Performance Evaluation 87 (2015) 60–73

Contents lists available at ScienceDirect

Performance Evaluation

journal homepage: www.elsevier.com/locate/peva

Per-node throughput and fairness analysis of IEEE 802.11 wireless networks with hidden nodes

Myung Woo Lee [a], Ganguk Hwang [a,*], Sumit Roy [b]

[a] Department of Mathematical Sciences and Telecommunication Engineering Program, KAIST, Daejeon, Republic of Korea

[b] Department of Electrical Engineering, University of Washington, Seattle, USA

ARTICLE INFO

Article history:
Available online 30 January 2015

Keywords:
Per-node throughput
Fairness
IEEE 802.11 DCF
Hidden node problem

ABSTRACT

This work seeks to develop an analytical model for the per-node throughput analysis of IEEE 802.11 WLAN networks with *hidden nodes* by extending Bianchi's model. With the analytic model we derive the per-node throughput of each node and quantify the impact of hidden nodes on per-node throughput. Through our analysis, we find that nodes having more hidden nodes are likely to have worse throughput performance than nodes having less hidden nodes, so resulting in unfairness in per-node throughput.

We next propose a new algorithm, called the fake collision algorithm, to solve the unfairness due to hidden nodes. The proposed fake collision algorithm allows nodes with poor throughput to acquire more transmission opportunities by slightly modifying the Binary Exponential Backoff algorithm of the IEEE 802.11 Distributed Coordination Function. To this end, the fake collision algorithm uses a new control parameter called the fake collision probability which can be obtained from a computation algorithm that we develop based on our analytic model. We show that the fairness in per-node throughput can be achieved with the fake collision probability for each node through simulation.

1. Introduction

Performance of Distributed Coordination Function (DCF) protocol for the IEEE 802.11 WLANs has been well analyzed, starting with the seminal work of Bianchi [1]. However, the limitations of this train of analysis is well-known, notably its lack of inclusion of 'hidden' nodes [2]. If two (source) nodes N_1, N_2 are outside the carrier sensing range[1] of each other, N_1 may initiate a transmission to a common receive node, while it is already receiving a packet from N_2, resulting in a packet collision.

The hidden node problem is commonplace in dense, infrastructure 802.11 networks [4,5]. In addition, obstacles such as walls or partitions, lead to additional hidden nodes. Thus it is most desirable to improve analytical estimates of 802.11 network performance by incorporating hidden nodes.

We have two main objectives in this work. The first is to develop an analytic model that provides improved estimates of 802.11 network in the presence of hidden nodes. To this end we extend Bianchi's model [1] as described next. In Bianchi's model, the state of a node is observed at slot times, called embedded epochs from now on, where the backoff counter of the node is decremented by one or refreshed. Assuming that the collision probability of a node is constant, the backoff counter

* Corresponding author. Tel.: +82 423502714; fax: +82 423505710.
E-mail addresses: guhwang@kaist.edu (G. Hwang), roy@ee.washington.edu (S. Roy).

[1] The carrier sensing range is the range inside which the received signal power at any receive node exceeds a sensing threshold value [3]. Any nodes that lie within the same carrier sensing range of each other, cannot transmit simultaneously.

http://dx.doi.org/10.1016/j.peva.2015.01.002
0166-5316/

and the backoff stage at each embedded epoch form a two dimensional discrete time Markov chain (DTMC). The performance of the IEEE 802.11 DCF is then analyzed by using the stationary distribution of the DTMC. It is assumed in Bianchi's model that the network does not have any hidden nodes, so that all embedded epochs of all nodes in the network are *almost* synchronized and hence the use of a single DTMC suffices for analysis. However, in the presence of hidden nodes, the embedded epochs of nodes are not well synchronized, i.e., a node may decrease its backoff counter when a hidden node transmits or freezes its backoff counter. To capture such characteristics of the hidden node problem, we consider *different DTMCs for different nodes* and compute the collision probability of each node in a completely different way, distinct from Bianchi's model. As a result, we compute the per-node throughput of each node separately, that in turn allows us to investigate network *unfairness*. As expected, if a node has more hidden nodes than others, the per-node throughput of the node worsens relatively. In addition, we see that 802.11 WLANs with RTS/CTS enabled perform better than WLANs with basic access mode as reported in [6,7], so it is recommended to use the RTS/CTS mode in the presence of hidden nodes. We validate our analytic model through simulation by using different types of network topologies both in the basic access mode and in the RTS/CTS mode. The per-node throughputs from simulation and our analytic model are compared, and we see that our analytic results are well matched with the simulation results.

Our second objective is to mitigate the unfairness problem in per-node throughput due to hidden nodes. By observing the reasons underlying the unfairness, e.g., the nodes with more hidden nodes have less transmission opportunities than those with less hidden nodes, we propose a new algorithm, called the *fake collision algorithm*, where the nodes with more hidden nodes are allowed to acquire more transmission opportunities than in the Binary Exponential Backoff (BEB) algorithm. To this end in the fake collision algorithm, when a node transmits its packet successfully, it stochastically *increases* its backoff stage by one according to the fake collision probability, thereby falsely mimicking a packet collision. More details are given in Section 3. Obviously, the higher the fake collision probability of a node, the less transmission opportunities it has. The fake collision probability thus acts a control parameter. We develop a computation algorithm to obtain the fake collision probability for each node that can achieve given feasible target ratios in per-node throughput. It is anticipated that introduction of the fake collision probabilities will cause a degradation in network throughput, but we show through simulation that this degradation is negligible.

Several works have attempted to modeling the hidden node problem [8–12]. The performance under unsaturated traffic condition is considered in [8,9]. In [8], all nodes are assumed to have the same number of hidden nodes, a clearly impractical scenario. Uplink and downlink throughputs are analytically derived in [9], but they do not consider the unfairness problem. In [10] the authors consider a special case where the number of nodes in the carrier sensing range is the same as the number of hidden nodes and investigate the throughput performance in the presence of hidden nodes. To solve the unsynchronization problem caused by hidden nodes (i.e., while a node transmits its packet, its hidden node still decreases its backoff counter) in the mathematical modeling, a new DTMC is proposed where embedded epochs are extended to all time points with fixed interval in [11]. [12] categorizes the collisions induced by a hidden node based on the packet transmission times of the hidden node. Most of previous studies investigate network throughput but per-node throughput is not investigated. In this paper, we propose a mathematical model to analyze the per-node throughput and this is essential to investigate fairness in per-node throughput.

Fairness issue in the hidden node problem is studied in [13–21]. In [13], the fairness problem when the packet length is variable is investigated in ad hoc networks and a new algorithm is proposed to achieve fairness in the case. In [14,15] they solve the hidden and exposed nodes problem by using power control algorithms. The fairness issues in the performance of the TCP protocol in ad hoc networks with the IEEE 802.11 DCF is considered in [16–18], and the performance of the UDP protocol in ad hoc networks with the IEEE 802.11 DCF is also studied in [19]. The unfairness in the three-flow problem is studied in [20] and its generalization is done in [21]. In [22] they propose two protocols to design fair and efficient MAC protocols in ad hoc networks which is immune to difficult topology configuration such as the hidden node problem. Previous studies on fairness consider ad hoc networks, but the current use of IEEE 802.11 is mostly in infrastructure networks. Moreover the probability of the presence of hidden nodes is high in infrastructure networks because of the widespread use of smartphones, laptop computers, etc. To the best of our knowledge, our work is the first to deal with fairness in per-node throughput in an infrastructure network and to propose an algorithm to solve the unfairness problem.

The organization of this paper is as follows. In Section 2, we develop an analytic model to analyze the per-node throughput of the IEEE 802.11 DCF infrastructure network with hidden nodes. We validate our analytic model through simulation and investigate the per-node throughput and fairness of the IEEE 802.11 WLAN in the presence of hidden nodes. In Section 3, the fake collision algorithm is proposed to mitigate unfairness due to hidden nodes. In Section 4, we give our conclusions.

2. System model

We consider an IEEE 802.11 infrastructure network with a single Access Point (AP). There are N nodes in the network including the AP. All nodes always have packets to transmit and use a single transmission rate. In the infrastructure network, we assume that all nodes except the AP always transmit their packets (such as RTS (Request-To-Send), CTS (Clear-To-Send), data packets, etc.) to the AP for communication, i.e., there are no direct communications between nodes except the AP. We do not consider the capture effect [23] in this paper, so any simultaneous transmissions by nodes always result in collision.

In this paper, we consider two transmission modes—the basic access mode and the RTS/CTS mode. While a winning node (backoff counter reaches 0) transmits its data packet in the basic access mode, a node first transmits an RTS packet in the