

# The Hidden Cost of Hidden Terminals

Feilu Liu\*, Jian Lin†, Zhifeng Tao§, Thanasis Korakis\*, Elza Erkip\* and Shivendra Panwar\*

\*ECE Department, Polytechnic Institute of NYU, Brooklyn, NY 11201

†School of ECE, Georgia Institute of Technology, Atlanta, GA 30332

§Mitsubishi Electric Research Laboratories (MERL), 201 Broadway, Cambridge, MA 02139

**Abstract**—The performance unfairness problem in a single cell IEEE 802.11 wireless local area network (WLAN) is considered. While existing research is based on the assumption that all nodes have the same transmission success probability and per-node throughput, this fairness exists only if all nodes within range of the access point can sense each other. Recent measurements suggest that this is not necessarily true and terminals can be hidden from each other. In this paper, the impact of hidden terminals on the performance unfairness among individual nodes is investigated via analysis, simulation and experimental measurements in a real network. In the presence of hidden terminals, it is observed that the widely accepted conclusion of equal performance among nodes does not hold any more. Instead, nodes far from the access point (AP) see more hidden terminals than those close to the AP, so they get more packet losses and lower throughput. This phenomenon is not due to inter-cell interference, or channel disparities among nodes, and is significant even when the RTS/CTS mechanism designed to mitigate the impact of hidden terminals is turned on. The simulation results show that for a 16-node WLAN with a fixed data rate of 6Mbps, the throughput of a node close to the AP is more than twice that of an edge node, due to hidden terminals.

**Index Terms**—Hidden terminal, wireless LAN, 802.11, CSMA, performance unfairness, throughput, measurement.

## I. INTRODUCTION

The IEEE 802.11 [1] distributed coordination function (DCF) is a medium access control (MAC) layer random access protocol based on carrier sense multiple access with collision avoidance (CSMA/CA). Due to the apparent “fair” nature of the CSMA/CA random access scheme, it is widely assumed that long term channel access fairness is guaranteed in 802.11 WLANs [2], [3]. Heusse et al. [3] further show that all nodes in a WLAN have the same throughput, even if they transmit at different data rates. While long term channel access fairness is valid when no hidden terminals are present, it is not true for networks with general topologies, where hidden terminals are almost inevitable. In fact, in this paper we argue that the channel access probability and per-node throughput are location-dependent, when nodes are randomly placed in a WLAN, due to hidden terminals.

The hidden terminal problem is closely related to the Transmission Range (TX\_Range), Carrier Sensing Range (CS\_Range) and Interference Range (IF\_Range) of stations

in WLAN [4] [5]. The TX\_Range is the range (with respect to the transmitting station) within which a transmitted frame can be successfully received. In 802.11 WLAN, there are a number of available data rates. The transmission ranges of different data rates are quite different [4], due to their different SNR requirements at the physical layer. The CS\_Range is the range (with respect to the transmitting station) within which the other stations detect a transmission. The IF\_Range is the range within which stations in receive mode will be “interfered with” by a transmitter, and thus suffer a loss. Measurement studies such as [4] demonstrate that  $\text{TX\_Range} < \text{IF\_Range} < \text{CS\_Range}$ .

Hidden terminals refer to the nodes within the interference range of the intended destination and out of the carrier sensing range of the source [5]. In a single-cell WLAN, in order for nodes to communicate with the AP, their distances from the AP cannot exceed the TX\_Range at the lowest data rate. Additionally, since every node can sense the AP, there is no hidden terminal problem for downlink traffic. However, for uplink traffic, a pair of nodes see each other as hidden terminals if the distance between them is greater than the CS\_Range, as illustrated in Fig. 1(a). Assuming nodes are randomly placed within the maximum transmission range of the AP, it is clear that the maximum possible distance between two nodes is twice the TX\_Range at the lowest data rate. However, measurements [4] for 802.11b networks demonstrate that the CS\_Range is about 1.5 times the TX\_Range at the lowest data rate (1Mbps), which matches our measurement results in 802.11g networks [6]. Ng and Liew’s measurements [7] for 802.11b networks show that the ratio between the CS\_Range and the TX\_Range at 11Mbps is 2.5. However, note that the TX\_Range for 11Mbps, the highest data rate in 802.11b, is the shortest and therefore hidden terminals are likely. So for general network topologies and variable data rates, a node may not be sensed by some of the other nodes, thus hidden terminals remain a problem. While the RTS/CTS mechanism is commonly assumed to “solve” this problem, we will show that it only partially mitigates, but does not eliminate it.

In the next subsection we briefly summarize the contributions of this paper and the related work. Then in the following sections we investigate the performance unfairness caused by hidden terminals via analysis, simulations and measurements.

This work is supported in part by the National Science Foundation (NSF) under grant CNS-0520054 and grant IIP-0430145, the New York State Center for Advanced Technology in Telecommunications (CATT) and the Wireless Internet Center for Advanced Technology (WICAT), an NSF Industry/University Cooperative Research Center at Polytechnic Institute of NYU.

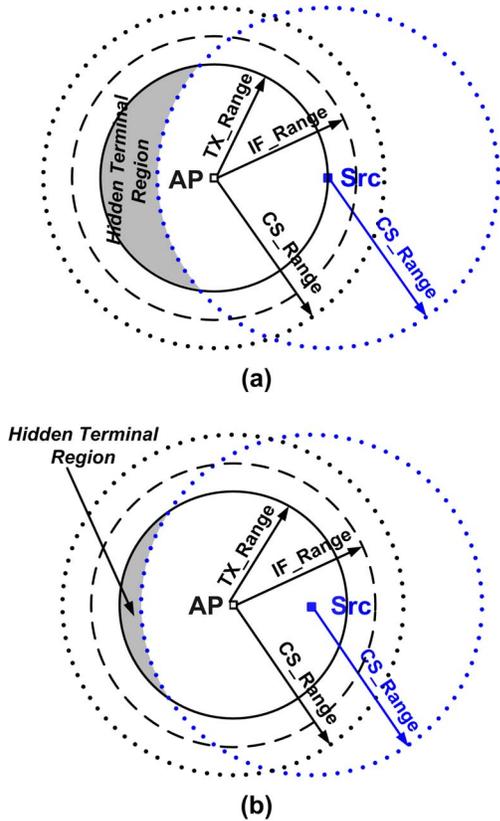


Fig. 1. Illustration of the hidden terminal problem in infrastructure mode 802.11 networks. Note that the hidden area in (a) is larger than that in (b) (where the source station is closer to the AP).

### A. Contributions and Relationship to the Literature

This paper focuses on the packet loss probability and the throughput of *individual nodes* in the presence of hidden terminals. We argue that hidden terminals result in performance unfairness among the nodes. We investigate the cause of this problem via analytical modeling, simulations and experimental measurements. Our simulations (to be reported in Section III) show that in a 16-node WLAN with a fixed data rate of 6Mbps, the throughput of a node far from the access point (AP) is the same as that of a node close to the AP when no hidden terminals are present; however, with hidden terminals, the throughput of a far-away station is less than half that of a close-by station. Therefore, it is hidden terminals, instead of the difference in channel qualities, that cause this unfairness. This presents a striking contrast to the widely adopted assumption of long term channel access fairness of CSMA/CA [2] [3] [8].

Although the literature on the hidden terminal problem is extensive, most of the research has focused on overall network performance measures [7], [9], [10], e.g., the aggregate throughput of all nodes. Only a few papers focus on the unfairness problem cause by hidden terminals. In [11] and [12], Chhaya and Gupta build an analytical model for 802.11 single-hop ad-hoc networks in the presence of hidden nodes and capture effects. The model reveals that the success probability of a transmission is higher when the receiver is

closer to the transmitter, assuming no channel errors. However, their conclusion is mainly based on capture effects [11], since a receiver gets stronger signals when the transmitter is closer and thus is more likely to successfully decode a packet collided by other transmissions. In our model, we exclude capture effects and only focus on the effect of hidden terminals on channel access unfairness. In addition, [11] and [12] assume that each pair of nodes are hidden from each other with equal probability, which we show is not correct for general network topologies. Similarly, Hung et al. [9] evaluated the network performance by assuming that the number of hidden nodes is constant for all transmissions. As a result, they did not take into account the location-dependent unfairness among the nodes and only evaluated the aggregate network throughput. Both [13] and [14] note that the number of hidden nodes that a transmitter observes is location-dependent, but they do not analyze the resulting performance disparity.

This paper fills the research gap in unfairness effects in the existing hidden terminal problem studies, which, though extensive, mainly focus on the overall network performance measures, e.g., the aggregate throughput of all nodes. In addition, we carry out experimental measurements to verify our argument.

## II. AN ANALYTICAL MODEL FOR THE HIDDEN TERMINAL PROBLEM

### A. System Model

We consider an 802.11 single-cell WLAN with only uplink traffic, wherein all transmissions are initiated by stations and destined to the AP. The AP is located at the center of the network and the other stations are randomly located within the AP's maximum transmission range with uniform distribution. Our measurement results (to be reported in Section IV) corroborate that the network performance in the presence of hidden nodes is worse when RTS/CTS is disabled. Therefore, we assume RTS/CTS handshake is active. As discussed in Section I, WiFi measurements [4], [6] show that CS\_Range is less than twice the TX\_Range at the lowest data rate. So we set

$$CS\_Range = \eta \times TX\_Range, \quad \eta \in (1, 2). \quad (1)$$

The TX\_Range here and in the following sections refers to the TX\_Range at the lowest data rate and is denoted as  $r$ . Other assumptions are listed below.

- 1) No capture effect, i.e., when two or more packets collide, all fail.
- 2) No channel errors.
- 3) All stations transmit at the same data rate, which can be any one defined by the 802.11 standard.
- 4) All stations are always in backlog state.

As in [2], the conception of "time slot" is extended to refer to any continuous time period that a station observes. The duration of a time slot in our model can be one of the following:

- $\alpha$ : the duration of a successful transmission.
- $\beta$ : the duration of a collision period.
- $\delta$ : the duration of a backoff time slot.

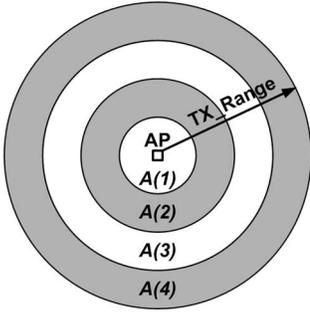


Fig. 2.  $M$  evenly spaced concentric annuli centered at the AP ( $M = 4$  in this figure).

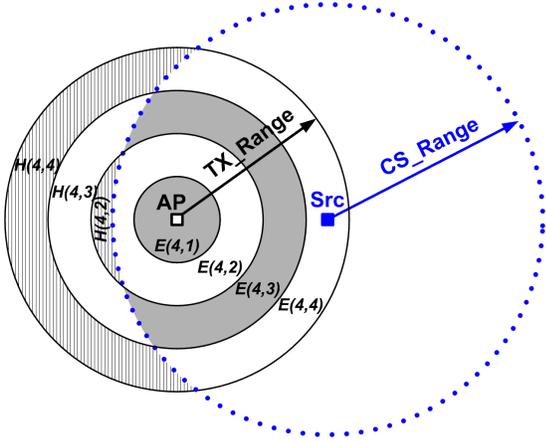


Fig. 3. Illustration of Hidden Region  $H(i, j)$  and Covered Region  $E(i, j)$ .

### B. Network Analysis

Assuming stations are randomly located in the network with uniform distribution, Fig. 1 shows that a station sees more hidden nodes when it is far away from the AP (Fig. 1(a)), compared with the case when it is close to the AP (Fig. 1(b)). Since hidden terminals cause more collisions, we expect that a node far away from the AP suffers a larger packet loss probability than a node close to the AP. To formulate this and to capture the location-dependent nature of the hidden terminal's impacts, we slot the whole area into  $M$  evenly spaced concentric annuli centered at the AP, as shown in Fig. 2. Each annulus  $A(i)$  ( $i \geq 2$ ) is confined by two circles with radius  $r(i-1)/M$  and  $ri/M$  respectively; while  $A(1)$  is the interior of the innermost circle centered at the AP with radius  $r/M$ . As we can see from Fig. 2, provided  $M$  is not too small, stations in annulus  $A(i)$  are at approximately the same distance  $d(i)$  from the AP, so they observe approximately the same number of hidden nodes. Consequently, nodes in  $A(i)$  have approximately the same collision probability  $P_c(i)$  and transmission probability  $\tau(i)$ . Of course, the larger  $M$  is, the better the approximations are. As in [2], we adopt the key assumption that each station independently makes a transmission attempt at any time slot with a constant probability. However, unlike [2], this probability is not equal for all nodes, and it depends on which annulus the node belongs to.

Following [2], we obtain the relationship between  $\tau(i)$  and  $P_c(i)$  for a node in annulus  $A(i)$  as:

$$\tau(i) = \frac{2(1 - 2P_c(i))}{(1 - 2P_c(i))(W + 1) + P_c(i)W[1 - (2P_c(i))^m]} \quad (2)$$

where  $i = 1, 2, \dots, M$ . Although our analytical approach is similar to Bianchi's work [2], there are key differences. First of all, Bianchi assumes a fully-connected network. But we adopt the more realistic assumption that nodes are randomly placed in the network with uniform distribution, thus causing hidden terminals. In addition, Bianchi derives the aggregate network throughput; while we obtain the throughput of *each node* (nodes at different locations have different throughput in the presence of hidden terminals).

We next derive the conditional collision probability  $P_c(i)$  in terms of transmission probability  $\tau(i)$ . For a source station ( $Src$ ) located in annulus  $A(i)$ , the hidden region  $H(i, j)$  is defined as the part of annulus  $A(j)$  that is out of the CS\_Range of  $Src$ ; while the covered region  $E(i, j)$  is defined as the part of annulus  $A(j)$  that is within the CS\_Range of  $Src$ . Fig. 3 shows the  $H(i, j)$  and  $E(i, j)$  for a source station located in  $A(4)$ . Note that  $H(4, 1)$  is zero in this example and not shown in the figure. Denote  $A_h(i, j)$  and  $A_e(i, j)$  as the areas of  $H(i, j)$  and  $E(i, j)$  normalized with respect to the total area within the AP's TX\_Range, respectively. Let  $R$ ,  $r$  and  $M$  be the CS\_Range, the TX\_Range and the number of annuli, respectively. Then  $A_h(i, j)$  and  $A_e(i, j)$  can be obtained as:

$$A_h(i, j) = S(i, j) - S(i, j - 1), \quad (3)$$

$$A_e(i, j) = [j^2 - (j - 1)^2]/M^2 - A_h(i, j), \quad (4)$$

where

$$S(i, j) = \begin{cases} [j^2(\pi - \theta) + j(i - \frac{1}{2})\sin \theta]/(\pi M^2) - R^2\varphi/(\pi r^2) & j = M - i + 1, \dots, M \\ 0 & \text{otherwise} \end{cases}$$

and

$$\begin{aligned} \theta &= \arccos[(r^2 + d^2 - R^2)/(2rd)], \\ \varphi &= \arccos[(d^2 + R^2 - r^2)/(2dR)], \\ d &= r(i - 1/2)/M. \end{aligned}$$

If the total number of stations in the network is  $N$ , a station in annulus  $A(i)$  sees an average  $NA_h(i, j)$  hidden nodes and  $NA_e(i, j)$  covered nodes in annulus  $A(j)$ .

A number of conditions have to be met for a successful transmission. We denote  $\rho$  as the number of backoff time slots that a RTS transmission spans, that is,

$$t_{rts} = \rho\delta, \quad (5)$$

where  $t_{rts}$  is the RTS transmission time. An obvious condition for a successful transmission is that no nodes within  $Src$ 's CS\_Range initiates transmissions in the same time slot as  $Src$  does. Since  $Src$ 's RTS signal cannot be sensed by its hidden nodes, another condition is that no hidden nodes transmit during the RTS transmission. As  $Src$  senses the channel before the transmission of RTS, we are sure that all nodes within

*Src*'s CS\_Range are idle in the time slot just before the RTS transmission. However, *Src* has no knowledge about the status of the hidden nodes. As a result, when *Src* initiates a transmission, a hidden node may be already transmitting an RTS, whose signal cannot be sensed by *Src*. So the third condition is that no hidden nodes transmits in the preceding  $t_{rts}$  time. If all of the three conditions are satisfied, the RTS will be successfully received by the AP, which then replies with a CTS. Once an RTS is successful, collisions due to hidden terminals in the following transmissions can be neglected, since the CTS from the AP could be heard by all nodes in the WLAN. Consequently, the conditional success probability  $P_s(i)$  given that a node in annulus  $A(i)$  initiates a transmission is

$$P_s(i) = \prod_{j=1}^M [1 - \tau(j)]^{N[A_e(i,j) + (2\rho-1)A_h(i,j)]}. \quad (6)$$

Then the conditional collision probability  $P_c(i)$  given that a node in annulus  $A(i)$  initiates a transmission is

$$P_c(i) = 1 - \prod_{j=1}^M [1 - \tau(j)]^{N[A_e(i,j) + (2\rho-1)A_h(i,j)]}. \quad (7)$$

$(i = 1, 2, \dots, M)$

Eq.'s (2) and (7) provide  $2M$  equations for  $2M$  unknowns, which can be solved numerically to obtain  $\tau(i)$  and  $P_c(i)$ ,  $i = 1, 2, \dots, M$ .

### C. Throughput Per Node

Normalizing the area of annulus  $A(i)$  with respect to the network area, we get

$$\text{Area of } A(i) = [i^2 - (i-1)^2]/M^2, \quad i = 1, 2, \dots, M. \quad (8)$$

Since we assume that nodes are randomly located in the network with uniform distribution, the expected number of stations located in annulus  $A(i)$  is proportional to the normalized area of annulus  $A(i)$ :

$$N(i) = N[i^2 - (i-1)^2]/M^2, \quad i = 1, 2, \dots, M. \quad (9)$$

The probability that all stations are idle in a time slot is

$$P_{idle} = \prod_{i=1}^M [1 - \tau(i)]^{N(i)}. \quad (10)$$

As the transmission probability  $\tau(i)$  is independent for each node, the probability that there is a successful transmission in a time slot is

$$P_{success} = \sum_{i=1}^M N(i)\tau(i)(1 - P_c(i)). \quad (11)$$

Hence, the probability that there is a collision in a time slot is

$$P_{collision} = 1 - P_{success} - P_{idle}. \quad (12)$$

Since most collisions occur when a node launches RTS during the transmission of a RTS by another node, the collision

period is the overlap time of these two RTS's, and  $\beta \approx 1.5t_{rts}$ . The per-node throughput for a node in annulus  $A(i)$  is

$$\text{Throughput}(i) = \tau(i)(1 - P_c(i))E[\text{Payload}]/T. \quad (13)$$

where  $E[\text{Payload}]$  is the expected payload length of a packet and  $T$  is the mean duration of a time slot given by

$$T = P_{idle}\delta + P_{success}\alpha + P_{collision}\beta. \quad (14)$$

## III. SIMULATIONS

To validate the analytical model in Section II, we have run extensive simulations with OPNET v12.0 [15].<sup>1</sup> The system parameters for the simulations and for the numerical solutions obtained from the model are set to typical 802.11g values, as summarized in Table I. The AP is located at the center

TABLE I  
PARAMETERS USED IN BOTH SIMULATIONS AND MODEL

Slot Time	9 $\mu$ s	W (CWMin)	31
SIFS	10 $\mu$ s	CWMax	1023
DIFS	28 $\mu$ s		

of the network, while the other stations are uniformly placed within the TX\_Range of the AP. We assume 16 nodes in the network. The AP does not initiate transmissions, while the other stations transmit UDP packets to the AP at 6 Mbps. WiFi measurements [4], [6] show that  $1 < \eta < 2$ . So we test the model for  $\eta = 1.0, 1.3, 1.6$  and  $2.0$ , respectively. Default values in OPNET are used for the other parameters. All nodes are always in backlog state and the payload size has been fixed to 1500 bytes. The RTS/CTS handshake has been turned on. In order to compare the results from simulation with that from our analytical model, we set the number of annuluses  $M$  to 20 and obtain the numerical results from the model.

Fig. 4 shows the per-node throughput and packet loss probability as a function of the distance from a node to the AP. The distance has been normalized with respect to the TX\_Range. As we can see, our analytical results of per-node throughput and packet loss probability match simulation results well. In fact, both the analytical model and simulations reveal a significant location-dependent unfairness in terms of packet loss probability and per-node throughput. For  $\eta=1.0, 1.3$  and  $1.6$ , the throughput for the closest node to the AP is five, four and two times as much as that for a node at the edge of transmission range, respectively. The unfairness becomes less significant as  $\eta$  increases (because of fewer hidden nodes). In addition, these two figures also show that when carrier sensing range is large enough ( $\eta = 2.0$ ) to eliminate all hidden terminals, far-away nodes have the same performance as those close-by nodes do. So it is clear that the performance unfairness in scenarios with  $\eta < 2.0$  is due to hidden terminals, rather than different channel qualities among the nodes.

<sup>1</sup>We found a bug in OPNET (v12.0 and v14.5) that manifests itself in a misuse of extended inter-frame space (EIFS). According to the 802.11 standard, when a node senses but cannot decode an RTS, it defers an EIFS period. The deferral should be canceled once a correct packet is received. However, in OPNET the EIFS is not properly canceled when a node correctly receives a packet. We have circumvented the bug in our simulations.

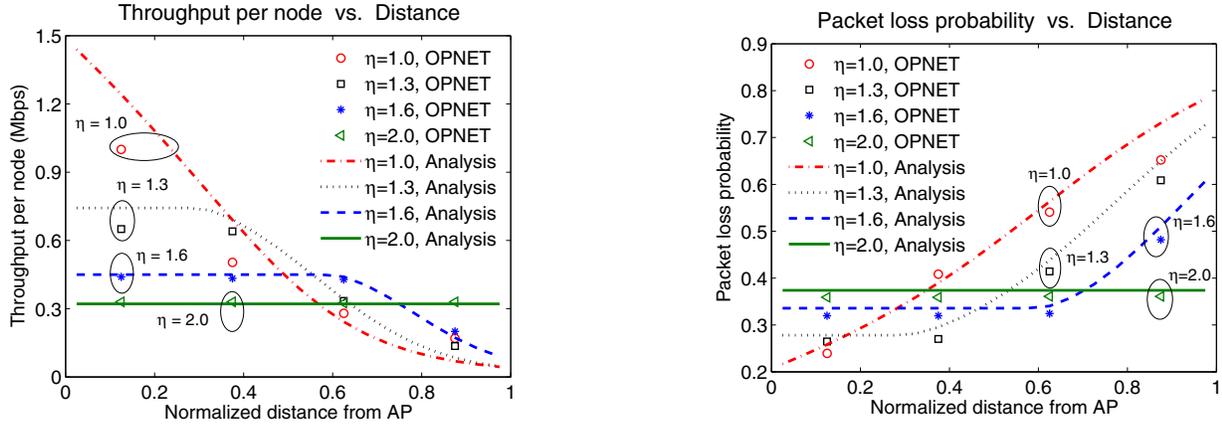


Fig. 4. Performance unfairness in a 16-node network

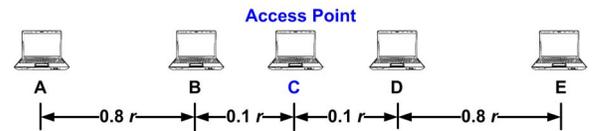
#### IV. EXPERIMENTAL MEASUREMENTS

We have set up a testbed to measure the MAC layer packet loss probabilities and the per-node throughput for individual nodes in a WLAN. The measurements are conducted in an open space at an abandoned airport. We have used five laptop computers (*A*, *B*, *C*, *D* and *E*) running Linux Fedora 5 (kernel: 2.6.16-prep). Each laptop is equipped with an Atheros 802.11g wireless card (chipset: Atheros AR5212) and uses the *MadWifi* driver [16] (version 0.9.4). To facilitate experimentation, the transmission power of each wireless card is fixed to 1 dBm.

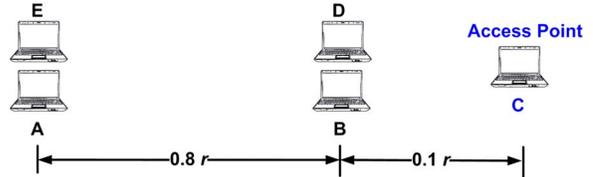
Two topologies are considered in our experiments, as shown in Fig. 5. Here  $r$  denotes the TX\_Range. Laptop *C* acts as the AP and does not initiate transmissions; the other laptops always have a backlog of UDP packets to transmit to *C*. The payload length of the packets are fixed to 1470 bytes.

The “HT” topology in Fig. 5(a) is designed to show the performance unfairness due to hidden terminals. Since CS\_Range is between  $1.2r$  and  $1.6r$ , close-by nodes *B* and *D* observe no hidden nodes, while far-away nodes *A* and *E* see each other as hidden nodes. Since far-away nodes have a worse channel than close-by nodes, one may argue that the performance unfairness may be due to the disparity in channel qualities, instead of hidden terminals. In order to discriminate between these two factors, we also designed the “No HT” topology in Fig. 5(b) for comparison. In Fig. 5(b), there are no hidden terminals. Moreover, the distances from station *A*, *B*, *D*, *E* to the AP in Fig. 5(b) are the same as their counterparts in Fig. 5(a).

Our measurements are performed under different traffic loads and at various data rates. Fig. 6 shows the experimental results obtained under saturated traffic and at 36Mbps data rate. When hidden terminals are present, we observe significant unfairness in both per-node throughput and packet loss probabilities. For example, in “RTS,HT” scenario, the throughput of a close-by node is about four times that of a far-away node. Without the presence of hidden terminals, however, we observe little unfairness. For instance, in “RTS,no HT” and “no RTS,no HT” scenarios, far-away nodes enjoy almost the same throughput as close-by nodes do. Note that the distances



(a) “HT” Topology – a topology *with* hidden terminals



(b) “No HT” Topology – a topology *without* hidden terminals

Fig. 5. Network topologies used in the experiments. Note that for each node, its distance from the AP is the same in both topologies.

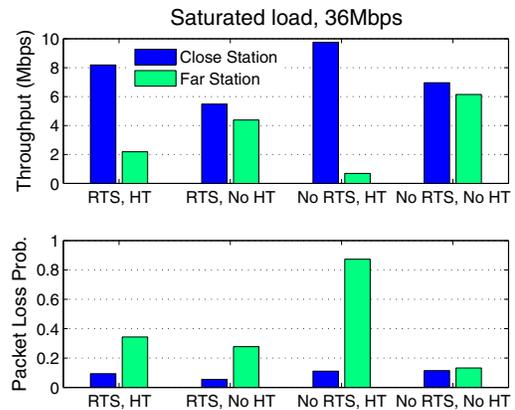


Fig. 6. Measured per-node throughput and packet loss probabilities under saturated load and at fixed data rate 36Mbps.

from station  $A, B, D, E$  to the AP in “No HT” topology is exactly the same as their counterparts in “HT” topology. Therefore, it is hidden terminals, rather than the difference in channel qualities, that cause the performance unfairness.

Apart from the saturation case, we have also conducted experiments under *non-saturated* load at 6Mbps data rate. We set the load of each node to 0.6 Mbps. Therefore the whole network load is 2.4 Mbps, which is about half of the aggregate throughput under saturated traffic. Fig. 7 reveals the performance of individual nodes. We observe an interesting phenomenon in the figure. The throughput of each node is equal to its offered load and does not depend on its location. However, the packet loss probability does. This is due to hidden nodes: a node far from the AP sees more hidden nodes than a node close to the AP does, so it experiences more collisions, which explains the bottom subfigure in Fig. 7; however, since the channel is not fully utilized, most collided packets will eventually be successfully re-transmitted, so the throughput of each node is the same as its offered load, which explains the top subfigure in Fig. 7. In scenario “RTS, No HT”, the packet loss probabilities for close-by stations and far-away stations are both very small ( $< 0.1$ ), but in scenario “RTS, HT”, the packet loss probability of a far-away station ( $\approx 0.4$ ) is much greater than that of a close-by station ( $\approx 0$ ). This demonstrates that the channel access unfairness due to hidden terminals prevails for non-saturated loads as well. We notice that the RTS/CTS exchange slightly alleviates this problem. The difference of packet loss probability between a close station and a far station is smaller in scenario “RTS, HT” ( $\approx 0.42$ ) than in scenario “No RTS, HT” ( $\approx 0.54$ ). Since packet loss is closely related to delay, the disparity in packet loss probability can cause unfairness in quality of service (QoS) for real-time applications. We have performed video streaming experiments and observed the QoS unfairness between close-by and far-away nodes. Due to the page limit, we do not report these results in this paper.

## V. CONCLUSION AND FUTURE WORK

In this paper, we argued that the widely accepted assumption of long term channel access fairness [2] [3] in WLANs does not hold in the presence of hidden terminals. Through analysis, simulations and experimental measurements, we conclude that when hidden terminals are present, the nodes close to the AP enjoy much higher transmission success probabilities and per-node throughput than those far from the AP. In our simulations and experiments, we contrasted scenarios with hidden terminals with scenarios without hidden terminals, where we found that far-away nodes have the same performance as the close-by nodes. Consequently, we argued that this performance unfairness is due to hidden terminals, not the difference in channel qualities. Such unfairness is observed under both saturated and non-saturated traffic loads and at various data rates. It exists even with RTS turned on. For simplicity, our investigation has been done in single cell WLANs, however, we believe this unfairness problem also exists in multi-cell WLANs. In single cell WLANs, the problem manifests itself

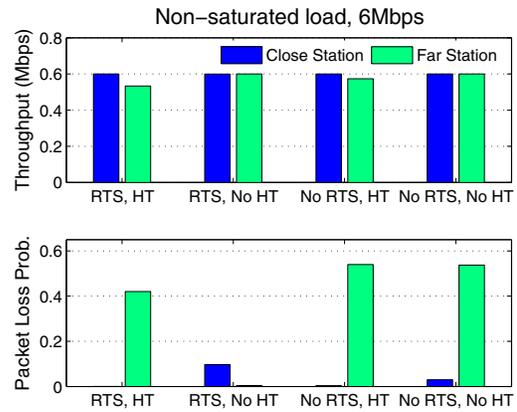


Fig. 7. Measured per-node throughput and packet loss probabilities under *non-saturated* load and at fixed data rate 6Mbps.

only in uplink transmissions; but in multi-cell WLANs, we believe it exists in both uplink and downlink transmissions. In the future, we plan to investigate this performance unfairness phenomenon in multi-cell WLANs.

## REFERENCES

- [1] ANSI/IEEE Std 802.11, “Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 1999.
- [2] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 535–547, Mar. 2000.
- [3] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, “Performance anomaly of 802.11b,” in *Proc. of INFOCOM*, 2003.
- [4] G. Anastasi, E. Borgia, M. Conti, and E. Gregori, “Wi-fi in ad hoc mode: a measurement study,” in *Proc. of PERCOM*, 2004.
- [5] K. Xu, M. Gerla, and S. Bae, “Effectiveness of RTS/CTS handshake in IEEE 802.11 based adhoc networks,” *Ad Hoc Network Journal*, vol. 1, pp. 107–123, Jul. 2003.
- [6] J. Lin, F. Liu, T. Korakis, Z. Tao, E. Erkip, and S. Panwar, “A WiFi measurement in 802.11g networks,” *Technical Note. Available online: (http://wireless.poly.edu/attachment/wiki/WikiStart/HTmeasurement.pdf?format=raw)*.
- [7] P. C. Ng and S. C. Liew, “Throughput analysis of IEEE 802.11 multi-hop ad hoc networks,” *IEEE/ACM Trans. on Networking*, vol. 15, pp. 309–322, Apr. 2007.
- [8] P. Liu, Z. Tao, S. Narayanan, T. Korakis, and S. S. Panwar, “CoopMAC: a cooperative MAC for wireless LANs,” *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 340–354, Feb. 2007.
- [9] F. Hung, S. Pai, and I. Marsic, “Performance modeling and analysis of the IEEE 802.11 distribution coordination function in presence of hidden stations,” in *Proc. of MILCOM*, 2006.
- [10] Z. Hadzi-Velkov and L. Gavrilovska, “Performance of the IEEE 802.11 wireless LANs and influence of hidden terminals,” in *Proc. of 4th Int’l Conf. on Telecommunications in Modern Satellite, Cable and Broadcasting Services*, 1999.
- [11] H. S. Chhaya and S. Gupta, “Throughput and fairness properties of asynchronous data transfer methods in the IEEE 802.11 MAC protocol,” in *Proc. of PIMRC*, 1995.
- [12] H. S. Chhaya and S. Gupta, “Performance of asynchronous data transfer methods of IEEE 802.11 MAC protocol,” *IEEE Personal Communications*, vol. 3, pp. 8–15, Oct. 1996.
- [13] H. Takagi and L. Kleinrock, “Optimal transmission ranges for randomly distributed packet radio terminals,” *IEEE Trans. on Communications*, vol. 32, pp. 246–257, Mar. 1984.
- [14] Y. Wang, N. Yan, and T. Li, “Throughput analysis of IEEE 802.11 in multi-hop ad hoc networks,” in *Proc. of WiCOM*, 2006.
- [15] *OPNET*. <http://www.opnet.com/>.
- [16] *MadWifi driver*. <http://madwifi.org/>.