Design of an Effective Loss-Distinguishable MAC Protocol for 802.11 WLAN

Qixiang Pang, Soung C. Liew, *Senior Member, IEEE,* and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*— In the IEEE 802.11 WLAN standard, the backoff algorithm assumes that all losses are due to collisions, while the auto-rate fallback algorithm assumes that all losses are due to link errors. The coexistence of these two types of losses in real networks reduces the efficiency of currently used algorithms. We propose a loss-distinguishable MAC layer protocol for 802.11 WLAN. No PHY layer modification is needed. Analysis shows that the new protocol is effective and has negligible overhead.**

***Index Terms*— IEEE 802.11, WLAN, MAC, protocol, loss distinguishing**

I. Introduction

CURRENT products implementing the IEEE 802.11 WLAN standard do not distinguish between frame losses due to collisions or link errors. For example, in 802.11 DCF [1], if the ACK frame in response to a data frame is not received, the sender assumes that the data frame has suffered a collision and doubles its contention window. The rationale is that a collision indicates a contention intensity higher than originally expected. However, in a wireless environment, the unsuccessful delivery of the data and ACK frames can also be caused by transmission errors over the wireless link. The assumption that all frame losses are due to collisions is not always true. If a frame is lost because of a random link error instead of a collision, doubling the contention window is inappropriate and could seriously degrade performance. Unnecessarily backing off when there are link errors will leave much of the airtime unused. When different stations experience different frame error rates (FER), fairness could be an issue too.

Another example of this problem is the Auto-Rate-Fallback (ARF) algorithm first proposed by Lucent in its WaveLAN-II product to accommodate different channel conditions [2]. ARF or its variants have been widely implemented in WLAN products. In ARF, the sender detects the channel condition by measuring the numbers of successful and failed transmissions, and adjusts its data rate to transmit the following data frames accordingly. In contrast to the assumption behind the standard backoff algorithm, ARF assumes all packet losses are due to link errors. When multiple stations coexist in a WLAN and collisions occur often, the ARF algorithm loses its validity.

In a real WLAN environment, the two types of losses can coexist. Without a way to distinguish the causes of the losses, the 802.11 WLAN may function improperly.

Manuscript received December 29, 2004. The associate editor coordinating the review of this letter and approving it for publication was Dr. Christos Douligeris. This work was supported by the the AoE scheme established under the University Grant Committee of Hong Kong (Project Number AoE/E-01/99) and the NSERC of Canada through grant STPGP 257684-02.

Qixiang Pang and Victor C. M. Leung are with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada. Soung C. Liew is with the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong.

Digital Object Identifier 123456789

II. Loss-distinguishable MAC Protocol

We enhance both the basic and RTS/CTS access procedures in the 802.11 WLAN standard with loss-distinguishing capability.

A. Loss Distinguishing in RTS/CTS Access Procedure

The RTS/CTS access procedure is optional in 802.11 WLANs. It is useful when the data frame size is very large, the number of stations is very large or there are hidden terminals.

The following loss distinguishing method in the RTS/CTS access procedure is straightforward and the 4-way message exchange sequence is not changed: (i) If both the CTS and then the ACK frames are received, the transmission is successful. (ii) If the CTS frame is received but the ACK frame is not, the transmission has failed, most likely due to a link error. (iii) If the CTS frame is not received, most likely a collision has occurred. Because RTS and CTS are short frames usually transmitted at a low rate, they usually have a low FER.

B. Loss Distinguishing in Basic Access Procedure

The basic access is the default access procedure and it is more efficient when there is no hidden terminal. However, the loss distinguishing method for the basic access is not so straightforward. The original basic access procedure does not provide enough feedback information for the sender to determine the reason of a frame loss. To distinguish the two types of losses, we propose to add a NAK control frame to DCF. The definition and usage of NAK here are slightly different from those in conventional protocols.

The loss distinguishing method is based on the following observation. The MAC data frame can be partitioned into two functional parts: the header and payload. The header contains information such as frame type, source address and destination address. If all stations in a WLAN BSS are close enough and can hear one another, collision occurs only when two or more stations send data frames in the same time slot. In this case, both the header and body will be corrupted. The receiver can neither receive the header nor the payload. Note that the air propagation time in a WLAN BSS (<2 μs) does not violate the validity of this statement since the transmission time of the PHY header is 192 μs and the MAC header is as long as

RECEIVER

- *If receiver receives correct MAC header:*
  - *If MAC body is correct, an ACK is sent back;*
  - *If MAC body is wrong, a NAK is sent back;*
- *If wrong MAC header is received, the receiver sends nothing.*

SENDER

- *If an ACK is received, the transmission is successful;*
- *If a NAK is received, a link error is assumed;*
- *If nothing is received, a collision is assumed.*

Fig. 1. Loss distinguishing using NAK control frame in basic access

112 μs at a 2 Mbps data rate in 802.11b [3].

If only one station sends a data frame and the frame is lost due to link errors, there is a good chance that the receiver will receive the header correctly. This is because in general the header is much shorter than the whole frame. By observing the content of the header, we can obtain information on who has sent the frame and who is the intended receiver.

When a link error occurs, a proper feedback message from the receiver will enable the sender to find out what has happened. We use the NAK frame to notify the sender that the data frame transmission has failed due to a link error. Fig. 1 describes the loss distinguishing method for the basic access procedure using the NAK frame.

The NAK frame can be implemented with exactly the same structure as the ACK frame except for a one-bit difference in the frame type field in the header. NAKs are sent at the same data rate as that for ACK transmissions.

Note that when there is a link error, the transmission of a NAK does not consume more bandwidth or collide with other frames at all because it occupies the time that would have been used by an ACK transmission. In the 802.11 standard, if a station receives a correct frame, it determines from the Duration field in the frame how long the frame and its ACK will occupy the channel, and it defers channel access accordingly. On the other hand, if a station receives an erroneous frame, according to the standard it must wait an Extended Inter-Frame Space (EIFS) time before its backoff timer starts to count down. The transmission times of an SIFS, an ACK frame, and a DIFS are already included in EIFS [1].

Although the header error rate (HER) is low in general, to further reduce it and the mis-delivery ratio of data frames as well, a Header Checksum Field (HCF) can be added into the data frame. This concept is borrowed from the Header Error Control (HEC) field in ATM cell header [4].

III. Overhead and Effectiveness Analysis

We use 802.11b as an example. The notations and parameter values used in this letter are given in Table I.

A. Overhead Analysis

The header checksum field results in an extra overhead in the new loss-distinguishable MAC protocol.

The total channel occupation time of a data frame includes the transmission times of the data frame and its ACK or NAK frame plus DIFS and SIFS. In the standard 802.11 MAC protocol, the total channel occupation time is given by

$$T_{std} = \left(PHY + \frac{MAC + Payload}{DataRate}\right) + \left(PHY + \frac{ACK\_NAK}{BasicRate}\right) + DIFS + SIFS \quad (1)$$

In the new loss-distinguishable protocol, it is given by

$$T_{new} = \left(PHY + \frac{MAC + HCF + Payload}{DataRate}\right) + \left(PHY + \frac{ACK\_NAK}{BasicRate}\right) + DIFS + SIFS \quad (2)$$

The overhead attributed to the HCF is therefore given by

$$Overhead = \frac{T_{new} - T_{std}}{T_{std}} \quad (3)$$

As seen in Table II, the shorter the payload, the bigger the overhead. Even in the worst case (2-byte *HCF*, 1-byte *Payload* and *DataRate* is same as *BasicRate*), the overhead is only about 1%. In realistic cases, the overheads are negligible.

TABLE I

Notations and parameter values of 802.11b

Notations	Descriptions	Values
MAC	MAC ovehead (header and checksum of data frame) in standard	224 bits
HCF	MAC header checksum field size	1 or 2 bytes
DIFS	the time of DIFS	50 μs
SIFS	the time of SIFS	10 μs
ACK_NAK	ACK or NAK frame size	112 bits
RTS	RTS frame size	160 bits
CTS	CTS frame size	112 bits
PHY	overhead at physical layer	192 μs
DataRate	physical rate for data frame	
BasicRate	physical rate for control frame	
Payload	MAC layer payload size	
BER	bit error rate	
HER	header error rate	
AER	ACK error rate	
NER	NAK error rate	
RTSER	RTS error rate	
CTSER	CTS error rate	
BoER	data frame body error rate	
FER	data frame error rate	

B. Effectiveness Analysis

The effectiveness of the loss distinguishable MAC protocol depends on the correct acquisition of header information and NAK for basic access and RTS/CTS frames for RTS/CTS access. The probability of misunderstanding a collision loss to be a link error loss (P_{ctoe}) is 0%. In cases of link errors, the loss distinguishing is probabilistic.

For RTS/CTS access, when either RTS or CTS frame is lost due to link errors, the sender will misunderstand it as a collision loss. Therefore the probability of misunderstanding a link error loss to be a collision loss (P_{etoc}) is

$$P_{etoc} = RTSER + CTSER - RTSER \times CTSER \quad (4)$$

For basic access, when a data frame is lost due to link errors, in the following two cases, the sender will not be able

TABLE II

OVERHEADS IN BASIC ACCESS WHEN *DataRate=BasicRate*

header checksum field	1-byte payload	100-byte payload	500-byte payload	1000-byte payload
1-byte	0.649%	0.395%	0.165%	0.087%
2-byte	1.299%	0.791%	0.306%	0.173%

to get a NAK correctly and thus misunderstand the loss to be a collision loss: (i) the header of the data frame is erroneous and therefore the receiver does not generate a NAK; (ii) the header is correct and NAK is generated but the NAK frame is erroneous. When a data frame is successfully delivered but the corresponding ACK is lost due to a link error, the sender will also misunderstand it as a collision loss. Therefore the probability of misunderstanding a link error loss to be a collision loss is

$$P_{etoc} = \frac{HER + (1-HER) \times BoER \times NER}{FER + (1-FER) \times AER} + \frac{(1-FER) \times AER}{FER + (1-FER) \times AER} \quad (5)$$

The success probabilities are then given by $1 - P_{ctoe}$ and $1 - P_{etoc}$ respectively.

Three sizes of payloads are examined: small payload (*Payload*=100 bytes), medium payload (*Payload*=500 bytes) and large payload (*Payload*=1000 bytes). The values of *HER*, *BoER*, *FER*, *NER*, *RTSER*, and *CTSER* are determined by their *BERs* and lengths respectively assuming an AWGN channel model.

The numerical results in Table III and Table IV show that the distinguishing probabilities under various cases are high and thus the proposed loss-distinguishable MAC protocol is effective. This can be attributed to the fact that the control frames and the data frame headers are in general much shorter than the data frames. Under an AWGN environment, they experience much smaller error rates than the data frame. We assigned the same value to *DataRate* and *BasicRate* in Table III and Table IV, therefore these tables give the lowest success probabilities. In most cases, *BasicRate* is smaller than *DataRate*; therefore the success probabilities are higher and the protocol is more robust and efficient.

For the basic access procedure, there is still room to further increase the probability of successful detection. To make the header information more reliable, either a FEC scheme or a lower transmission rate for the header can be used. The simplest FEC scheme is to repeat the header a number of times, as in Bluetooth [5]. Transmission at a lower rate is more error-resistant when the SNR is the same, e.g., the BER at 2 Mbps is only about 1% of that at 11 Mbps [6][7][8].

IV. CONCLUSION

To our knowledge, this letter is a first attempt to address the loss distinguishing issue in IEEE 802.11 WLANs, especially for the basic access procedure. The proposed loss distinguishing method does not modify the PHY layer and therefore it is easy to implement. Numerical analysis shows that its overhead is trivial and the loss distinguishing effectiveness is high.

TABLE III

EFFECTIVENESS ANALYSIS OF LOSS DISTINGUISHING IN RTS/CTS ACCESS (*DataRate=BasicRate*)

BER	1e-5	5e-5	1e-4	5e-4
RTSER	0.002	0.008	0.016	0.077
CTSER	0.001	0.006	0.011	0.054
1-P_{etoc}	99.7%	98.6%	97.3%	87.3%
1-P_{ctoe}	100%	100%	100%	100%

TABLE IV

EFFECTIVENESS ANALYSIS OF LOSS DISTINGUISHING IN BASIC ACCESS (*DataRate=BasicRate*, 1-BYTE *HCF*)

BER	1e-5	5e-5	1e-4	5e-4
HER	0.002	0.010	0.019	0.092
AER	0.001	0.006	0.011	0.054
NER	0.001	0.006	0.011	0.054
FER(small payload)	0.010	0.050	0.098	0.403
FER(medium payload)	0.041	0.191	0.345	0.880
FER(large payload)	0.079	0.337	0.561	0.984
1-P_{etoc} *(small payload)*	73.3%	72.9%	72.3%	67.6%
1-P_{etoc} *(medium payload)*	92.9%	92.3%	91.5%	84.1%
1-P_{etoc} *(large payload)*	96.2%	95.6%	94.7%	85.7%
1-P_{ctoe}	100%	100%	100%	100%

The loss distinguishing capability newly introduced in this letter brings much freedom to the design of new algorithms. For examples, the standard backoff algorithm can be improved by doubling the backoff timer only when a collision loss is detected. The ARF algorithm can be improved to reduce the data rate only when a link error loss is detected. Some preliminary simulation results have shown that these improvements to the backoff algorithm and the ARF algorithm can increase throughput significantly.

Our focus in this letter is an MAC layer solution to the loss distinguishing issue. It is possible to further enhance loss distinguishing by integrating physical layer information, such as SNR and RSS values of the received frames (either successful or erroneous). We have considered only an AWGN environment in this letter. When link errors are bursty, more thorough solutions may rely on physical layer enhancements and cross-layer design. This is left as future work.

REFERENCES

[1] IEEE Std 802.11-1999, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," Jun. 2003.
[2] A. Kamerman, L. Monteban, "WaveLAN-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs Technical Journal*, vol.2, no.3, pp.118-133, Aug. 1997.
[3] IEEE Std 802.11b-1999, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher-speed physical layer extension in the 2.4 GHz band," Sep. 1999.
[4] ATM Forum, "ATM user-network interface specification V3.0," Sep. 1993.
[5] IEEE Std 802.15.1, "Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)," Jun. 2002.
[6] IEEE Std 802.15.2, "Coexistence of wireless personal area networks with other wireless devices operating in unlicensed frequency bands," Aug. 2003.
[7] T.S. Rappaport, *Wireless Communications: Principles and Practices*, Prentice Hall, 1996.
[8] J.G. Proakis, *Digital Communications*, McGraw-Hill, 1995.