Throughput Analysis of IEEE802.11 Multi-hop Ad hoc Networks

Ping Chung Ng, *Student Member, IEEE* and Soung Chang Liew, *Senior Member, IEEE*

Abstract—**In multi-hop ad hoc networks, stations may pump more traffic into the networks than can be supported, resulting in high packet-loss rate, re-routing instability and unfairness problems. This paper shows that controlling the offered load at the sources can eliminate these problems. To verify the simulation results, we set up a real 6-node multi-hop network. The experimental measurements confirm the existence of the optimal offered load. In addition, we provide an analysis to estimate the optimal offered load that maximizes the throughput of a multi-hop traffic flow. We believe this is a first paper in the literature to provide a quantitative analysis (as opposed to simulation) for the impact of hidden nodes and signal capture on sustainable throughput. The analysis is based on the observation that a large-scale 802.11 network with hidden nodes is a network in which the carrier-sensing capability breaks down partially. Its performance is therefore somewhere between a carrier-sensing network and an Aloha network. Indeed, our analytical closed-form solution has the appearance of the throughput equation of the Aloha network. Our approach allows one to identify whether the performance of an 802.11 network is hidden-node limited or spatial-reuse limited.**

***Index Terms*—Wireless Networks, Ad hoc Networks, Multi-hop Networks, IEEE 802.11, Capacity, Performance Analysis**

I. Introduction

A wireless multi-hop ad hoc network provides quick and easy networking in circumstances that require temporary network services or when cabling is difficult. The IEEE 802.11 Distributed Co-ordination Function (DCF), based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), is the most popular MAC protocol used in wireless ad hoc networks.

In wireless networks, interferences are location-dependent. For a traffic flow from a source node to a destination node in a multi-hop network, the nodes in the middle of the path have to contend with more nodes when forwarding the traffic of the flow. Experiencing lighter contention, the source node may inject more traffic into the path than can be forwarded by the later nodes. This may result in excessive packet losses and re-routing instability. When there are multiple flows, unfairness may also arise when some flows experience higher contention than other flows.

The capacity of wireless networks has been studied extensively. Much of the previous work focused on computing theoretical throughput bounds (e.g. [1][2]). Some of these throughput limits are obtained under the assumption of global scheduling [3][4]. The popular IEEE 802.11 wireless networks in use today are not amenable to such global scheduling.

This paper primarily focuses on 802.11 and 802.11-like networks. Although there were also prior investigations [5][6] on how to modify the 802.11 protocol to solve performance problems, we try not to perturb the protocol too drastically so that the same standard-based equipment can be used without major redesign.

To devise schemes to achieve high throughput and fairness in multi-hop networks, it is important to be able to analyze the *contention experienced by a node* as a function of the network topology and traffic flows in a quantitative manner. Such an analysis is currently lacking in the literature, possibly due to the fact that the analysis is complicated by the existence of hidden-node and signal-capturing effects. This paper is a first attempt toward such a quantitative analysis. The analysis yields insight into the impact of different network parameters and properties on performance. As an example, we use our analysis to establish the optimal offered load for a traffic flow in this paper.

Most previous studies of the hidden-node problem of 802.11 were conducted by simulations [2][7]. References [8][9] extended the hearing graph framework in [10] to model hidden nodes and node mobility using a Markov chain. They established a relationship between the average number of stations hidden from each other and the likelihood of a station remaining in its Basic Service Area. Their results on the effect of hidden nodes on throughput, however, were obtained from simulations, not analysis. In addition, the signal capture property that allows a packet to be received successfully despite transmissions by hidden nodes was ignored.

The rest of this paper is organized as follows. In Section II, we review the major performance problems in multi-hop ad hoc

Manuscript received March 14, 2005; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor S. Palazzo. This work was supported by the Areas of Excellence scheme (Project Number AoE/E-01/99) and the Competitive Earmarked Research Grant (Project Number 414305) established under the University Grant Committee of the Hong Kong Special Administrative Region, China.

P. C. Ng was with the Chinese University of Hong Kong, Hong Kong. He is now with the Department of Engineering Science, University of Oxford, Oxford, OX1 3PJ, U.K. (e-mail: ping.ng@eng.ox.ac.uk).

S. C. Liew is with the Chinese University of Hong Kong, Hong Kong. . (e-mail: soung@ie.cuhk.edu.hk).

networks and suggest possible solutions to them. Our real-network experiments confirm the offered load control solution. Section III analyzes factors which degrade the throughput, and formulate a method to estimate the optimal offered load in a single multi-hop traffic flow. In particular, we present the derivation of the throughput limits imposed by (i) carrier sensing and (ii) hidden nodes. For simplicity, the analysis in Section III is based on a specific inter-node distance in the multi-hop flow. The analysis is extended to the general case in the Appendix. We show that in general, the throughput of a single multi-hop flow is hidden-node limited and not carrier-sensing limited. Section IV gives an example where two opposite directional multi-hop flows may cause the throughput to be carrier-sensing limited instead. Section V concludes this paper.

II. Performance Problems in 802.11 Multi-hop Networks: Single-Flow Investigation

In a multi-hop ad hoc network, sources may inject more traffic into the network than can be supported. This may result in two problems: 1) high packet loss rate, and 2) re-routing instability. In this section, we use an 8-node string multi-hop network as an example to illustrate these problems. In Fig. 1, the distance between consecutive nodes is fixed to 250m. Node 1 sends a UDP traffic stream to node 8. The traffic is generated at node 1 in a saturated manner in which as soon as a packet is transmitted to node 2, another is waiting in line. The traffic at later nodes all originates from node 1 and is not saturated.

The simulations in this paper were conducted using NS2.1b9 [11]. All nodes communicate using identical, half-duplex wireless radio based on the 802.11 DCF, with data and basic rates set at 11Mbps. The RTS/CTS mechanism is turned off. Nodes are stationary. The transmission range is 250m and the carrier-sensing range is 550m. The Ad hoc On-Demand Distance Vector (AODV) routing protocol and the two-ray propagation model are used. The capture threshold *CPThreshold* is set to 10dB which induces the interference range for a link of length 250m to be 445m. Unless specified otherwise, all data sources are UDP traffic streams with fixed packet size of 1460bytes.

A. High Packet-Drop Rate

Figure 2 shows the per-hop throughput of an 8-node flow obtained from simulations. The throughputs plotted are obtained by averaging over one-second intervals.

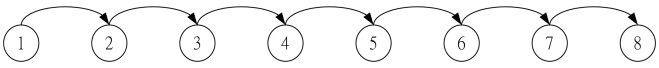
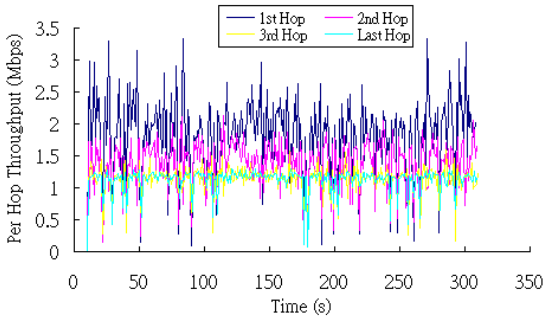


Figure 1. UDP traffic flow with node 1 as the source and node 8 as the destination in an 8-node multi-hop traffic flow

In Fig. 1, node 1 can sense the transmissions from nodes 2 and 3. This means node 1 must share the channel capacity with them. As a result, the throughput of the first hop is approximately 1/3 of the total channel capacity. Node 2, on the other hand, can be interfered by nodes 1, 3 and 4. This results in approximately 1/4 of the total channel capacity for the second hop. After that, each node must compete with four other nodes. The per-hop throughput stabilizes from the third hop to the last hop with approximately 1/5 of the total channel capacity. The first and the second nodes pump more packets to the following nodes than they can forward. This results in excessive packet drops at the second and the third node.

As shown in Fig. 2, the average throughput drops from 1.83Mbps at the first hop to 1.13Mbps at the last hop. In other words, about 40% of packets are lost in transit. This high packet-loss rate is undesirable, especially for real-time traffic without a retransmission mechanism at the upper protocol layer.



Hop	Mean	Var	Max	Min
1st	1.826	0.356	3.336	0.089
2nd	1.394	0.150	2.126	0.146
3rd	1.141	0.043	1.577	0.268
Last	1.130	0.032	1.305	0.078

Figure 2. Per-hop throughputs of an 8-node flow

B. Re-routing Instability

Figure 2 also shows that the throughputs tend to oscillate widely over time. The throughput oscillations are caused by triggering of the re-routing function. In the multi-hop path, nodes 1 and 2 sense fewer interfering nodes than later nodes. As a result, they pump more traffic into the network than it can support. This results in a high contention rate at the later nodes. When one of the later nodes fails to transmit a packet after a number of retries, it declares the link as being broken. The routing agent is then invoked to look for a new route. Before a new route is discovered, no packet can be transmitted, causing the throughput to drop drastically. In the string network topology under study, there is only one route from node 1 to node 8, so the routing agent will eventually "re-discover" the same route again. The breaking and rediscovery of the path results in the drastic throughput oscillations observed. For a general network with multiple paths from source to destination, the same throughput oscillations will still be expected. This is because the declaration of the link failure is caused by self-interference of traffic of the same flow at adjacent nodes. More details on re-routing instability can be found in [12][13].

1) Hidden-Node Problem

Besides the collisions of packets among nodes inside a carrier sensing range, the hidden-node problem further increases the

chance of link-failure declarations. Consider Fig. 3. When node 4 sends a packet to node 5, node 2 senses the channel to be busy while node 1 senses the channel to be idle, since node 4 is inside the carrier-sensing range of node 2 but outside that of node 1. Once node 1 senses the channel as idle, it may count down its back-off contention window until zero and transmit a packet to node 2.

If the transmission from node 4 is still in progress, node 2 will continue to sense the channel as busy, and it will not receive the packet from node 1. As a result, node 2 will not return an ACK to node 1. Node 1 may then time out and double the contention window size for retransmission later.

Meanwhile, node 4 transmits the packet successfully and is not aware of the collision at node 2. When transmitting the next packet, node 4 will use the minimum contention window size. The hidden-node scenario favors node 4, and the chance of collision at node 2 can not be reduced even though node 1 backs off before the next retry. The hidden-node problem increases the chance of multiple retries by node 1, making the wrong declaration of link failures and therefore re-routing instability more likely.

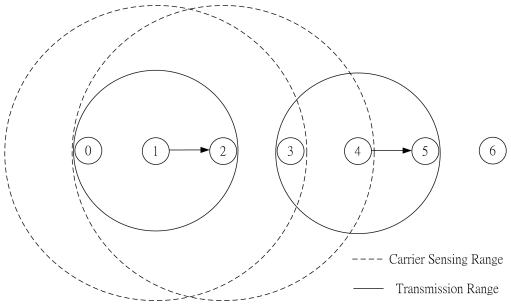


Figure 3. Node 4 as a hidden node to node 1

Note that the negative effect of a hidden node is much more than that of a contending node within the carrier-sensing range. This is because the carrier-sensing capability in the CSMA protocol breaks down with respect to the hidden node, making collisions much more likely.

The RTS/CTS mechanism in 802.11 is designed to solve the hidden node problem. However, using RTS/CTS in multi-hop networks does not eliminate the hidden node problem. For more details, the reader is referred to [5], in which it was argued that when the carrier-sensing range is larger than two times of the transmission range, RTS/CTS is no longer needed. In this paper, we assume the use of the basic access mode without RTS/CTS.

C. Solutions to High-Packet Loss Rate and Re-routing Instability

Reference [14] demonstrated the existence of an instability problem for a TCP traffic flow in a multi-hop network. It provided a solution to solve TCP instability by limiting the traffic at the transport layer. The solution assumes TCP Vegas and limits the TCP window size to at most 4. As a result, only a maximum of four packets can be in transit in the path at any one time. This prevents a node from hogging the channel for a long period of time.

Two observations are as follows. First, it is not clear that the solution is effective when there are multiple TCP flows along the same path, or when TCP flows on adjacent paths may interfere with the flow on the path. Second, the instability problem is caused by false declaration of link failures which is rooted at the link layer. This problem is not a phenomenon for TCP traffic only, but also for other types of traffic. Therefore, we believe a more general approach should attempt to solve this problem at the link layer.

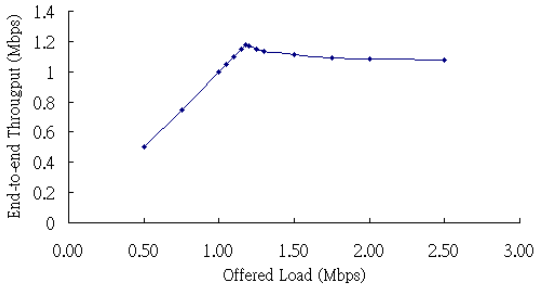


Figure 4. End-to-end throughput versus offered load in a 12-node flow

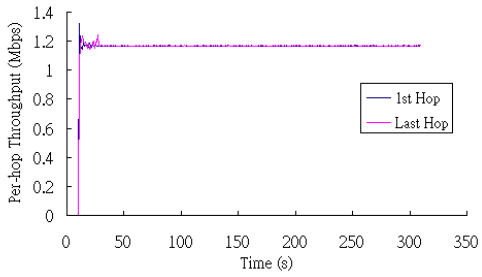


Figure 5. Per-hop throughputs with offered load control (at 1.18Mbps).

There are two possible link-layer solutions: 1) do not declare link failures before a new path can be discovered; or 2) control the offered load at the source to reduce contention rate.

1) Link-Failure Re-routing

Strictly speaking, in the above scenario the link has not failed, although it is congested and the attempt to look for a new path is definitely warranted. However, before a new route can be discovered, one should continue to use the old route. That is, a "don't-break-before-you-can-make" strategy should be adopted. We refer interested readers to [12][13] in which the "don't-break-before-you-can-make" strategy was implemented. Simulation results in the paper showed that the strategy can prevent the re-routing instability problem and reduce the throughput variations in multi-hop ad hoc networks drastically.

2) Controlling Offered Load

To prevent high packet loss rate for a flow, the offered load must be controlled. Figure 4 plots the simulation end-to-end throughputs of a 12-node multi-hop path versus offered load. The peak throughput is obtained at offered load of 1.18Mbps. Offered load beyond this is unsustainable and high loss rate results because Throughput < Offered Load. This existence of an optimal offered load for a multi-hop path was also pointed

out in [2]. In this paper, we provide an analysis to estimate the maximum sustainable throughput, and in doing so, reveal the factors that govern it.

Controlling offered load also prevents the instability problem even when the link-failure-triggered re-routing in the routing agent is enabled. Figure 5 shows that the instability problem is eliminated by setting the offered load at the optimal sending rate (1.18Mbps). However, the instability problem is solved by avoiding congestion condition rather than the removal of the problematic strategy of suspending the link usage before a new route can be discovered. A temporary external interference source (e.g., a nearby microwave oven) can easily cause the condition to arise again. We believe that even when offered-load control is exercised, a mechanism to deal with re-routing instability, such as that in [12][13], is still needed.

Figure 6. A 6-node multi-hop wireless network

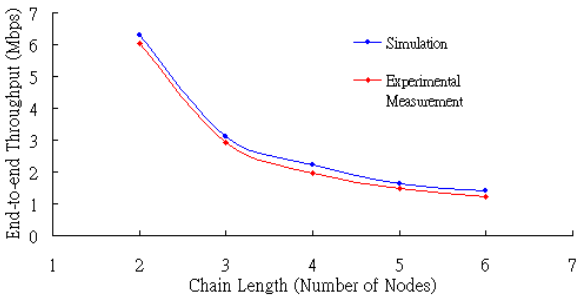


Figure 7. End-to-end throughput versus number of nodes in a string multi-hop network with saturated traffic source

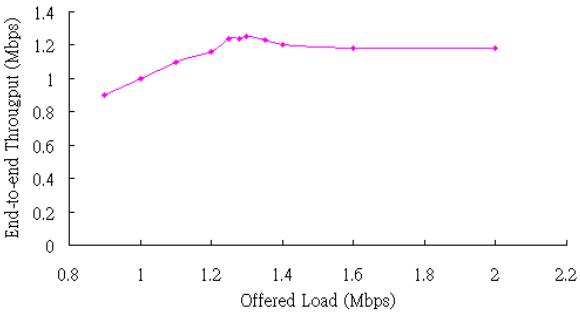


Figure 8. Experimental Measurements of end-to-end throughput versus offered load in a 6-node flow

D. Verification of NS-2 Simulator Under Multi-hop Network Setting

To verify the accuracy of the NS-2 simulator, we set up a real 6-node multi-hop network with six symmetric DELL Latitude D505 laptop PCs with 1.5GHz Celeron Mobile CPU and 512MB RAM. Each node has a Buffalo WLI2-CF-S11 IEEE 802.11b Wireless LAN card (as shown in Fig. 6). All nodes run RedHat Linux 9 with HostAP [15] driver. To facilitate experimentation, we fixed the transmission power of each WLAN card to a small value (-38dBm), with basic and data rates set at 11Mbps. We obtained the transmission range of TxRange $\approx$ 2m and the carrier-sensing range of CSRange $\approx$ 5m=2.5*TxRange by following similar approaches as mentioned in [16]. We fixed the routing table of each node and set the distance between successive nodes to 2m. The data sources are UDP traffic streams with fixed packet size of 1460bytes. Figure 7 shows that the simulation throughputs match closely with the experimental measurements, indicating that our simulations do not contain major deficiencies. We adjusted the offered load at the source in the 6-node network. Figure 8 shows the existence of the optimal offered load (1.25Mbps). This confirms our simulation results.

III. Throughput Analysis of a Single Multi-hop Traffic Flow

We now consider the problem of determining the optimal offered load (i.e., the maximum sustainable throughput) for a single flow in a multi-hop network. The throughput is limited by two factors: 1) the hidden-node problem; and 2) the carrier sensing mechanism. Our analysis is a two-step process. In step 1), we consider the capacity limited by the hidden-node problem. In step 2), we validate the result obtained by step 1 by the analysis of the carrier-sensing mechanism to ensure the optimal offered load can be sustained by the network. We first analyze the impact of these two factors. After that, we present numerical results showing that the analytical results match the simulation results closely. Our analysis yields a closed-form solution, which we believe provides the insight and foundation for the study of more complex situations involving multiple flows in future work.

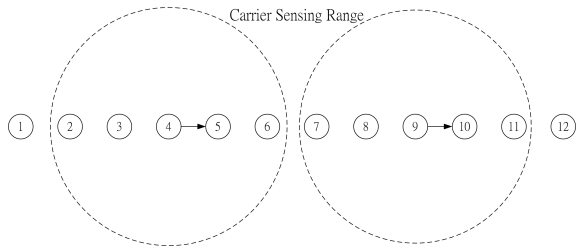


Figure 9. A 12-node string multi-hop network

A. Step 1: Capacity Limited by the Hidden-node Problem

We will express the throughput of a single flow in terms of the airtime used by a node. Figure 9 shows a chain of 12 nodes.

The traffic flows from left to right. Imagine that this is a longer chain with more nodes extending to the left of node 1 and the right of node 12. By the time the traffic reaches node 1, a "steady state in space" has been reached in which all nodes experience the same situation without the boundary effects. The question we ask is "What is the maximum throughput that can flow through this chain?"

Consider a long stretch of time in the interval [0, *Time*], which contains the idle times, contention window back-off times, transmission times, collision times, and times waiting for the completions of transmissions by other nodes within the same carrier-sensing range.

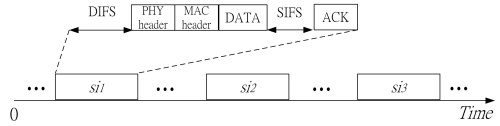


Figure 10. A long time interval [0, *Time*] and *Si*

Let Si be the airtimes within this interval that are used by a "steady-state" node *i*. As shown in Fig. 10, Si consists of the airtimes used by successive packets of node i, $si1, si2, si3, \ldots$ We define sij to include the transmission time of the jth data packets (PACKET), the transmission time of the corresponding acknowledgements (ACK) from node (i+1), the durations of the distributed interframe space (DIFS), and the durations of the short interframe space (SIFS). Also, included in sij are the times used up for retransmissions in case of collisions. However, sij does not include the count-down of the idle slots of the contention window, since adjacent nodes can count down together and these count-down times are not unshared resources used up exclusively by node i.

Let $x = |Si|/Time$, T = traffic throughput (in Mbps) flowing through the a "steady-state" node (and therefore also the end-to-end throughput), and ρ = the collision probability for a transmission. Then, we have.

$$T = x \cdot (1-\rho) \cdot d \cdot data\_rate \quad (1)$$

where $d = DATA/(DIFS + PACKET + SIFS + ACK)$ which is the proportion of time within x that is used to transmit the data payload; and $data\_rate$ is the data transmission rate. Note that *DATA* is the pure payload transmission time of a packet, while *PACKET* includes transmission times of the physical preamble, MAC header, and other higher-layer headers.

For simplicity, we assume that the carrier-sensing mechanism eliminates collisions to the extent that they are negligible, and that collisions are predominantly caused by hidden nodes. Consider node 4 in Fig. 9. Our assumption means that the transmission of node 4 will not collide with the transmissions of nodes 2, 3, 5, and 6; but the transmissions of node 1 and node 7 may collide with the transmission of node 4 due to the hidden-node effects.

To derive ρ, we consider the "vulnerable period" induced by the hidden nodes. During a vulnerable period, a node may suffer a collision if it transmits a packet. ρ can be decomposed into two factors: 1) the DATA-DATA collision probability (ρ_{HN}) ,and 2) the ACK-ACK collision probability (ρ'_{HN}). They are related as follows:

$$\rho = 1-(1-\rho_{HN})(1-\rho'_{HN}) \quad (2)$$

In the following subsections, we first explain the effect of the packet arrival order on signal capture. Then, we derive ρ_{HN} and ρ'_{HN}. We show that the latter is relatively small and can be ignored.

Our analysis is based on the following assumptions:

(A.1) The transmission of a node is independent of the transmissions of nodes outside its carrier sensing range.

(A.2) The packet collision probability of a node with nodes inside its carrier sensing range is negligible, thanks to the carrier-sensing property of CSMA. In other words, collisions due to simultaneous count-down of contention window to zero by two nodes within each other's carrier sensing range are negligible compared with collisions caused by hidden nodes.

1) Signal Capture

In Fig. 11, both nodes 4 and 7 have a packet to transmit. This may cause the aforementioned hidden-node collision. However, the signal capturing property may still allow a packet from node 4 to be received successfully, provided it transmits before node 7.

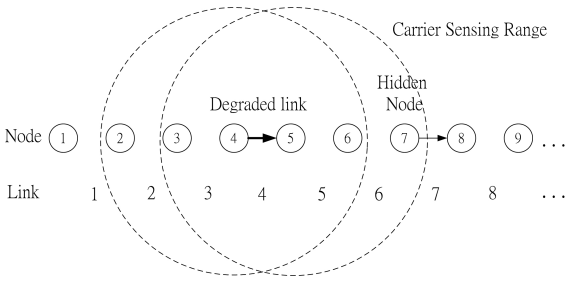


Figure 11. Node 7 as a hidden-node to node 4

More specifically, suppose that node 4 transmits first and the signal power of the transmission received at node 5 is P_4. Node 7 then transmits a packet with power of P_7 at node 5. If $P_4 > P_7 + CPThreshold$ (note: power in dBm and *CPThreshold* in dB), where *CPThreshold* is the capture threshold, then no collision occurs, and node 5 can still receive the packet from node 4 successfully.

However, according to the default operation in most commercial 802.11 products and in the NS-2 simulator, if node 7 transmits first, node 5 senses the signal from node 7 and will then consider the channel as being busy. In that case, a newly arriving packet from node 4 to node 5 will be ignored by node 5 even if $P_4 > P_7 + CPThreshold$. This will cause node 4 to interpret the failure as a collision and the exponential backoff

algorithm of the 802.11 MAC protocol will then be triggered. This is a form of hidden-node collisions. We will explain later in Section IV.B that a receiver "restart' mode can remove this problem. For the time being, we assume this default operation in the following analysis.

For the sake of argument, suppose that *CPThreshold* is set to be 10dB. Let d be the fixed distance between nodes. In this case, node 4 and node 7 are separated by a distance larger than the carrier sensing range. Thus, node 4 and node 7 can send packets at the same time. From [17], in a two ray propagation model, the signal-to-noise ratio at node 5 is

$$SNR = P_4 / P_7 = (2d/d)^4 = 2^4 = 16 > CPThreshold$$

This means that the power level of the packet transmitted by node 4 and received at node 5 is always more than *CPThreshold* higher than the power level of the received signal from node 7.

2) Analysis of Vulnerable Period induced by Hidden Nodes for DATA-DATA-collisions

In the analysis of the hidden-node problem, the key is to identify the vulnerable period during which the transmission of a node will collide with the transmission of a hidden node. This is illustrated in Fig. 12. Note that a hidden-node collision only occurs if the transmissions of nodes 4 and 7 overlap and that the transmission of node 7 precedes that of node 4. More specifically, after receiving the PHY header from node 7, node 5 will declare the channel as busy and will not receive the data from node 4 for the duration of the transmission time of the MAC header and DATA. In fact, node 5 can sense the signal from node 7, but not that from node 8. Thus, the ACK from node 8 to node 7 does not interfere with the transmission of link 4.

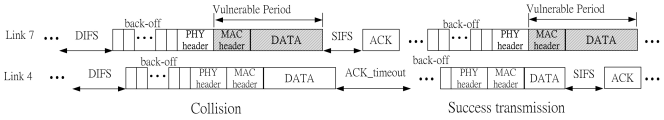


Figure 12. Collision occurs when the transmission of node 4 begins inside the vulnerable period.

If this were an Aloha network, nodes 4 and 7 could collide at anytime during the interval [0, *Time*]. However, in a carrier-sense network, some of the times during this interval must be removed from the "sample space" in the analysis of collision probability.

Consider Fig. 9. When node 5 or 6 transmits, node 4 and node 7 will not by assumption (A.2). This means that *S4*, *S5*, and *S6* are non-overlapping; and *S5*, *S6*, and *S7* are non-overlapping. In particular, node 7 cannot cause collision on node 4 during *S5* and *S6*. Now, nodes 5 and 6 use up $2 \cdot x$ fraction of the airtime during [0, *Time*]. The remaining fraction of airtime where node 4 and node 7 may collide is (1- $2 \cdot x$). Since node 7 uses x fraction of remaining airtime for transmissions, the vulnerable period induced by node 7 on node 4 is

$$\rho_{HN} = \frac{x}{1-2x} \cdot a \qquad (3)$$

by assumption (A.1), where

$$a = \frac{MAC\_Header + DATA}{DIFS + PACKET + SIFS + ACK}$$

is the fraction of time used for transmitting the MAC header and data.

3) Analysis of Vulnerable Period induced by Hidden Nodes for ACK-ACK-collisions

In Fig. 13, nodes 1 and 4 are outside the carrier-sensing range of each other. At a given time, both nodes 1 and 4 attempt to send a packet to nodes 2 and 5, respectively.

Node 1 is outside the carrier-sensing range of node 4, so the transmission of node 1 does not affect the transmission of node 4. However, node 2 is inside the carrier-sensing range of node 4. Node 4 can sense the ACK returned from node 2 to node 1. When the ACK from node 5 overlaps with the ACK from node 2 at node 4 and the ACK from node 5 reaches node 4 later than that of node 2 as shown in Fig. 14, a collision occurs.

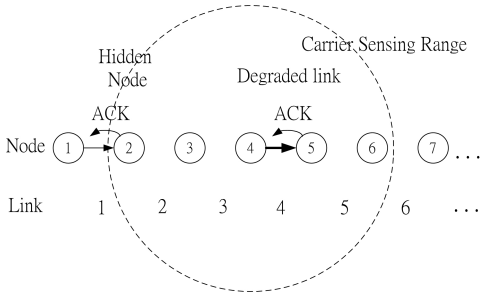


Figure 13. Node 2 as a hidden node to node 5

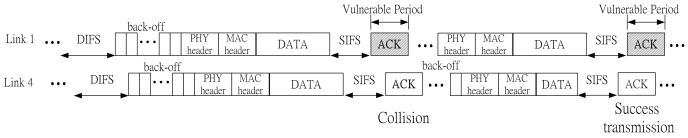


Figure 14. Collision occurs when the ACK from node 5 begins inside the vulnerable period.

However, this ACK-ACK collision can only occur if the transmission of node 4 begins at time t < SIFS later than the transmission of node 1. When t > SIFS, the transmission of node 4 is still in progress and node 4 is not aware of the transmission of ACK from node 2: that is, node 4 will not be able to read the physical preamble in ACK from node 2 and initiate the physical carrier-sensing mechanism that prevents node 4 from receiving the ACK from node 5 later. In fact, if we further consider the physical reception and transmission turnaround time, the value of t is even smaller and this further reduces the chance of ACK-ACK collision. Therefore, no collisions can occur if t > SIFS. Under the randomization assumption of (A.1), the chance for t < SIFS equals:

$SIFS/(DIFS + PACKET + SIFS + ACK) = 0.0064$ under the settings in Table I. Therefore, the ACK-ACK collision rarely happens. This has been borne out by our simulations, in which we could not detect ACK-ACK collisions due to the

hidden-node problem. We will therefore assume that the degradation caused by ACK-ACK collisions is negligible in our analysis henceforth. That is, equation (2) becomes

$$\rho \approx \rho_{HN} \tag{4}$$

4) Sustainable Throughput

Substituting equations (3) and (4) in (1), we have

$$T = x \cdot (1 - a \cdot \frac{x}{1-2x}) \cdot d \cdot data\_rate \tag{5}$$

Physically, there are two factors affecting T in the opposing directions. As x increases, more airtime is used by a node and there is less idling, and this should push T up. However, larger x also leads to a larger vulnerable period, pulling T down.

Differentiating (5) with respect to x and setting $dT/dx = 0$, the optimal value of x that maximizes the throughput is given by

$$x^* = \frac{(2+a) - \sqrt{a^2 + 2a}}{4 + 2a} \tag{6}$$

Substituting equation (6) in (1) yields the maximum sustainable throughput $T(x^*)$. The offered load should be set to a value smaller than $T(x^*)$ to prevent excessive packet loss.

B. Step 2: Capacity Limited by Carrier Sensing Property

To validate the maximum throughput $T(x^*)$ obtained by step 1 in Section III.A, we have to ensure the optimal value x^* can be sustained by the carrier-sensing network. Carrier sensing prevents simultaneous transmissions of nodes within the carrier-sensing range of a node. This imposes a limit on channel spatial-reuse. Potentially, the throughput could be limited by carrier sensing rather than hidden nodes. The maximum throughput derived above is due to hidden nodes. We now consider whether carrier sensing further reduces the sustainable throughput. We focus on the local observation of a particular node. The carrier-sensing range may not coincide with the interference range. When the carrier-sensing range is smaller than the interference range, simultaneous transmissions that result in excessively packet collisions may occur; when the carrier-sensing range is larger than the interference range, simultaneous transmissions that do not cause collisions may be disallowed. It is the latter that causes "unnecessary limit" on the network capacity. For the former, this can be the case when the data rate is set as the same transmission bit rate for sending physical headers. For example, in 802.11b, both data rate and PHY bit rate can be set to 1Mbps. In our simulations, nodes use 1Mbps for sending physical headers and 11Mbps as the data bit rate which causes the carrier-sensing range larger than the interference range (a case of the latter). We refer the reader to [18] for a scheme that modifies the carrier-sensing mechanism in 802.11 to achieve scalable network capacity. In the following analysis, we assume the normal 802.11 operation.

Let Ci be the airtime used for counting down the contention window of node *i*. Consider node 4 as the *local observer*. Within the time window [0, *Time*], it can only observe the airtimes used by the nodes within its carrier-sensing range, as illustrated in Fig. 9. So, as far as node 4 is concerned, it only observes *C*4, *S*2, *S*3, *S*4, *S*5 and *S*6. Note that it does not observe the countdowns of nodes 2, 3, 5, and 6. In particular, *C2*, *C3*, *C5*, and *C6* may overlap with *C4*. From node 4's point of view, the total airtimes used up by these nodes cannot exceed *Time*. Thus, $|C4 \cup S2 \cup S3 \cup S4 \cup S5 \cup S6| \le Time$.

Define $y = |C4 \cup S2 \cup S3 \cup S4 \cup S5 \cup S6| / Time$, to be the fraction of airtime used up by these nodes within the interval [0, *Time*]. Now, $|C4 \cup S2 \cup S3 \cup S4 \cup S5 \cup S6|$ can be decomposed using the inclusion-exclusion principle:

$|C4 \cup S2 \cup S3 \cup S4 \cup S5 \cup S6| = |C4| + |S2| + |S3| + ... + |S6| - |C4 \cap S2| - |S2 \cap S3| - |S2 \cap S4| - ... + |C4 \cap S2 \cap S3| + |S2 \cap S3 \cap S4| + ...$

However, we note that the intersection of the airtimes used by any three nodes or above is null, thanks to carrier sensing. Also, node 4 can count down only if nodes 2, 3, 5 and 6 are not transmitting, thus $C4 \cap Si$ for i = 2, 3, 5, 6 is null. In addition, the intersections of airtimes used by two nodes are non-null only for $S2 \cap S5$, $S3 \cap S6$, and $S2 \cap S6$. We therefore have

$$y \cdot Time = |C4| + \sum_{i=2}^{6} |Si| - |S2 \cap S5| - |S3 \cap S6| - |S2 \cap S6| \tag{7}$$

Let $z = |Ci| / Time$. By assumption (A.2), the packet collision probability is negligible. Before the transmission of a data packet, the node randomly chooses a contention window size between [0, $CW_{\min} - 1$] for countdown. The average time for counting down the contention window becomes $(CW_{\min} - 1) \cdot \sigma / 2 = 15.5 \cdot \sigma$ where σ is the mini slot time. We can express z in term of x,

$z = x \cdot c$

where $c = \dfrac{(CW_{\min} - 1) \cdot \sigma / 2}{DIFS + PACKET + SIFS + ACK}$

Consider the overlapped airtimes of node 2 and node 5. When node 3 or 4 transmits or when node 4 is counting down, node 2 and 5 do not transmit, by virtue of carrier sensing. The remaining fraction of airtime where *S*2 and *S*5 may overlap is (1-2*x*-*cx*). The intersection of *S*2 and *S*5, or *S*3 and *S6*, yield x^2 within this overlapped airtime. Thus, we have

$$|S2 \cap S5| = |S3 \cap S6| = \frac{x^2}{1 - (2 + c)x} \cdot Time \tag{8}$$

Nodes 3 and 6 face the same situation. Hence, $|S2 \cap S5| = |S3 \cap S6|$ in (8).

For $|S2 \cap S6|$, the amount of airtime of node 2 that may overlap with that of node 6 is ($|S2| - |S2 \cap S5|$), and the amount of airtime of node 6 that may overlap with that of node 2 is ($|S6| - |S3 \cap S6|$). The "sample space" within which *S*2 and *S*6 may overlap is [0, *Time*] – *S*3 – *S*4 – *S*5 – *C*4. As a result, we have

$$|S2 \cap S6| = \frac{(|S2| - |S2 \cap S5|) \cdot (|S6| - |S3 \cap S6|)}{Time - |S3| - |S4| - |S5| - |C4|}$$

The above gives

$$|S2 \cap S6| = \frac{(x - x^2/(1-(2+c)x))^2}{1-(3+c)x} \cdot Time \quad (9)$$

Substituting equations (8) and (9) into (7), we have

$$y = (5+c)x - \frac{2x^2}{1-(2+c)x} - \frac{x^2(1-(3+c)x)}{(1-(2+c)x)^2} \quad (10)$$

To validate the x^* obtained by step 1, we substitute x^* into equation (10). The value of x^* for $y < 1$ is a "feasible region". However, if $y(x^*) > 1$, the system is limited by the spatial-reuse restriction caused by the carrier-sensing mechanism.

Let the x at which $y(x) = 1$ be x'. This corresponds to a saturated case where the node always has packets to send, so either it is counting down, transmitting a packet itself, or sensing the transmission by a neighbor. The saturated case may not occur if the system is hidden-node limited because packets from upstream fail to arrive fast enough to keep the node busy all the time.

In fact, if the throughput obtained from x' is greater than the throughput obtained from x^* of equation (6), then the system throughput is limited by hidden nodes and the maximum sustainable throughput $T(x^*)$ can be supported by the network. However, if the throughput obtained from x' is smaller than that from x^*, The optimal throughput of the hidden-node limited analysis can be obtained by substituting x^* into equation (5) while that of the carrier-sensing limited analysis can be acquired by substituting x' into equation (1) with the collision probability caused by hidden-terminal (ρ) set to zero. In the next subsection, we show that for the case under study, the system throughput is hidden-node limited.

C. Numerical Results

In Sections III.A and III.B, we have provided the analysis on the capacity limited by 1) hidden nodes and 2) the carrier sensing mechanism. We now examine the numerical results. Table I shows the system parameters assumed, and the associated analytical T and y.

For 1), Figure 15 shows the simulation results, which indicate that the optimal offered load (or sustainable throughout) decreases as the number of nodes increases in a string multi-hop topology. For chains with more than 20 nodes, the optimal offered load stabilizes at 1.16Mbps. Our analytical result yields 1.218Mbps, a close match. As a validation, we note that this analytical optimal offered load value matches the experimental result (1.25Mbps) in Section II.D well.

For the analytical results, Fig. 16 plots network throughput T (left y-axis) versus x as limited by the hidden-node effect, and y (right y-axis) versus x as limited by carrier sensing. The maximum $T(x^*)$=1.218Mbps is achieved with x^*=0.245. For x^*, y = 0.952 < 1. This means that the capacity of the network is limited by hidden nodes rather than carrier sensing and $T(x^*)$ can be sustained by the network. Note that when the number of nodes within a carrier-sensing region is large and the number of hidden nodes is small, the capacity could in principle be limited by carrier sensing instead. This could be the case, for example, when the carrier sensing range is much larger than that of the transmission range. Table II shows the analytical and simulation results for various DATA packet sizes. Again, our analytical results match closely with the simulation results, particularly for large packet sizes.

TABLE I. System parameters and Max Throughput.

Packet payload (*DATA*)	1460 bytes
UDP/IP header	20 bytes
MAC header	28 bytes
PHY header	24 bytes
ACK size	14 bytes
Channel bit rate	11 Mbps
PHY header bit rate	1 Mbps
Slot time σ	20 *u*s
SIFS	10 *u*s
DIFS	50 *u*s
$CW_{\min}$	32
$CW_{\max}$	1024
Retransmission limit	7
x^*	0.24445
$T(x^*)$	1.2183Mbps
$y(x^*)$	0.95166
x'	0.3110
$T(x')$	2.3421Mbps
$y(x')$	1

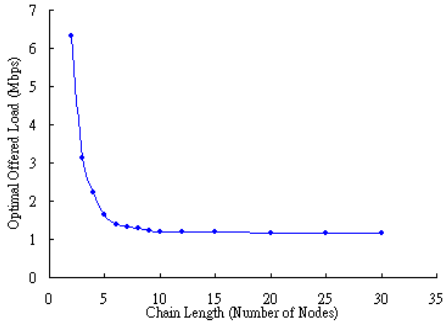


Figure 15. Optimal offered load versus number of nodes in a string multi-hop network.

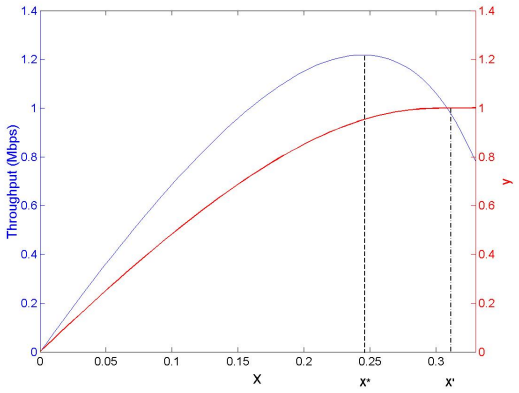


Figure 16. The flow throughput T in Mbps (left y-axis) and the fraction of airtime y used by all nodes within the carrier-sensing range of a particular node (right y-axis) versus the airtime x used by the node.

TABLE II. Analytical and Simulation Results of Variable Length Packets

Packet Length (bytes)	Analytical Result (Mbps)	Simulation Result (Mbps)	Percentage Error (%)
1460	1.218	1.160	4.787
1000	1.002	0.964	3.807
500	0.752	0.677	9.984

For the interested reader, reference [19] showed that the carrier-sensing mechanism of 802.11 may impose a constraint on channel spatial-reuse that is overly restrictive, making the network performance non-scalable. The same paper also provides a scheme that modifies 802.11 slightly to achieve scalable performance. We believe the scheme may relieve both the carrier-sensing and hidden-node effects being investigated here, although further study will be needed to validate this conjecture.

D. General Throughput Analysis of a Single Multi-hop Traffic Flow

In the previous subsections, we have shown that the capacity of a single string multi-hop network is hidden-node limited when the distance between two successive wireless nodes is set to the maximum transmission range (i.e., 250m). In this subsection, we discuss the capacities of other string network topologies. In particular, we show that our analytical results, again, match simulation results closely when we reduce the distance between two successive nodes to 170m and 130m. We study the link distance up to 130m because some intermediate nodes may be skipped if the node-to-node distance is less than 125m. Since this general analysis is similar to the analysis in Subsections III.A and III.B, we refer interested readers to the Appendix for details.

Let k be the number of nodes within a carrier-sensing range (CSRange, i.e., 550m) and let l be the uniform distance between two successive nodes. For example, $k=2$ if $l=250m$ (the minimum value of k since nodes are separated by maximum transmission range), $k=3$ if $l=170m$ and $k=4$ if $l=130m$ (this is the largest value of k, since closer packing with larger k allows data signal to jump over successive nodes).

We now examine the numerical results when the distance between two successive nodes is set to 170m (k=3) and 130m (k=4). Figure 18 plots the optimal values of x by 1) hidden nodes and 2) the carrier sensing property when k=2 to 4. In these three cases, x^* is less than x' which means the capacities of these string network topologies are still hidden-node limited rather than carrier-sensing limited. As a side note, the graph also implies that if a strategy could be devised to remove the hidden-node effect, considerable throughput improvement could be obtained.

Figure 19 shows the simulation results for chains with 50 nodes. Our hidden-node analytical results match closely with simulation results.

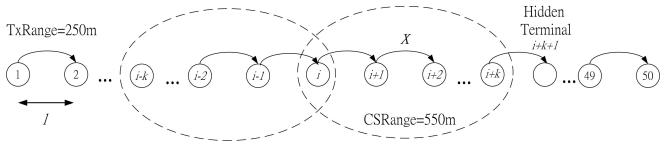


Figure 17. A 50-node string multi-hop network with variables k and l.

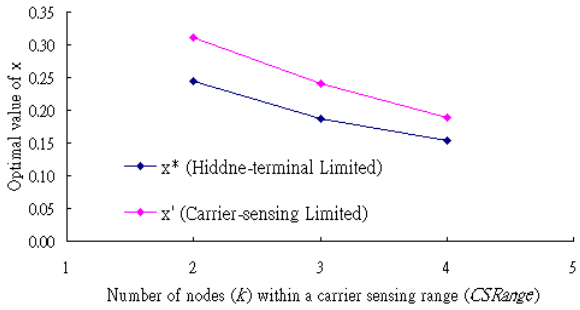


Figure 18. Optimal values of x versus number of nodes within a carrier sensing range

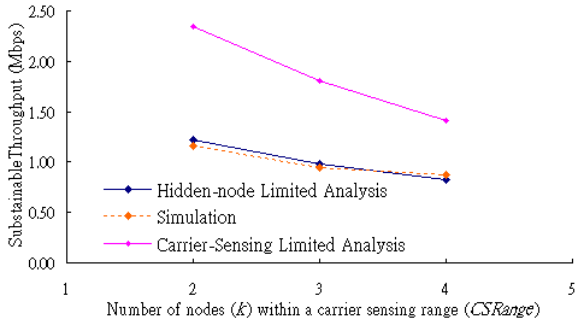


Figure 19. Sustainable throughput versus number of nodes within a carrier sensing range

E. Throughput Analysis on Topologies with Variable Distances between Successive Nodes

In an arbitrary network with multiple flows, different nodes experience different numbers of competing nodes, and this may cause uneven throughput distributions. When some nodes transmit more traffic than others, they also induce much larger

vulnerable regions than other nodes. This severely increases the chance of collisions to certain nodes and complicates the analysis.

In our previous analysis, we assume the distances between successive nodes are constant such that all nodes experience the same situation. However, this assumption may be invalid when distances between successive nodes vary. Figure 20 shows an example. The link between node 17 and node 18 suffers from five hidden-nodes (i.e., nodes 20 to 24). Node 17 can sense four nearby nodes (i.e., nodes 15, 16, 18, 19). The link between node 20 and node 21 suffers from one hidden-node (i.e., node 24). Node 20 has to share the channel capacity with five other nodes (i.e., nodes 18, 19, 21, 22, 23).

Simulation shows that the maximum throughput of the flow in Fig. 20 is 0.70Mbps, a 40% reduction compared with the maximum throughput (1.16Mbps) of a linear flow with nodes separated by 250m. This throughput is even smaller than that of a linear flow with nodes separated by 130m (0.88Mbps). This means the capacity is not limited by the closer packing at the end of the flow (node 20 to 25), but limited by the larger vulnerable period induced by the multiple hidden nodes.

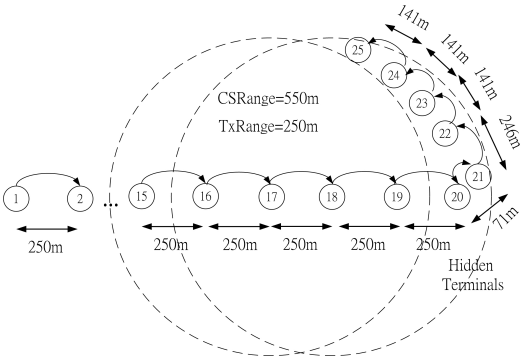


Figure 20. A 25-node multi-hop network with multiple hidden-nodes

The different numbers of hidden nodes and carrier-sensed nodes complicate the analysis. Because of the asymmetry, the airtimes used by different nodes are different, complicating the analysis. A possible analytical method is to use an iterative approach: First, we obtain the airtime used by the last node (e.g., node 24 in Fig. 20), x_n, in terms of the throughput T. Then, T as a function of x_{n-1}, x_n is computed. From this, we obtain x_{n-1} in terms of T. This is repeated until we have x_1 in terms of T. Then, we compute the maximum T. This iterative approach, however, does not yield a nice closed-form solution.

F. TCP Traffic Analysis

1) Single TCP Traffic Flow

We now extend the analysis to consider TCP traffic sources. For TCP traffic, in addition to the TCP DATA packets, nodes have to transmit TCP ACKs. This changes the fraction of time used for transmitting the MAC headers, TCP DATA and TCP ACK. Thus,

$$a = \frac{MAC\_Header*2 + TCP\_DATA + TCP\_ACK}{DIFS*2 + MAC\_Header*2 + TCP\_DATA + SIFS*2 + ACK*2 + TCP\_ACK}$$

Similar to the analysis in Section III.A, the traffic throughput (in Mbps) is

$$T = x \cdot (1-\rho) \cdot d \cdot data\_rate$$

where

$$d = \frac{DATA}{DIFS*2 + MAC\_Header*2 + TCP\_DATA + SIFS*2 + ACK*2 + TCP\_ACK}$$

Table III shows the system parameters assumed, and the associated analytical T and y. The maximum $T(x^*)$=0.852Mbps is achieved with x^*=0.253. For x^*, y = 0.915 < 1. This means that the capacity of the network is still limited by hidden nodes rather than carrier sensing. In simulation, for chains with 8 nodes using TCP Reno traffic sources, the optimal network throughput is obtained at 0.812Mbps. This is a close match with the analytical result.

TCP adopts a sophisticated Additive-Increase-Multiplicative-Decrease (AIMD) congestion control mechanism which, if taken into consideration in all its details, may complicate the analysis considerably. It has been shown that TCP working on top of an ad hoc network yields lower throughput than the potential capacity of the network [14]. Previous work [14] proposed to modify the TCP window size to limit the offered load. This, however, destroys the layering concept because the upper layer needs to be designed specifically to accommodate a lower-layer problem. In a separate piece of work [12] [13], we have identified the root cause of the throughput sub-optimality and instability to be the "faulty" re-routing function inherent in many *ad hoc* routing schemes, including the widely adopted AODV scheme. This faulty re-routing function also carries over to the NS-2 simulator. Our simulation above has adopted a "don't-break-before-you-can-make" re-routing strategy as originally proposed in [12][13] to get rid of the re-routing instability problem. With this strategy, we reach a different conclusion on the effectiveness of TCP on ad hoc networks. Specifically, our simulation in this paper shows that TCP can automatically zoom into an offered traffic load which is very close to the optimal sustainable load of the network (as estimated from our analysis which does not consider AIMD). In that sense the optimal offered load as obtained from our analysis is still valid. Indeed, with TCP as the end-to-end traffic controller, the optimal offered load is achievable without needing another traffic regulator at the ingress to the ad-hoc network to control the input IP traffic. A more detailed analysis of the TCP behavior in ad-hoc networks to explain our observation above at a more fundamental level would be interesting for further investigation.

TABLE III. System parameters and Max Throughput for TCP traffic

Packet payload (*DATA*)	1500 bytes
TCP/IP header	60 bytes
x^*	0.2529
$T(x^*)$	0.8524Mbps
$y(x^*)$	0.915

2) Two Opposing TCP Traffic Flows

Consider a chain network topology with a TCP traffic source at each end to transmit data to the other end of the network. Analytically, the fraction of time used for transmitting the MAC headers, TCP DATA and TCP ACK (i.e., *a*) and the proportion of time within *x* that is used to transmit the data payload (i.e., *d*) remain the same as in Section III.F.1. However, each node uses *x/2* for one of the two flows. Thus, the traffic throughput (in Mbps) of a TCP flow becomes

$$T_{a\_flow} = \frac{x}{2} \cdot (1-\rho) \cdot d \cdot data\_rate$$

The maximum $T_{a\_flow}(x^*)$ =0.426Mbps is achieved with x^* =0.253. This, again, matches closely with the simulation result (0.407Mbps) in an 8-node chain network.

IV. Discussions of Other Special Cases

In Section III, we have shown that the capacities of string network topologies are hidden-node limited. In this section, we demonstrate a carrier-sensing limited scenario. In addition, we give a practical solution by which the hidden-node problem can be eliminated and the sustainable throughput can be boosted.

A. Carrier-sensing Limited Example

Figure 21 shows two flows with opposite directions in an 11-node multi-hop network. Two UDP traffic sources at node 6 and node 7 transmit data to each end (node 1 and node 11) through the 5-hop (to the left) and 4-hop (to the right) networks respectively. In this scenario, there is no hidden node since the sender of each link can carrier-sense other transmitters that can be sensed by the receiver of the link.

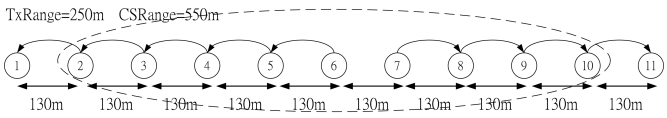


Figure 21. An 11-node multi-hop network with two opposite directional flows.

Consider node 6 as the local observer and nodes within its carrier-sensing range in Fig. 21. The total airtimes used up by these nodes cannot exceed *Time*. That is, $|C6 \cup S2 \cup S3 \cup \ldots \cup S9 \cup S10| \le Time$.

Simulation shows that the optimal sustainable throughput for each flow is obtained at 0.920Mbps which is higher than the simulation throughput (0.870Mbps) obtained in a single flow multi-hop case as shown in Fig. 19. This means the throughput is boosted by releasing the bundle of hidden-node as there is no hidden-node problem in this specific topology.

B. A Practical Solution to Improving Throughput

In Sub-section III.C, we have shown that the optimal value of *x* obtained by hidden-node analysis (*x**) is less than that of the carrier-sensing analysis (*x'*). This means the network throughput is limited by hidden nodes rather than the carrier-sensing mechanism. If the hidden-node problem can be eliminated, we can increase the sustainable throughput.

To do this, node 5 as shown in Fig. 11 must be able to receive the signal from node 4 successfully even though node 5 can sense the signal from node 7. This usually *cannot* be achieved in the default receiver operation described below.

Although not specified exactly in the standard, the default receiver operation of most 802.11 products and the NS-2 simulator assumes a clean separation of the PHY and MAC layer, as follows. When the receiver detects signal power above a certain threshold P_{rth}, then it will attempt to decode the PHY header. If the PHY header can be decoded, then the length and coding rate of the payload can be determined. The physical layer will then attempt to receive the whole packet. This whole packet will then be forwarded to the MAC layer, which can then check the destination MAC address in the MAC header to see if this packet is targeted for the receiver. Typically, once the physical layer starts to receive the payload, it will not abort. This is so even if this payload is not targeted for the receiver, and another stronger signal containing a packet targeted for the receiver arrives in the midst of the first reception. As far as the physical layer is concerned, it does not read the MAC address in the payload. In our example above, once the physical layer of node 5 begins to sense (hence receives) a signal from node 7, it will not abort even if node 4 then sends a signal to node 5. Of course, the MAC layer of node 5 will later find that it has a corrupted packet.

In some commercial 802.11 chips (e.g., Atheros Chip), there is a so-called "restart mode" in the receiver design. If the receiver is in the midst of receiving a signal, another signal with sufficiently large power margin arrives (say, 10dB stronger), the receiver will switch to receive the new signal. If the new signal contains a packet destined for the receiver, the receiver will then return an ACK to the sender. This feature can be used to remove the hidden-node problem in multi-hop networks. As far as we know, the 802.11 standard does not say whether there should be restart or not. A reason why restart mode is by default not enabled in commercial products could be that the receiver's ACK for the later packet might collide with the earlier transmission if it is still in progress (i.e., the earlier transmission has a longer packet than the later transmission). Reference [20], however, shows that provided the CSRange is sufficiently large, such a collision will not occur when restart mode is enabled so that the node can safely receive its DATA packet proper and return an ACK. In particular, reference [20] proves two conditions that can guarantee a hidden-node-free operation in a general network: (i) restart mode and (ii) a lower-bound requirement on the CSRange.

For the linear network topology under consideration, when nodes 4 and 7 transmit at the same time (as shown in Fig. 11), the signal to noise ratio (*SNR*) at node 5 is 16 (as shown in Sub-section III.A.1) which is sufficiently larger than the capture threshold (*CPThresh*=10dB). With the restart mode, node 5 can switch to receive the stronger signal from node 4 even if the signal from node 7 reaches node 5 before that of node 4. In this way, the vulnerable period induced by the hidden-node (node 7) can be eliminated.

We implemented the restart mode in NS2. Figure 22 shows the simulation results. The sustainable throughput can be boosted up to 50% with the use of the restart mode. In Fig. 22, the optimal theoretical throughputs can be used as benchmarks for comparisons and are obtained under the assumption of perfect scheduling. For example, as shown in Fig. 23, nodes 1, 4, 7, 10 … are scheduled to transmit simultaneously when k=2 and this yields 1/3 of the total channel capacity (1/3*6.3=2.1Mbps).

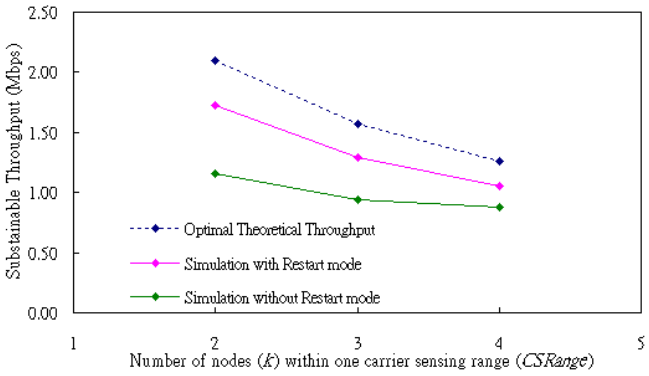


Figure 22. Sustainable throughput with restart mode versus number of nodes within a carrier sensing range

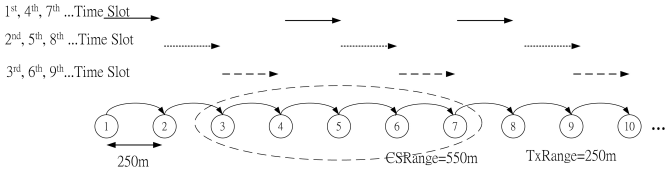


Figure 23. A single string multi-hop network with transmissions of prefect scheduling

V. Conclusion

This paper has been an attempt to identify the maximum throughput that can be sustained in an 802.11 multi-hop network. We believe that this is a first paper in the literature to provide a *quantitative analysis* on the fundamental impact of hidden nodes and carrier sensing on system throughput. Our contributions are three-folds:

We have shown that uncontrolled, greedy sources can cause unacceptably high packet-loss rate and large throughput oscillations. Judicious offered load control at the sources, however, can eliminate these problems effectively without modification of the 802.11 multi-access protocol. Our simulations and real-network experiments have confirmed the existence of this optimal offered load in a 6-node multi-hop network.

We have established an analytical framework for the study of the effects of hidden nodes and carrier-sensing operation. This analysis allows one to determine whether the system throughput is hidden-node limited or spatial-reuse limited. In particular, we have shown that the maximum sustainable throughput is limited by two factors: (i) the vulnerable periods which depend on the numbers of hidden nodes and the fraction of airtime in the time horizon when hidden-node collisions may occur; (ii) the number of nodes within a carrier-sensing region and the total airtime used up by them.

We have studied the single-flow case in detail. The throughput limitation of a single multi-hop flow is typically dominated by the hidden-node effect of (i). However, a modification on the receiver design can eliminate the hidden-node effect so that the throughput is limited by (ii) instead. Throughput improvement as high as 50% is possible.

We have also found that TCP can zoom in reasonably well to the "ideal" offered load as obtained by our analysis after the incorporation of a "don't-break-before- you-make" strategy in the ad-hoc routing protocol. This allows the widely-deployed TCP protocol to be adopted in multi-hop ad-hoc networks without modifications and without the need for an explicit lower-layer offered-load controller. Our analysis has not considered the detailed operation of the additive-increase-multiplicative-decrease congestion control mechanism of TCP. A more in-depth analysis of the TCP behavior in ad-hoc networks to explain our observation at a more fundamental level would be interesting for further investigation.

The single-flow analysis in this paper serves as a "building block" for the study of the multiple-flow case, in which besides the self-interference induced by traffic of the same flow, there are also mutual interferences among traffic of different flows. Reference [21] is an attempt at a generic sensor-network situation in which information is collected from many sources and forwarded toward a single data-collection sink. More complicated situations with overlapping multiple flows remain to be further investigated. We believe the approach in this paper provides a good foundation for such an extension.

Appendix

A. General Throughput Analysis of a Single Multi-hop Traffic Flow

Let k be the number of nodes within a carrier-sensing range (CSRange, i.e., 550m) and let l be the uniform distance between two successive nodes. Figure 17 illustrates a string network topology with variables k and l.

1) Capacity Limited by Hidden Nodes

Following similar approaches in deriving the vulnerable period induced by hidden-node as shown in Section III.A.2, we can express ρ_{HT} in term of x. In Fig. 17, when node $i+1$ to $i+k$ transmit, node i and node $i+k+1$ will not. This means that S_i to S_{i+k} are non-overlapping; and S_{i+1} to S_{i+k+1} are non-overlapping. In particular, node $i+k+1$ cannot cause collision on node i during S_{i+1} to S_{i+k}. Now, nodes $i+1$ to $i+k$ use up $k \cdot x$ fraction of the airtime during [0, *Time*]. The remaining fraction of airtime where node i and node $i+k+1$ may collide is (1- $k \cdot x$). Since node $i+k+1$ uses x fraction of remaining airtime for transmissions, the vulnerable period induced by node $i+k+1$ on node i is

$$\rho_{HN} = \frac{x}{1-k\cdot x}\cdot a \tag{11}$$

Again, as explained in Section III.A.3, the ACK-ACK collision can only occur if the transmission of node i begins at time t < SIFS later than the transmission of node $i-k-1$. Therefore, the ACK-ACK collision rarely happens. Thus we assume that the degradation caused by ACK-ACK collision is negligible in our analysis.

a) Sustainable Throughput

Substituting equations (11) and (4) in (1), we have

$$T = x\cdot(1-a\cdot\frac{x}{1-k\cdot x})\cdot d\cdot data\_rate \tag{12}$$

Differentiating (12) with respect to x and setting $dT/dx = 0$, the optimal value of x that maximizes the throughput is given by

$$x^* = \frac{(k+a)-\sqrt{a^2+ka}}{k^2+ka} \tag{13}$$

Substituting equation (13) in (12) yields the maximum sustainable throughput $T(x^*)$.

2) Capacity Limited by Carrier Sensing Property

Carrier sensing prevents simultaneous transmissions of nodes within the carrier-sensing range of a node. Consider node i as the local observer and nodes within its carrier-sensing range in Fig. 17. The total airtimes used up by these nodes cannot exceed *Time*. That is,

$$|C_i \cup S_{i-k} \cup S_{i-k+1} \cup ... S_i \cup ... S_{i+k}| \le Time$$

Define $y = |C_i \cup S_{i-k} \cup S_{i-k+1} \cup ... S_i \cup ... S_{i+k}|/Time$, to be the fraction of airtime used up by these nodes within the interval [0, *Time*]. Now, $|C_i \cup S_{i-k} \cup S_{i-k+1} \cup ... S_i \cup ... S_{i+k}|$ can be decomposed using the inclusion-exclusion principle:

$$\begin{aligned}|C_i \cup S_{i-k} \cup S_{i-k+1} \cup ... S_i \cup ... S_{i+k}| = {} & |C_i| + |S_{i-k}| + |S_{i-k+1}| + ... |S_{i+k}| \\ & - |C_i \cap S_{i-k}| - |S_{i-k} \cap S_{i-k+1}| - |S_{i-k} \cap S_{i-k+2}| - ... \\ & ... + |C_i \cap S_{i-k} \cap S_{i-k+1}| + |S_{i-k} \cap S_{i-k+1} \cap S_{i-k+2}| + ...\end{aligned} \tag{14}$$

However, we note that the intersection of the airtimes used by any three nodes or above is null, thanks to carrier sensing. Also, node *i* can count down only if nodes *i-k*, *i-k+1* …, *i+k-1* and *i+k* are not transmitting, thus $C4 \cap Si$ is null. In addition, the intersections of airtimes used by two nodes are non-null only for $|S_j \cap S_{j+m}|$ for any node *j* where $m \ge k+1$.

We therefore have

$$\begin{aligned}y\cdot Time = {} & |C_i| + \sum_{j=i-k}^{i+k} |S_j| - \sum_{j=i-k}^{i-1} |S_j \cap S_{j+k+1}| - \sum_{j=i-k}^{i-2} |S_j \cap S_{j+k+2}| - \\ & - \sum_{j=i-k}^{i-3} |S_j \cap S_{j+k+3}| - ...\end{aligned} \tag{15}$$

Consider the overlapped airtimes of node $i-k$ and node $i+1$. When node $i-k+1$ to i transmits, node $i-k$ and $i+1$ do not, by virtue of carrier sensing. The remaining fraction of airtime where S_{i-k} and S_{i+1} may overlap is $(1-k\cdot x-c\cdot x)$. In particular, we have

$$|S_{i-k} \cap S_{i+1}| = |S_{i-k+1} \cap S_{i+2}| = \frac{x^2}{1-(k+c)\cdot x}\cdot Time \tag{16}$$

Nodes $i-k+1$ and $i+2$ face the same situation. Hence, $|S_{i-k} \cap S_{i+1}| = |S_{i-k+1} \cap S_{i+2}|$ in (16).

For $|S_{i-k} \cap S_{i+2}|$, the amount of airtime of node $i-k$ that may overlap with that of node $i+2$ is $(|S_{i-k}| - |S_{i-k} \cap S_{i+1}|)$, and the amount of airtime of node $i+2$ that may overlap with that of node $i-k$ is $(|S_{i+2}| - |S_{i-k+1} \cap S_{i+2}|)$. The "sample space" within which S_{i-k} and S_{i+2} may overlap is [0, *Time*] $-S_{i-k+1} - S_{i-k+2}$ -…$-S_{i+1} - C_i$. As a result, we have

$$\begin{aligned}|S_{i-k} \cap S_{i+2}| &= \frac{(|S_{i-k}| - |S_{i-k} \cap S_{i+1}|)\cdot(|S_{i+2}| - |S_{i-k+1} \cap S_{i+2}|)}{Time - |S_{i-k+1}| - |S_{i-k+2}| - ... - |S_{i+1}| - |C_i|} \\ &= \frac{(x-x^2/(1-k\cdot x))^2}{1-(k+1+c)x}\cdot Time\end{aligned} \tag{17}$$

Let $D_m \cdot Time = |S_j \cap S_{j+m}|$. If node $j+m$ is within the carrier-sensing range of node j or vice versa, their airtime cannot overlap due to the carrier-sensing mechanism. Thus,

$D_m \cdot Time = |S_j \cap S_{j+m}| = 0$ if $m \le k$

For $m > k$, following similar approaches as with equations (16) and (17), we have,

$$D_{k+1} = |S_j \cap S_{j+k+1}|/Time = \frac{x^2}{1-(k+c)x}$$

$$D_{k+2} = |S_j \cap S_{j+k+2}|/Time = \frac{(x-D_{k+1})^2}{1-(k+1+c)x}$$

$$D_{k+3} = |S_j \cap S_{j+k+3}|/Time = \frac{(x-D_{k+1}-D_{k+2})^2}{1-(k+2+c)x+D_{k+1}}$$

$$D_{k+4} = |S_j \cap S_{j+k+4}|/Time = \frac{(x-D_{k+1}-D_{k+2}-D_{k+3})^2}{1-(k+3+c)x+2D_{k+1}+D_{k+2}}$$

$$\begin{aligned}D_{k+n} &= |S_j \cap S_{j+k+n}|/Time \\ &= \frac{(x-D_{k+1}-D_{k+2}-D_{k+3}...-D_{k+n-1})^2}{1-(k+n-1+c)x+(n-2)D_{k+1}+(n-3)D_{k+2}...+D_{k+n-2}}\end{aligned}$$

where $k+n \le 2k$, thus $n \le k$

So, in general,

$$\begin{aligned}D_{k+n} &= |S_j \cap S_{j+k+n}|/Time \\ &= \frac{(x-\sum_{m=1}^{n-1} D_{k+m})^2}{1-(k+n-1+c)x+\sum_{m=2}^{n-2} mD_{k+n-m-1}}\end{aligned} \tag{18}$$

Substituting into (18) into (15),

$$y = (2k+1+c)x - k\cdot D_{k+1} - (k-1)\cdot D_{k+2} - (k-2)\cdot D_{k+3} - ...$$

$$y = (2k+1+c)x - \sum_{i=1}^{k}(k-i+1)\cdot D_{k+i} \tag{19}$$

The value of x for $y > 1$ is an "infeasible region". Again, let the x at which $y(x) = 1$ be x'. If the throughput obtained from x' is greater than the throughput obtained from x^* in equation (13), then the system throughput is limited by hidden nodes. However, if the other way round, the system is limited by the carrier-sensing mechanism.

REFERENCES

[1] P. Gupta, P. R. Kumar, "The Capacity of Wireless Networks", *IEEE Trans. Inform. Theory*, Vol.46, No.2, pp.388-404, Mar. 2000.

[2] J. Li, C. Blake et al., "Capacity of Ad Hoc Wireless Networks", *ACM MobiCom'01*, Rome, Italy, July 2001.

[3] K. Jain et al. "Impact of Interference on Multi-hop Wireless Network Performance", *ACM MobiCom'03*, San Diego, USA, Sept. 2003.

[4] M. Kodialam, T. Nandagopal, "Characterizing Achievable Rates in Multi-hop Wireless Networks: The Joint Routing and Scheduling Problem", *ACM MobiCom'03*, San Diego, USA, Sept. 2003

[5] K. Xu, M. Gerla, S. Bae, "How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks?", *IEEE GLOBECOM '02*, Vol. 1 , pp. 17-21, Nov. 2002.

[6] S. Ansari et al. "Performance Enhancement of TCP on Multihop Ad hoc Wireless Networks", *IEEE ICPWC'02*, pp. 90-94, Dec. 2002.

[7] Z. Hadzi-Velkov, L. Gavrilovska, "Performance of the IEEE 802.11 Wireless LANs under Influence of Hidden", *IEEE PWCS'99*, pp. 221-225, Feb. 1999.

[8] S. Khurana et al., "Effect of Hidden Terminals on the Performance of IEEE 802.11 MAC Protocol", *IEEE LCN'98*, pp. 12-20, Oct. 1998.

[9] S. Khurana et al., "Performance Evaluation of Distributed Co-Ordination Function for IEEE 802.11Wireless LAN Protocol in Presence of Mobile and Hidden Terminals", *IEEE MASCOTS'99*, pp.40-47, Oct. 1999.

[10] F. A. Tobagi, L. Kleinrock, "Packet switching in radio channels: Part ii - the hidden terminal problem in carrier sense multiple-access and the busy-tone solution", *IEEE Trans. on Commun.*, pp.1417–1433, December 1975.

[11] "The Network Simulator–ns2",http://www.isi.edu/nsnam/ns

[12] P. C. Ng, S. C. Liew, "Re-routing Instability in IEEE 802.11 Multi-hop Ad hoc Networks", *IEEE WLN'04*, Nov. 2004, Tampa, USA.

[13] P. C. Ng, S. C. Liew, "Re-routing Instability in IEEE 802.11 Multi-hop Ad-hoc Networks," *OCP Ad-hoc & Sensor Wireless Networks, An International Journal*, Vol. 2, No. 1, 2006

[14] S. Xu, T. Saadawi, "On TCP over Wireless Multi-hop Networks", *IEEE MILCOM 2001*, Vol.1, pp.282-288, Oct. 2001.

[15] "HostAP" driver, http://hostap.epitest.fi/

[16] G. Anastasi, E. Borgia et al., "Wi-Fi in Ad Hoc Mode: A Measurement Study", *IEEE PERCOM'04*, March 2004.

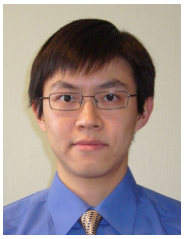
[17] T. Rappaport, "Wireless Communications: Principles and Practice", Prentice Hall, New Jersey, 2002.

[18] P. C. Ng, S. C. Liew, L. B. Jiang, "Achieving Scalable Performance in Large-Scale IEEE 802.11 Wireless Networks," *IEEE WCNC'05*, Mar. 2005

[19] P.C. Ng, S. C. Liew, L. B. Jiang, "A Performance Evaluation Framework for IEEE 802.11 Ad hoc Networks", *ACM PE-WASUN'04*, Venice, Italy, Oct. 2004.

[20] L. Jiang and S. C. Liew, "Removing Hidden Nodes in IEEE 802.11 Wireless Networks," *IEEE Vehicular Technology Conference*, Sept 2005.

[21] C. P. Chan and S. C. Liew, "Data-Collection Capacity of IEEE 802.11-like Sensor Networks," *IEEE ICC*, Istanbul, Turkey, June 2006.



Ping-Chung Ng (S'04) received the B.Eng. (highest honor) and M.Phil. degrees in information engineering from the Chinese University of Hong Kong (CUHK), in 2003 and 2005, respectively. His master thesis received the outstanding thesis award of the faculty of engineering, CUHK, in 2005. He and his supervisor, Dr. Soung-Chang Liew, in CUHK won the best paper awards in the *1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2004)* the *4th IEEE International Workshop on Wireless Local Network (IEEE WLN 2004)*. Since October 2005, he receives the Croucher Foundation Scholarship to work toward the D.Phil. degree in engineering science at Oxford University, Oxford, U.K. His current research interests include the capacity of wireless ad-hoc networks, medium access control, ad-hoc routing protocols and MIMO.

Soung C. Liew (S'84-M'87-SM'92) received his S.B., S.M., E.E., and Ph.D. degrees from the Massachusetts Institute of Technology. From 1984 to 1988, he was at the MIT Laboratory for Information and Decision Systems, where he investigated Fiber-Optic Communications Networks. From March 1988 to July 1993, Soung was at Bellcore (now Telcordia), New Jersey, where he engaged in Broadband Network Research. Soung is currently Professor at the Chinese University of Hong Kong. Soung's research interests include wireless networks, Internet protocols, multimedia communications, optical networks, and broadband packet switch design. Most recently, he has been working on 1) wireless applications and communications protocols, focusing on performance, security, and mobility issues; and 2) wireless LAN and *ad hoc* network designs. Besides academic activities, Soung is also active in the industry. He co-founded two technology start-ups in Internet Software and has been serving as consultant to many companies and industrial organizations. He is currently consultant for the Hong Kong Applied Science and Technology Research Institute (ASTRI), providing technical advice as well as helping to formulate R&D directions and strategies in the areas of Wireless Internetworking, Applications, and Services. Soung is the holder of three U.S. patents and Fellow of IEE and HKIE. He is listed in Marquis Who's Who in Science and Engineering. He is the recipient of the first Vice-Chancellor Exemplary Teaching Award at the Chinese University of Hong Kong. Recently, Soung and his student won the best paper awards in the *1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2004)* the *4th IEEE International Workshop on Wireless Local Network (IEEE WLN 2004)*. Publications of Soung can be found in www.ie.cuhk.edu.hk/soung.