Analysis of the Hidden and Exposed Terminal Effects in Wireless Networks with Cooperative ARQ

J. Alonso-Zárate*, L. Alonso**, G. Kormentzas***, and Ch. Verikoukis*

*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)
Av. Carl Friedrich Gauss, 7, CTTC, 08860, Castelldefels, Barcelona (Spain)
Email:[jesus.alonso, cveri]@cttc.es
**Dept. of Signal Theory and Comms., Universitat Politècnica de Catalunya (UPC)
Av. Esteve Terradas, 7, EPSC, 08860, Castelldefels, Barcelona (Spain)
Email: luisg@tsc.upc.edu
*** University of the Aegean
Email: gkorm@aegean.gr

Abstract. Cooperative Automatic Retransmission Request (C-ARQ) schemes allow those users which overhear a transmission to act as spontaneous relays when a packet has been received with errors at destination. When these users assist a source-destination pair in the retransmission process, the area exposed to the original transmission increases in comparison with non-cooperative ARQ schemes. In addition, the extension of the transmission time, due to the retransmissions, increases the vulnerability of a transmission to the hidden terminal problem. The paper provides a performance analysis of the hidden and exposed terminal effects in an 802.11-based wireless network where a C-ARQ scheme is executed at the Medium Access Control (MAC) layer. The presented analysis is supported by computer-based simulations.

1 Introduction

In this paper we analyze the hidden and exposed terminal problems in the context of Cooperative Automatic Retransmission Request (C-ARQ) schemes. When a C-ARQ scheme is executed at the Medium Access Control (MAC) layer, communication takes place in four steps whenever a data packet is received with unrecoverable errors at destination. First, the source transmits a data packet to the destination. Note that, due to the broadcast nature of the wireless channel, this transmission can be overheard by some of the stations within the transmissions range of the transmitter besides the intended destination. Second, the destination broadcasts a Call for Cooperation (CFC) packet. This packet invites all the potential helpers, i.e., those users which were able to decode the original

---

This work has been supported by NEWCOM++ (IST-216715), PASSENGER (PIEF-GA-2008-219561), and CENTENO (TEC2008-06817-C02-02).

transmission from the source, to assist in the transmission. Some of them become active relays (helpers) and a cooperation phase is initiated. In the third step, all the active relays attempt to assist the destination by retransmitting copies of the original transmission. These copies might be exact, recoded, compressed, or simply amplified versions of the original transmission [1]. Although the relays or helpers might transmit orthogonally in time, frequency, or code, we will focus on time-orthogonal retransmissions, which might have a simpler implementation. Finally, the destination attempts to combine the different independent copies of the original packet and acknowledges, either positively or negatively, the reception or reconstruction of the original packet. The cooperation phase is finished.

Several works in the literature have evaluated C-ARQ schemes from a fundamental point of view [2, 3, 4]. These works focus on the analysis at the PHY layer and usually assume simplified topologies with just one relay or in single-hop scenarios. These works have shown that C-ARQ can significantly increase the performance of wireless communications. However, still more work has to be done in upper layers of the protocol stack in the light of practical application of C-ARQ. This is the motivation for the main contributions presented in this paper, which are:

1. 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.
2. Evaluation of a practical case study wherein the relays of a C-ARQ scheme transmit orthogonally in time.

Extensive computer simulations have been carried out to assess the accuracy of the theoretical analysis and, for the practical implementation of the C-ARQ, we have focused our work on the Persistent Relay CSMA (PRCSMA) protocol first described in [5] and further analyzed in [6].

The rest of the paper is organized as follows. In Section II we explain the hidden and exposed terminal problems and we discuss them in the context of C-ARQ schemes. In Section III we analyze the utilization factor of a network executing a C-ARQ scheme at the MAC layer and taking into account both the hidden and the exposed terminal problems. In Section IV we conduct both numerical evaluation and computer simulations to assess the performance of a network in the presence of hidden and exposed terminals when a C-ARQ scheme is executed at the MAC layer. Finally, Section V concludes the paper.

2 Problem Statement and Discussion

The presence of hidden and exposed terminals in 802.11-based wireless networks has a direct impact on the performance of the communications. We evaluate in this paper how the execution of a C-ARQ scheme at the MAC layer modifies these two problems. The fact that the active relays become transmitters and receivers at some point in time forces us to revisit the hidden and exposed terminal effects on the overall performance of the network.

The first observation is that the vulnerability period of a transmission to a hidden terminal is extended if retransmissions are 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 but out of the range of the current transmitter. 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). In addition, it is worth observing that the relays can be hidden terminals for other third transmissions thus affecting the overall performance of the network. The increase of the offered load including retransmissions must be taken into account when evaluating the effects of the hidden terminals.

Regarding the exposed terminal problem, it has to be noted that 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 exposed terminal problems within the context of a C-ARQ scheme. We first consider the operation of the network without C-ARQ and we then discuss how the execution of a C-ARQ scheme with time-orthogonal relays modifies the analysis.

3 Throughput Analysis

3.1 Scenario and Definitions

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 (including those performed by the relays). 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 of the network as

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

where U_{LOS} is the throughput of a network wherein all the stations are in the transmission range of each other (Line Of Sight, LOS) and e_2 is the throughput reduction factor due to the collisions caused by hidden terminals. For convenience and in order 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

$$U_{LOS} = \frac{S}{B+I}. \tag{2}$$

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. The computation of the terms S, B and I can be found in [7].

3.2 Throughput with Hidden Terminals

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

$$e_2 = \left[\frac{I}{B+I} p^{T_s/\tau}\right]^{N-1}, \tag{3}$$

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 farther than r from the transmitter and can thus 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

$$N = \rho\pi\left(2r\right)^2/\rho\pi r^2 = 4. \tag{4}$$

3.3 Throughput with Exposed Terminals

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

$$U = U(g) + U(g_e). \tag{5}$$

In this expression, g_e represents the additional data traffic rate (packets per second) that would be transmitted in the network if the exposed terminal problem was solved. In order to compute this, let us 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

$$\beta = \left(\frac{B}{B+I}\right)(1-p)\left(\frac{E_2}{E}\right) \tag{6}$$

of additional transmissions will occur in the medium simultaneously with ongoing transmissions and without incurring in a collision. The fraction $E2/E$ represents the ratio of the number of terminals exposed to an ongoing transmission to the total number of terminals in the transmission range of a transmitter. This terms has be derived in [7] and is equal to 0.42.

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 later in Section 4 where some numerical evaluation is performed.

3.4 Throughput Analysis with C-ARQ

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

$$T_s' = T_s(1-p_e) + (T_s + T_{COOP})\,p_e, \tag{7}$$

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, denoted by T_s. However, in the case of an 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, and as mentioned before, it is necessary to consider that the vulnerability period for any transmission is longer, as $T_s' > T_s$ if $p_e \neq 0$.

In addition, 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

$$\beta' = \beta(1-p_e) + \beta_{C-ARQ}\,p_e. \tag{8}$$

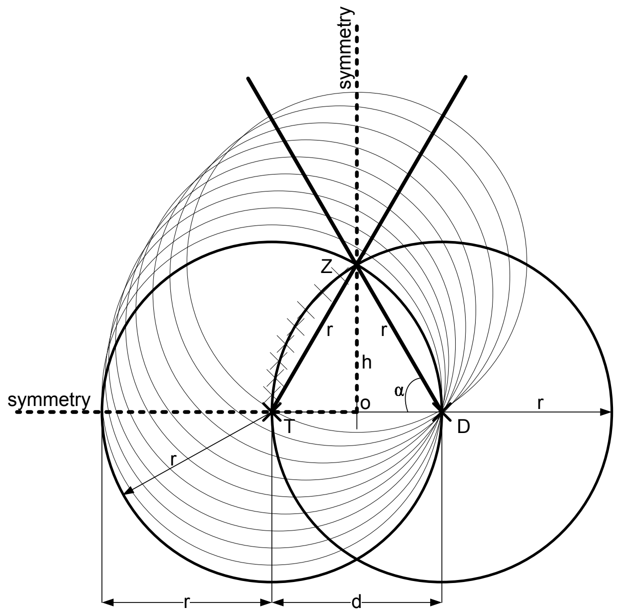

Fig. 1. Exposed Area (description)

The value of β is the same as the one computed with (6). 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 $E2$. To proceed with this analysis we support our discussion with Fig. 1.

In this figure we consider that station T is transmitting a packet to a destination D, located 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.2. 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

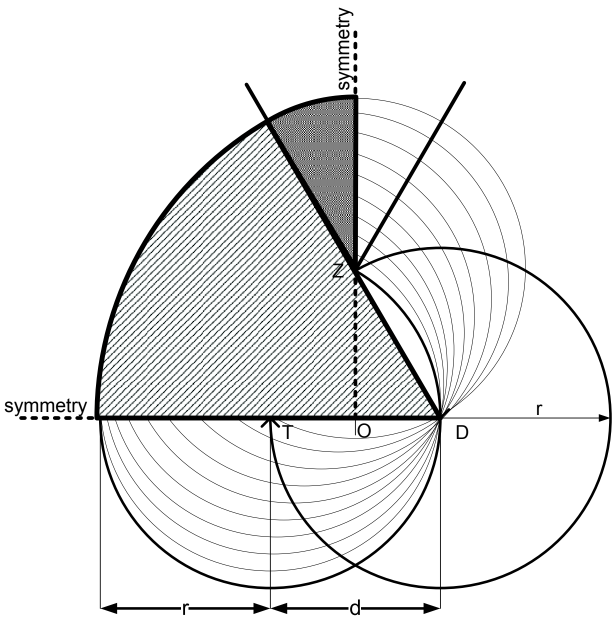

Fig. 2. Exposed Area (calculation)

$$E_{C-ARQ} = 4\left[A_s(r+d,\alpha) + A_s(r,\frac{\pi}{2}-\alpha) - A_t\right]. \tag{9}$$

$A_s(a,b)$ 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

$$A_t = \left[(d/2)\, r\sin(\alpha)\right]/2. \tag{10}$$

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 was solved can be expressed as

$$\beta_{C-ARQ} = \left(\frac{B}{B+I}\right)(1-p)\left(\frac{E_{C-ARQ}}{E}\right). \tag{11}$$

With this value it is possible to compute the value of β' in (13) and thus 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, also supported by computer simulations.

4 Performance Evaluation

4.1 Scenario

In this section we evaluate the performance of two different ad hoc IEEE 802.11 scenarios:

1. An homogeneous layout where a number of $M = 5$ users are in LOS conditions and, according to (4), a total of $4M = 20$ terminals are located in the surroundings of these users, homogeneously distributed. In this scenario we assume that the RTS/CTS handshake is able to completely solve the hidden terminal problem so that we can focus on the analysis on the exposed terminal problem.
2. The same scenario as before, but considering 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 the impact of the presence of exposed stations in a network is.

We have used the theoretical analysis presented in the previous section and we have also supported the results with simulations carried out with a C++ simulator. The simulator executes the protocol rules without using any of the theoretical expressions presented in this paper. In all cases, the average packet error probability has been fixed to $p_e = 0.5$ for the transmission of data and $p_e = 0$ for control packets due to the use of the most robust coding and modulation scheme used for the control plane. The channel between the relays and the destination is assumed to be error-free as we assume that the active relays are very close to the destination. Although any other value could be used, we assume that exactly two successful retransmissions from the relays are required to attempt to decode the original packet at destination. Regarding the offered load to the network, we assume a homogeneous traffic distribution (all the stations contribute equally to the total offered load) and generate Poisson traffic with parameter g and thus

$$\begin{aligned} p &= \tfrac{(g\tau)^0}{0!}e^{-g\tau} = e^{-g\tau}, \\ p_1 &= \tfrac{(g\tau)^1}{1!}e^{-g\tau} = g\tau e^{-g\tau}, \\ \beta' &= 1 - e^{g_e\tau} => g_e = \tfrac{-\ln\left(1-\beta'\right)}{\tau}. \end{aligned} \tag{12}$$

The length of data packets has an exponential distribution with average 1500 bytes. According to [9], these are the size and distributions that better represent the data traffic of a WLAN. The rest of the parameters for both analysis and simulation are summarized in Table 1.

For each scenario, two ARQ schemes are compared:

1. Plain ARQ, if retransmissions are requested from the original source station.
2. C-ARQ, if retransmissions are requested from a number of relays which overheard the original transmission.

Table 1. 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

For the execution of the C-ARQ, we consider that the relays use the Persistent Relay CSMA (PRCSMA) protocol described in [5] (and further analyzed in [6]) to gain access to the channel. For completeness we review the operation of PRCSMA in the following subsection.

4.2 PRCSMA Overview

PRCSMA is a protocol designed to coordinate the retransmission of the relays in a C-ARQ scheme. Whenever a destination receives a data packet with errors, it broadcasts a CFC packet. All the users which overheard the original transmission and receive this CFC packet become active relays and contend to get access to the channel in order to assist the destination. The operation of PRCSMA is essentially based on the rules of the IEEE 802.11 MAC protocol, except for the two following modifications:

1. The relays perform a backoff right after receiving the CFC broadcast by the destination asking for cooperation. This initial backoff is necessary to avoid a certain collision among all the relays willing to cooperate.
2. The relays do not expect any ACK for each retransmission as they are not the original source of the transmitted packet. Therefore, the overhead associated to the retransmissions can be reduced.

The closed-form equation to compute the value of T_{COOP} in (7) within the context of PRCSMA can also be found in [5] and [6].

4.3 Results

The throughput, as defined in (1), is plotted in Fig. 3. The first observation is the good match between the model and the simulations. Simulation results always show a slightly better throughput than those obtained with the theoretical analysis. This is due to the assumption made in the theoretical analysis by which we always consider the worst case in terms of exposed terminal area. Recall that in the analysis we assumed that the destination is always located at the edge of the transmission range of the source and that the relays are placed at the edges of the intersection of the transmission ranges of the source and the destination.

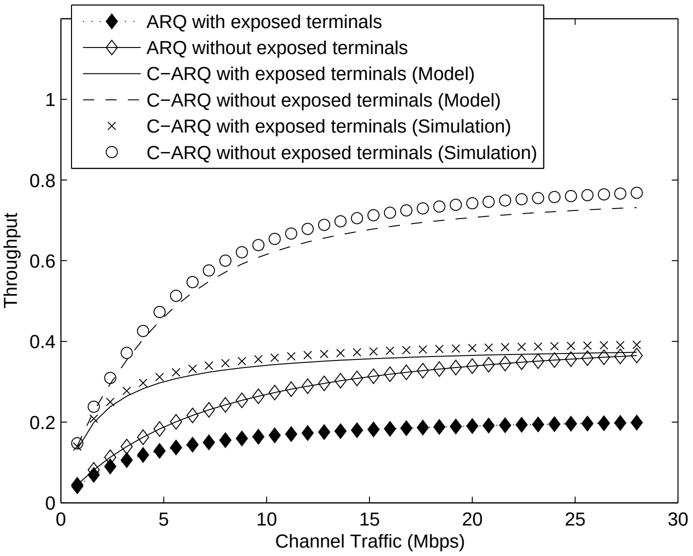

Fig. 3. Throughput

However, the results obtained through simulation show that the approximation in the theoretical model is fairly accurate, as the difference between model and simulation is always below 5%.

In terms of the exposed terminal problem, it is possible to see that there is a remarkable difference between the performance of a network with and without exposed terminals. In fact, this difference becomes more outstanding in the cooperative case, where, as expected, the area exposed to the transmissions is larger.

Therefore, 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). Note that, as shown in Fig. 3, the performance of network with C-ARQ could be improved in up to 100% if the exposed terminal problem could be solved. This will be our motivation for future work.

5 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.

The hidden terminal problem remains almost unaltered except for the fact that the longer transmission times, due to retransmissions, are more vulnerable to potential hidden terminal transmissions. On the other hand, both numerical evaluation and computer simulations show that the C-ARQ scheme 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 cooperation.

Future work will be aimed at extending this model to include the theoretical model of PRCSMA in the analysis and at designing 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, Oct. 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, Jan. 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, Apr. 2008.
5. J. Alonso-Zárate, 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, Dec. 2008.
6. J. Alonso-Zárate, C. Verikoukis, and L. Alonso, “Performance analysis of a persistent relay carrier sensing multiple access protocol,” *IEEE Transactions on Wireless Communications*, pp. 5827–5831, Dec. 2009.
7. D. Vassis 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.
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. J. Yeo, M. Youssef, and A. Agrawala, “Characterizing the IEEE 802.11 traffic: The wireless side,” University of Meryland, College Park, Tech. Rep. CS-TR-457, Mar. 2004.