Throughput Analysis of IEEE 802.11 Distributed Coordination Function in Presence of Hidden Stations

Shahriar Rahman *

Abstract

This paper investigates saturation and finite load throughputs of distributed coordinated function (DCF) as specified IEEE 802.11 wireless local area network (WLAN) protocol in presence of hidden stations. To study throughput of IEEE DCF, we extend Tobagi and Kleinrock's hidden terminal model [1] and incorporate it into Bianchi's Markov model of DCF [2]. We use the latter model to derive a general analytical model for DCF that may be used to find throughput under various traffic loads. We show that this model can take hidden stations in static environments into account and provides limited results in dynamic environments where wireless stations may move arbitrarily. The analytical model and throughput results are validated against simulations using direct sequence spread spectrum (DSSS) physical layer (PHY) and wireless media access layer (MAC). Simulations show that analytical results are valid under the assumed conditions.

Keywords: wireless, local area network, 802.11, CSMA, throughput, saturation, finite-load, hidden node

1 Introduction

1.1 Motivation

Recent advances in wireless technology have enabled portable devices with wireless capabilities that allow network communication even while a user is in motion. To deal with this wireless connectivity need, various wireless communication Standards have been developed [2]. IEEE has standardized PHY and MAC layers for WLANs through 802.11 workgroup. IEEE 802.11 standard has emerged as the leading WLAN protocol today. This protocol has two medium access methods. The mandatory *distributed coordination function* (DCF) method and the optional *point coordination function* (PCF) method. Both of these methods provides time bounded services. DCF is an asynchronous data transmission function, which best suits delay insensitive data (e.g. email, ftp). It is available for both infrastructure and ad hoc configurations and it can be either used exclusively or in combination with PCF in an infrastructure network (PCF is only available in infrastructure networks).

The "hidden node problem" is well known in wireless networks where two communicating nodes can communicate with a third station, but cannot directly communicate with each other due to physical or spatial limitations. The presence of hidden nodes may result in significant network performance degradation. It also causes unfairness in accessing the medium because a station's location may imply a larger transmission privilege. The root of the problem is that a station causes interference as it fails to detect the existence of a transmission from another station and thus assumes that the medium is free and available to transmit. CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) scheme, which is commonly used in Ethernet networks, alleviates this problem by explicitly detecting collisions on the medium. CSMA/CA (*CSMA with Collision Avoidance*) cannot detect collisions as wireless radios are half-duplex and cannot transmit while they are receiving and vice-versa. Therefore, CSMA/CA schemes try to avoid collisions using schemes similar to DCF.

1.2 Problem Definition

We define our problem with an example (Figure 1). Suppose, stations A and B are within the communication range of each other and station C is within communication range of station B, but not of A. Therefore, it is possible that both stations A and C could try to transmit to station B at the same time causing a collision. A and C are said to be hidden from each other forming a "hidden node pair". The collision causes both stations to defer their transmissions until the medium is sensed free again. The number of retransmissions in presence of hidden nodes may be indeterminate. Extending the three station example

*Stanford University, Department of Electrical Engineering, Stanford CA USA 94305. Tel/Fax: 408-307-6282/526-6875 Email: sirahman@stanford.edu

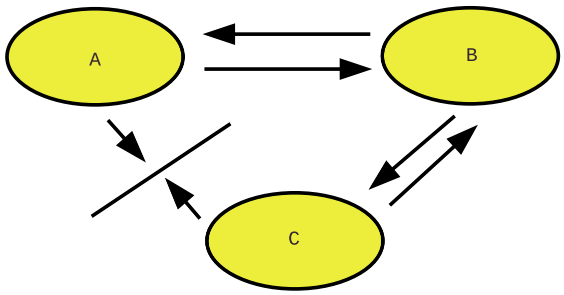

Figure 1: Hidden node problem

to a larger network, one may observe that as the number of hidden node stations increases, loss in network throughput suffers immensely [6].

The center of our problem is to quantify the loss of throughput of 802.11 DCF under basic CSMA access mechanism. Though there exist a number of works based on simulations (e.g. [4], [6]), we believe it is possible to find network throughput analytically when hidden nodes are present in either a static or a dynamic environment. Validation of the analytical model provides practical throughput figures under these conditions.

The goal of our work is to develop an analytical model of saturation and finite load throughputs of 802.11 DCF in presence of hidden nodes in static and dynamic environments and validate it through simulations.

1.3 Related Works

The two areas of relevent works are: 1) IEEE 802.11 DCF research and 2) hidden station modeling in CSMA/CA.

Several researchers [2], [3], [4] have studied the efficiency of the IEEE 802.11 protocol by investigating the maximum throughput that can be achieved under various network configurations. They analyze the backoff mechanism and propose alternatives to the standard mechanisms in order to improve performance. Bianchi in [2] presents a simple analytical model to compute saturation throughput performance assuming a finite number of stations and ideal channel conditions. [3] extends the same model and takes into account the frame retry limits, which predicts throughput of 802.11 DCF more accurately. However, there is no known work which looks into finite load throughput of 802.11 DCF and that takes protocol parameters such as various timeouts into account.

Tobagi and Kleinrock in [1] had proposed a framework for modeling hidden terminals in CSMA networks. Let $i = 1, 2, ... , M$ index the M terminals. An MxM square matrix H $= [m_{ij}]$ is used to model hidden terminals, where the m_{ij} entry is as follows-

$$m_{ij} = \begin{cases} 1 & \text{if stations } i \text{ and } j \text{ can hear each other} \\ 0 & \text{otherwise} \end{cases}$$

Since stations that hear the same subset of the population behave similarly, stations with identical rows or columns are said to form groups. This framework is extended in [5] to accurately predict interference resulting from presence of hidden terminals. Khurana, et. al. incorporates both hidden terminals and mobility of wireless stations into throughput calculations in [6]. Their study shows that delay increases significantly in presence of hidden terminals; using RTS/CTS helps mitigate the effect of hidden terminals. However, this study lacks any analytical study to accurately predict throughput and concentrates on the effects of hidden terminals and mobility on throughput and stations blocking probability through simulations only.

1.4 Our Contribution

The two main contributions of our work are-

1. An analytical model based on Bianchi's original model of 802.11 DCF with station retry limits that accurately predicts finite load throughput incorporating *ACK-timeout* and *CTS-timeout* parameters.

2. An analytical model that incorporates presence of hidden terminals in static and dynamic environments for saturation and finite load throughput calculations.

Rest of the paper is organized as follows. Section 2 provides background on IEEE 802.11 protocol with emphasis on DCF, Bianchi's model and saturation throughput models. Section 3 models hidden stations in static environments and in presence of station mobility. Section 4 presents our models for saturation and finite load throughputs in presence of hidden stations. Section 5 captures some simulation results from *ns-2* that provide model validation and finally, discussions and conclusion appear in Section 6.

PHY	*Slot size*	*Window size*
FHSS	50 μs	16-1024
DSSS	20 μs	32-1024
IR	8 μs	64-1024

Table 1: Slot time, minimum/maximum contention window od different PHYs [2]

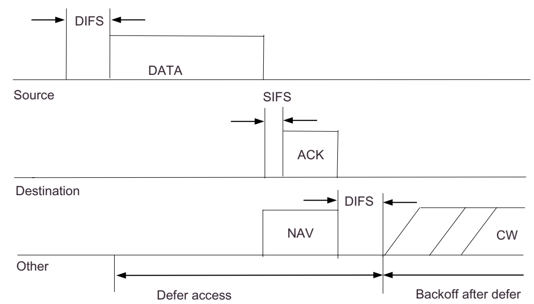

Figure 2: Basic access mechanism of 802.11 DCF

2 Background

2.1 IEEE 802.11 DCF Primer

This section briefly summarizes 802.11 DCF as it is specified by IEEE 802.11 MAC. For a more complete specification, refer to [7]. A station with a new packet to transmit monitors the channel activity. If the channel is idle for a period of time equal to a *distributed interframe space* (DIFS), the station transmits. If the channel is sensed busy (either immediately or during the DIFS), the station monitors the channel until it is measured idle for a DIFS. The station generates a random backoff interval before transmitting (this is the Collision Avoidance feature of the protocol). This minimizes the probability of collision with packets being transmitted by other stations. In addition, to avoid channel capture, a station must wait random backoff time between two consecutive new packet transmissions, even if the medium is sensed idle in the DIFS time with an exception when fragmentation is used. Fragmentation is a mechanism provided by protocol to split a *MAC service data unit* (MSDU) to multiple *MAC protocol data units* (MPDU) when the side of the MSDU exceeds the maximum payload size.

DCF employs a discrete-time backoff scale. The time immediately following an idle DIFS is slotted, and a station is allowed to transmit only at the beginning of each slot time. The slot time size, σ, is set equal to the time needed at any station to detect the transmission of a packet from any other station. As shown in Table I, it depends on the physical layer, and it accounts for the propagation delay, for the time needed to switch from the receiving to the transmitting state (*RX-TX-Turnaround-Time*), and for the time to signal to the MAC layer the state of the channel (busy detect time).

DCF adopts an exponential backoff scheme. At each packet transmission, the backoff time is uniformly chosen in the range $(0, w-1)$, where w is called *contention window* (CW). Its value depends on the number of transmissions failed for the packet. At the first transmission attempt, w is set equal to CW_{min} or minimum contention window. After each unsuccessful transmission, w is doubled, up to a maximum value $CW_{max} = 2^m * CW_{min}$. The values CW_{min} and CW_{max} are PHY-specific and are summarized in Table I.

The backoff time counter is decremented as long as the channel is sensed idle. It is "frozen" when a transmission is detected on the channel, and reactivated when the channel is sensed idle again for more than a DIFS. The station transmits when the backoff time reaches zero. Figure 2 illustrates this operation. Two stations A and B share the same wireless channel. At the end of packet transmission, station B waits for a DIFS and then chooses a backoff time before transmitting the next packet. After a DIFS, the packet is transmitted. Note that the transmission of packet A occurs in the middle of the Slot. As a consequence of the channel sensed busy, the backoff time is frozen, and the backoff counter decrements again only when the channel is sensed idle for a DIFS. An ACK is transmitted by the destination station to signal the successful packet reception. The ACK is immediately transmitted at the end of the packet, after a period of time called *short inter-frame space* (SIFS). As the SIFS (plus the propagation delay) is shorter than a DIFS, no other station is able to detect the channel idle for a DIFS until the end of the ACK. If the transmitting station does not receive the ACK within a specified *ACK-Timeout*, or it detects the transmission of a different packet on the channel, it reschedules the packet transmission.

The above describes a two-way handshaking technique for the packet transmission is called *basic access mechanism* (BAS). DCF defines an additional fourway handshaking technique known as *RTS/CTS access mechanism* (RTS). A station that wants to transmit a packet, waits until the channel is sensed idle for a DIFS, follows the backoff rules explained above, and then, instead of the packet, preliminarily transmits a short RTS frame requesting to reserve the channel. When the receiving station detects an RTS frame, it responds, after a SIFS, with a CTS frame. The transmitting station is allowed to transmit its packet only if the CTS frame is correctly received. The frames RTS and CTS carry the information of the length of the packet to be transmitted. This information can be read by any listening station, which is then able to update a *network allocation vector* (NAV) containing the information of the period of time in which the channel will remain busy. When a station is hidden from either the transmitting or the receiving station, by detecting just one frame among the RTS and CTS frames, it can suitably delay further transmission, and thus avoid collision. Using the same method, it eliminates the hidden station problem.

2.2 DCF Backoff Model

The basic backoff model we use appears in [2] and is extended in [3]. We start with the following variables for our analyses, which are same as [2], [3]-

- n Fixed number of contending stations
- p Pr(transmitted packet collides)
- τ Pr(station transmits in a randomly chosen slot)
- W_i Window size at slot, i
- m Maximum backoff stage

We have, using either DSSS or FHSS PHY, the following-

$$W_i = \begin{cases} 2^i W & \text{if } i \leq m' \\ 2^{m'} W & \text{if } i > m' \end{cases}$$

where $W = CW_{min} + 1$ and $2^{m'}W = CW_{max} + 1$. m can be larger than m' as specified in [7] while CW is constant after that as shown in (1). In this equation, m also represents the maximum retransmission limit. In the Markov chain developed in [2], the non-null transition probabilities account in order-

1. The decrements of the backoff timer.
2. After a successful transmission, backoff timer of a new packet starts from backoff stage 0.
3. An unsuccessful transmission makes the backoff stages to increase.
4. At the maximum backoff stage, the CW will be reset if the transmission is unsuccessful or restart the backoff stage for new packet if the transmission is successful.

Using the same analyses as [3] (which is omitted here for simplicity), the stationary probabilities are found for τ. An equation of importance to us is-

$$p = 1 - (1 - \tau)^{n-1} \tag{1}$$

This shows that a packet will collide is there is a single transmission from any other station. Both $p \in (0, 1)$ and $\tau \in (0, 1)$ are typically solved using numerical methods or the analytical models as described in [3]. However, τ could also be computed using scheduler's history at stations to predict future estimates.

2.3 Saturation Throughput Analysis

The throughput analyses use notations from [3], which we shall continue using throughout the paper-

- P_{tr} Pr(at least one transmission in a given slot)
- P_s Pr(a transmission is successful)
- P_{idle} Pr(a given slot is empty or idle)
- P_{coll} Pr(a slot contains a collision)
- S_s Normalized saturation throughput
- S_f Normalized finite load throughput
- T_s E[the channel is sensed busy due to a successful transmission]
- T_c E[the channel is sensed busy due to collision]
- PAK E[fixed packet size including PHY and MAC headers]
- δ Propagation delay in wireless medium

Using these notations, the saturation throughput is calculated using P_{tr}, since n stations contend on the channel, and each transmits with probability τ, i.e.,

$$P_{tr} = 1 - (1 - \tau)^n \tag{2}$$

A packet transmission is successful only when exactly one station transmits on the channel, conditioned on the fact that at least one station transmits, i.e.,

$$P_s = {n\tau\left(1-\tau\right)^{n-1}} \Big/ {P_{tr}} \tag{3}$$

Finally, throughput is given by the successful information transmitted per unit time, i.e.,

$$\begin{array}{l} S_s = E[payload]/E[slot] \\ S_s = P_{tr}P_sPAK/ \\ ((1-P_{tr})+P_{tr}P_sT_s+(1-P_s)P_{tr}T_c) \end{array} \tag{4}$$

The values of T_s and T_c are dependent on the access mechanisms and are noted here with appropriate superscripts below as per [3]-

$$\begin{array}{l} T_s^{bas} = DIFS+PAK+\delta+SIFS+ACK+\delta \\ T_c^{bas} = DIFS+PAK+SIFS+ACK \\ T_s^{rts} = DIFS+RTS+SIFS+\delta+CTS+ \\ SIFS+\delta+PAK+SIFS+\delta+ACK+\delta \\ T_c^{rts} = DIFS+RTS+SIFS+CTS \end{array} \tag{5}$$

These equations form the basis of our throughput analysis.

3 Hidden Stations & 802.11 DCF

3.1 Hidden Stations in Static WLANs

We extend the hearing graph framework of [1] in this section. For ease, we call it a *reachability* graph, R of the WLAN consisting of n wireless stations. Based on the spatial characteristics of the stations, the WLAN is transformed into a connectivity matrix as follows-

$$R = \begin{bmatrix} r_{11} & r_{12} & r_{13} & .. & .. & r_{1n} \\ r_{21} & r_{22} & r_{23} & .. & .. & r_{2n} \\ .. & .. & & .. & & \\ .. & .. & & & .. & \\ r_{n1} & r_{n2} & r_{n3} & .. & .. & r_{nn} \end{bmatrix}$$

An entry in this matrix, r_{ij} indicates a station, i reach another station, j, i.e. $j = r(i)$. We assume unidirectional wireless channels and hence, the opposite may not be necessarily true, i.e. i may or may not reach j. Since two stations that hear the same subset of the population, it is assumed that they can be part of the same group of the reachability graph. This grouping is formed by collecting identical rows or columns into k groups, where $k \leq n$. By definition, if any station, i of a group, k ($i \in k$) can reach any station, j of another group, l ($j \in l$), group l is said to be reachable

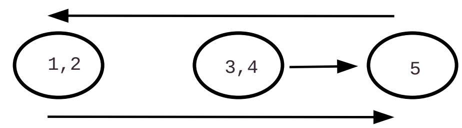

Figure 3: Reachability of a 5-station Wl

by group, k. A 5 station reachability graph can be as follows-

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We see that stations 1 and 2 have identical rows and stations 3 and 4 have identical columns. Since they both share the same property that different groups can reach the same subset of population, this allows to form the following reachability graph-

In a static WLAN, the stations are stationary (a typical example could be people in a conference using wireless links for network access however are not mobile at all). There is no transition between groups in this graph. This implies that stationary probabilities of a group's reachability remain constant throughout the network lifetime. Before proceeding further with analysis, we define the following parameters-

$P_{r(j)}$	Pr(a group is reachable from group j)
$P_{h(j)}$	Pr(a group is hidden from group j)
$N_{r(j)}$	Number of reachable groups from group j
$N_{h(j)}$	Number of hidden groups from group j
$N_{t(j)}$	Total number of groups in the vicinity of j
N_k	Average number of stations in all groups
N_{re}	E[Number of reachable stations in the network]
N_{he}	E[Number of hidden stations in the network]

Using the model of Figure 3, we estimate $P_{r(j)}$ and $P_{h(j)}$ of any WLAN network. Note that $P_{r(j)}$ and $P_{h(j)}$ may only take binary values based on presence of a forward link between the group j resides in and the target group. $P_{r(n)}$, expected reachability of a group, can be found by placing station j in any group, i of total k groups, summing up all reachable groups from i and taking the proportion of the total number of groups in the vicinity of i, i.e.,

$$P_{r(n)} = \sum_{j=1}^{k} (N_{r(j)}/N_{t(j)})/k \tag{6}$$

Since the groups can only be reachable or hidden, $P_{h(n)} = 1 - P_{r(n)}$. Using $P_{r(n)}$, we find the expected number of reachable groups in the network as $N_{r(n)} = P_{r(n)}.n$. Note that the expected number of reachable stations in the network can be found by calculating the average number of stations per group. The expected number of reachable stations is found as $N_{re} = N_{r(n)}.N_k$. In a static WLAN, the expected number of total reachable stations determines the collision probabilities. It should be noted that in large practical WLAN networks, it may not be possible to accurately calculate the number of hidden stations as the connectivity matrix dimensions may be quite large.

3.2 Hidden Stations in Dynamic WLANs

Hidden stations in a dynamic WLAN may move arbitrarily. For simplicity, we consider low to moderate movements only and make the following assumptions-

- Stations roaming within a group has zero net effect on the reachability graph of the network.

- There is no drastic movement by which a station may go beyond its adjacency graph. The *adjacency* graph of a station, i in a group, j constitutes the hidden groups in the vicinty of j which is determined by the physical locations of the groups. There may be l such groups, where $l \leq k$. Note that adjacent groups include both reachable and hidden groups since there may be obstacles causing stations to be not reachable, however, through movements, groups may become either hidden or reachable. An example adjacent graph with both reachable ('solid line') and hidden ('dotted line') groups is shown in Figure 4.

- Holding time at each group exhibited by a station, i is random. This motivates the adjacency graph to be modelled as a Markov chain. Further, the future transition probabilities of the chain is solely dependent on the current group or state (memoryless property), which is also a required condition for Markov chains. A typical example is shown in Figure 5.

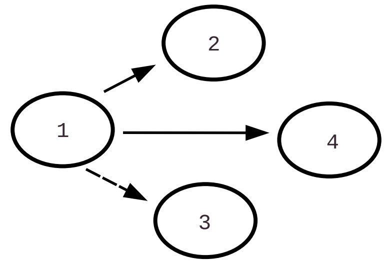

Figure 4: Adjacency graph of a grou

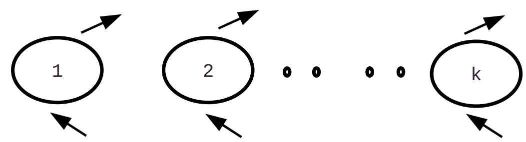

Figure 5:k-state Markov chain of a dynamic WLAN

- Since a reachable=>reachable or hidden=>hidden transitions has no effect on network throughput, we are only interested in reachable=>hidden and hidden=>reachable state transitions. The former is expected to lower and the latter is expected to higher throughput.

We analyze this Markov chain using a controlled parameter called, μ which is the probability of a reachable station to remain reachable through a transition. We introduce this parameter, which has practical significance to be explained later. Using it we find that the probability that it does not remain reachable, is $1-\mu$. As there are l hidden states in the Markov chain, a reachable group may go to any of them or another reachable group with equal probabilities. This gives the reachable=>hidden probabilities as $(1-\mu)/(l-1)$. On the other hand, it is unknown how the transition probabilities of a hidden station changes. We assume that they make transitions to any other group (or itself) with equal probabilities, i.e., $1/l$.

Therefore, we have the following balance equations to solve, $P_{r(j)}$ and $P_{h(j)}$-

$$P_{r(j)} + \sum_{j=1}^{l-1} P_{h(j)} = 1$$

Using the equal probability assumption, we can write the above equation as following-

$$P_{r(j)} + (1 - l)P_{h(j)} = 1$$
$$(1 - \mu/l - 1)P_{r(j)} = (1/l)P_{h(j)}$$

Solving these equations, one may get-

$$P_{r(j)} = 1/(1 + l(1 - \mu)) \tag{7}$$

Note how this is independent of the number of hidden groups in the adjacency graph. One of the power of this analysis is that to model large networks, one needs not to analyze the entire network. It should be sufficient to analyze a subset of all adjacency graphs in order to find $P_{r(n)}$ and use it to predict throughput. If it is desired to find $P_{r(n)}$ over the entire network, it can be calculated from $P_{r(j)}$ by finding and summing it for each adjacency graph in the network-

$$P_{r(n)} = \sum_{j=1}^{k} P_{r(j)}/k \tag{8}$$

Rest of the analysis is identical to static WLAN case. Using this model, we may estimate the expected number of hidden stations in a dynamic WLAN by tuning a single parameter, μ. μ is dependent on several network parameters, such as rate of mobility, nature of network, e.g. infrastructure or ad hoc, etc. and a more complete analysis of μ is outside the scope of this work.

4 Our Throughput Models

4.1 Saturation Throughput Model

In order to find saturation throughput, we use Bianchi's throughput model [2] and integrate the hidden station probabilities into it. The three essential parameters of calculating throughput using payload transmitted per slot formula are: P_s, P_{idle}, and P_{coll}. Note that we calculate the throughput loss suffered by the reachable nodes of the network and assume that in the worst case, a packet is always available for transmission from the hidden groups of the network, i.e., $P_{tr} = 1$. We also assume that both reachable and hidden stations transmit with the same probability, τ. Hence, P_s is given by the probability that exactly one reachable station transmits on the channel, i.e.,

$$P_s = N_{re}\tau(1 - \tau)^{N_{re}-1} \tag{9}$$

Under the saturation condition, a slot can never be empty, i.e., $P_{idle} = 0$. Finally, a slot contains a collision with probability $1 - P_s$. Using these values, the saturation throughput, S_s reduces to the following from (4),

$$S_s = P_s PAK/(P_s T_s + P_{coll} T_c) \tag{10}$$

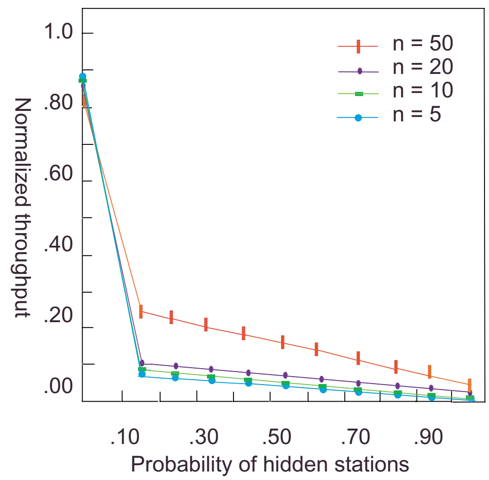

Figure 6: Saturation throughput from theoretical mode

The lengths of sucess and collision times, T_s and T_c are given by-

$$T_s^{bas} = DIFS + PAK + \delta + SIFS + ACK + \delta$$
$$T_c^{bas} = DIFS + PAK + SIFS + ACK\_Timeout$$

We plot the throughput numbers for 5, 10, 20 and 50 station WLANs in Figure 6. This plot shows that throughput drops more than 65 percent when where is any hidden station from the no hidden station case. As probability of hidden stations increase, throughput further decreases. The initial loss for low hidden station probabilities is smaller for large networks. This occurs due to the geometric nature of successful transmission probabilities.

4.2 Finite Load Throughput Model

Saturation throughput analyzes 802.11 DCF with assumption that there are packets always available for transmission from any station in the network, which is not always true in real WLANs. Throughput under arbitrary traffic loads is an important step towards a general model of multihop wireless network employing 802.11 DCF. It is also necessary to accurately predict throughput in presence of hidden stations as the assumption that hidden stations always have packets to transmit is may not be true in real WLANs. We develop a finite load throughput analysis model here using the following assumptions-

- Packets arrive in the network according to a Poisson process with rate λ packets/sec. This is the arrival process, $A(t)$ into the system.

- Each station has infinite buffer space, i.e. packets are never dropped due to shortage of memory at a station and will always be transmitted as per the protocol.
- Wireless channels are error-free, i.e. throughput loss can happen only due to collisions. Packet losses due to medium error are not considered.
- The network consists of heterogeneous users with different traffic loads, which can be characterized into groups. For networks with hidden stations, it is further assumed that a hidden or reachable group has the same traffic load. This simplifies traffic load patterns in reachability and adjacency graphs.

Suppose there are k different groups within the network. Let there be n_i stations in group i with arrival rates λ_i. Note that the total number of stations from each group is $\sum_{i=1}^{k} n_i = n$. Each group consists of a large number of users who collectively form an independent Poisson source with an aggregate mean packet arrival rate λ_i each such that $\sum_{i=1}^{k} \lambda_i = \lambda$. We define a packet transmission to be successful in group i, if it is free from interference caused by packets from group i. A packet transmission is totally successful when it is successful among all groups. A packet transmission from group i is totally successful if the following two mutually independent conditions are satisfied-

- The packet transmission is successful in the group i, $P_{s(i)}$.
- The packet transmission is successful in all other groups such that $j \neq i$, $P_{s(j)}$.

Similarly, a collision occurs when there is a transmission from in the same time slot from either a station in the group, i or any other group, j for $j \neq i$, giving p_i,

$$p_i = 1 - (1-\tau_i)^{n_i - 1} \prod_{j=1, j\neq i} (1-\tau_j)^{n_j} \tag{11}$$

Probability of at least one transmission in a time slot is given by the following as there are k contending groups in which each station transmits with probability, τ_i in group i, i.e.,

$$P_{tr(n)} = 1 - \prod_{j=1}^{k} (1-\tau_j)^{n_j} \tag{12}$$

Using the successful transmission criterion, we may find $P_{s(i)}$ as a total sucess of a transmission from any group in the network conditional upon at least one transmission, i.e.,

$$\begin{aligned} P_{s(i)} &= n_i \tau_i (1-\tau_i)^{n_i - 1} \\ P_{s(j)} &= \prod_{j=1, j\neq i}^{k} n_j \tau_j (1-\tau_j)^{n_j} \\ P_{s(n)} &= \sum_{i=1}^{k} P_{s(i)} P_{s(j)} / P_{tr(n)} \end{aligned} \tag{13}$$

These probabilities can be readily inserted into (4) in order to accurately estimate finite load throughput of DCF, i.e.,

$$\begin{aligned} &S_f = P_{tr(n)} P_{s(n)} PAK / \\ &(1-P_{tr(n)})\sigma + P_{tr(n)} P_{s(n)} T_s + P_{tr(n)} (1-P_{s(n)}) T_c \end{aligned} \tag{14}$$

Although we use it for basic access only although it can be used for RTS/CTS mechanism as well. Further, this model can be used to analyze throughput with finite traffic loads in presence of hidden stations. Since a station has no knowledge about the hidden groups we assume that there may be as many hidden nodes as there are reachable and later show through simulations that it is a close approximation. Thus the transmission probabilities of reachable groups change, i.e.,

$$P_{tr(n)} = 1 - \prod_{i=1}^{k} (\prod_{j\in r(i), j\neq i} (1-\tau_j)^{2n_j}) \tag{15}$$

Similarly, for a successful transmission, a station must succeed in its own group and its adjacent groups, i.e.,

$$P_{s(j)} = \prod_{j\in r(i), j\neq i} n_j \tau_j (1-\tau_j)^{2n_j} \tag{16}$$

Now both $P_{s(n)}$ and S_f can be found using equations (13) and (14) respectively.

We have developed an analytical model for 802.11 DCF throughput employing basic access mechanism in presence of hidden stations. We have also developed a general finite throughput model for DCF, which can be used to accurately predict finite load throughput of the protocol employing either access mechanisms. Next, we validate our model using simulations.

5 Simulation Results

We performed simulations using *ns-2* [8] wireless module. We modified CMU's scene and traffic generators to generate wireless scenes of different sizes, mobility rates, consisting of hidden stations, and random pause times; and traffic loads of different packet sizes

Parameter	*Value*
Packet payload	8640 bits
MAC header	272 bits
PHY header	128 bits
ACK	112 bits + PHY header
RTS	112 bits + PHY header
CTS	112 bits + PHY header
Channel bit rate	1 Mbit$/s$
Propagation delay	1 μs
Slot time	50 μs
SIFS	28 μs
DIFS	128 μs
ACK-Timeout	200 μs

Table 2: Simulation parameters

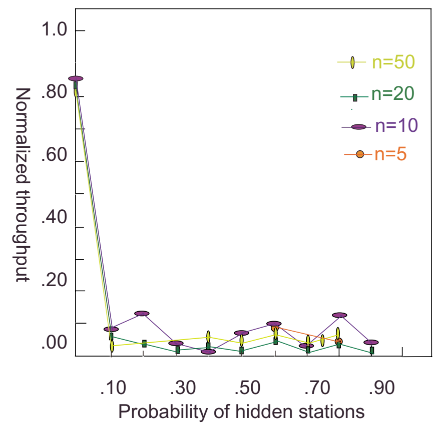

Figure 7: Saturation throughput from simulati

and inter-packet intervals. We used overscribed *constant bit rate* (CBR) traffic for saturation and different rate (< link speed) traffic for finite load throughput simulations. In all cases UDP links were used for transport. It was possible to easily calculate throughput using scripts to extract bytes transmitted on a per station basis from the trace files. Other essential parameters of simulations are summarized in Table 2.

ns-2 implements DSSS PHY and defaults to RTS/CTS for wireless simulations. We modified RTS-threshold to 3000 bytes in order to use basic access mechanism for our packet size. We next summarize our saturation throughput results from simulations. Please note that this is the first of the following planned simulations:

- Saturation throughput of static WLANs
- Finite-load throughput of static WLANs
- Saturation throughput of dynamic WLANs
- Finite-load throughput of dynamic WLANs

5.1 Saturation Throughput Results

For saturation throughput, we simulated 5, 10, 20 and 50 station networks. Saturation throughput results are plotted in Figure 7. These results show that throughput degradation due to presence of hidden stations is similar to our prediction from the theoretical model. The drop in throughput from no hidden station case is almost identical for all network sizes. This is different from the theoretical model. However, the important characteristics of both agree quite closely. This validates our saturation throughput model.

The differences observed between the model and simulation may be attributed to the fact that there may not be packets from the hidden stations at all time slots.

6 Discussions, Conclusions and Future Work

The hidden station model that we have developed for both static and dynamic environments are sophisticated and can be used for analyzing their effects on a variety of networks employing carrier sense and medium sharing. Our saturation throughput model in presence of hidden stations is in close compliance with practical simulation under the same network configurations. We believe that this model can be viewed as an extension to Bianchi's original model.

So far the simulation results presented are limited and may be completed using the framework and thus validate the finite-load throughput model. Another interesting work may be to simulate the Markov chain used to model dynamic WLANs.

The proposed model for finite-load throughput is computationally expensive and may require some simplifications. An important step towards developing a general model IEEE 802.11 DCF and its derivatives would be to use heuristics and other techniques to predict finite-load throughput with sufficient accuracy. The model may also accommodate variable rates of traffic. Different types of traffic types, such as Bernoulli IID, expoential, bursty, etc. may be used in simulations to land on a truely general model of the protocol. Finally, the model can be used in ad hoc wireless networks deploying DCF across multiple service sets (*independent basic service set* or IBSS).

The assumptions made about the relationship between the number of hidden stations in adjacency graph may not be true in many cases. One may look into whether there is any fixed relationship between the number of reachable stations and the number of hidden stations. This may help in finding some limits of the number of hidden stations there may be. At the end, it may be claimed that the work undertaken in this project was a worthwhile analysis and although the protocol has offered solutions to the problem we modeled, deriving analytical models of the problem area was one of the most satisfying factors of the work.

References

[1] Kleinrock, L., Tobagi, F., "Packet Switching in Radio Channels, Part II - The Hidden Terminal Problem in Carrier Sense Multiple Access and the Busy Tone Solution," *IEEE Transactions on Communication*, V23, pp. 1417-1433, 1975

[2] Bianchi, G., "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE Journal on Selected Area in Communications*, V18, N3, 2000

[3] Wu, H., Peng, Y., Long, K., Cheng, J., Ma, J.,"Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis And Enhancement," *IEEE INFOCOMM*, 2002

[4] Ho, T., Chen, K., "Performance Analysis of IEEE 802.11 CSMA/CA Medium Access Control Protocol," *Int Conf on PIMRC*, Taipei, Taiwan, pp. 407-411, 1996

[5] Huang, K., Chen, K., "Interference Analysis of Non-persistent CSMA with Hidden Terminals in Multi-cell Wireless Data Networks," *Int Conf on PIMRC*, Toronto, Canada, pp. 907-911, 1995

[6] Khurana, S., Kahol, A., Gupta, S., Srimani, P., "Performance Evaluation of Distributed Co-Ordination Function for IEEE 802.11 Wireless LAN Protocol in Presence of Mobile and Hidden Terminals," *In MASCOTS*, pp. 40-47, 1999

[7] "IEEE standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," *ISO/IEC 8802-11:1999(e)*, August 1999

[8] *ns-2* Network Simulator (Version 2.96), August 2002