Journal of ELECTRICAL ENGINEERING, VOL 71(2020), NO5, 365–367

sciendo

COMMUNICATIONS

Fair MAC protocol for IEEE 802.11 wireless LANs with hidden node problem

Woo-Yong Choi

In IEEE 80211 wireless LANs, hidden nodes can disrupt the backoff algorithm of other nodes that are located outside the physical carrier sensing range of hidden nodes. The fairness problem between the nodes that are vulnerable and not vulnerable to the hidden node problem is dealt with in this paper. We propose an efficient fair MAC protocol to resolve the fairness problem.

K e y w o r d s: wireless LAN, MAC, hidden node problem, fairness problem

1 Introduction

To satisfy the rapidly growing demand of wireless data delivery, advanced wireless LAN systems, such as IEEE 802.11 n and 802.11 ac, have been developed and deployed in hotspot environment [1,2]. The interference from moving objects and humans significantly degrades the transmission signal of nodes [3]. The hidden node problem and the fairness problem between the nodes that are vulnerable and not vulnerable to the hidden node problem are worsened by the interference from moving objects and humans. In the literature, the fairness problem that is caused by the hidden node problem has been addressed [4,5]. In [4], the authors developed a mathematical model to capture the effect of the hidden node problem on the MAC throughput and the fairness among nodes. A new PHY protocol and power control mechanism was proposed to eliminate the hidden node problem in [5]. However, the dynamic nature of the hidden node problem has not been considered to develop a MAC protocol for resolving the fairness problem in infrastructure IEEE 802.11 wireless LANs [4,5].

In this paper, to resolve the fairness problem that is caused by the hidden node problem, we propose an efficient fair MAC protocol that adjusts contention windows of the DCF (Distributed Coordination Function) protocol according to the dynamic nature of the hidden node problem. In the proposed MAC protocol, to capture the dynamic nature of the hidden node problem, AP (Access Point) collects the physical carrier sensing information among nodes and the information of whether each node is active (that is, has data to transmit) or not during CFPs (Contention-Free Periods) by polling each node and receiving the response frames. AP piggybacks on the polling frames two-bit information of whether or not each recipient of the polling frames is vulnerable to the interference from active hidden nodes, and whether or not each recipient is a hidden node. AP broadcasts beacon frames that contain new contention windows for the backoff algorithm of the nodes that are not vulnerable to the hidden node problem. The fairness problem can be resolved by dynamically increasing contention windows for the nodes that are not vulnerable to the hidden node problem, and having other nodes use legacy contention windows.

2 Proposed fair MAC protocol

According to the standard of IEEE 802.11 wireless LANs, CFPs and CPs (Contention Periods) are alternated with each other [6]. AP polls nodes to grant transmission opportunities according to the PCF (Point Coordination Function) protoco

While AP polls node i and node i responds with data frame or null frame (if node i has no data to transmit) during CFPs, other nodes can obtain the MAC address of node i by the reception of the polling frame, and determine whether or not the response transmission signal of node i can be heard by the physical carrier sensing. Therefore, during the course of APs polling and each nodes responding, each node i can maintain the set S_i of the MAC addresses of other nodes the transmission signal of which can be heard by the physical carrier sensing. We implicitly assume that the carrier sensing information is symmetric, that is, if node i can hear node j, then node j can hear node i. AP can efficiently collect the physical sensing information S_i8217 s among nodes by having each node i piggyback the change of S_i on the response frames. A similar method was employed for APs collecting the physical carrier sensing information among nodes in [7]. Furthermore, AP can detect that node i is active (or inactive) if node i transmits the response data frame

Department of Industrial and Management Systems Engineering, Dong-A University, Nakdong-daero, Saha-gu, Busan, Korea, wychoi77@dau.ac.kr

DOI:10.2478/jee-2020–0050, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

Table 1. Values of PHY parameters

Parameters	Values
Transmission rate	6.5 Mbps
RTS, CTS and ACK transmission rate	6 Mbps
SIFS	16 μs
PIFS	25 μs
DIFS	34 μs
Time slot	9 μs
Max. backoff stage	7
PHY header trans. length	20 μs

(or null frame). We assume that all nodes should transmit data or null frames when they are given transmission opportunities by AP. If a polled node transmits no response frame continuously, AP can disassociate the node with itself. Let us denote the sets of the MAC addresses of all nodes associated with AP and active nodes by S and S_a, respectively. Then, AP can derive for each node i the set H_i of the MAC addresses of active hidden nodes that can disrupt the backoff algorithm of node i and the set G_i of the MAC addresses of inactive hidden nodes as follows

$$H_i = \{j \in S | i \notin S_j\} \cap S_a, G_i = \{j \in S | i \notin S_j\} \cap \overline{S}_a. \quad (1)$$

AP piggybacks on the polling frame destined for node j one-bit information of whether or not node j is vulnerable to the hidden node problem, that is, whether or not H_j is nonempty. Furthermore, AP piggybacks on the polling frame for node j one-bit information of whether or not node j is a hidden node, that is, whether or not node j belongs to one of Hi' s and G_i's. All nodes that were informed to be vulnerable to the hidden node problem or to be hidden nodes should transmit their data frames through the reservation scheme based on RTS (Request to Send) and CTS (Clear to Send) frames during CPs. Other nodes can optionally use the reservation scheme to increase their MAC performance.

Let us assume that node i has $|H_i| (> 0)$ active hidden nodes, and currently performs the backoff algorithm with contention window CW. Node $j \in H_i$ can disrupt the backoff algorithm of node i by attempting to transmit RTS frame during the period from T_j, which is the number of time slots for the transmission of RTS frame of node j, before the end of backoff period of node i to T_i, which is the number of time slots for the transmission of RTS frame of node i, after the end of backoff period. This has the effect of extending the contention window of node i. Using the renewal theory in [8], the probability that the number of time slots for the residual life of backoff period and the transmission of RTS frame of node i is less than or equal to $T_i + T_j$ can be obtained by

$$p_{i,j} = \frac{T_j(2\ CW - T_j + 1) + 2(CW + 1)T_i}{(CW + 2\ T_i)(CW + 1)}. \quad (2)$$

The transmission rates of RTS frame of nodes i and j can be estimated by the previous transmission rates of RTS frames of nodes i and j. If the previous transmission rates of RTS frames are not available to AP, T_i and T_j can be estimated as the rates in basic rate set that are closest to the previous transmission rates of the response frames of nodes i and j during CFPs. Assuming the independent interference of $|H_i|$ hidden nodes to the backoff algorithm of node i, the probability that the backoff algorithm of node i is interfered by any hidden node can obtained by

$$p_i = 1 - \prod_{j \in H_i} (1 - p_{i,j}). \quad (3)$$

Due to the hidden node problem, the contention window of node i is, on the average, extended to

$$CW_{\text{new}} = (1 - p_i)CW + p_i(CW + T_i) = CW + p_i T_i. \quad (4)$$

AP broadcasts beacon frames that contain the positive integer closest to the average of CW'_{new}s of the nodes that are vulnerable to the hidden node problem for each backoff stage. New contention windows are used for the backoff algorithm of the nodes that are not vulnerable to the hidden node problem. The nodes that are vulnerable to the hidden node problem use legacy contention windows for their backoff algorithm.

3 Simulation results

We assume that in a circular service area, $n = 100, 200, 8230, 500$ of IEEE 802.11 n nodes continuously attempt to transmit data frames to AP, and 20% of nodes are located in boundary area and are hidden nodes. Due to the interference of moving objects and humans, each node that is located in boundary area suffers from the hidden node problem, and is vulnerable to the interference from 5% of other boundary nodes.

We experimented three MAC transmission methods during CPs, which are the DCF protocol without the reservation scheme based on RTS and CTS frames, the DCF protocol with the use of the reservation scheme for all uplink data transmissions and the fair MAC protocol proposed in the previous section of this paper. The size of user payloads that are included in data frames is fixed to 5.000 bits. To see the maximized performances of three MAC transmission methods under the hidden node problem, data transmissions are assumed to fail only when two or more transmissions collide. For each case of three MAC transmission methods and $n = 100, 200, 8230, 500$, simulation was conducted during 2×10^8 time slots. The values of PHY parameters that are assumed for simulation experiment are shown in Tab. 1. The values of PHY parameters were also used in [3].

We compare overall average throughputs per node of three transmission methods for each n in Fig. 1 where the DCF protocol with the reservation scheme and the proposed MAC protocol are shown to have far better overall throughputs than the DCF protocol without the reservation scheme. The DCF protocol with the reservation scheme and the proposed MAC protocol have very similar overall throughputs. In Fig. 2, for the DCF protocol with the reservation scheme and the proposed MAC protocol, we present relative difference between average throughputs per nodes that are vulnerable and not vulnerable to the hidden node problem with respect to overall throughputs per nodes. From Fig. 2, compared with the DCF protocol with the reservation scheme, our proposed fair MAC protocol is shown to reduce relative difference between the throughputs of nodes that are vulnerable and not vulnerable to the hidden node problem. Our proposed MAC protocol reduces, on the average, about 22% of relative difference compared with the DCF protocol with the reservation scheme.

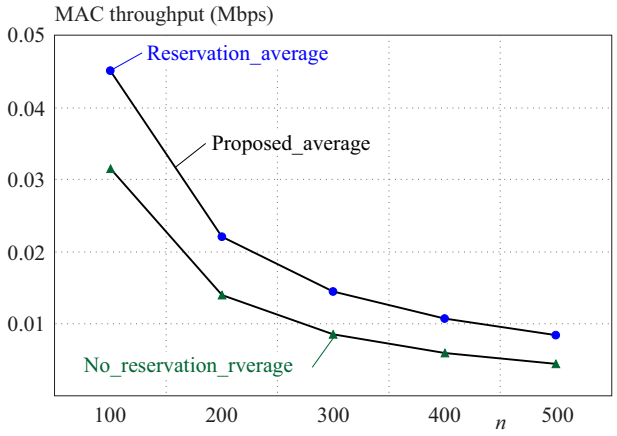

Fig. 1. Overall MAC throughput per node

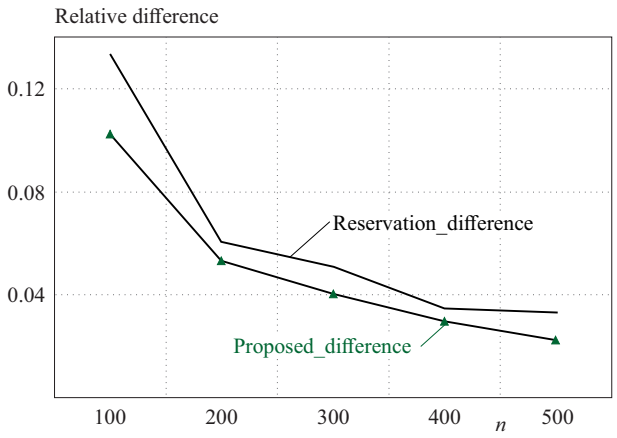

Fig. 2. Throughput difference of vulnerable and nonvulnerable nodes

4 Conclusions

We proposed a new fair MAC protocol for IEEE 802.11 wireless LANs to resolve the fairness problem between nodes that are vulnerable and not vulnerable to the hidden node problem. To provide fair access to wireless medium for nodes, we dynamically adjust contention windows for the backoff algorithm of nodes that are not vulnerable to the hidden node problem having other nodes use legacy contention windows. Simulation results show that our proposed MAC protocol significantly improves the fairness among nodes compared with the DCF protocol with the reservation scheme.

Acknowledgements

This work was supported by the Dong-A University research fund.

References

[1] IEEE Std 802.11n,"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Throughput", *IEEE Press*, 2009.

[2] IEEE Std 802.11ac,"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Enhancements for Very High Throughput for Operation in Bands Below 6 GHz", *IEEE Press*, 2013.

[3] W.-Y. Choi,"Efficient MAC Protocol for IEEE 802.11 Wireless LANs with Obstructing Objects", *Journal of Electrical Engineering* vol. 70, pp. 486 488, 2019.

[4] O. Ekici and A. Yongacoglu,"Fairness and Throughput Performance of Infrastructure IEEE 802.11 Networks with Hidden-Nodes", *Physical Communication* vol. 1, pp. 255 265, 2008.

[5] L. B. Jiang and S. C. Liew,"Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks", *IEEE Transactions on Mobile Computing* vol. 7, pp. 34 49, 2008.

[6] IEEE, "IEEE Wireless LAN Edition", *IEEE Press*, 2003.

[7] W.-Y. Choi,"Clustering Algorithm for Hidden Node Problem in Infrastructure Mode IEEE 802.11 Wireless LANs", *Proc. of IEEE ICACT* 2008, pp. 13351338, 2008.

[8] S. M. Ross, *Stochastic Processes* John Wiley & Sons, 1996.

Received 20 June 2020

Woo-Yong Choi was born in Busan, Korea 1970. He received the BS, MS and PhD degrees in industrial engineering from POSTECH in 1992, 1994 and 1997, respectively. From 1997 to 2001 he was a senior member of technical staff at Hyundai Electronics Industries Co., Ltd.. From 2001 to 2005 he was a senior member of technical staff at ETRI. Since 2005 he has been with Department of Industrial & Management Systems Engineering at Dong-A University, where he is currently a full tenured professor.