certain moment, and its transmission range is represented in the figure as a circle of radius r centered at T. We denote by E the area of that circle. If the transmission from T is referred to a station within the region $E1$, delimited by the points ABFD in the figure, then L should remain silent to avoid a collision even in the case it wants to transmit a packet. On the other hand, if the transmission of T is referred to a station within the region $E2$, limited by the points ABDC in the figure, then L is exposed and it unnecessarily will defer its transmission as it would not collide with the ongoing transmission from T. However, following the rules of the IEEE 802.11, L will remain silent. Therefore, assuming that the stations are uniformly distributed across the network area and that transmissions occur equiprobably to all stations, then there is a proportion $E2/E$ of deferral periods performed by station L that are not necessary. Considering the regular operation of the IEEE 802.11, the fraction $E2/E$ can be found in [9] equal to 0.42.

We assume that there exists an ideal mechanism that allows stations to know when they should transmit or not, always respecting ongoing transmissions but avoiding the exposed terminal problem. The probability that a deferral period occurs because the medium is busy is determined by the probability that the medium is busy, which is equal to $B/(B+I)$, times the probability that a packet arrives within a slot, which is $(1-p)$. Therefore, if stations can know when to transmit during another transmission and when not, then a ratio

$$\beta = \left(\frac{B}{B+I} \right) (1-p) \left(\frac{E_2}{E} \right) \quad (11)$$

of additional transmissions will occur in the medium simultaneously with ongoing transmissions and without incurring in a collision. This means that an extra proportion of traffic load g_e , also expressed in packets per second, would be transmitted in the network, such that the probability that a packet arrives in a time slot is β . Then, the computation of g_e from β is simple if we know the distribution describing the packet generation rate. An example of this will be presented in the next section where some numerical evaluation is performed.

Let now investigate how the use of a C-ARQ scheme modifies this analysis. It is worth observing that the duration of a successful transmission can be expressed as

$$T'_s = T_s(1 - p_e) + (T_s + T_{COOP})p_e, \quad (12)$$

where p_e is the probability that a packet is received with errors and thus cooperation is requested. Therefore, if there is no error, the duration of a transmission is determined by the regular operation of the IEEE 802.11 Standard. However, in the case of error, the duration of a successful transmission is equal to T_s plus the duration of the cooperation phase, denoted by T_{COOP} . This duration is determined by the number of required retransmissions and the MAC protocol used to coordinate the relays. Accordingly, it will be necessary to consider this new transmission time when either evaluating the hidden or the exposed terminal problems.

First, taking into account that the destination of the transmissions does not change when cooperation is executed and that collisions occur only at destination, the hidden terminal problem remains unaltered. However, as mentioned before, it is necessary to consider that the vulnerability period for any transmission is longer, as expressed in (12).

On the other hand, since the relays also take part in the communication, the exposed area is enlarged when compared to a non-cooperative ARQ scheme. In this case, the ratio of additional transmissions that could be performed if the exposed terminal problem is avoided can be determined by

$$\beta' = \beta(1 - p_e) + \beta_{C-ARQ}p_e. \quad (13)$$

The value of β is the same as the one computed with (11). For the computation of β_{C-ARQ} it is necessary to consider the area exposed to the retransmissions by the relays, which is different from E_2 . To proceed with this analysis we support our discussion with Fig. 2.

In this figure, we consider that station T is transmitting a packet to a destination D, placed at a distance d , which, by definition, is lower or equal than r (transmission range of T). The potential relays for this communication lie within the overlapping area of the transmitting and receiving ranges of both T and D, respectively. Regarding the exposed terminal problem, the worst case will correspond to the one when the exposed area is maximized. This happens when the relays are

placed at the edges of the overlapping area of the transmission ranges of T and D. Therefore, if we want to compute the total area that can be affected by the exposed terminal problem, we should consider the area within the limits defined by the infinite circles of radius r whose centers can be placed along the edge of the overlapping area of the transmission ranges of T and D. As it is shown in the figure, in order to compute this area, it is possible to define two symmetry axes which define four regions with equal areas.

To make the exposition clearer, let have a look at Fig. 3.

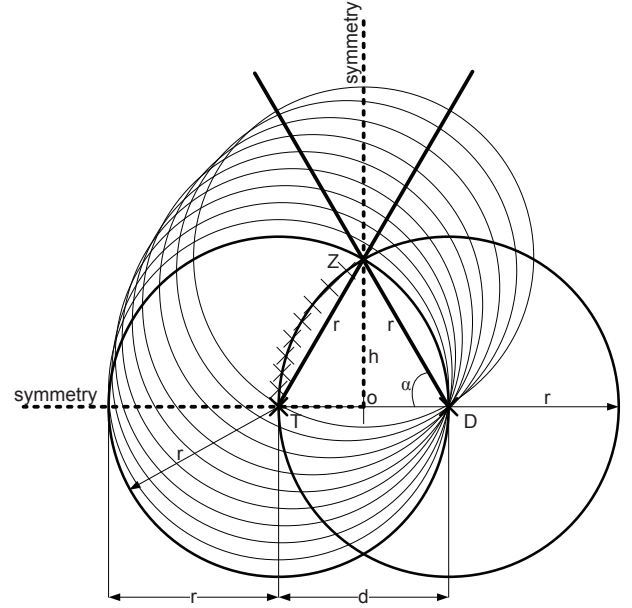


Fig. 2. Exposed Area (description)

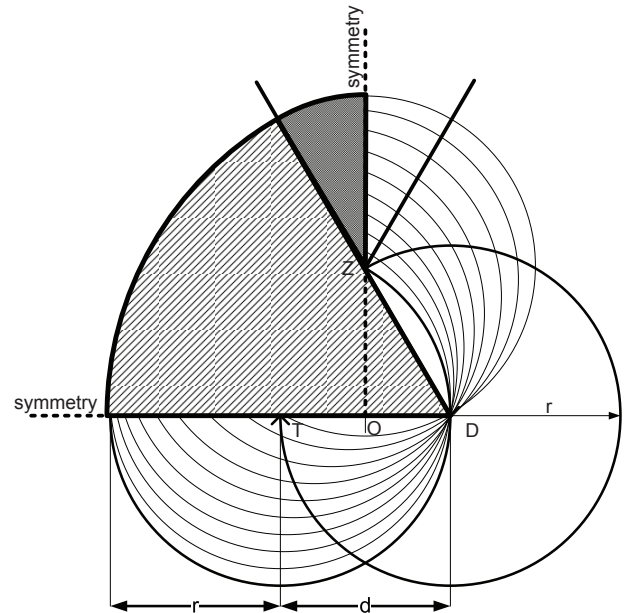


Fig. 3. Exposed Area (calculation)

We can compute the exposed area as four times: *i*) the area of the stripped sector of radius $(r + d)$ and angle α , plus *ii*) the area of the shadowed sector of radius r and complementary angle of α (i.e., $\pi/2 - \alpha$), minus *iii*) the area of the triangle delimited by the vertices DOZ. Accordingly, the area subject to the exposed terminal problem, denoted by E_{C-ARQ} , can be computed as

$$E_{C-ARQ} = 4 \left[A_s(r + d, \alpha) + A_s(r, \frac{\pi}{2} - \alpha) - A_t \right]. \quad (14)$$

$A_s(a, b)$ denotes the area of a sector of radius a and angle b , and can be computed as $A(a, b) = (1/2)a^2b$. A_t is the area of the triangle formed by the vertices DOZ, which can be computed as

$$A_t = [(d/2)r \sin(\alpha)] / 2. \quad (15)$$

By simple observation of the figure it is possible to write that $\alpha = \arccos(\frac{d/2}{r})$, and finally, the ratio of additional traffic that could be transmitted if the exposed terminal problem is solved can be expressed as

$$\beta_{C-ARQ} = \left(\frac{B}{B + I} \right) (1 - p) \left(\frac{E_{C-ARQ}}{E} \right). \quad (16)$$

With this value it is possible to compute the value of β' in (13), and thus to evaluate the impact of the increased exposed area due to the use of a C-ARQ scheme at the MAC layer.

In the next section we present some numerical evaluation with a practical case study.

IV. NUMERICAL EVALUATION

A. Scenario

In this section we use the analysis presented in the previous section to evaluate the performance of an ad hoc IEEE 802.11 network where a C-ARQ scheme is executed upon the reception of a packet with errors. The probability of receiving a packet with errors is $p_e = 0.5$. We consider that the relays transmit one after another without contending for the channel and exactly two retransmissions are required at reception in order to recover the original packet. We evaluate the performance of the network under three different conditions:

- 1) An ideal situation without hidden or terminal stations, where all the stations are in Line of Sight (LOS) with each other (clear channel conditions).
- 2) A scenario with the presence of hidden and exposed stations.
- 3) A scenario where we consider that the exposed stations can know when they can transmit or not. By comparing this case with the previous one, it is possible to evaluate which is the impact of the presence of exposed stations in a network. We consider in this case $d = r$.

In all cases we compare the results to that of an 802.11 network without C-ARQ as a benchmark performance.

Regarding the offered load to the network, we assume a Poisson traffic distribution with parameter g and thus

$$\begin{aligned} p &= \frac{(g\tau)^0}{0!} e^{-g\tau} = e^{-g\tau}, \\ p_1 &= \frac{(g\tau)^1}{1!} e^{-g\tau} = g\tau e^{-g\tau}, \\ \beta' &= 1 - e^{g\tau} \Rightarrow g_e = \frac{-\ln(1-\beta')}{\tau}. \end{aligned} \quad (17)$$

Data packets have an exponential distribution with average 1500 bytes. According to [10], these are the size and distributions that better represent the data traffic of a WLAN. The rest of the parameters are summarized in Table I.

B. Results

The channel utilization, as defined in (1), is plotted in Fig. 4. First, it is worth observing that the LOS channel condition provides high channel utilization ratios. Under these clear channel conditions, the RTS/CTS mechanism provides efficient protection against the occurrence of collisions, and thus the performance grows as the traffic load increases.

However, in the conditions when we consider the presence of hidden and exposed terminals, the utilization factor drops as the offered traffic increases. The higher the data traffic, the higher the probability of collision and also the more evident the exposed terminal problem becomes.

If we compare the curves for the regular operation of the network (lines without markers in the figure) with those with the execution of the C-ARQ scheme (lines with the circular marker in the figure) we see that faster retransmissions from the relays help in enhancing the channel utilization rate.

TABLE I
SYSTEM PARAMETERS

Parameter	Value	Parameter	Value
Data Tx. Rate Source	6 Mbps	Ctrl. Tx. Rate Source	6 Mbps
Data Tx. Rate Relays	54 Mbps	Ctrl. Tx. Rate Relays	6 Mbps
MAC header	34 bytes	PHY preamble	96 μs
DIFS	50 μs	SIFS	10 μs
ACK length	14 bytes	SlotTime (τ)	10 μs
RTS length	20 bytes	CTS and CFC length	14 bytes
Required retx.	2	Packet error prob. (p_e)	0.5

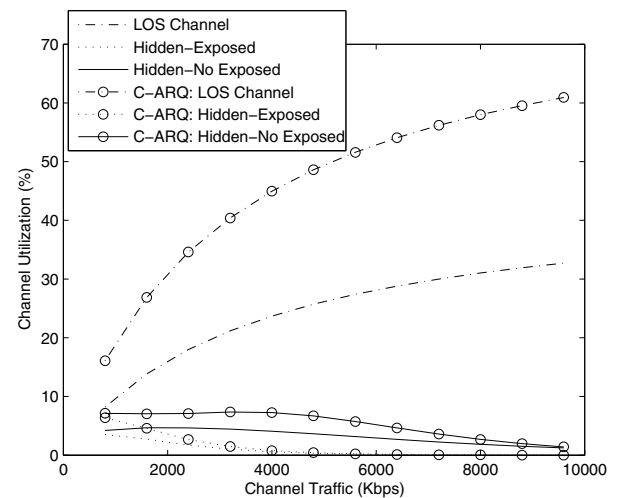


Fig. 4. Channel Utilization (%)

However, it is interesting to see that when executing the C-ARQ, the amount of exposed traffic is higher than without C-ARQ.

In order to better evaluate this effect, we plot in Fig. 5 the amount of channel utilization lost by the exposed terminal problem, i.e., the term $U(g_e)$ expressed in (10). It is worth seeing that in the C-ARQ case, the fact that more than one station is involved in the link from the source to the destination enlarges the exposed area, as we already discussed in the previous section. Note that, just as an example, when the channel traffic load is equal to 4 Mbps, the amount of exposed data traffic in the C-ARQ scheme doubles that of the network without C-ARQ. Despite that, the channel utilization with C-ARQ is still better than without C-ARQ, as it was shown in Fig. 4. This is due to the fact that although the exposed area is larger, the duration of the exposition is shorter due to the shorter transmission times yielded by the cooperative transmission.

According to this discussion, it seems clear that the design of an efficient mechanism to combat the exposed terminal problem will benefit both schemes (with and without C-ARQ). However, in the C-ARQ case the improved performance will be greater.

Therefore, the quantitative analysis presented in this paper shows that:

- 1) A network executing a C-ARQ at the MAC layer outperforms a network without C-ARQ in the considered scenario.
- 2) The C-ARQ is more affected by the presence of exposed terminals than the non-cooperative ARQ scenario due to the enlargement of the exposed area of any transmission when a cooperative phase occurs. Therefore, a tradeoff should be carefully managed between the improved performance attained by the C-ARQ scheme and the exacerbation of the exposed terminal problem. Under some conditions, it may not be suitable to execute

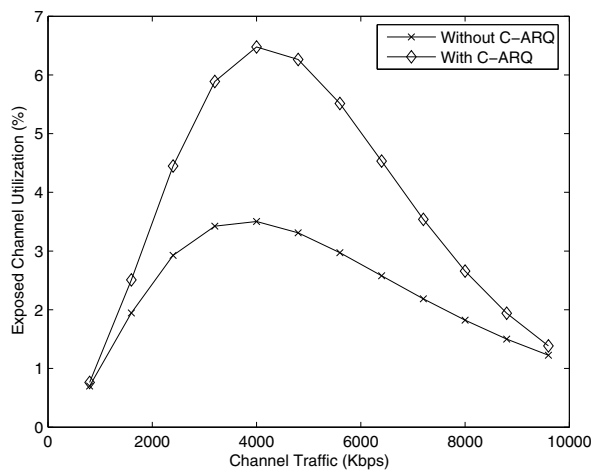


Fig. 5. Exposed Channel Utilization (%)

cooperation.

- 3) The design of efficient mechanisms to reduce the exposed terminal problem would boost the achievable utilization factor in a network executing a C-ARQ scheme.

V. CONCLUSIONS

We have evaluated in this paper how a C-ARQ scheme executed at the MAC layer modifies the analysis of the hidden and exposed terminal problems in IEEE 802.11 networks. While the hidden terminal problem remains almost unaltered, the fact that different transmitters are involved in a link between a source and a destination enlarges the area where the exposed terminal problem can occur.

We have presented the theoretical analysis of the channel utilization factor of a network with and without C-ARQ. We have considered the presence of both hidden and exposed terminals and results show that despite the fact that the C-ARQ scheme is more affected by the presence of exposed terminals the overall channel utilization factor is still higher than in the scenario without C-ARQ. Results also show that the design of efficient mechanisms to combat the presence of exposed terminals would remarkably benefit the performance of C-ARQ schemes as they inherently increase this effect as a counter effect of the mechanism.

Future work will be aimed at extending this model to consider the overhead of the MAC protocol required to coordinate the retransmissions from the relays and at the design of efficient mechanisms to combat the exposed terminal problem in the C-ARQ scenario.

REFERENCES

- [1] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communications in wireless networks," *IEEE Communications Magazine*, pp. 74–80, October 2004.
- [2] M. Dianati, X. Ling, K. Naik, and X. Shen, "A node-cooperative ARQ scheme for wireless ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 46, pp. 1032–1044, May 2006.
- [3] E. Zimmermann, P. Herhold, and F. Fettweis, "On the performance of cooperative relaying protocols in wireless networks," *European Transactions on Communications*, vol. 16, pp. 5–16, January 2005.
- [4] I. Cerruti, A. Fumagalli, and P. Gupta, "Delay model of single-relay cooperative ARQ protocols in slotted radio network with poisson frame arrivals," *IEEE/ACM Transactions on Networking*, vol. 16, pp. 371–382, April 2008.
- [5] J. Alonso-Zarate, E. Kartsakli, C. Verikoukis, and L. Alonso, "Persistent RCSMA: A MAC protocol for a distributed cooperative ARQ scheme in wireless networks," *EURASIP Journal on Advanced Signal Processing, Special Issue on Wireless Cooperative Networks*, p. 13, December 2008.
- [6] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2007.
- [7] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas of Communications*, vol. 18, pp. 535–547, March 2000.
- [8] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part II - the hidden terminal problem in carrier sense multiple-access and the busy-tone solution," *IEEE Transactions on Communications*, vol. 23, pp. 1417–1433, 1975.
- [9] D. Vassiss and G. Kormentzas, "Performance analysis of IEEE 802.11 ad hoc networks in the presence of exposed terminals," *Elsevier Ad hoc Networks*, vol. 6, pp. 474–482, May 2008.
- [10] J. Yeo, M. Youssef, and A. Agrawala, "Characterizing the IEEE 802.11 traffic: The wireless side," University of Maryland, College Park, Tech. Rep. CS-TR-457, March 2004.