Understanding Interference and Carrier Sensing in Wireless Mesh Networks

Jeongkeun Lee*, Sung-Ju Lee[†], Wonho Kim*, Daehyung Jo*, Taekyoung Kwon*, and Yanghee Choi*

*School of Computer Science and Engineering, Seoul National University [†]Mobile and Media Systems Lab, Hewlett-Packard Laboratories Email: jklee@mmlab.snu.ac.kr, sjlee@hp.com, whkim@mmlab.snu.ac.kr, cdh@mmlab.snu.ac.kr, tkkwon@snu.ac.kr, yhchoi@snu.ac.kr

Abstract

Wireless mesh networks aim to provide high speed Internet service without costly network infrastructure deployment and maintenance. The main obstacle in achieving high capacity wireless mesh networks is interference between the mesh links. In this article, we analyze the carrier sensing and interference relations between two wireless links and measure the impact of these relations on link capacity on an indoor 802.11a mesh network testbed. We show that asymmetric carrier sensing and/or interference relations commonly exist in wireless mesh networks and study their impact on the link capacity and fair channel access. In addition, we investigate the effect of traffic rate on link capacity in the presence of interference.

I. INTRODUCTION

Most research in Wireless mesh networks (WMNs) focuses on the capacity improvement in the mesh backbone. As wireless mesh nodes typically have no mobility and employ CSMA protocols in a multi-hop environment, interference is the main obstacle in achieving high capacity. Understanding the wireless link behavior in the face of interference helps to manage the network

This work was supported in part by the Hewlett-Packard Laboratories University Relations Program and the National Information Society Agency (NIA) of Korea.

performance by various measures: traffic engineering, route selection, layout planning, etc. Because of the multihop nature of WMNs, WMNs suffer from hidden interference and self interference. Hence, the effects of interference is more severe than in single-hop WLANs.

Recent work proposes to use multiple channels and/or multiple radios [1] to overcome interference and increase capacity. Nevertheless, we concentrate our effort on studying interference together with carrier sensing in a single channel WMNs as (i) it is a good first step in investigating the wireless channel behavior with interference, (ii) its findings still apply to networks with multiple channels and radios, and (iii) many deployed WMNs use only a single radio and channel because of low cost and complexity [2].

We study interference on WMNs by investigating its relation with CS. We categorize their relations on two wireless links and carry out testbed experiments to evaluate their effect on the link performance. Using our indoor 802.11a testbed measurements, we study the degree of interference on each relation category and also the fairness of channel access between the two links. We use both saturated and rate-controlled network traffic to investigate the impact of traffic load on link performance.

The IEEE 802.11 standard suggests the use of RTS/CTS to solve the hidden interference problem. The RTS/CTS mechanism however, is shown to be ineffective in eliminating the hidden node problem [3] and fails to increase the multihop capacity [4]. Thus, we investigate the CS and interference relations without considering RTC/CTS.

We believe the testbed experimental analysis helps us better understand interference and its impact on capacity: an aspect that is critical for the protocol design and wireless capacity improvement. We characterize non-endpoint sharing pairwise 802.11 links based on their carrier sensing and interference relation. This method of link pair categorization was proposed by Garetto *et al.* [5] using modeling and simulation. But there is a need to validate models in a real system deployment. We describe the behavior of 802.11 links based on measurements and present new findings that modeling and simulation can not reveal.

The rest of the article is organized as follows. We provide a background study in Section II. The next two sections present testbed results and analyses. The relation of carrier sensing and interference with saturated traffic is investigated in Section III and rate-controlled traffic in Section IV. We conclude in Section V.

II. BACKGROUND

In order to define CS and interference relations, we consider two links L_1 and L_2 that do not share end-points. On L_1 and L_2 , nodes S_1 and S_2 transmit data to nodes R_1 and R_2 , respectively, as illustrated in Fig. 1. Arrows in the figure indicate the directions of data/ACK packets, interference signals, and sensed signals. The CS relation between the two links is decided by the two senders S_1 and S_2 , while the interference relation depends on how one sender affects the other link: i.e., S_1 's effect on L_2 , and S_2 's effect on L_1 .

A. CS Relation

In the 802.11 CS mechanism, a wireless station withholds its transmission when it senses an ongoing transmission on the medium. In Fig. 1, when S_1 senses S_2 's transmission, a CS relation exists between the two links and we say L_2 is carrier sensed by L_1 . We estimate whether S_1 senses the transmission of S_2 by observing S_1 's broadcast transmission throughput when S_2 is transmitting simultaneously. When S_1 senses S_2 's transmission, due to the 802.11 CSMA/CA mechanism, its transmission throughput is about a half of the throughput measured when S_1 does not sense S_2 's transmission. Fig. 1 illustrates an asymmetric CS relation. In our testbed network deployed in HP Labs in Palo Alto, 17% of the node pairs exhibit asymmetric CS relation, 14% of them exhibit mutual CS relation, and 69% of node pairs do not sense each other.

B. Interference Relation

We define the interference relation independently of the CS relation. In Fig. 1, if S_1 and S_2 simultaneously transmit and S_2 's transmission hinders R_1 's reception of S_1 's packet, we say L_1 is interfered by L_2 (or S_2) regardless of whether the interferer S_2 is carrier sensed by S_1 . In reality, if both S_1 and S_2 sense each other, they do not transmit simultaneously assuming the carrier sensing and collision avoidance mechanisms. We however define the interference relation independently of the CS relation for the simplicity of case enumeration.

Interference becomes more effective as the signal-to-interference-ratio (SIR) at R_1 becomes smaller due to S_2 's transmission. The SIR is defined as "Received Signal Strength (RSS) from S_1 minus RSS from S_2 " in dB scale. If the SIR at R_1 goes below a certain threshold, (which depends on the PHY bit rate of S_1 's transmission,) S_2 effectively interferes R_1 's reception of packets from S_1 . If SIR is above the threshold, the physical layer capture (PLC) in 802.11 occurs and S_1 's signal is successfully received at R_1 despite S_2 's simultaneous transmission. The arrival timing order and received signal strengths of two packets at a receiver determines whether PLC occurs [6].

Note that R_1 being able to receive S_2 's packets does not necessarily mean that R_1 is interfered by S_2 . Its converse is not true, either. For example, if S_1 is much closer to R_1 than S_2 is, R_1 can still decode the packets from S_1 due to high SIR despite the interferer S2. In general, interference is determined by the SIR relation between the two senders and one receiver. Thus, estimating interference solely based on the existence of a communication link, which is popular in the literature, is not correct, and hence recent research tends to use the SIR-based interference models.

As we consider large data packets (i.e. MAC frame size is 1064 bytes), we ignore the interference caused by ACK packets as its frame size is 14 bytes. Supporting observations have been made in [7]. This simplification helps us to focus on the interaction between CS and inter-data packet interference.

C. State Representation of Carrier Sensing and Interference

Although CS and interference states can be continuous, we consider a binary states for both CS and interference for simplicity. If S_1 senses S_2 's transmission, the CS state of L_1 by L_2 is expressed as C_1 :1, and otherwise C_1 :0. Similarly, if L_1 suffers interference from L_2 (or S_2), the interference state of L_1 by L_2 is F_1 :1, and otherwise F_1 :0. Thus, the CS and interference relation of a link to the other link is defined as one of four states: 11, 10, 01, and 00. In the example in Fig. 1, L_1 's state by L_2 is C_1 :1 / F_1 :1 and the state of L_2 by L_1 is C_2 :0 / F_2 :0. We use a subscript X for a *don't care* state; X can be either 1 or 0.

III. CARRIER SENSING AND INTERFERENCE WITH SATURATED TRAFFIC

To help understanding, we distinguish between the throughput at a transmitter (TX) and the goodput at a receiver (RX). Throughput is defined as the number of bits per second transmitted at the transmitter's application whereas goodput is defined as the number of bits per second received at the receiver's application. In the presence of interference, RX goodput may be smaller than TX throughput.

In this section, in order to understand the effect of CS and interference on the capacity of two links, we first consider the case-by-case link throughput/goodput when both senders always have packets to send (i.e., traffic is saturated). Because each of CS and interference relations between two links can have one of four states (11, 10, 01, and 00) as shown in Section II-C, the number of combinations of two links' CS and interference states is 16.

We first exclude the four cases when two senders sense each other $(C_1C_2:11, F_1F_2:XX)$ as our measurement shows that there is little interference in these cases. Both links have a fair share of broadcast/unicast throughput/goodput.

After excluding the above four cases, we have 12 remaining cases. The cases where only L_1 is interfered and the cases where only L_2 is interfered result in symmetric throughput/goodput scenarios. We thus ignore one of two symmetric interference states and exclude three cases when only L_2 suffers interference (F_1F_2 :01). We consider three cases where only L_1 suffers interference (F_1F_2 :10).

We now have nine remaining cases as shown in Fig. 2 (A). The row index represents the CS relation and the column index represents the interference relation. Although we see two pairs of symmetric cases (*cases 1, 4* and *cases 3, 6*), we do not remove them for the sake of presentation. Based on the nine cases' distinctive performance characteristics, we classify them into four groups as shown in Fig. 2 (B)

A. Test-bed Experiments

We embodied nine network topologies corresponding to Fig. 2 (A) on our testbed which consists of small-form factor single-board computers with mini-PCI 802.11a cards using Atheros chipset. To embody each topology case with different CS and interference relations, we controlled the node placement, transmission power, and transmission/receiving antennas. The applications on S_1 and S_2 generate UDP packets of 1000 bytes and continuously send them to R_1 and R_2 respectively, to make their output queue always backlogged (saturated). Each broadcast/unicast transmission period was 30 seconds. During the entire experiments, the PHY rate is fixed at 6 Mbps, which is the lowest and the most robust bit rate in IEEE 802.11a. We used a clear 802.11a channel to avoid interference from other networks.

We first measure the maximum achievable throughput/goodput of a link which will be used as a reference value. Each link's maximum TX throughput (sending traffic rate at a transmitter) and RX goodput (traffic rate successfully delivered to a receiver) are measured by activating one link while deactivating the other link. The measured maximum throughput/goodput of broadcast/unicast are about 5 Mbps in our experiments. Because of the PHY/MAC overhead, the maximum throughput/goodput is approximately 5 Mbps although the PHY bit rate is 6 Mbps. We call this 5 Mbps "interference-free" throughput/goodput as the *channel capacity* of 6 Mbps PHY rate.

For each nine topology cases, we measured the throughput and goodput of UDP broadcast and unicast of L_1 and L_2 when both links are simultaneously active and the input traffic is always backlogged. We verified that each link's interference-free throughput and goodput reach the channel capacity before testing the simultaneous transmissions. Fig. 3 shows the throughput/goodput of each link for the nine cases with saturated traffic. We now analyze the unique performance characteristics of the four groups classified in Fig. 2 (b) based on the observations from Fig. 3.

B. No Interference

Because both links in this group (*cases 3, 6, and 9*) are free from interference, goodput is the same with throughput for every cases. Analyzing this group helps us understand the effects of (especially asymmetric) carrier sensing on TX throughput.

Case 9 shows the expected results: when two links operate independently without sensing each other, both links fully utilize the channel capacity.

When the CS relation is asymmetric, the TX throughput of the sender which does not sense the other sender is the channel capacity as expected (L_2 in case 3 and L_1 in case 6). The throughput of the carrier sensing sender however, differs from the expectation that it is the half of channel capacity. For broadcast, TX throughput is 2 Mbps (smaller than 2.5) while it is 3.1 Mbps for unicast. For broadcast, we identify Extended Inter-Frame Spacing (EIFS) of 802.11 as the cause of smaller throughput. In 802.11 MAC, a node that has received a packet that it could not decode may go into the EIFS mode and waits until either receiving an error-free frame or the expiration of EIFS time which is longer than the double of Distributed Inter-Frame Spacing (DIFS) time in 802.11.

Let us take *case* 6 for example. Suppose the carrier sensing sender S_2 attempts to transmit a broadcast data and chooses a backoff counter that is smaller than S_1 's, as illustrated by ' S_2 wins'

in Fig. 4 (A). Because S_1 does not sense S_2 's transmission, S_1 also starts its transmission. As S_1 's transmission starts later then S_2 's, S_2 receives only the latter part of S_1 's transmission right after finishing its own transmission. Because S_2 missed the preamble and PHY header of S_1 's packet, S_2 is unable to decode S_1 's packet and hence goes into the EIFS mode. While S_1 waits for EIFS duration, S_1 begins its backoff counter earlier than S_2 , which increases the possibility that S_1 will win the channel contention and start the next transmission before S_2 's backoff counter expires (' S_1 wins' in Fig. 4 (A)). In this manner, S_2 , the sender which carrier senses, has transmission probability of less than 50% after its previous transmission. According to 802.11 MAC standard, EIFS occurs only when the PHY indicates to the MAC that an 802.11 frame transmission has begun but did not result in the correct reception of a complete MAC frame. In Fig. 4 (A) where S_2 can not recognize the beginning of S_1 's frame transmission which takes place while S_2 is transmitting, based on the standard EIFS should not occur. Our backoff time measurement and analysis, however, prove that EIFS occurs in the case of Fig. 4 (A)) with our Atheros 802.11 cards. We believe the card can recognize a 802.11 frame transmission with its preamble missed although the card can not decode the frame correctly.

When unicast traffic is examined, we observe a different scenario as illustrated in Fig. 4 (B). In this case, the carrier sensing sender S_2 receives an ACK from its receiver R_2 after its data transmission; thus, S_2 is less likely to sense the latter part of S_1 's transmission and go into the EIFS mode than the broadcast scenario. Furthermore, because S_2 does not sense R_1 's ACK transmission, S_2 will start decrementing its backoff counter while S_1 is receiving an ACK from R_1 . Thus, S_2 with unicast transmission, has the transmission probability greater than 50% not only after its previous transmission (second ' S_2 wins' in Fig. 4 (B)) but also after yielding the channel by sensing S_1 's data transmission (first ' S_2 wins' after busy state).

We confirmed the above arguments by observing the transmission order and inter-transmission time of S_1 and S_2 by using a 802.11 packet sniffer.

C. One-way Hidden Interference

In this group of cases 2, 5, and 8, where the interference relation is asymmetric and at least one of two senders cannot sense the other, the goodput exhibits severe unfairness between the two links. In particular, with unicast transmission, the link whose interference state is F:1 has nearly zero goodput while the other link's goodput is close to the channel capacity. We can take the following two lessons.

1) Hidden node problem occurs no matter which sender is hidden: We observe that a link is interfered when at least one of the senders of the link pair is hidden; either the sender of the link or the interfering sender of the other link (i.e., C_1C_2 is 10, 01, or 00). The term hidden interference commonly refers to only the case C_1C_2 :00. However, two more cases should be addressed: (1) the sender is hidden from the interferer (e.g., in case 2, S_1 is hidden from its interference S_2 and L_1 has almost zero unicast goodput), and (2) the interferer is hidden from the sender (e.g., the interferer S_2 in case 5 is hidden and L_1 has almost zero unicast goodput).

2) The winner takes it all: In this group, the interference-free (F:0) link takes most, if not all, of the channel capacity with unicast traffic. This is evident in case 5, where the broadcast goodput result shows a nearly fair share between the two links whereas the unicast goodput share is extremely unfair. It is due to the exponential backoff mechanism, which form a vicious cycle in case 5 as follows:

- 1) S_1 of the interfered link L_1 increases its contention window when it does not receive an ACK from R_1 .
- 2) S_1 's packet transmission rate decreases.
- 3) S_2 gets more chances to transmit while S_1 refrains its transmission due to the increased contention window. S_2 's TX throughput hence increases.
- 4) As the interferer S_2 's TX throughput increases, the packet drop rate of L_1 increases, and S_1 's contention window is again doubled.

As the above cycle repeats, L_1 's unicast RX goodput drastically drops and reaches near zero while L_2 takes most of the channel capacity. Note that this phenomenon in unicast contrasts that of broadcast. Because there is no explicit ACK mechanism for broadcast packets, the sender does not know whether its broadcast packet is collided and no backoff occurs. That is why the broadcast TX throughput of the interfered links in this group does not decrease despite packet collisions resulting from interference.

D. Mutual Interference & Asymmetric CS

In this group of cases 1 and 4, we find that if both links suffer from interference and the CS relation is asymmetric, the link that does not sense takes most of the channel capacity. The sender sensing the other sender's transmissions, for example S_1 in case 1, begins to yield

the channel which in turn, will decrease the other link's (L_2) collision probability at R_2 . L_1 's collision probability at R_1 however, remains high as L_2 does not sense L_1 and hence does not yield the channel. Thus, S_1 's contention window increases faster than S_2 's. Therefore, L_2 takes most of the channel capacity and L_1 's goodput reaches almost zero.

In this group, the aggregate broadcast goodput (3 Mbps) is much less than the aggregate unicast goodput (4.4 Mbps). In broadcast, the carrier sensing sender (e.g., S_1 in case 1) is not aware of the interference due to the lack of ACK feedback and does not backoff or decrease its transmission rate. Thus, both links suffer from interference and broadcast goodput degradation.

E. Mutually Hidden Interference

In this group of *case* 7, both links interfere and are hidden from each other, which results in poor performance of both links. The goodput degradation becomes intensified because of saturated traffic from both senders. This problematic topology scenario commonly exists as 22% of link pairs in our 10-node testbed fall into this category. Note that in this case, the payload size as well as the PHY bit rate can yield a somewhat different throughput/goodput as reported in [8]. We found that our measurement results follow the model in [8]. For example, the performance degradation becomes intensified as the larger payload size is used.

When we observe the aggregate goodput with unicast for all four groups, there are important findings. The aggregate unicast goodput reaches at least almost the channel capacity in all groups except this *Mutual Hidden INT* group. In the other groups, if any one of two senders senses the other, the aggregate unicast goodput reaches almost the channel capacity regardless of the interference relation. This is true even in cases when both links interfere with each other, as shown in *cases 1 and 4*. In the example of *case 1*, due to the backoff mechanism, S_1 decreases its transmission rate, which helps the other to survive interference.

F. Occurrence Frequency

We measured how frequently each of four groups occurs in our 10-node testbed deployed in HP labs. Fig. 5 shows the layout of the deployed testbed from our topology management program. Note that in this experiment, we did not control the antenna/node positions and transmission power to observe the natural topological characteristics. We choose a pair of links where each link has greater than 2.5 Mbps interference-free goodput. We found a total of 152 such pairs.

In Fig. 5, we can observe that many links are asymmetric in the natural deployment. Fig. 2 (b) shows the occurrence percentage of each group from the 152 pairs in our testbed. Note here we examine link pairs and not node pairs. The occurrence frequency of *one-way hidden interference* group contains all the six cases including the excluded symmetric three cases. As for the cases when both senders sense each other (which are omitted in Fig. 2), the occurrence frequency is 39%.

G. Summary

The major findings from our measurement study are listed as follows. First, when the CS relation is asymmetric, the carrier sensing sender has more TX throughput with unicast transmission than with broadcast transmission due to 802.11 MAC mechanisms (EIFS and unicast ACK). Second, hidden interference should include two asymmetric cases (i) when the interferer is hidden from the sender, and (ii) when the sender is hidden from the interferer. Third, in *one-way hidden interference* group and *mutual interference* & *asymmetric CS* group, the unicast goodput share is extremely unfair. In our testbed results, about 24% of link pairs suffer from this extreme unfairness. Fourth, in *mutually hidden interference* group which occurs frequently (22%), both links suffer from poor performance.

IV. CARRIER SENSING AND INTERFERENCE WITH RATE-CONTROLLED TRAFFIC

We now investigate the link behavior with rate-controlled traffic. A sender's application program periodically transmits packets by the given traffic rate. The UDP transmission rate (TX throughput) can not exceed the given rate in any cases. We observed that the broadcast/unicast throughput/goodput results for 1 Mbps traffic rate range between 0.8 and 1 Mbps in all cases. Two links have fair share of goodput regardless of the relation between interference and CS when the traffic load is light (1 Mbps).

We present the 2.5 Mbps traffic rate results in Fig. 6. Below are the findings from this experiment:

The links that had low goodput in the saturated channel scenario have greater goodput (up to 2.5 Mbps) as we test with the rate-controlled traffic. Furthermore, the aggregate unicast goodput with rate-controlled traffic becomes almost as high as the aggregate goodput from the saturated scenarios in some cases; compare *cases 5 and 8* in Figs. 3 and 6.

This observation gives an important hint to traffic engineering and network management. As most off-the-shelf wireless LAN and mesh devices do not support TDMA-like link scheduling, we cannot avoid link interference in the CSMA MAC systems even if the link interference information is available. Mesh backbone networks are usually stationary and operated/managed by a single operator. Thus, after we obtain the CS and interference information (by measurement or prediction), we can control the traffic intensity on each link by selecting the appropriate routing paths and shaping the traffic at the mesh nodes. By doing so, although it is not possible to completely avoid link interference and packet collisions in CSMA systems, we can control the effect of link interference and eventually utilize the network capacity more efficiently as the given CS and interference relations allow.

2) Packet drop rate is significantly reduced with rate-controlled traffic. In case 1 in Fig. 6, L_1 suffers (hidden) interference from L_2 and its unicast TX throughput is smaller than broadcast TX throughput. In unicast mode, how frequently S_1 performs backoff depends on L_2 's traffic rate. Note that however, its unicast RX goodput is equal to the unicast TX throughput while broadcast RX goodput is less than half of the broadcast TX throughput. With rate-controlled interfering traffic, we observe that the transmission failure rate is not so high as to cause packet drops. In 802.11 MAC, by default, the failure of four consecutive retransmissions indicates a packet drop. Because the interfering L_2 's traffic rate is controlled, L_2 does not exploit all the channel idle time during L_1 's backoff. This allows L_1 to use some portion of the channel.

This observation of reduced packet drop rate gives another implication of traffic engineering in multi-hop wireless networks. Multi-hop routing protocols consider a wireless link to be broken when consecutive packets drop and use an alternate path or attempt to rediscover a route even though the link is active and could be suffering from only temporary interference. This re-routing instability [9] causes drastic performance degradation. Thus, rate control can not only alleviate MAC-level fairness problem but also mitigate upper-layer performance variation in wireless mesh networks.

V. CONCLUSION

Understanding the link behavior in the presence of interference is the key in achieving high capacity wireless mesh networks. We addressed this important task by studying the interaction of interference and carrier sensing. We experimentally characterized the different couplings of carrier sense and interference relations that are possible between two 802.11 links. We investigated the impact of these relations on the capacity of the link pairs, with both saturated and rate-controlled traffic. We showed that the asymmetric carrier sensing and interference relations together with the traffic intensity determine the link capacity and the channel access fairness.

We value this experimental study as a first step towards a more comprehensive understanding of interference in wireless mesh networks. First, we are now studying a measurement-based approach to estimate the topology of a given (deployed) wireless network - carrier sense relation, interference relation and link performance. The RSS-based prediction (RBP) methodology [10] shows that we can estimate link throughput/goodput by using the measurement data of this paper. Second, although we have studied only one-hop links in this paper, we can apply our scheme to multi-hop routes. In fact, because our scheme identifies hidden interferers and its impact on link capacity, we can estimate the self interference (or intra-flow interference) of multi-hop routes by evaluating the relation between each pair of non-adjacent links on the route (e.g., first and third links of the route, first and fourth links, second and fourth links, etc.). Extending our work to multiple interferers is not as straightforward. A simple solution is to generate additional carrier sensing/interference relations that consider multiple links. This approach however, will result in a large number of relation cases, and generating each case topology is a difficult task. We believe a measurement-based modeling is more efficient and effective approach for multi-link interference. Applying the major findings of this study, such as the impact of asymmetric carrier sensing relations on hidden interference and link capacity, into multi-link interference modeling is part of our ongoing work.

REFERENCES

[2] Tropos Networks. http://www.tropos.com/.

^[1] K. Ramachandran, E. Belding-Royer, K. Almeroth, and M. Buddhikot, "Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks," in *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006.

^[3] K. Xu, M. Gerla, and S. Bae, "How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks?" in Proc. IEEE GLOBECOM, Taipei, Nov. 2002.

- [4] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, "Architecture and Evaluation of an Unplanned 802.11b Mesh Network," in *Proc. ACM MobiCom*, Cologne, Germany, Aug. 2005.
- [5] M. Garetto, J. Shi, and E. W. Knightly, "Modeling Media Access in Embedded Two-Flow Topologies of Multi-hop Wireless Networks," in *Proc. ACM MobiCom*, Cologne, Germany, Aug. 2005.
- [6] A. Kochut, A. Vasan, A. Shankar, and A. Agrawala, "Sniffing out the correct physical layer capture model in 802.11b," in *Proc. IEEE ICNP*, Berlin, Germany, Oct. 2004.
- [7] J. Padhye, S. Agarwal, V. Padmanabhan, L. Qiu, A. Rao, and B. Zill, "Estimation of Link Interference in Static Multi-hop Wireless Networks," in *Proc. Internet Measurement Conference (IMC)*, Berkeley, CA, USA, Oct. 2005.
- [8] H. Chang and V. Misra, "802.11 Link Interference: A Simple Model and A Performance Enhancement," in Proc. NETWORKING, Waterloo, Canada, May 2005.
- [9] P. C. Ng and S. C. Liew, "Re-routing instability in IEEE 802.11 multi-hop ad-hoc networks," in *Proc. IEEE LCN*, Tampa, FL, USA, Nov. 2004.
- [10] J. Lee, S. Lee, W. Kim, D. Jo, T. Kwon, and Y. Choi, "RSS-based Carrier Sensing and Interference Estimation in 802.11 Wireless Networks," in *Proc. IEEE SECON*, San Diego, CA, 2007.



Fig. 1. Example of carrier sensing and interference between L_1 and L_2 .



(A) 9 Carrier Sensing and Interference cases



(B) Four Groups (the number in parenthesis is the occurrence frequency of each group in our testbed)

Fig. 2. Nine distinct cases and four groups. In the group names, INT denotes interference.



Fig. 3. Link throughput/goodput for nine cases in two saturated links.



Fig. 4. Channel access scenario of asymmetric CS links.



Fig. 5. Snapshot of a testbed deployment



Fig. 6. Link throughput/goodput for nine cases with 2.5 Mbps traffic.