The Fundamental Role of Hop Distance in IEEE802.11 Multi-Hop Ad Hoc Networks

Yan Gao, Dah-Ming Chiu
Department of Information Engineering
The Chinese University of Hong Kong
Email: {ygao4, dmchiu}@ie.cuhk.edu.hk

John C.S. Lui
Department of Computer Science Engineering
The Chinese University of Hong Kong
Email: cslui@cse.cuhk.edu.hk

Abstract

In wireless networks, it is well understood what throughput can be achieved by nodes who can hear each other (i.e. nodes within a single cell)[1, 3]. The effects of nodes beyond the sensing range (known as hidden nodes) on a sender are complicated and difficult to analyze. Consequently, how to analytically model multi-hop adhoc networks, specially networks based on the popular IEEE802.11 standards remains largely open. In a recent paper [2], the throughput of a particular wireless network topology (linear network with a given number of hidden nodes) has been derived analytically. In this paper, we unify previous results on single-cell models, and results characterizing different types of hidden node interference and the analysis of [2], to derive a general solution for throughput given a linear network of arbitrary density *and* transmission distance *between source and destination nodes. An important insight from our model is that there is a certain transmission distance, which is less than the maximum transmission distance, that optimizes throughput in such networks. This result is verified using ns-2 simulation with both single as well as multiple flows.*

1 Introduction

There has been much interest in modelling the performance of multi-hop ad hoc networks. The seminal paper by Gupta and Kumar [6] derived theoretical bounds for the capacity of ad hoc wireless networks. But for wireless networks in real-life, such as networks based on IEEE802.11 standards, the media access control is far form optimal, and achieve less throughput than the bounds.

For IEEE802.11 networks, the binary exponential backoff mechanism of Distribution Coordination Function (DCF) has been well studied [1, 3]. These results have been successfully used to analyze the throughput of single-cell networks, namely the case when all nodes can hear each other. However, in multi-hop ad hoc networks, the behavior of a node is dependent not only on its neighbors' behavior, but also on the behavior of hidden nodes. This makes modelling such networks extremely difficult.

Previous studies [2, 5, 7] have shown that the interference of hidden nodes is location dependent: whether a node is a hidden node or not depends on the location of that node relative to the sender, as well as how far the sender is transmitting. Therefore, even if the topology of the wireless network is given, how much a flow is affected by the interference from hidden nodes depends on how far each node chooses to transmit a packet in the next hop. It is also well-known that the achievable throughput for each node decreases as the number of active nodes in its neighborhood increases [4, 6]. This leads to the following intuition. In a multi-hop ad hoc network, if all flows choose to use short hop distances[1] to forward packets, then more channel contention will result. This is especially true since an IEEE802.11 node does not adjust its transmission power down when transmitting to its close neighbors. Therefore short hop transmission does not help spectrum reuse, and achieves less *bit-distance* (in the sense of [6]) than long hop transmission . On the other hand, if all flows choose to use long hop transmission, then there will be more hidden node interference. This argument implies that there exists an optimal transmission distance for maximizing end-to-end throughput. The main result of this paper is to develop an analytical model to study IEEE802.11 multi-hop ad hoc networks to confirm this intuition.

We build our model by extending some exciting new results in studying the capacity of wireless networks, both for single-cell [1, 3] and multi-hop wireless networks [2, 5]. The main contribution of our work is to unify the model of binary exponential backoff of [1, 3] and the analysis of the hidden node effect on throughput in [2, 5] into one model.

[1] In this paper, hop distance implies the ”transmission” distance for a hop.

Based on our model, we obtain a hop distance that achieves the highest end-to-end throughput. We verified using ns-2 simulation that indeed higher throughput is achieved compared to traditional minimum hop count routing strategy in a linear network.

The organization of the paper is as follows. We first review the important previous results that our work is based on in Section 2. Our model and analytical results are derived in Section 3. We discuss some ns-2 simulation results that are used to validate our model in Section 4. In Section 5, we show that the conclusion of the optimal transmission distance is also applicable in a two-dimensional network. Finally, we discuss future directions and conclude in Section 6.

2 Review of Important Previous Work

There are a large number of papers on wireless ad hoc networks. In this section, we review a few papers which have important influence on our work.

2.1 Analysis of Single-Cell Networks

By definition, in single cell networks all nodes can hear each other's transmission. This problem was first studied by Bianchi [3], who provided a Markov chain model for the distributed coordination function (DCF) and applied it to analyze single-cell 802.11 networks. Later, authors of [1] derived a general formula relating the collision probability γ to the rate of transmission attempts by a node **in single-cell network** is given as follows:

$$G(\gamma) = \frac{1 + \gamma + \gamma^2 \cdots + \gamma^K}{b_0 + \gamma b_1 + \gamma^2 b_2 \cdots + \gamma^K b_K}. \quad (1)$$

Note, K is the maximum number of attempts of transmitting a packet by the DCF (at the $(K+1)^{th}$ attempt either the packet succeeds or is discarded). So the numerator is the expected number of transmission attempts for a single packet. In the denominator, b_k denotes the mean back-off duration (in time slots) at the k^{th} attempt for a packet, $0 \leq k \leq K$; so the whole denominator represents the expected total back-off duration for a packet.

The above formula is derived under the assumptions that all nodes use the same DCF back-off algorithm (homogeneous assumption) and to a given node, other nodes' back-off processes are statistically independent of its own (decoupling assumption).

We will also make these assumptions to relate a node's collision probability to the attempt rate by that node. Except in our case, collisions will primarily be caused by hidden nodes rather than nodes that can hear each other.

2.2 Hidden Node Problems

In analyzing the performance of wireless multi-hop networks, one always needs to consider the impact of hidden nodes. Hidden nodes are the possible interfering nodes which cannot be sensed by the sender. The RTS/CTS mechanism was introduced in IEEE802.11 to deal with this problem. However, the use of RTS/CTS does not eliminate the hidden node problems completely in multi-hop networks [2, 5].

The cause of these interference issues can be chased back to two basic types of hidden nodes: *physical* hidden nodes and *protocol* hidden nodes.

Physical hidden nodes This type of hidden node was first described in [5]. It can be explained using the example in Figure 1.

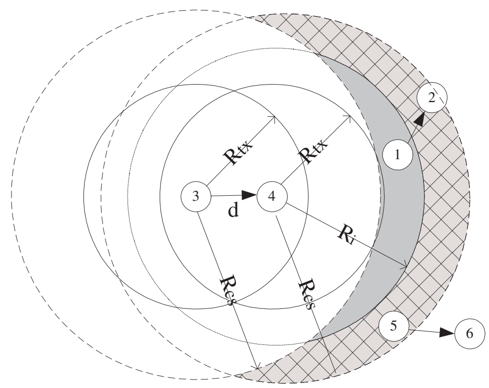

Figure 1. Hidden Node Problems

When a sender (node 3) transmits to a receiver (node 4) at a distance d away, the received power at the receiver is proportional to $1/d^4$. Another node at distance r away from the receiver will cause interference unless the signal to interference power ratio (SIR) exceeds certain threshold. Assume this SIR threshold to be 10. That means, to avoid interference the following must be satisfied:

$$SIR = P_r/P_i = (\frac{r}{d})^4 \geq 10$$

where P_r denotes the received power and P_i denotes the power of the interfering signal. This equation gives a lower bound on r so that no interference will occur. Conversely, we can define an *interference range* as a distance R_i from the receiver such that nodes falling within that range may cause interference. Using the above SIR threshold, we have

$$R_i = \sqrt[4]{10} * d = 1.78 * d \quad (2)$$

In Figure 1, given the sender is d away from node 4, any node within the interference range - represented by the circle centered at node 4 with radius R_i - may potentially interfere with the transmission from node 3 to 4 (note, d is in the range of [0, R_{tx}], so R_i may be greater than R_{tx} when d is large enough).

There are two mechanisms protecting the transmission from this form of hidden nodes interference: (i) the CTS sent from the receiver (node 4); and (ii) the sensing of node 3's transmission by the potential interferer. Protection mechanism (i) covers all the nodes in the circle centered at receiver (node 4) with radius R_{tx} (transmission range of the receiver). Protection mechanism (ii) covers all the nodes in the circle centered at the sender (node 3) with radius R_{cs} (the sensing range of the transmitter). The shaded area in Figure 1, an area within the interference range but outside of both protection range, thus represents the area where potential physical hidden nodes reside. In particular, when node 3 is transmitting to node 4, node 1's transmission to node 2 will cause physical hidden node type of collision. Since this hidden node problem is a function of the physical interference range, we named it the *physical hidden node problem*.

Protocol hidden nodes This hidden node problem is present because the sender does not hear as far as the receiver. For the same sensing range, as shown in Figure 1, the cross-lined area which can be heard by receiver (node 4) is out of the sensing range of the sender (node 3). When a transmission from node 5 to node 6 is started first, because of 802.11 protocol, any node hearing this transmission will be "frozen". This means node 4 shuts itself down from receiving. But the sender (node 3) has no idea about what is taking place at node 5 (the interfering hidden node). To node 3, the channel is idle. Therefore, node 3 would transmit to node 4 while the transmission of node 5 is in progress. A collision will occur, since no ACK or CTS will be sent to node 3 by node 4. In this case, since the hidden node problem is caused by the limitation of the protocol, we name it Protocol Hidden Node Problem. For more detail, readers are referred to [2]. Note, the authors of [2] gave the same arguments for why the RTS/CTS mechanism is ineffective against this type of hidden node problem.

In [5], the authors argued that when the carrier sensing range is larger than two times of the transmission range, RTS/CTS is no longer needed for solving the hidden node problem. But if RTS/CTS is disabled, it may lead to false blocking [9] of nodes further away. In particular, if RTS/CTS access mode is used, node 3's unsuccessful transmission will falsely block the transmission attempts of the nodes within the transmission range of node 3, but if basic access mode (e.g., disable the RTS/CTS) is used, the unsuccessful transmission will block the nodes within the carrier sensing range of node 3. Note that, hidden node problem is introduced in this paper because we need to compute the collision probability. But the false blocking problem does not lead to collision. Therefore, in this paper we assume the use of basic access mode only.

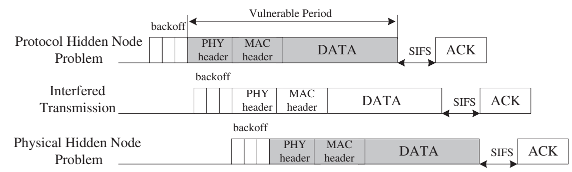

Figure 2. Collision occurs when the transmission overlaps the vulnerable period of hidden node

Note that, a subtle difference between physical hidden node and protocol hidden node is that the collision caused by physical hidden node may happen only if the hidden node transmits after the interfered node. Otherwise, if the hidden node started transmitting before the interfered node and a collision resulted, then it would be considered as a protocol hidden node induced collision.

Note that, authors in [2] mentioned that there is an ACK-ACK collision caused by exposed nodes, but compared with the hidden node problem, the ACK-ACK collision rarely happens and it has insignificant impact on the overall performance. Therefore, in this context, we assume the degradation caused by exposed nodes is negligible.

2.3 Analysis of Multi-hop Networks

Recently, [2] provides a simple model to analyze the throughput of a multi-hop network with a linear topology. The key is to identify the effect of hidden nodes as well as the effect due to the contention for channel from neighbors.

Each hidden node's transmission in the linear network has a *vulnerable* period as illustrated by the shaded parts in Figure 2. The vulnerability is in possibly colliding with the sender's transmission. Note that for a *physical* hidden node collision to occur, the interfered transmission must overlap and precede the vulnerable period (shaded part of the bottom transmission in Figure 2) of the hidden node. Alternatively, for a *protocol* hidden-node collision to occur, the interfered transmission must overlap and follow the vulnerable period (shaded part of the top transmission in Figure 2) of the hidden node.

The authors [2] study the effect of hidden node and capacity limited by the carrier sensing property "separately". They analyzed a special network topology as illustrated in Figure 3. Nodes are placed exactly 200 meters apart and all transmissions are between neighboring nodes ($d = 200$). A single source at the most left node destines the most right node and all other nodes are forwarders.

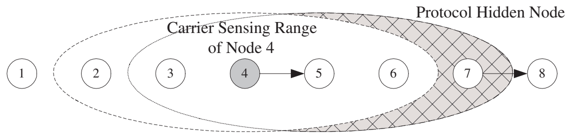

Figure 3. A Special ROD network

The collision probability caused by hidden node problem, is given by

$$\gamma = \frac{ax}{1-2x}. \tag{3}$$

Here x is defined as normalized *airtime* that a "steady-state" node transmits. These transmissions include both successful ones and collisions. Intuitively the numerator ax denotes the vulnerable period of hidden node transmission, where a is the fraction of transmission time devoted to the data packet. The *in-between* nodes (node 5 and 6 in the figure) are able to sense the transmission of the considered node (node 4) and the hidden node (node 7). Therefore, any overlap of the considered node and hidden node cannot be possible during in-between nodes' transmission. That is why $2x$ (airtime of the 2 in-between nodes) is removed from the sample space, which gives us the denominator. It also can be thought in this way: collision happens under the condition that in-between nodes do not transmit.

The total airtimes used up by the nodes in a neighborhood, is given by

$$y = 5x - 2\frac{x^2}{1-2x} - \frac{x^2}{1-2x} \cdot \frac{1-3x}{1-2x}. \tag{4}$$

As shown in figure 3, there are 5 nodes in each neighborhood. The total airtime includes the sum of airtime of those the considered node (node 4) can hear, minus some *overlapped airtimes*. What is overlapped airtime? For example, in figure 3 node 2's transmission and node 5's transmission may overlap because the two nodes don't hear each other. Since there are two in-between nodes (node 3 and node 4) whose airtimes should be removed from the sample space, we have the overlapped airtime between node 2 and 5 equal to $\frac{x^2}{1-2x}$. In other words, for each pair of nodes (in the considered node's neighborhood) that cannot hear each other, there is an overlapped airtime that needs to be removed from the simple sum of neighborhood airtimes. This is the key complexity of the problem.

In this particular example, there are three overlapped airtimes: the overlap between node 2 and 5, between node 3 and 6, and between node 2 and 6. For the former two cases, the overlap is $\frac{x^2}{1-2x}$ as derived above. For the latter case, the overlap expression can be expressed as:

$$\text{overlapped airtime betwen 2 and 6} = \frac{(x - \frac{x^2}{1-2x})^2}{1-3x}.$$

The numerator is the product of the portion of airtimes of node 2 and node 6 that may overlap (some part of node 2 and 6's airtimes already overlap with in-between nodes hence must be removed). The denominator is the sample space with the in-between airtimes removed. This is the last term of equation (4). It is pointed out [2] that the dominating effect limiting the channel capacity is due to hidden nodes in the network.

While the ideas in [2] establishes an exciting new direction, the study is quite limited in several ways. The network analyzed is a special case of linear networks with specific spacing between nodes, such that there is only a limited number of hidden nodes. They also assumed a single flow, which excluded the physical hidden node problem from being in effect. Furthermore, their solution technique does not derive collision probability, idle time and throughput explicitly.

3 Our Model and Analysis

In this section, we will combine the above results to establish a framework for modelling multi-hop ad hoc networks. Then, we apply this framework to analyze linear networks.

3.1 A General Model For IEEE 802.11 Node

Our basic approach is to assume the network is homogeneous, in the sense that each node sees other nodes the same as itself. Because of this symmetry, it is possible to define a node's own variables in terms of the corresponding variables for its neighboring nodes, and solve for them as a fixed point problem. This assumption is also the basis for the analysis in [1, 3].

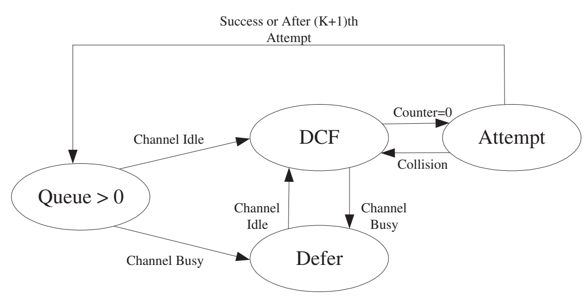

Figure 4. The State Diagram for an IEEE 802.11 Node

A node's behavior is illustrated in figure 4. Since our objective is to figure out the throughput capacity, we assume there is a nonempty queue at each node. Whenever the channel is free, a node always has a packet to send. After checking the data queue, the node senses the channel.

If the channel is busy, the node enters the "defer" state until the channel is idle. If the channel is idle, the node enters the DCF state in which the node resumes its cycle of sensing and count down. When the binary backoff counter reaches zero, the node make an attempt at transmitting its packet. This transmission may either succeed, or result in a collision. In the latter case, it returns to the DCF state (to perform binary exponential backoff); in the former case (or if the maximum attempts has been made), it restarts at checking its data queue.

Roughly speaking, a node spends its time in one of three states. The time spent in the "DCF" state corresponds to the channel idle time; the time spent in the "defer" state corresponds to the channel busy time due to other nodes transmitting; the time spend in the "attempt" state corresponds to the time the node itself is transmitting.

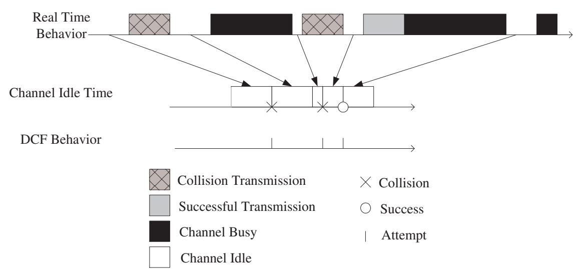

Figure 5. Real Time Sequence, and after removing the channel activities, the behavior of the DCF in channel idle slots

As shown in figure 5, it is clear that we can remove the channel activities, so that the DCF can be seen as an independent function running in the channel idle slots. Each node has its own DCF process, but they are independent of each other. As we have explained in section 2.1, $G(\gamma)$ characterizes the DCF behavior and denotes attempts per channel idle slot. Given the values of the system parameters, $G(\gamma)$ is only a function of the collision probability. Therefore, from a channel's idle probability P_{idle}, we can compute the attempt probability per slot:

$$P_t = P_{idle} \times G(\gamma). \tag{5}$$

Equation (5) implies that if we can find a way to express channel idle probability P_{idle} and collision probability γ in terms of attempt probability P_t, then this equation turns into a fixed point problem. The solution P_t of the fixed point problem can then be used to calculate the capacity per node

$$\text{Throughput} = P_t \times \frac{T}{\tau} \times (1-\gamma) \times D \times data\_rate \tag{6}$$

where T is the total transmission time for each packet (i.e. DIFS+PACKET+SIFS+ACK), τ is the slot time, and D is the ratio of effective transmission time (i.e. DATA/(DIFS+PACKET+SIFS+ACK)).

Unfortunately, deriving the exact equations for the fixed point problem is non-trivial because the impact of the hidden nodes depends on many factors, including their locations relative to the sender and sender's transmission distance. In other words, the general solution involves topology information. Therefore, we next examine how topology information affects our model by using a relatively simple example.

3.2 Analysis of Regular One-Dimension Network

A regular one-dimension (ROD) network is a network of wireless nodes placed equi-distance apart in a straight line. Theoretically, such a network is characterized by a single parameter[2], the density of nodes δ. In a regular network, all the nodes are symmetric, which makes an analytical model tractable. A One-dimension network can be seen as the basic unit of multi-hop ad hoc networks. Note that ROD networks are assumed in previous studies [2, 4] as well.

Let R_{cs} be the sensing range for each node. Given a ROD network with density δ, each node (say i) has a neighborhood of n nodes (situated at both sides) where $n = 2R_{cs}\delta$. Out of this neighborhood of nodes, n_{pr} is the numbers of nodes that may cause protocol hidden node problem, whereas n_{ph} is the number of nodes that may cause physical hidden node problem. As discussed in Section 2.2, the values of n_{pr} and n_{ph} depend on the density δ, and the distance between the transmitter and receiver d. In general,

$$n_{pr} = d\delta, \tag{7}$$

$$n_{ph} = \begin{cases} (2.78d - R_{cs})\delta, & 2.78d > R_{cs}, \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

In previous studies [2, 4], nodes are placed exactly 200 meters apart and all transmissions are between neighboring nodes ($d = 200$). In this case, $n = 5$, $n_{pr} = 1$ and $n_{ph} = 0$, as depicted in Figure 3.

As we have discussed earlier, in order to solve the capacity function in Equation (6), P_{idle} and γ should be expressed in terms of P_t. As we have mentioned in Section 2.3, the authors in [2] have proposed expressions for γ and channel busy proportion for a special network topology ($n = 5$, $n_{pr} = 1$ and $n_{ph} = 0$), as illustrated in figure 3.

Therefore in our model the collision probability[3], is given by equation (3). Note that since P_t denotes the attempt probability per slot, we have $x = \frac{P_t}{\tau} \times T$.

[2] In practice, in our simulation topologies, there is always a finite number of nodes. But for a sufficiently large network, the boundary effects are not significant.

[3] Actually, there are lots of other factors that may cause collision such as exposed node problem or neighboring nodes sending packets at same slot. But when compared with the collision caused by hidden node problem, these cases rarely happens.

The channel idle probability can be expressed as

$$P_{idle} = 1 - y = 1 - 5x + 2\frac{x^2}{1-2x} + \frac{x^2}{1-2x} \cdot \frac{1-3x}{1-2x}. \quad (9)$$

Here y denotes the normalized total airtime, which includes the channel busy time and the transmission time from a node's viewpoint, So $1 - y$ is the channel idle time ratio.

Now we have P_{idle} and γ in terms of x ($x = \frac{P_t}{\tau} \times T$), we can substitute them into equation (5) and get a fixed point problem. This problem can be solved in $[0, 1]$ by standard numerical method. It turns out with the same system parameter values, our result is very close to that obtained in [2]. Although the simulation is based on a finite linear network, the results still match with our model because the throughput for the simulation case is limited by the nodes in the center (our model is for the nodes in center).

Note that, in [2] the authors analyze the effect of the hidden node problems and carrier sensing property separately. They compared the two effects and chose the one limiting the capacity to decide the nodal airtime and hence the maximum flow throughput. Our model is different in that we unify the two effects into one fixed point equation instead of separately expressing them. With this equation, we can compute the capacity directly. But the most interesting thing is, although the methodologies are different, the numerical results match. We consider this as further validation for our model.

3.3 Analysis of ROD with Arbitrary Density

In Section 3.2, we have analyzed a special case (when the neighborhood size $n = 5$). Based on this method, we find a general expression for P_{idle} and γ for the ROD networks. The key is how to express the overlapped airtimes between certain nodes based on topological information of the network. In the earlier example, a 5-neighbor network, any three consecutive nodes do not overlap at all. But the nodes which are three hops away from each other may overlap; as well as the nodes which are four hops away. This is because in this specific network, nodes more than three hops away cannot hear each other. But in a ROD network with arbitrary density, which nodes in the same neighborhood are too far to hear each other? In general, suppose a neighborhood is a circle with a radius of R_{cs}, then any two nodes more than R_{cs} apart cannot hear each other. In ROD networks, the distance can be redefined in terms of n (the neighborhood size) - any two nodes more than $\frac{n-1}{2}$ apart cannot hear each other and may have overlapped airtime.

As shown in figure 6, In a n-neighbor network, let C_{nk} denote the overlapped airtime of two nodes whose distance is $\frac{n-1}{2} + k$ apart. The derivation of C_{nk} are as follows.

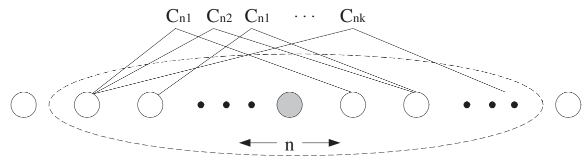

Figure 6. Nodes may overlap in ROD networks

For $k = 1$, we have

$$C_{n1} = \frac{x^2}{1 - \frac{n-1}{2}x}. \quad (10)$$

The numerator denotes the part of overall per node transmission time which may overlap each other (in C_{n1} it is x, the whole transmission time may overlap). The denominator denotes the possible sample space for the two nodes' overlap. In this case, since the two nodes can hear the in-between nodes, they cannot overlap during these nodes' transmissions. So we should eliminate the time occupied by the in-between nodes from the sample space.

For $k = 2$, we have

$$C_{n2} = \frac{(x - C_{n1})^2}{1 - (\frac{n-1}{2} + 1)x}. \quad (11)$$

Here we should omit the part which have overlapped in C_{n1} from x. (This is the same method used in the example in Section 3.2.)

Finally, we have the general expression.

$$C_{nk} = \frac{(x - \sum_{i=1}^{k-1} C_{ni})^2}{1 - (\frac{n-3}{2} + k)x + \sum_{i=1}^{k-2}(k-1-i)C_{ni}}. \quad (12)$$

Again, the numerator is x minus the part which denotes the overlapped time with these in-between nodes; and the denominator is 1 minus the time occupied by these in-between nodes.

Now, let us express P_{idle} in terms of C_{nk}. It is easy to see that there are $(n - \frac{n-1}{2} - k)$ node pairs which have C_{nk} as overlapped airtime. The idle time can be expressed as $1 - nx$, except part of this time is the sum of overlapped airtimes which we should add back. Therefore,

$$P_{idle} = 1 - nx + \sum_{k=1}^{\frac{n-1}{2}} (\frac{n+1}{2} - k)C_{nk}. \quad (13)$$

Additionally, we can also express the collision probability γ in terms of C_{nk}. C_{nk} is overlapped airtime; let γ_k be the corresponding collision probability caused by this overlap. So we write

$$\gamma_k = \frac{aC_{nk}}{x - \sum_{i=1}^{k-1} C_{ni}}. \quad (14)$$

The above formulae look quite complex. However, we can prove by mathematical induction the following equation is true

$$C_{nk} = \frac{x^2}{1-(\frac{n-1}{2})x} \times (\frac{1-(\frac{n+1}{2})x}{1-(\frac{n-1}{2})x})^{k-1}. \quad (15)$$

Equation (15) implies that γ_k is independent of k, and it can be expressed as

$$\gamma_k = \frac{ax}{1-(\frac{n-1}{2})x}. \quad (16)$$

The overall collision probability γ can be expressed in terms of γ_k

$$\gamma = 1-\prod(1-\gamma_k) = 1-(1-\frac{ax}{1-(\frac{n-1}{2})x})^{n_{pr}+n_{ph}}. \quad (17)$$

Substituting equations (13) and (17) into (5), we have

$$\frac{x}{1-\frac{n-1}{2}x} = \frac{T}{\tau}(\frac{1-(\frac{n+1}{2})x}{1-\frac{n-1}{2}x})^{\frac{n+1}{2}} G(\gamma(x)). \quad (18)$$

This is the fixed point equation that one can use to solve for the maximum throughput analytically.

3.4 Optimal Hop Distance

When considering a network where every node is a source of traffic, density δ is an explicit parameter of the network. If there is only a given number n_s of traffic sources in the network, then the density of active nodes in the network is an implicit parameter dependent on n_s and the transmission distance d. For a ROD network where the hop distance is d, the density is given by n_s/d.

Figure 7 shows a ROD network with 2 sources. Both flows choose d hop distance for forwarding, and it is easy to see that this implies $\delta = \frac{2}{d}$.

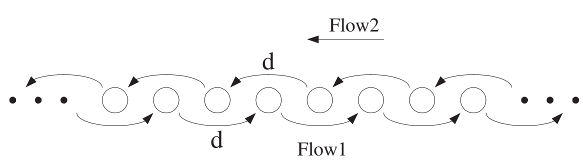

Figure 7. ROD network with 2 sources

.

The above discussion implies that better throughput should be achieved with longer hop distance (hence lower density). This is always true in single-flow ROD networks (which will be validated in next section). For more than one source, however, as we have discussed in Section 2.2, longer hop distance is more likely to lead to hidden node problems, hence cause degradation in performance. Therefore, there is a need to balance the advantage and the disadvantage of hop distance.

In single-flow networks, only one *protocol* hidden node is involved no matter how long the hop distance is. Since each node uses the same hop distance, and there are no active nodes from other flows, there will not be any *physical* hidden node or more than one *protocol* hidden node. But single-flow is not a good assumption, as in real life scenarios there are more likely multiple simultaneous flows.

To study inter-flow interference, we introduce a two-source ROD network as shown in figure 7. One flow is from right to left and the other is from left to right. In order to evaluate the effect of hop distance, we manually configure the routing for each flow so that they choose alternating nodes as the next hop. For two flow networks, we already know the implicit density is $\delta = \frac{2}{d}$. Hence the neighborhood size is $n = 2R_{cs}\delta$. Given $R_{cs} = 550m$ and equations (7) and (8) for number of hidden nodes, we can compute the actual values of n, n_{pr} and n_{ph}. Substituting n, n_{pr} and n_{ph} into equation (18), and with given system parameters as in TABLE 1, we have a fixed point equation, which gives the relationship between the airtime x and hop distance d. And correspondingly from equation (6) we know the relationship between the throughput and d, hence we can plot Figure 8.[4] The x-axis is the hop distance in meters, and the y-axis is achieved throughput computed based on the airtime.

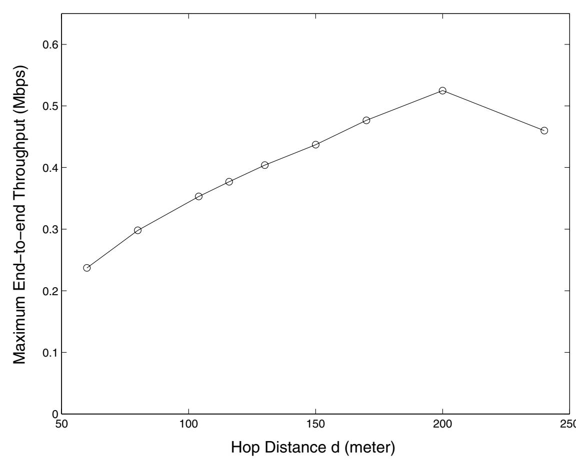

Figure 8. ROD network with 2 sources: End-to-end Throughput Capacity V.S. Hop Distance d

Obviously, the result shows that there is an optimal hop distance less than the physical maximum transmission distance (250 meters). In this case, the optimal hop distance

[4]Since the airtime is given by the fixed point equation rather than a closed form solution, we have to use standard numerical methods to produce the values for plotting.

is about 200 meters. In ROD network, this distance is a threshold beyond which physical hidden node problem appears (according to equations (7) and (8)). That means before physical hidden node joins in, the advantage of increasing hop distance dominates the disadvantage. But physical hidden node breaks this tendency and cause overall degradation to the performance.

4 Simulation Validation

Our simulation environment was created using the simulator ns2.27 [8], which simulates wireless networks based on IEEE802.11 standard. TABLE 1 shows the system parameters assumed, and the RTS threshold is set to 5000 so that nodes do not use RTS/CTS handshake.

Table 1. System Parameters

Transmission range R_{tx}	250m
Carrier-Sensing range R_{cx}	550m
CPThreshold	10dB
Propagation model	TwoRayGround
Packet payload	1500 bytes
UDP 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	20 μs
SIFS	10 μs
DIFS	50 μs
CW_{min}	32
CW_{max}	1024
Retransmission limit	7
Traffic pattern	CBR
Transport protocol	UDP

To find the maximum throughput for each case, we need to ensure all nodes are running with saturated load levels. In the simulation, since the network topology is finite, the boundary nodes can transmit at a higher rate than the nodes at the center [2, 4]. Therefore in our simulation, we manually adjust the offered load to the optimum value to achieve the maximum stabilized throughput. With this maximum throughput we verify our analytical result of the ROD network capacity.

4.1 Validation of Single Source ROD Network

In order to minimize the boundary effect, we deployed a very long chain of nodes to make sure the end-to-end throughput is dominatingly limited by the capacity of center nodes. The first node is the only source and the last node is its destination. We vary the offered loads until the system achieves the maximum stabilized throughput with respect to a given hop distance.

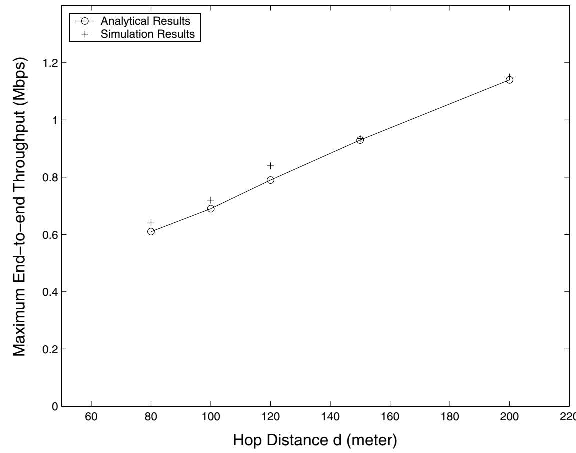

Figure 9. The capacity of single source ROD network: Simulation vs Analysis

In Figure 9, each point we plot corresponds to a distinct neighborhood size, n. For example, $n = 5$ is when $d = 200$, $n = 7$ is when $d = 150$, $n = 9$ is when $d = 120$ and so forth. As we increase the hop distance, hence reduce n, there is reduced neighbor contention and therefore higher throughput. In a single source network, for $200 < d <$maximum distance, the neighborhood size n will remain at 5, so the maximum throughput will remain flat. All values from the analytical model are derived by numerical method with the same system parameters as simulation (see Table 1). Figure 9 shows that the analytical results are reasonably close to the simulation results, and that the analytical model is able to accurately predict the capacity of the single source ROD network.

4.2 Validation of 2-Source ROD Network

The 2-source ROD network is shown in Figure 7. Following the same procedure as in Section 4.1, we plot the results in Figure 10

This time, we plot the average throughput of one flow against the hop distance (hence it is about half of the single flow ROD throughput). As in the single flow ROD case (Figure 9), throughput increases with increased hop distance until $d = 200$. This time, when $d = 200$ the neighborhood size is $n = 11$ and the neighborhood size continues to decrease beyond $d = 200$ (when $d = 240$, $n = 9$). So theoretically, throughput should continue to increase. However, this time as d increases beyond 200, in addition to protocol

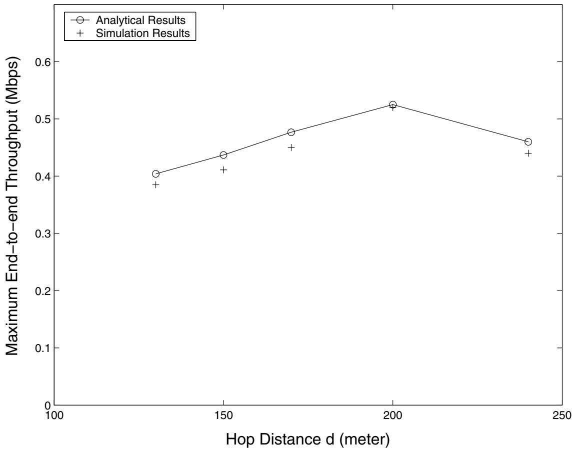

Figure 10. The Capacity of ROD network with 2 sources: Simulation V.S. Analysis

hidden nodes, *physical* hidden node (from other flow) interference also comes into effect. The additional hidden node effect dominates, and the throughput drops. The optimal throughput is achieved at approximately $d = 200$.

The simulation results again closely match the analytical results, validating our model for 2-source ROD networks.

4.3 Comparison with traditional wireless routing

In the simulation experiments above we used manual routing. This is done by manually configuring an application agent at each forwarding node.

For 2-flow ROD networks, the results imply optimal throughput can be achieve using 200 meters as hop distance. In order to support this claim, we designed a simulation experiment with traditional wireless routing. We deploy DSDV in the linear network in which candidate forwarding nodes are uniformly distributed between sources and destinations with high density. Two flows are generated: one is from the most right to the most left, the other is reverse direction. Given the same network size as the simulation shown in figure 10 (about 2400m, $200m \times 12$), all the experiments with DSDV routing protocol show that the maximum end-to-end throughput is no more than $0.47Mbps$, significantly less than $0.52Mbps$, the optimal simulation result in 2-source ROD network. Since DSDV is roughly equivalent to a minimum-hop-count routing algorithm, it would pick the longest-hop-distance nodes to be forwarders, which is not optimal according to our model. The result implies that it will be helpful to the system capacity if we take the consideration of optimal hop distance into the routing algorithm design.

5 Two-dimensional Network Investigation

We have shown that there exists an optimal transmission distance by which maximum throughput is achieved in ROD networks. In this section we will show that the conclusion of the optimal transmission distance is also applicable in a two-dimensional network.

To study the effect of the transmission distance on throughput capacity in two-dimensional networks, we consider an $N \times N$ lattice network as shown in Figure 11. All nodes are evenly separated by a same distance d. Nodes in the first column are the source nodes, and each of them injects traffic into the networks destined for nodes in the last column. It has been discussed in [2] that fairness is achieved by offered load control. So in our simulation, we obtain the maximum sustainable end-to-end throughput by adjusting offered load such that each flow satisfies fairness constraint. In order to eliminate the boundary effect, we choose a 10×10 lattice network in the simulation.

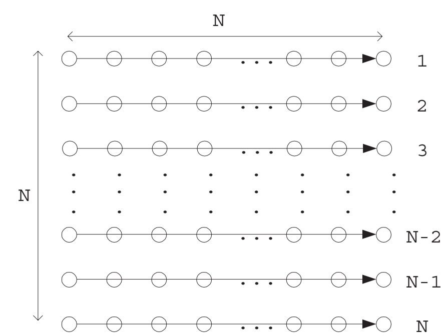

Figure 11. An $N \times N$ Lattice Network Topology with N Traffic Flows From Left to Right

Figure 12 illustrates the result. It shows that the optimal sustainable end-to-end throughput are achieved in the transmission distance which is less than the transmission range (250m). The result can be explained in the same way as the case in one dimension network: Longer transmission distance will result in less nodes in a neighborhood (sharing the channel). Before physical hidden nodes appear ($d < 200$), the throughput capacity of the nodes in the center of the network will increase as d increases. But when the phenomenon of physical hidden node occurs ($d \approx 250$ in this case), even the advantage of having less contentions cannot compensate the degradation caused by the additional hidden node problem. So one can observe when $d = 250m$, the maximum per-flow throughput is much less than that with $d = 200m$. Therefore the result further support our claim on optimal transmission distance in multi-hop networks.

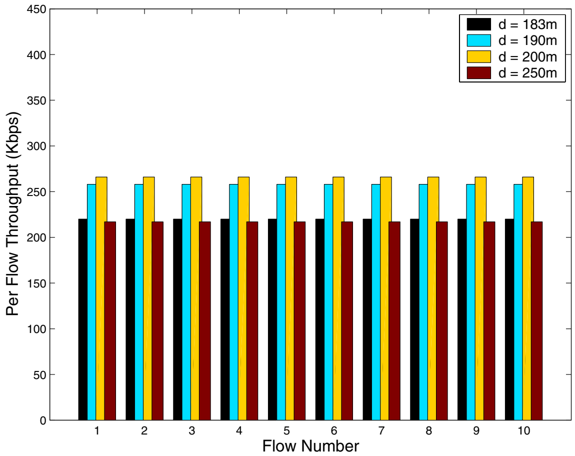

Figure 12. Maximum Per-flow Throughput with Different Hop Distances

6 Conclusion

First, we summarize the major contributions of this paper:

1. We proposed a general model for the study of the capacity of IEEE802.11 multi-hop ad hoc networks. This model captures the inherent tradeoff between the effects of hidden node problems (physical and protocol) and the effects of channel contention by nodes who can hear each other (in a neighborhood).

2. Using this model, we have analyzed the capacity of regular one-dimensional (or linear) networks. It is validated by simulation results that this model is accurate in predicting the maximum system throughput. We also simulated a two-dimensional network with nodes placed on a regular grid and multiple flows. The result also confirms our analysis.

3. Based on our models, we observe the importance of hop distance in achieving optimal end-to-end throughput.

   We believe this insight is important for designing multi-hop ad hoc routing algorithms in wireless networks.

Looking forward, these results also open up many directions for further research. In particular, we are working along the following areas: (a) generalize to an arbitrary network topology, (b) assume all nodes have random traffic to send, and (c) study the effect of non-ideal physical layer model, such as the transmission range is not a disk. Some of these scenarios will not be amenable to analytical results, but it would be interesting to see whether, or to what extent, our optimal hop distance idea still applies.

Acknowledgement: We thank Professor Soung Liew for stimulating discussions. It is Professor Liew who motivated us to work on this problem. We are also grateful to our shepherd, Professor Jennifer Hou, for her insightful suggestions.

References

[1] A. Kumar, E. Altman, D. Miorandi and M. Goyal. ”New insights from a fixed point analysis of single cell IEEE 802.11 wireless LANs”, Proceedings of the IEEE Infocom, 2005.

[2] C. Ng, and S. C. Liew, ”Offered Load control in IEEE 802.11 Multi-hop Ad-hoc Networks”, The 1st IEEE International Conference on Mobile Ad-hoc and Sensor System, Oct 2004.

[3] G. Bianchi. ”Performance analysis of the IEEE 802.11 distributed coordination function”, IEEE Journal on Selected Areas in Communications, March 2000.

[4] J. Li, C. Blake, Douglas S.J. De Couto, H. I. Lee, R. Morris, ”Capacity of Ad Hoc Wireless Networks”, ACM MobiCom’01, Rome, Italy, July 2001.

[5] K. Xu, M. Gerla, and S. Bae. ”How effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Network”, In Proc. IEEE GlobeCom’02, Taipei, Taiwan, Nov. 2002

[6] P. Gupta, P. R. Kumar, ”The Capacity of Wireless Network”, IEEE Trans. On Information Theory, Vol.46, No.2, pp.388-404, Mar. 2000.

[7] S. Ray, D. Starobinski and J. B. Carruthers, ”Performance of Wireless Networks with Hidden Nodes: A Queuing-Theoretic Analysis”, Journal of Computer Communications, Special issue on the Performance of Wireless LANs, PANs, and Ad Hoc Networks, in press

[8] ”The Network Simulator-ns2”, http://www.isi.edu/nsnam/ns

[9] S. Ray, J. B. Carruthers and D. Starobinski, ”RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs”, WCNC 2003: Wireless Communications and Networking Conference. New Orleans: March 16 - 20, 2003