A Unified Approach to Error Protection in Medium Access Control Design

Guerino Giancola, Luca De Nardis, Maria-Gabriella Di Benedetto

Info-Com Department, University of Rome "La Sapienza"
Via Eudossiana, 18 – 00184, Rome, Italy
Ph: (+39) 0644585483 – Fax: (+39) 064473300 – E-mail: giancola@infocom.uniroma1.it

ABSTRACT

In this paper we address the problem of designing error protection mechanisms for Medium Access Control (MAC) protocols with Quality of Service (QoS) constraints. The analysis focuses on the typical case of Wireless Local Area Networks (WLANs) which are characterized by slowly time-varying channels. An analytical approach to efficient management of transmission, formalized as an optimization problem, is presented, and an algorithm for error protection and control for both real-time and non-real-time services is proposed.

I. INTRODUCTION

Two basic problems in the design of Medium Access Control (MAC) protocols with Quality of Service (QoS) are the efficient management of the resource, and the need for fulfilling QoS requirements despite the unpredictable behaviour of the channel. When the MAC is capable of adjusting error protection to the time-varying nature of the channel, the above problems can be strongly mitigated.

In this paper, we propose an analytical approach for selecting and designing error protection schemes for traffic sources requiring QoS. The paper is organized as follows. Section 2 illustrates error protection at the MAC level. Section 3 describes the reference scenario. Section 4 analyzes the connection between QoS and resource allocation. Section 5 describes the error protection algorithm. Finally, Section 6 contains the conclusions.

II. ERROR PROTECTION AT THE MAC LEVEL

In the realistic scenario of a channel which introduces errors on the transmitted units, mechanisms of either retransmission or error correction, or both, may be needed in the MAC in order to improve system efficiency ([1]-[3]).

Packet retransmission mechanisms ([4]), commonly indicated as Automatic Repeat on reQuest (ARQ), are based on the repetition of corrupted MAC Protocol Data Units (MACPDUs). Error detecting codes, such as a Cyclic Redundancy Check (CRC), are embedded in each transmitted data unit, and are used by the receiver to detect errors on incoming data packets. This approach however introduces delays which might be incompatible with real-time features.

Forward Error Correction (FEC) ([5]) introduces redundancy in each MACPDU. Here, no delays are introduced, but overhead is required with the drawback of an efficiency loss. In order to mitigate this loss FEC codes may be combined within ARQ mechanisms, giving rise to the so-called Hybrid ARQ ([6]).

III. REFERENCE SCENARIO

Each traffic source is characterized by two sets of parameters. The first, denoted *Tspecs*, collects parameters describing source traffic activity. The second, denoted *Qspecs*, contains QoS requirements. A complete traffic activity description allows best performance in resource allocation efficiency. In realistic scenarios however traffic description can be given only statistical and parametrical. *Tspecs* corresponds for example to the Dual Leaky Bucket (DLB) parameters described in [7], i.e. the peak rate of the flow p (bits), the average rate of the flow r (bits), the token buffer dimension b (bits), and the maximum source packet size M (bits). With reference to *Qspecs*, we characterize each source by two QoS parameters, i.e. the maximum tolerable end-to-end delay D_{MAX} in seconds, and the minimum percentage of packets F (0÷100) required at destination within D_{MAX}. Note that the same set of parameters is used for both real-time and non-real-time services, with no explicit reference to classes of traffic.

The proposed MAC protocol uses fixed-size MACPDUs of L_{PDU} bits, composed of a fixed-size *header* of L_H bits and a fixed-size *payload* of $L_P = L_{PDU} - L_H$ bits. The *header* contains the information used by the MAC for managing the transmission of a MACPDU. It may contain error detection codes such as CRC, but no FEC. The *payload* conveys bits originating from source packets segmentation, and redundancy bits eventually introduced by the FEC. The payload is therefore composed of two parts: a FEC field of L_{FEC} bits, and an effective payload for user data of $L_{EFF} = L_P - L_{FEC}$ bits. Note that while L_{FEC} and L_{EFF} may vary in different MACPDU, L_{PDU}, L_H, and L_P are fixed.

In order to avoid unnecessary re-transmissions which could affect simulation results a Selective Repeat ARQ strategy is implemented.

Resource allocation is based on the definition of a MAC frame of D_F secs. D_{sys} is the maximum delay introduced by the MAC for the transmission of a single MACPDU.

We assume a slowly time-varying channel characterized by a Bit Error Rate (BER) indicated by p_b. We also assume that the transmitter knows the exact value of p_b by estimation of the reverse channel. p_b is assumed to be constant within D_{MAX}. This assumption is valid only when considering slow-moving terminals. The introduction of a more realistic error model will be object of future work.

We discard incorrectable errors in the *header* field, and restrict the present analysis to error protection on the *payload*.

IV. QoS AND RESOURCE ALLOCATION

4.1 Capacity vs. Delay

For a given source activity model (i.e. for given *Tspecs*), the experienced delay D depends on the amount of capacity reserved by the MAC. When reserved capacity increases, the end-to-end delay decreases. In order to express this trade-off in analytical terms, we introduce two functions: the Capacity function $X(Tspecs,D)$ and the Delay function $\Delta(Tspecs,C)$.

The Capacity function $X(Tspecs,D)$ is the capacity in bit/s which is necessary for guaranteeing a maximum delay D to a generic source described by *Tspecs*. The Delay function $\Delta(Tspecs,C)$ evaluates the end-to-end delay when the MAC reserves the capacity C. If for example *Tspecs* are expressed in terms of DLB parameters, both the Capacity function and the Delay function can be derived based on [7], and write as follows:

$$\mathrm{X}(Tspecs,D)=\frac{p\cdot b-r\cdot M}{(D-D_{sys})\cdot(p-r)+b-M} \tag{1}$$

$$\Delta(Tspecs,C)=\left[\frac{p-C}{p-r}(b-M)+M\right]\cdot\frac{1}{C}+D_{sys} \tag{2}$$

Tspecs are used by the MAC for predicting the number of bits emitted by the source in a generic time interval, and based of this data for evaluating the minimum bit rate R_{min} which is necessary in order to avoid overflow of the source buffer. In the DLB case, R_{min} is equal to the token buffer rate r, i.e. to the average flow rate. The MAC operates by first assigning R_{min}, which in turn leads to the following delay:

$$D_0=\Delta(Tspecs,R_{\min}) \tag{3}$$

Qspecs however impose that D_0 be lower than D_{MAX} . In case $D_0>D_{MAX}$, the MAC understands that R_{min} is too low. The general rule for required capacity is therefore:

$$C=\mathrm{X}\left(Tspecs,\min\left\{D_{MAX},\Delta(Tspecs,R_{\min})\right\}\right) \tag{4}$$

Note that Eq.(4) does not contain any explicit differentiation between real-time and non-real-time traffic.

If however errors are present during transmission, Eq.(4) must be modified in order to take into account the presence of ARQ, i.e:

$$C=\mathrm{X}\left(Tspecs,\min\left\{D_{MAX}-N_R\cdot RTT,\Delta(Tspecs,R_{\min})\right\}\right) \tag{5}$$

where N_R represent the maximum number of retransmissions of the ARQ, and RTT the estimated round-trip-time, i.e. the time necessary for the retransmission request plus the time needed for the retransmission of a MACPDU. According to Eq.(5), N_R must satisfy:

$$N_R\le N_R^{(\max)}=\left\lfloor\frac{D_{MAX}-D_{sys}}{RTT}\right\rfloor \tag{6}$$

where $\lfloor x\rfloor$ is the inferior integer part of x.

4.2 Capacity vs. Protection

In the design of an error protection mechanism at the MAC level, a first step is the conversion of F, i.e. the minimum percentage of source packets which should be correctly delivered within D_{MAX}, into a MAC parameter. The key point is that a source packet of L_A bits is segmented by the MAC into a set of $N_A=\lceil L_A/L_{EFF}\rceil$ MACPDUs, where $\lceil x\rceil$ is the superior integer part of x. The MAC module must translate the constraint imposed by F into a maximum MACPDU loss probability P_L.

When only FEC is present (i.e. no ARQ), the probability to receive a source packet free of errors becomes the probability to receive N_A MACPDUs with a tolerable amount of corrupted bits. In this case, one has:

$$P_L\le 1-\left(\frac{F}{100}\right)^{\frac{1}{\lceil L_A/L_{EFF}\rceil}} \tag{7}$$

Note that L_A in Eq.(7) can vary from packet to packet. For simplification we substitute to L_A the maximum source packet size M. M can be eventually found in *Tspec*s (as in the DLB case), but can also be dynamically estimated by the MAC in correspondance to each admitted source. Equation (7) rewrites:

$$P_L\le 1-\left(\frac{F}{100}\right)^{\frac{1}{\lceil M/L_{EFF}\rceil}} \tag{8}$$

If both FEC and ARQ are implemented, then larger P_L values can be tolerated. In particular, since each MACPDU is lost when (N_R+1) different transmissions are discarded at the receiver, the MACPDU loss probability becomes:

$$P_L\le\sqrt[1+N_R]{1-\left(\frac{F}{100}\right)^{\frac{1}{\lceil M/L_{EFF}\rceil}}}\triangleq\Pi(F,L_{EFF},N_R) \tag{9}$$

where N_R is limited by $N_R^{(MAX)}$ of Eq.(6). In Eq.(9) we assume independent and identically distributed errors on retransmissions.

The function $\Pi(F,L_{EFF},N_R)$ is the desired MAC parameter. The MAC can evaluate the necessity for the presence of an error protection mechanism on the basis of $\Pi(F,L_{EFF},N_R)$. Consider in fact a channel with a bit error rate p_b. In case of unprotected transmission each MACPDU would suffer the following packet loss probability:

$$P_E^{(MAX)}(p_b) = 1-(1-p_b)^{L_P} \tag{10}$$

The MAC establishes whether an error protection mechanism is needed by comparing Eq.(10) with the maximum tolerable MACPDU loss rate when the MAC has neither FEC nor ARQ as expressed by:

$$E_0(F) = \Pi(F, L_P, 0) = 1-\left(\frac{F}{100}\right)^{\frac{1}{\lceil M/L_P \rceil}} \tag{11}$$

If $P_E^{(MAX)} \leq E_0(F)$, meaning that the channel produces an average packet loss rate which is acceptable in terms of QoS fulfilment, all MACPDUs can be transmitted without any protection mechanism. $E_0(F)$ depends only on source and system parameters, and can be interpreted as a threshold for the introduction of error protection at the MAC level. In fact, for same p_b, some sources may require error protection while other sources may not. Figure 1 shows an example of average packet loss probability $P_E^{(MAX)}$ against different threshold values corresponding to sources with three F values (99, 99.99, 99.9999). In the proposed example, no error protection is needed for any of the sources when BER < $2\cdot10^{-10}$. When BER lays between $2\cdot10^{-10}$ and $2\cdot10^{-8}$, an error protection mechanism is necessary for the source with highest F only. When BER lays between $2\cdot10^{-8}$ and $2\cdot10^{-6}$, two sources require error protection. Finally, all sources require error protection for BER > $2\cdot10^{-6}$.

Once the MAC has established the necessity for an error protection, it must decide the FEC size as a function of the number of retransmissions N_R. In order to select a FEC size, the MAC first evaluates the maximum tolerable MACPDU packet loss rate, with no FEC (i.e. $L_{EFF}=L_P$), and N_R allowed retransmissions, expressed by:

$$E_1(F, N_R) = \Pi(F, L_P, N_R) = \sqrt[N_R+1]{1-\left(\frac{F}{100}\right)^{\frac{1}{\lceil M/L_P \rceil}}} \tag{12}$$

The MAC then compares $E_1(F,N_R)$ against $P_E^{(MAX)}$. The case $E_1(F,N_R) \geq P_E^{(MAX)}$ indicates that N_R retransmissions are sufficient for fulfilling the requirements with no need for FEC. Oppositely, when $E_1(F,N_R) < P_E^{(MAX)}$, a FEC scheme becomes necessary in order to increase MACPDU robustness against errors. For given channel condition (i.e. for a given p_b) and given N_R, the FEC must compensate the gap between $P_E^{(MAX)}$ and $E_1(F,N_R)$. The larger the gap, the larger the FEC size required by each MACPDU payload. An increase in L_{FEC}, however, corresponds to a decrease in the effective payload L_{EFF}, and a corresponding decrease in the maximum tolerable MACPDU loss rate $P_L^{(MAX)} = \Pi(F,L_{EFF},N_R)$ (see Eq.(9)) which is due to the increase in the number of MACPDUs needed for conveying the information. The modification of the FEC size aimed at filling up the gap between $P_E^{(MAX)}$ and $E_1(F,N_R)$, also has the effect of altering the required level of protection for each MACPDU. This problem can only be solved by means of an iterative algorithm.

If k indicates the maximum number of errors accepted by the FEC, and under the hypothesis of statistical independent errors, the MACPDU loss rate P_L is given by:

$$P_L = 1-\sum_{j=0}^{k}\binom{L_P}{j}\cdot p_b^{\,j}\cdot(1-p_b)^{L_P-j} \tag{13}$$

Equation (13) must be overturned in order to express the corrective capability k as a function of both bit error rate p_b and a target packet loss probability P_L. As shown in [8], this can be obtained as follows:

$$k = \mathrm{K}(p_b, P_L) = \left\lceil L_P \cdot p_b + erfc^{-1}(2\cdot P_L)\cdot\sqrt{2\cdot L_P\cdot p_b\cdot(1-p_b)}\right\rceil \tag{14}$$

where $erfc(x)$ is the complementary error function defined as:

$$erfc(x) = 1-\frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,dt \tag{15}$$

Once the corrective capability k is fixed, the MAC must evaluate the number of redundancy bits which must be introduced in the payload in order to guarantee such a level of protection. Since the FEC field length however depends on the particular FEC scheme, it is convenient to introduce the following unspecified function:

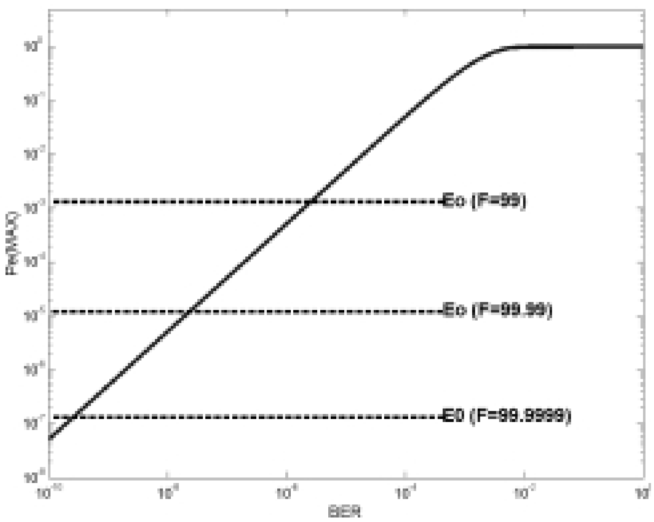

Figure 1 - $P_E^{(MAX)}$ vs. BER, and comparison with different thresholds values Eo corresponding to sources with three F values (99, 99.99, 99.9999) (L_P=512 bits, M=4096 bits)

$$L_{FEC} = \Lambda(k, L_P) \quad (16)$$

For a given packet size L_P, and for a requested corrective capability k, $\Lambda(k,L_P)$ determines the corresponding FEC field size L_{FEC} . Suppose for example a FEC scheme based on a Reed-Solomon code ([5]). One has:

$$\Lambda(k, L_P) = \min\left\{ 8 \cdot \left\lceil \frac{L_P}{8} \right\rceil, 16 \cdot k \right\} \quad (17)$$

According to Eqs.(14) and (16), in order to guarantee a packet loss probability P_L with a bit error rate p_b, the FEC size must be:

$$L_{FEC} = \Lambda[\mathrm{K}(p_b, P_L), L_P] \quad (18)$$

As observed above, we cannot proceed however by simply introducing $P_L^{(\mathrm{MAX})} = \Pi(F,L_{EFF},N_R)$ as expressed by Eq.(9) into Eq.(18). We propose thus an iterative algorithm based on successive approximations. This algorithm is parametrical in N_R and is initialized by estimating the current bit error rate p_b, which allows evaluation of $P_E^{(MAX)}$ as expressed in Eq.(10). If $P_E^{(MAX)} > E_0$ (see Eq.(11)), the MAC module proceeds with the selection of the error protection mechanism, else it transmits all PDUs without protection on the payload field. The first step for selecting the FEC size is comparing $P_E^{(MAX)}$ with $E_1(F,N_R)$ (see Eq.(12)). If $P_E^{(MAX)} \leq E_1(F,N_R)$, no FEC is required (i.e. $L_{EFF}=L_P$). Otherwise, i.e. $P_E^{(MAX)} > E_1(F,N_R)$, the following iterative steps are applied:

- step 1) The *new* packet loss probability nP_L is set equal to $E_1(F,N_R)$;
- step 2) The *old* packet loss probability oP_L is set equal to nP_L;
- step 3) The FEC size L_{FEC} is determined through Eq.(18) by considering oP_L as the target packet loss probability P_L;
- step 4) The effective payload length L_{EFF} is evaluated ($L_{EFF}=L_P-L_{FEC}$);
- step 5) According to Eq.(9), the new packet loss probability nP_L is given by $\Pi(F,L_{EFF},N_R)$;
- step 6) nP_L and oP_L are compared:

  - $nP_L \neq oP_L$ indicates that the maximum tolerable MACPDU loss rate $P_L^{(\mathrm{MAX})} = \Pi(F,L_{EFF},N_R)$ has been affected by the new FEC size. The procedure must be repeated from step 2) to step 6). The procedure converges thanks to the non-linear dependence on L_{EFF} of the function $\Pi(F,L_{EFF},N_R)$.
  - $nP_L = oP_L$ indicates that the FEC has been correctly designed.

Once the FEC size L_{FEC} is fixed, we can evaluate the effect of segmentation realized at the MAC layer. Because of the presence of both the MACPDU *header* and the FEC field, the capacity C given by Eq.(5) becomes:

$$C_{eff} = C \cdot \frac{\left\lceil \frac{M}{L_{EFF}} \right\rceil \cdot L_{PDU}}{M} \quad (19)$$

The final step consists in expressing C_{eff} in terms of the number N_{PDU} of MACPDU per frame which should be reserved for the source. This value can be expressed as follows:

$$N_{PDU} = \left\lceil \frac{C_{eff} \cdot D_F}{L_{PDU}} \right\rceil \cdot \left(1 + \Delta N_{ARQ}\right) \quad (20)$$

where the term ΔN_{ARQ} takes into account the average number of MACPDUs per frame which will be retransmitted by the ARQ mechanism. This term can be expressed as follows:

$$\Delta N_{ARQ} = \sum_{j=1}^{N_R} \left[\Pi(F, L_{EFF}, N_R)\right]^j \quad (21)$$

V. UNIFIED APPROACH TO ERROR PROTECTION

For a given number of allowed retransmission N_R, Eq.(20) expresses the required number of MACPDUs per frame for a source with *Qspecs* which generates traffic according to *Tspecs*. In order to optimize transmission efficiency, the MAC must simply select the value of N_R between 0 and $N_R^{(MAX)}$ leading to the lower N_{PDU} value. Note that the selection of N_R depends on the actual p_b value; The procedure should therefore be repeated at each observed bit error rate variation.

Performance of the proposed algorithm for two sources with different characteristics both in traffic activity and in QoS is presented. The following parameter values are adopted: L_P = 512 bits, L_H = 88 bits (i.e. L_{PDU} =600 bits), D_{sys} = 0.02 secs., D_F = 0.01 secs., RTT = 0.05 secs. For both sources, DLB parameters are used for *Tspecs*, and Reed-Solomon codes are used for the FEC.

The first source (*source A*) represents a typical real-time application and is characterized by the following *Tspecs*: p=64 Kbits/s, r =32 Kbits/s, M=*576* bits (i.e. M=72 bytes, as in the Voice over IP protocol), b=11.520 bits (i.e. b=20·M). With reference to *Qspecs*, *source A* requires D_{MAX}=0.1 secs. and F=99.9. According to Eq.(6), only one retransmission is permitted for *source A*. Figure 2 compares the required number of MACPDUs per frame corresponding to the case of only FEC and no ARQ, with the case of an hybrid ARQ, with one possible retransmission. We observe that the combined FEC+ARQ scheme with only one retransmission achieves best performance only when the BER is higher than $2 \cdot 10^{-2}$. Moreover, since Fig.2 considers only BER values which satisfy the condition $L_{FEC} \leq L_P$, we can also note that when the channel is worsening, it becomes necessary to introduce retransmissions in order to fulfil QoS constraints.

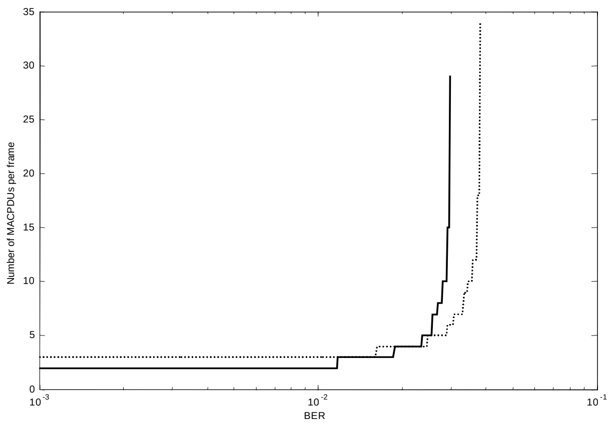

Figure 2 – N_{PDU} for source A corresponding to only FEC (solid line) and Hybrid ARQ with one possible retransmission (dotted line).

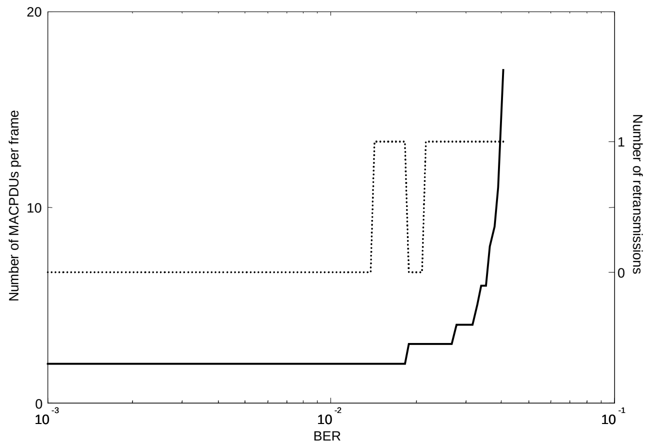

Figure 3 – N_{PDU} (solid line) and optimum number of retransmissions (dotted line) for source A.

Figure 3 shows results of application of the proposed algorithm when considering *source A*. For each BER value, transmission efficiency is optimized by selecting and dimensioning the error protection mechanism which minimizes N_{PDU}. When BER is between $2{\cdot}10^{-3}$ and $3{\cdot}10^{-3}$, the schemes with N_R=0 and N_R=*1* have about same performance: this justifies the peculiar pattern of the dotted line in Fig.3.

The second source (*source B*) is a high bit-rate and non-real-time application with the following *Tspecs*: *p*=1024 Kbits/s, *r* =768 Kbits/s, *M=4096* bits, b= 409600 bits (i.e. *b*=100·*M*). With reference to *Qspecs*, *source B* requires D_{MAX} =1 secs. and F=99.999999. According to Eq.(6), up to 20 retransmissions are permitted for *source B.* Figure 4 shows the results obtained, and highlights the need for a high number of retransmissions when p_b>10^{-3}.

VI. CONCLUSIONS

An analytical approach for selecting and designing error protection schemes at the MAC layer for traffic sources requiring QoS was proposed. The resulting algorithm maximizes transmission efficiency by selecting and dimensioning an error protection mechanism which takes into account both channel status and QoS constraints. The algorithm was tested for both real-time and non-real-time

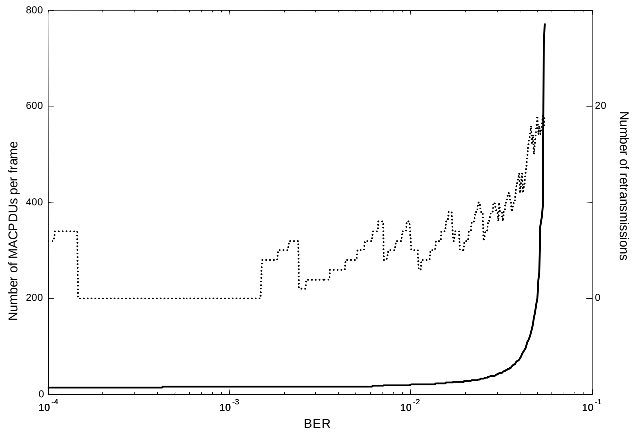

Figure 4 – N_{PDU} (solid line) and optimum number retransmissions (dotted line) for source B.

traffic sources. In both cases, results confirm that the algorithm is capable of optimizing resource allocation by adapting error protection to channel performance. In particular, we demonstrated the necessity of admitting re-transmissions of MAC protocol data units for higher BER values.

ACKNOWLEDGEMENTS

This work was supported by the European Union under Project No. IST-2001-32710: "Ultra-wideband Concepts for Ad-hoc Networks (U.C.A.N.)", and Project No. IST-2000-25197: "Whyless.com - The Open Mobile Access Networks"

REFERENCES

[1] Eckhardt, D.A.; Steenkiste, P.; *"Improving wireless LAN performance via adaptive local error control"*, in Proceedings of the Sixth International Conference on Network Protocols, 13-16 Oct 1998, Page(s): 327-338.

[2] Jeong-Hwan Seo; Hyun-Taek Oh; Seung-Woo Seo; *"A new MAC and DLC scheme considering channel conditions in wireless ATM*", Vehicular Technology Conference Proceedings, 2000, VTC 2000, Tokyo. 2000 IEEE 51st, Volume: 2, 2000, Page(s): 987-991 vol.2

[3] Peng Ge; McKinley, P.K.; *"Comparisons of error control techniques for wireless video multicasting"*, in Proceedings of the 21st IEEE International Conference on Performance, Computing, and Communications, 2002, Page(s): 93-102.

[4] Benice, R.; Frey, A., Jr.; *"An Analysis of Retransmission Systems"*, Communications, IEEE Transactions on, Volume: 12, Issue: 4, Dec 1964, Page(s): 135-145.

[5] M.Y. Rhee, "*Error-correcting coding theory"*, McGraw-Hill, 1989, Page(s). 319-325.

[6] Wicker, S.B.; *"An error control technique for high data rate communication networks"*, INFOCOM '89. Proceedings of the Eighth Annual Joint Conference of the IEEE Computer and Communications Societies., 23-27 Apr 1989, Page(s): 594-601 vol.2.

[7] White, P.P; *"RSVP and integrated services in the Internet: a tutorial",* IEEE Communications Magazine, vol. 35, May 1997, Page(s). 100-106.

[8] Giancola, G.; Falco, S.; Di Benedetto M.G.; *"A Novel Approach to Error Protection in Medium Access Control Design"*, in Proceedings of the 4th IEEE Workshop on Mobile and Wireless Communication Networks, MWCN2002, Sept. 2002, Page(s): 337-341.