Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computer Communications 28 (2005) 1179–1192
computer communications
www.elsevier.com/locate/comcom

Performance of wireless networks with hidden nodes: a queuing-theoretic analysis

Saikat Ray*, David Starobinski, Jeffrey B. Carruthers

Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA

Received 21 July 2004; accepted 21 July 2004
Available online 11 September 2004

Abstract

Hidden nodes are a fundamental problem that can potentially affect any wireless network where nodes cannot hear each other. Although the hidden node problem is well known, so far only few papers have quantified its effects in a comprehensive manner. This paper represents a first step towards getting a quantitative insight into the impact of hidden nodes on the performance of wireless networks. We first carry out an exact queuing-theoretic analysis for a 4-node segment and derive analytical expressions for the probability of packet collision, the mean packet delay, and the maximum throughput, based on a model that closely follows the IEEE 802.11 standard. We then extend the analysis and provide an approximation for a general linear topology that is asymptotically exact at low load. Finally, we perform detailed simulations to validate our analytical results and show their applicability to predict the performance of IEEE 802.11 networks with hidden nodes. The simulation and analysis closely match. Moreover, they reveal that the impact of hidden nodes propagates through the network causing some nodes to saturate at load as low as 15% of the capacity.

Keywords: IEEE 802.11; Hidden nodes; Collision probability; Delay analysis; Maximum throughput analysis

1. Introduction

In recent years, IEEE 802.11 standard wireless local area networks (WLANs) have rapidly gained popularity and become the solution of choice for networking homes and campuses [1]. These, networks use a variant of carrier sense multiple access (CSMA) to control channel access by the nodes [2].

In CSMA, a node is allowed to transmit a packet only if it senses the channel idle. Packet collisions are rare as long as nodes can hear each other and the propagation delay is small. However, in wireless networks, nodes often cannot hear each other. Such networks are then likely to suffer from the so-called *hidden* node problem. This problem is illustrated in Fig. 1. In this topology, node C cannot hear node A's transmissions. However, if node C transmits while node A is transmitting, node A's packet will collide. Node C is the hidden node in this case. Note that this logical topology may in fact represent more complex networks; we provide an example in Section 3.1.

Since hidden nodes cause packet collisions, their presence can severely affect the performance of wireless networks. As a matter of fact, the author of Ref. [3] considers the hidden node problem to be one of the 'top ten challenges' in future wireless architectures. Although some hidden node mitigation techniques do exist, such as the *RTS/CTS* mechanism, they incur significant overhead and are often not used [4–6]. In the IEEE 802.11 standard, for instance, the *RTS/CTS* mechanism is only optional. Thus, in practice, wireless networks are often exposed to the hidden node problem. As wireless networks proliferate, it is therefore, vital to analyze and accurately quantify the impact of hidden nodes on network performance; not only to help understand the behavior of current networks, but also to help design future networks.

Although the hidden node problem is well known, few papers so far have been devoted to evaluating its impact on network performance. Instead, most previous works have

* Corresponding author. Tel.: +1 617 358 0533; fax: +1 617 353 6440.
E-mail addresses: saikat@bu.edu (S. Ray), staro@bu.edu (D. Starobinski), jbc@bu.edu (J.B. Carruthers).

0140-3664/$ - see front matter
doi:10.1016/j.comcom.2004.07.024

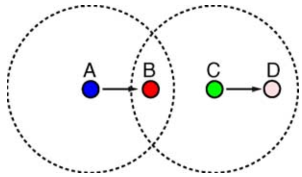

Fig. 1. Packet collision due to a hidden node. If nodes A and C transmit simultaneously, node A's packet will collide.

focused on hidden node mitigation techniques, see [7] and references therein. We describe some of the main related work in Section 2.2. In particular, we find that analytical models developed in previous work do not capture queuing and retransmission effects and oftentimes lead to inaccurate performance evaluation or trivial solutions (such as a single node capturing the channel).

This paper contributes to the fundamental understanding of how hidden nodes impact wireless networks. Our analytical models closely follow the IEEE 802.11 standard, and take into account queuing and retransmissions at each node. We first consider elementary 4-node topologies and derive *exact* expressions for (i) the probability of packet collision, (ii) the average packet delay, (iii) and the maximum throughput. We then extend the analysis to a general linear topology by iteratively applying the results obtained for the elementary topology. Although this extended analysis is provably exact only at low load, our simulations show that it remains fairly accurate over a wide range of load values. Using the NS simulator, we also show that our analysis predicts the performance of IEEE 802.11 networks with hidden nodes in a remarkably accurate fashion. Both the analysis and simulation reveal an interesting propagation effect which causes the nodes in the linear network to saturate at offered traffic load of as low as 15% of the (isolated) capacity, even though each node shares the channel with only one other node. This effect is reminiscent of influence-propagation phenomena observed in the context of multi-rate wireless networks [8].

This paper is organized as follows. In Section 2, we provide the relevant background on the IEEE 802.11 protocol necessary for understanding this paper and discuss related work. In Section 3, we describe our model and notation. As a motivation, we also present a simple analysis that ignores queuing and retransmission dynamics and show its limitation. Then, in Section 4 we present the main results of this paper. In particular, analytical expressions for the probability of packet collision, maximum throughput, and mean packet delay for an elementary 4-node topology are provided in Sections 4.1, 4.2 and 4.3, respectively, and an extension of these results to a general linear topology is presented in Section 4.4. Several of the more technical proofs are deferred to Section 5. We then present simulation results in Section 6, and conclude the paper in Section 7.

2. Background

2.1. Outline of the IEEE 802.11 basic access method

In this section, we describe some of the salient features of the IEEE 802.11 Wireless LAN protocol that are most relevant to the rest of this paper. The protocol is described in detail in Ref. [1].

The IEEE 802.11 MAC protocol supports two types of access mode: *point coordination function* (PCF) and *distributed coordination function* (DCF). The DCF mode is more commonly used.

The DCF mode is essentially equivalent to CSMA. A node transmits a *DATA* packet if it senses the channel to be idle. The receiver, upon receiving an error-free packet, returns an *Acknowledgment* (*ACK*) packet. If no *ACK* packet arrives in response to a *DATA* packet, the packet is retransmitted. The maximum allowed number of retransmissions is in general quite large. For instance, the default setting is 16 in Cisco aironet cards [9]. The retransmissions are separated by *backoff intervals*, which are integer multiples of *BackoffSlotTime*. The *BackoffSlotTime*, 20 μs, is a small fraction of the transmission time of a *DATA* packet (e.g. a 1500 byte packet takes about 12×10^3 μs when transmitted at 1 Mb/s rate). Therefore, in most cases, an unsuccessful transmission is retransmitted within a short amount of time.

The DCF mode also supports the optional *RTS*/*CTS* handshake that is designed to mitigate the hidden node problem. Since we are interested in quantifying the impact of hidden nodes in this paper, we will assume that nodes do not use this method, as it is often the case in practice.

2.2. Related work

The CSMA protocol was introduced by Kleinrock and Tobagi in Ref. [2]. The authors also noted the hidden node problem, and proposed an alternate protocol, called the *busy tone multiple access* (BTMA) in Ref. [10]. In these papers, the analysis of the protocols has been carried out under the assumption that 'the interarrival times of the point process defined by the start times of all the packets plus retransmissions are independent and exponentially distributed'; i.e. those form a Poisson process. This assumption is referred to as a 'random-look' assumption since Poisson arrivals see time-averages (the so-called PASTA property) [11]. Many subsequent papers use the same assumption as a basis for their analysis, e.g. [12–14] which propose various improvements over the basic CSMA/BTMA and [15] which point out the possible existence of hidden nodes in infrastructure mode WLAN.

The 'random-look' assumption might be reasonable when the average retransmission delay is large compared to the packet transmission time. However, in the IEEE 802.11 standard, the retransmission delay is small compared to the packet transmission time. Thus, one should not expect