PERFORMANCE ANALYSIS OF THE IEEE 802.11-BASED WIRELESS NETWORKS IN THE PRESENCE OF HIDDEN STATIONS

by

FU-YI HUNG

A Dissertation submitted to the

Graduate School-New Brunswick

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Professor Ivan Marsic

And approved by

_____

_____

_____

_____

New Brunswick, New Jersey

October, 2009

ABSTRACT OF THE DISSERTATION

Performance Analysis of IEEE 802.11-Based Wireless Networks

in the Presence of Hidden Stations

By Fu-Yi Hung

Dissertation Director:

Professor Ivan Marsic

The IEEE 802.11 is the most widely used standard in WLAN currently. It can support not only a WLAN with an access point but also an ad hoc wireless network. The key for being able to support various wireless networks is the Distribution Coordination Function (DCF) which is one of channel access methods in the IEEE 802.11 Medium Access Control (MAC) protocol. The DCF is a random access method where each station has the right to initiate a transmission without any central coordination. Hence, this method is useable not only in infrastructure network configurations but also in distributed and self-organized wireless networks. However, this random access method unavoidably introduces the hidden station problem that multiple stations simultaneously transmit packets to a common destination resulting in packet collision at the destination. This problem results from that DCF does not support the destination coordinating the traffic inside its transmission range. The hidden station problem is unique to wireless networks and significantly degrades the performance of wireless networks, but this problem has been ignored in previous studies.

We propose our research work that model and analyze the performance of wireless networks including the hidden station effect in access-point and ad hoc type wireless networks. In access-point based wireless networks, we present a modified two-dimensional Markov chain model that characterizes the network performance in the presence of hidden stations. This model generalizes the existing work on IEEE 802.11 DCF performance modeling, and it is validated by comparison with ns-2 simulation. Second, in wireless ad hoc networks, the hidden station effect is different from that in an access-point based wireless network. Furthermore, this effect largely depends on the sender-receiver distance and physical carrier-sensing range. We devise a spatiotemporal analytical model that estimates the number of hidden stations based on the sender-receiver distance and physical carrier-sensing range. In addition, we also use our two-dimensional Markov chain model to evaluate the network performance under the hidden station effect in wireless ad hoc network. This result is in agreement with the result obtained by ns-2 simulation.

Acknowledgement

Firstly, I would like to express my sincere gratitude to Professor Ivan Marsic, my advisor, for his guidance, comments, and encouragement throughout my Ph.D. studies at Rutgers, The State University of New Jersey. I have benefited very much from working under his supervision.

I also would like to thank Professor David G. Daut, Professor Dario Pompili and Professor Liang Cheng for serving on my dissertation committee. Their valuable comments and suggestions have greatly aided the completion of this study.

Special thanks are given to my parents and wife, for their encouragement and support throughout my studies.

Table of Contents

List of Tables

List of Figures

List of Figures

Chapter 1

Introduction

1.1 Overview of 802.11 Networks

IEEE 802.11 [1] is the most popular standard used in Wireless Local Area Network (WLAN) because 802.11 based WLANs are easy to deploy and easy to use. This standard can support not only the infrastructure WLAN but also the wireless ad hoc network. An infrastructure WLAN is composed of one access point (AP) as the center of communications and some stations located within the coverage area of the AP. Every station in this network communicates only with the AP and does not directly communicate with the other stations even if the destination station is located inside its transmission range. On the other hand, a wireless ad hoc network consists of a group of stations that directly communicate with one another instead of relying on an AP to forward the frames to the destination stations. Wireless ad hoc networks are applicable where there is no support of infrastructure networks. Hence, they are popular for use in military and rescue operations. The key for being able to supporting various wireless networks is the Medium Access Control (MAC) protocol that allows for stations staring their transmission on the channel without any central coordination.

1.2 IEEE 802.11 MAC Protocol

The MAC protocol includes two channel access methods: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). The DCF is the Basic access method of the 802.11 MAC. It is a random access method where each station has the right

to initiate its transmission without any central coordination. So, this method is useable not only in infrastructure network configurations, but also in distributed and self-organized wireless networks. On the other hand, the PCF is an optional access method. It is a polling-based access method that uses a virtual carrier-sense mechanism aided by an access priority mechanism to control the channel access. It provides a contention-free frame delivery to and from the access point. However, PCF only supports infrastructure network configurations because it needs an access point to manage the channel access. This method is not widely implemented in currently deployed WLANs.

1.3 The Hidden Station Effect

The random access method is a key element of DCF to support various wireless networks: infrastructure and ad hoc networks. However, this method unavoidably introduces the *hidden station problem* [2, 3] because of multiple simultaneous transmissions on the same channel without any coordination resulting in packet collision on the destination. The hidden station problem is unique to wireless networks because of two characteristics of wireless channels. First, a station cannot sense the channel to detect a collision simultaneously while sending a packet on the same channel. Secondly, a station cannot sense its packet collided with another packet from a hidden station because of limited radio coverage. For example, if stations A and C are inside the transmission range of station B but cannot sense each other's transmission, they are hidden station to each other. When station A is transmitting a packet to station B, station C could transmit another packet to station B simultaneously resulting packet collision on station B.

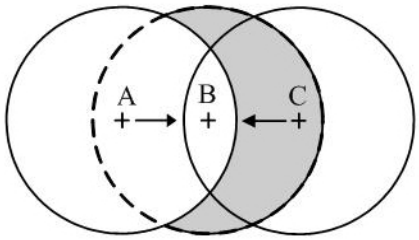


Figure 1.1: Illustration of the hidden station problem.

1.4 Outline of the Dissertation

The rest of this dissertation is organized as follows. In Chapter 2, we summarize the IEEE 802.11 distribution coordination function. In Chapter 3, we study the hidden station effect in access-point based wireless networks throughput a spatiotemporal analytical model. In Chapter 4, we present a two-dimensional Markov chain model that characterize the network throughput in access-point based wireless networks in the presence of hidden station effect. In Chapter 5, we investigate the hidden station effect in wireless ad hoc networks through defining the semi-hidden station and using the spatiotemporal analytical model. In Chapter 6, we propose an analytical model that describes the optimal physical carrier-sensing range in wireless ad hoc networks. In addition, we extend our two-dimensional Markov chain model that represents the network throughput of wireless ad hoc networks in the presence of regular and semi-hidden stations. Finally, several conclusions and future work are described in Chapter 7.

Chapter 2

The IEEE 802.11 Distribution Coordination Function

2.1 CSMA/CA and Backoff Procedure

The IEEE 802.11 MAC [1] protocol is used to coordinate multiple stations transmitting on a shared channel. The IEEE 802.11 MAC architecture includes two access methods: a fundamental access method called Distributed Coordination Function (DCF) and an optional access method called Point Coordination Function (PCF). The PCF is a polling-based access method that uses a virtual carrier-sense mechanism aided by an access priority mechanism to control the channel access. It provides a contention-free frame delivery to and from the access point but it only supports infrastructure network configurations because it needs an access point to manage the channel access. On the other hand, the DCF is a contention-based access method that uses a random access method where each station can initiate its transmission without any infrastructure support. As a result, this method is able to support both infrastructure type WLAN and ad hoc wireless networks. It is widely used in currently available Wi-Fi products.

The DCF is based on the CSMA/CA mechanism and a backoff procedure to reduce the collision probability between multiple stations accessing the same channel. The CSMA/CA mechanism defines these two channel states: *idle* and *busy*. If a station can detect signal on the channel and the energy level of the signal exceeds the threshold, then its Clear Channel Assessment (CCA) mechanism shall report the channel as busy; otherwise it considers the channel as idle. This threshold is called physical carrier sensing

threshold. In DCF, a station has to sense the channel state before transmitting a packet. If the channel is sensed as idle then it transmits the packet; otherwise, it goes to its backoff procedure that defers its transmission by a random period of time and then senses the channel again. When a station executes the backoff procedure, it randomly chooses an integer from the interval $(0, W_0 - 1)$ with a uniform probability. The W_0 is known as the initial or minimum size of the contention window and this property is known as truncated backoff procedure. During the backoff procedure, if the station senses the channel as idle, it decrements the timer by one backoff slot. If the channel is sensed as busy, the timer is frozen. After the channel becomes idle again, the timer is resumed from the frozen slot and counts down the remaining backoff slots. After the timer finishes the countdown, the station transmits. If the transmission fails, the station doubles the contention window size and repeats the backoff procedure. After every failed transmission, the exponential backoff mechanism doubles the contention window size up to a predefined maximum range.

2.2 Basic Access Method

The DCF includes two access techniques: Basic and Request-To-Send/ Clear-To-Send (RTS/CTS) access mechanisms. The Basic access method is a two-way handshaking mechanism as shown in Figure 2.1. After waiting for a DCF Inter-Frame Space (DIFS) period and finishing its backoff procedure, the source sends a data frame to the destination. The destination waits for a Short Inter-Frame Space (SIFS) period and then replies with an ACK frame to confirm this successful transmission regardless to the busy/idle state of the channel. Any other station that can sense the transmitting data frame will determine the

channel state as busy. If it has a packet in queue to transmit, then it will suspend its transmission process until the end of the ACK frame plus a DIFS time.

2.3 RTS/CTS Access Method

On the other hand, the RTS/CTS access method is a four-way handshaking access method as shown in Figure 2.2. After waiting a DIFS period and completing the backoff procedure, the source sends a RTS frame to reserve the channel. After receiving the RTS frame, the destination waits for a SIFS period and replies with a CTS frame to the source. The source detects the CTS frame and waits a SIFS period, and then it sends a data frame. If the destination correctly receives the data frame, the destination responds with an ACK frame to confirm this transmission. Any other station that can sense the RTS or CTS frames will set its Network Allocation Vector (NAV) to defer its transmission process until the end of the ACK frame plus a DIFS time.

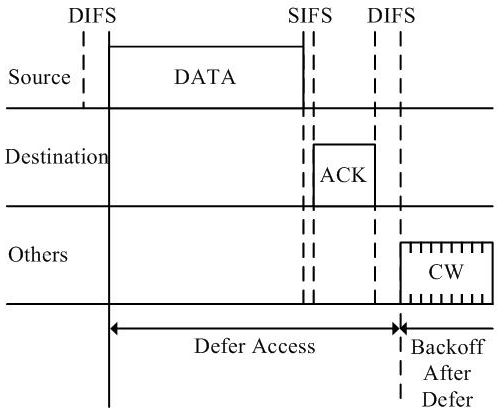


Figure 2.1: Timing diagram for the Basic access method.

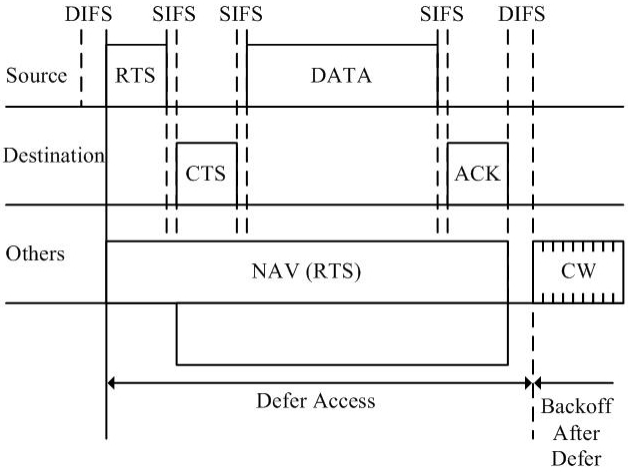


Figure 2.2: Timing diagram for the RTS/CTS access method.

Chapter 3

The Hidden Station Effect in Wireless Local Area Networks

3.1 Spatial Analysis of the hidden station effect

When the source transmits a data frame to the destination, any station that can sense the transmission from both the source and destination, is called a *covered station*. On the other hand, any station that does not sense the transmission from the source but can sense the transmission from the destination is called a *hidden station*. Consider a wireless network composed of an access point and some mobile stations randomly distributed around it. The transmission in this network can be classified as downstream and upstream traffic: sending a packet from the access point to a station is called the downstream traffic; and sending a packet in the reverse direction is called upstream traffic. There is no hidden station problem in the downstream traffic because all stations can sense the transmission from the access point. However, not all stations can sense the transmission of one another in the upstream traffic so the hidden station problem exists in this condition. In order to study the hidden station effect, we focus on the upstream performance of the network in this dissertation.

The hidden station problem exists for the upstream traffic, however, this does mean that it happens always. A key question is, how frequently the hidden station problem occurs for the upstream traffic of a wireless network? First, what is the theoretical average number of hidden stations from a station's viewpoint in a random topology? Consider the scenario as shown in Figure 3.1, where a station, called *S*, is randomly located within the transmission range of an access point, called *D*. Let the A_S and A_D represent the circle areas covered by

the transmission ranges of the *S* and *D*, respectively. Any other station is a covered station to station *S* if it is located in the intersection area of the two circles, denoted as $A_{S\cap D}$. On the other hand, if a station is located in the shaded area, denoted as A_{D-S}, then it is a hidden station to *S*. Let *d* denote the distance between the *S* and *D*. The shaded area A_{D-S} can be derived as

$$A_{D-S} = \pi \cdot R_t^2 - 4\int_{d/2}^{R_t} \sqrt{R_t^2 - x^2}\, dx \tag{3-1}$$

When $d = 0$, the shaded area A_{D-S} is zero. When $d = R_t$, the shades area reaches it maximum value that equals to $0.61\ \pi\ R_t^2$. If the station *S* is randomly located in *D*'s transmission range, the average shaded area is $0.41\ \pi\ R_t^2$ [14]. For example, if there are 8 stations randomly distributed around an access point and each station competes with 7 other stations to communicate with the access point, then the average number of the hidden station to a station is $7 \times 0.41 = 2.87$ and the average number of the covered station to a station is 4.13.

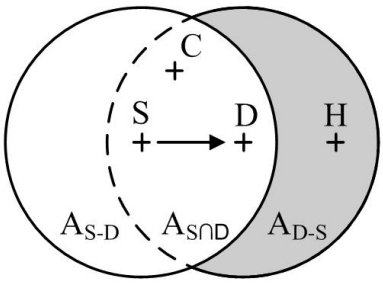


Figure 3.1: Analysis of the intersection area between the transmission ranges for stations *S* and *D*.

We study the probability of no hidden station for the upstream scenario through the Monte Carlo method as shown in Figure 3.2. Given n stations, we randomly deploy them around the access point. For each station, we count how many of the remaining $(n - 1)$ stations are hidden to this station. Secondly, we calculate the average number of hidden stations over all stations. We assume that the transmission range (R_t) equals the receiving range in this study. We find that this probability decreases rapidly as the number of stations in a wireless network increases. When the physical carrier sensing range (R_{cs}) equals to the transmission range, this probability is lower than 50% in the network of 3 stations. Even when we choose a large physical carrier sensing range, such as $R_{cs} = 1.75R_t$, this probability is still lower than 50% if the number of station is more than 10. Obviously, the hidden station problem happens frequently in the WLAN with an access point.

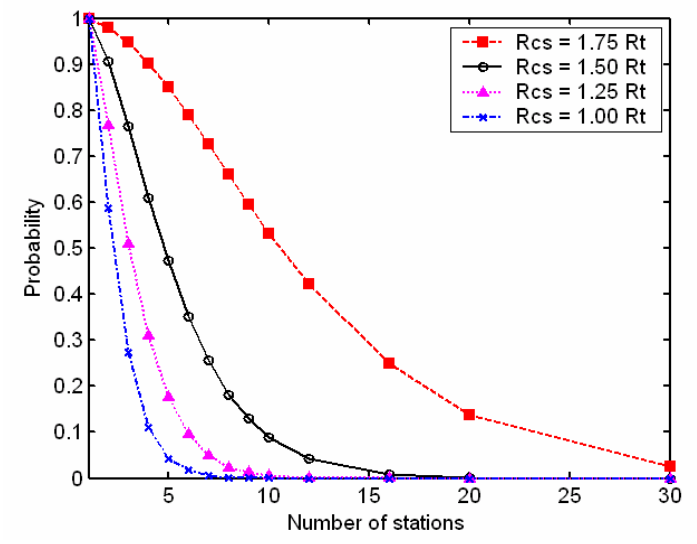


Figure 3.2: Probability of no hidden station in a wireless network.
R_{cs} = the physical carrier sensing range; R_t = the transmission range.

Another important question is how seriously affected is the performance of the 802.11 DCF by the hidden station phenomenon. We study this question by using both spatial and temporal analyses methods as follows.

3.2 Temporal Analysis of the Hidden Station Effect

3.2.1 Basic Access Method

When the source transmits a data frame to the destination, the covered station will determine the channel as busy and defer its transmission. A packet collision between the source and a covered station occurs only if the covered station transmits its frame before it senses the transmission from the source. The possible collision period between two stations is called the *vulnerable period*. This period for a covered station in the Basic access method is the minimum period of time from the time that the source starts to transmit a data frame to the time that the covered station detects this ongoing transmission. In IEEE 802.11, this period of time is defined as one *slot time*, shown in Figure 3.3, which includes a CCA time, an Rx-Tx (switching from the receiving to the transmitting state) turnaround time, an air propagation time and a MAC processing delay [1]. On the other hand, when the source transmits a data frame to the destination, the hidden stations will determine the channel as idle until they receive an ACK frame from the destination. Any hidden station could transmit another frame to the destination in this period of time (a data frame and a SIFS time). Based on the ACK procedure of the 802.11 DCF, after a successful reception of a data frame from the source, the destination will reply with an ACK frame after a SIFS period from the successful reception, without regard to the busy or idle channel state. If a station transmits another frame in the period of SIFS time between the data and ACK frame

and the destination correctly receives the data frame from the source, then the destination will still reply an ACK frame to confirm the success of the transmission. So, the vulnerable period for a hidden station in the Basic access method equals the length of a data frame as shown in Figure 3.3. If the packet arrival rate, from the upper layer to the MAC layer, is the same for all the stations, then a longer vulnerable period to hidden stations means that a hidden station could transmit a frame with a higher probability in the vulnerable period. So, the probability of collision within the vulnerable period with a frame from a hidden station is much higher than the probability of collision with a frame from a covered station.

When a frame sent from the source collides with another one from a covered or hidden station, the source will conclude that this transmission has failed if it does not receive an ACK frame after an ACK_Timeout period in the Basic access method. This period, from the beginning of the data frame to the end of the ACK_Timeout, is called the *collision time*. The source wastes one collision time in each frame collision event, regardless of whether the collided frame comes from a covered or a hidden station.

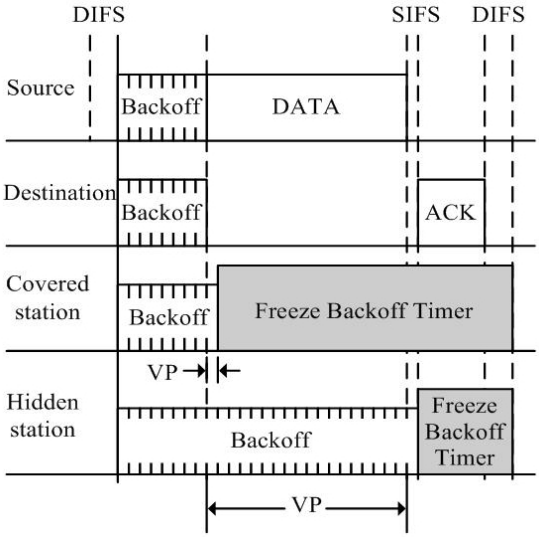


Figure 3.3: The vulnerable period for the covered and hidden stations: the Basic access method.

3.2.2 RTS/CTS Access Method

As in the Basic access method, when the source transmits a data frame to the destination, the covered stations will determine the channel as busy and defer their transmission for the duration of the NAV. The vulnerable period for a covered station in the RTS/CTS access method is also a slot time. On the other hand, when the source transmits a data frame to the destination, the hidden stations may determine the channel as idle before they receive a CTS frame from the destination. Based on the RTS/CTS procedure of the 802.11 DCF, the destination will reply a CTS frame only if it receives the RTS frame correctly and it senses the channel as idle. If the hidden station transmits another frame in the period of SIFS between the RTS and CTS frame, the destination will determine the channel as busy and will not reply with a CTS frame, even if it correctly receives the RTS frame. So, the vulnerable period for a hidden station in the RTS/CTS access method equals the sum of the RTS frame and a SIFS time as shown in Figure 3.4.

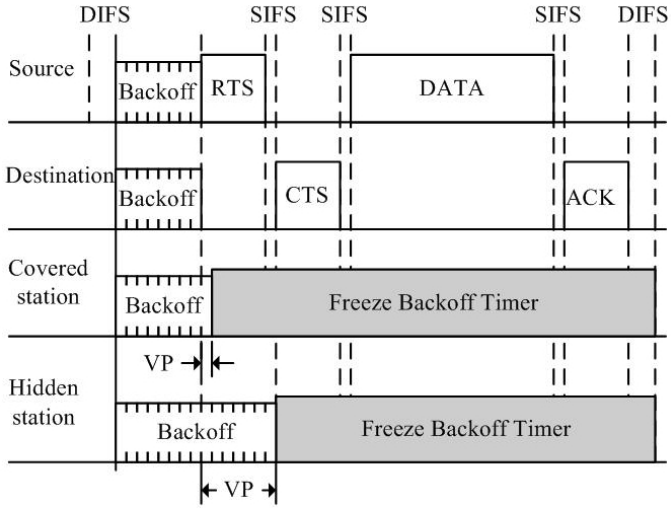


Figure 3.4: The vulnerable period for the covered and hidden stations: the RTS/CTS access method.

When two frames collide at the destination, the source will conclude that its transmission has failed if it does not receive a CTS frame after a CTS_Timeout period. So, the collision time in RTS/CTS access method is the length of a RTS frame and a CTS_Timeout as listed in Table 3.1. Comparing the hidden station effect on the Basic and RTS/CTS access methods, the vulnerable period for the covered station in the RTS/CTS access method is same as that in the Basic access method. However, unlike the Basic access method, the vulnerable period for hidden stations in RTS/CTS access method is a fixed length period, a RTS frame plus a SIFS time, and does not depend on the length of the data frame from the source. In general, the length of a data frame is longer than that of a RTS frame and a SIFS time, 362 μs in 802.11b DSSS, and the ACK_Timeout equals to the CTS_Timeout. So, the RTS/CTS access method reduces both the vulnerable period and collision time for the hidden stations. However, the RTS/CTS access method introduces an overhead, a RTS/CTS handshaking period, in every successful transmission.

Based on our temporal analysis, if the packet arrival rate on all stations is the same, the packet collision probability between the source and a hidden station is higher than that between the source and a covered station, because the vulnerable period in the former scenario is longer than that in the latter scenario. To determine an accurate relationship between the vulnerable period and the packet collision probability, we use a two-dimensional Markov chain model described in the next section.

Table 3.1: The vulnerable period and collision time.

Mode / Parameter	Vulnerable period	Collision time
Basic: Covered ST	A slot time (20 μs)	DATA + ACK_Timeout (DATA + 364 μs)
Basic: Hidden ST	DATA	DATA + ACK_Timeout (DATA + 364 μs)
RTS/CTS: Covered ST	A slot time (20 μs)	RTS + CTS_Timeout (716 μs)
RTS/CTS: Hidden ST	RTS + SIFS (362 μs)	RTS + CTS_Timeout (716 μs)

Chapter 4

Performance Analysis of the 802.11 DCF in Wireless LAN

In this chapter, we propose a generalized analytical model to evaluate the performance of the 802.11 DCF including the Basic and RTS/CTS access methods, in the presence of both covered and hidden stations. We also extend our study to non-saturation and saturation traffic conditions. We use a two-dimensional Markov chain model [7–9] to evaluate the collision probability in Section 4.1 and derive the network average throughput in Section 4.2.

4.1 Transmission Probability

In this analysis, we assume the following conditions: (a) ideal channel condition, i.e., no channel error due to noise; (b) constant and mutually independent collision probability of a packet transmitted by each station, regardless of the number of collisions already suffered; and, (c) fixed number of stations in the network.

Consider the number of contending stations, defined as n, to be fixed. Let the station's backoff state $b(t)$ be the stochastic process representing the value randomly chosen for the backoff countdown timer. We will assume that the probability of collision for a frame is not related to how many collisions this frame already suffered. In other words, the probability p of a transmitted packet colliding with another packet is independent of the station's backoff stage $s(t)$. This is only approximately true for relatively large contention

windows and the number of stations. So, the two-dimensional process $\{s(t), b(t)\}$ can be modeled as a discrete-time Markov chain, shown in Figure 4.1.

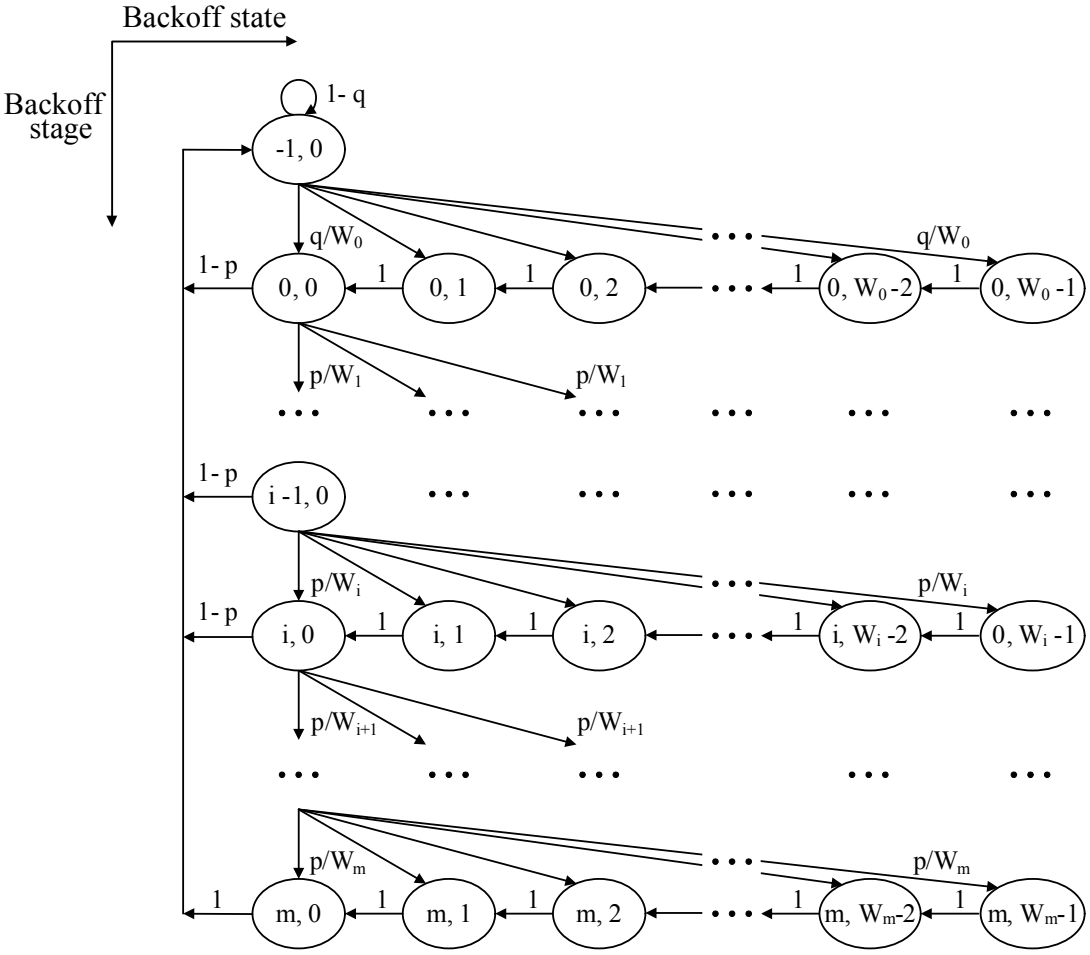


Figure 4.1: Markov chain model for backoff procedure.

Based on the IEEE 802.11 Standard [1], the size of the contention window, also called the backoff window, increases exponentially from the minimum contention window, W_0, to the maximum contention window, W_{max}. It can be represented by

$$W_i = \begin{cases} 2^i W_0 & ,0 \le i < m' \\ 2^{m'} W_0 = W_{\max} & ,i \ge m' \end{cases} \tag{4-1}$$

where m is the maximum backoff stage and m' is the backoff stage at which the contention window reaches the maximum value, W_{max}, and remains at W_{max} after this stage (thus, the name "truncated backoff procedure"). Without loss of generality, we set $m = m' = 5$ in this dissertation.

We assume that q represents the probability of at least one packet waiting for transmission at the station during a slot time. If $q = 1$, then the station is in a saturation condition. In this Markov chain, the transition probabilities are given according to

$$\begin{aligned}
&P(-1,0 \mid -1,0) = 1-q && \\
&P(0,k \mid -1,0) = \frac{q}{W_0} && 0 \le k \le W_0 - 1 \\
&P(i,k \mid i-1,0) = \frac{p}{W_i} && 0 \le k \le W_i - 1, \quad 1 \le i \le m \\
&P(-1,0 \mid i,0) = 1-p && 0 \le i \le m-1 \\
&P(-1,0 \mid m,0) = 1 && \\
&P(i,k-1 \mid i,k) = 1 && 1 \le k \le W_i - 1, \quad 0 \le i \le m
\end{aligned} \tag{4-2}$$

Let $b_{i,k} = \lim_{t\to\infty} P\{s(t)= i, b(t)= k\}$, $i \in (0,m)$, $k \in (0,W_i - 1)$ be the stationary distribution of the Markov chain. By using the normalization condition for a stationary distribution, we have

$$1 = b_{-1,0} + \sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} b_{i,k} \tag{4-3}$$

Based on the chain regularities, we can obtain $b_{0,0}$ in (4-4). The stationary probability τ_1 that a covered station will transmit in a randomly chosen time slot and collide with the frame transmitted by the source, can be represented as

$$b_{0,0} = \frac{2q(1-p)(1-2p)}{2(1-p)(1-2p)+q(1-2p)(1-p^{m+1})+qW_0(1-P)[1-(2P)^{m+1}]} \tag{4-4}$$

$$\tau_1 = \sum_{i=0}^{m} b_{i,0} = \frac{1-p^{m+1}}{1-p} \cdot b_{0,0} \tag{4-5}.$$

The stationary probability τ_2 that a hidden station will transmit during the vulnerable period and collide with the frame transmitted by the source, can be represented as

$$\tau_2 = \sum_{i=0}^{m}\sum_{k=0}^{V} b_{i,k} = \tag{4-6}$$

$$= \begin{cases} \left[(V+1)\cdot\left(\frac{1-p^{m+1}}{1-p}\right) - \left(\frac{V(V+1)}{2W_0}\right)\cdot\left(\frac{1-(\frac{p}{2})^{m+1}}{1-(\frac{p}{2})}\right)\right]\cdot b_{0,0} & ,V<W_0 \\ \left[\frac{1}{2}\cdot\left(\frac{1-p^X}{1-p}\right) + \frac{W_0}{2}\cdot\left(\frac{1-(2p)^X}{1-(2p)}\right) + (V+1)\cdot\left(\frac{p^X-p^{m+1}}{1-p}\right) - \left(\frac{V(V+1)}{2W_0}\right)\cdot\left(\frac{\left(\frac{p}{2}\right)^X - \left(\frac{p}{2}\right)^{m+1}}{1-\left(\frac{p}{2}\right)}\right)\right]\cdot b_{0,0} & ,W_{X-1}<V<W_X \\ & ,1\le X\le m \\ 1 & ,V>W_m \end{cases}$$

where V is the vulnerable period length in the units of backoff slots. X is the minimum backoff stage at which the contention window size is greater than V. For example, if $W_1 < V \le W_2$, then use $X = 2$ in (4-6). As already noted, τ_1 is a special case of τ_2 because τ_1 can be considered as the vulnerable period with the duration of one slot time. Using $V = 0$ and $X = 0$ in first case of (4-6) can verify this.

In the stationary state, the collision probability p is the probability that at least one covered station transmits in the same backoff slot as the source, or at least one hidden station transmits in the vulnerable period. Thus, P can be expressed as

$$p=1-(1-\tau_1)^{n_C-1}(1-\tau_2)^{n_H} \tag{4-7}$$

where n_C is number of the covered stations that includes the transmitting station itself, and n_H is the number of the hidden stations. The total number of contending stations, n, equals $n = n_C + n_H$. We solve the nonlinear set of equations (4-4) – (4-7) using a numerical iteration method to obtain τ_1 and τ_2.

4.2 Throughput Analysis

Let P_{tr} be the probability that there is at least one transmission in the considered slot time, that is

$$P_{tr} = 1-(1-\tau_1)^n \tag{4-8}.$$

The probability of a successful transmission, P_s, is the probability that exactly one station transmits on the channel, conditioned on having at least one station transmit. This probability can also be viewed as the probability of having one of n backlogged stations transmit and none of the covered stations transmit in the same time slot, as well as having none of the hidden stations transmit in the vulnerable period. Then, the probability of a successful transmission is

$$P_S = \frac{n\tau_1(1-\tau_1)^{n_C-1}(1-\tau_2)^{n_H}}{P_{tr}} \tag{4-9}.$$

The normalized system throughput S can be represented as

$$S = \frac{P_S P_{tr} E[P]}{(1-P_{tr})\sigma + P_S P_{tr} T_S + (1-P_S) P_{tr} T_C} \tag{4-10}$$

where the $E[P]$ is the average packet length and σ is the duration of an empty backoff slot. The T_S and T_C are the average times the channel is sensed busy because of a successful transmission or a collision, respectively. They are different in the Basic and RTS/CTS access methods

$$\begin{aligned} T_S^{bas} &= H + E[P] + \delta + SIFS + ACK + \delta + DIFS \\ T_C^{bas} &= H + E[P] + \delta + ACK\_Timeout \end{aligned} \tag{4-11}$$

where $H = PHY\_Header + MAC\_Header$. The δ is the propagation delay. The $ACK\_Timeout = SIFS + ACK + DIFS$. For RTS/CTS access method, the T_S and T_C can be expressed as

$$\begin{aligned} T_S^{rts} &= RTS + \delta + SIFS + CTS + \delta + SIFS \\ &\quad + H + E[P] + \delta + SIFS + ACK + \delta + DIFS \\ T_C^{rts} &= RTS + \delta + CTS\_Timeout \end{aligned} \tag{4-12}$$

where $CTS\_Timeout = SIFS + CTS + (2 \times \sigma)$.

4.3 Simulation Setup

In order to validate our analytical model, we compare its results with simulation results obtained using the simulation tool ns-2 [15]. All the parameters used in analytical model and simulation tool are summarized in Table 4.1. The following assumptions are used in our ns-2 simulation: (a) the access point and all stations have a same transmission range, (b)

the carrier-sensing range equals to the transmission range, and (c) all antennas are omni-directional, so the transmission and carrier-sensing ranges are circular.

Table 4.1: System parameters used in simulation

MAC header	224 bits
PHY header	192 bits
RTS	160 bits + PHY header
CTS	112 bits + PHY header
ACK	112 bits + PHY header
DIFS	50 μs
SIFS	10 μs
Slot Time (σ)	20 μs
Propagation Delay (δ)	1μs
W_0	32
W_{max}	1024

Both ring and random topologies are used in our ns-2 simulation.

(I) *Ring topology*: This topology is used to focus on the hidden station effect and reduce the capture effect. It is composed of one access point located in the center of a ring and several stations uniformly distributed on the ring. There are several benefits of using the ring topology. First, the capture effect can be ignored because of equal distance from the access point to all stations. Second, this topology is symmetric relative to the access point in the center. Hence, the average individual throughput on all stations is the same. Another benefit is that we can easily control the number of hidden stations by varying the ring radius. The number of hidden and covered stations is defined from each station's viewpoint. The transmission range and carrier sensing ranges are set at 250 meters. In this study, we vary the ring radius, denoted as R, to obtain different number of hidden stations in the 8-station network: (a) R = 120 meters—each station can sense all the packets from the other 7 stations, so there are no hidden stations and there are 7 covered stations; (b) R = 130

meters—only 1 station is hidden and the other 6 are covered; (c) R = 155 meters—3 hidden stations and 7 covered stations; (d) R = 180 meters—5 hidden stations and 2 covered ones.

(II) ***Random topology*****:** In general, the mobile stations are randomly distributed in a real wireless network so that the individual station-to-center distance and the number of hidden stations for each mobile station are not equal across the competing stations. In this dissertation, we only study the average number of hidden stations and aggregate network throughput. In our simulation of the random topology, we randomly deploy mobile stations around one access point for 20 experiments to obtain the average number of the hidden station as shown in Table 4.2 and the aggregate network throughput as shown in the next section.

Table 4.2: Average number of the hidden station over twenty experiments.

No. of mobile stations	Theoretical average no. of hidden stations	Average no. of hidden stations in ns-2 and our analytical model
2	0.41	0.45
4	1.23	1.25
8	2.87	2.90
16	6.15	6.20

4.4 Simulation Results and Discussion

First, we consider the hidden station effect on the network throughput as the network is reconfigured from the non-saturation to the saturation condition in both the ring and random topologies. The data payload is set as 250 Bytes. As the offered load increases, the throughput, as shown in Figures 4.2 – 4.5, can be divided into three conditions: non-saturation, transition and saturation conditions.

(I) ***Non-saturation Condition*****:** This region is from the zero load until the load for which the peak throughput is achieved. Initially, as the offered load increases the throughput equals to the offered load and so it increases linearly before reaching its maximum value. In this condition, the average interval between two consecutive transmissions of a station is very long, because the offered load is fairly low. Almost all the packets can be transmitted successfully within the retransmission limit without delaying the next packet. In the presence of hidden stations, the throughput curve remains the same, but the peak value is reached sooner, at a lower offered load. The greater the number of hidden stations, the sooner the peak throughput will be reached. Comparing the peak throughput between two access methods, the RTS/CTS access method (Figures 4.3 and 4.5) outperforms the Basic access method (Figures 4.2 and 4.4) in presence of the same number of the hidden station and this difference of the peak throughput between two access methods is getting large as the number of hidden stations increases. On the other hand, if there are no hidden stations, the peak throughout of the Basic access method is higher than that of the RTS/CTS access method, because of the overhead imposed by the RTS and CTS dialogue. In this non-saturation region, the throughput calculated by our analytical model matches that obtained by ns-2 very well in both the ring topology (Figures 4.2 and 4.3) and random topology (Figures 4.4 and 4.5).

(II) ***Transition Condition*****:** This region is from the load at which the peak throughput is achieved until the load for which the throughput reaches the steady state. As the offered load increases, the throughput decreases from its maximum value to a steady state one. Comparing the throughput obtained by our analytical model and ns-2 simulation in this

transition condition, our analytical model overestimates the peak throughput especially for the Basic access method in the presence of hidden stations. The difference of the peak throughput between our analytical model and ns-2 simulation is about 3%, 10%, 20% and 35% in the ring topology network of 0, 1, 3 and 5 hidden stations, respectively (Figure 4.2). This deviation between the throughput of out analytical model and ns-2 simulation is similar in the random topology network (Figure 4.3). This is caused by a numerical error between the exact and approximate solution to (4-4)–(4-7). This set of equations represents a nonlinear system in the three unknown p, τ_1 and τ_2, which can be solved only by numerical method such as numerical iteration method. In this transition region, the amplitude of the overshoot increases as the number of hidden station increases. The overshoot is defined as the difference between the peak value (maximum throughput) and the steady value (saturation throughput) and it can be represented as the percentage of the steady value. In the Basic access method, the overshoot is about 0%, 35%, 60% and 75% in the ring topology network with 0, 1, 3 and 5 hidden stations, respectively (Figure 4.2). On the other hand, the overshoot is about 0%, 5%, 12% and 20% in the same scenarios by using the RTS/CTS access method in our analytical model (Figure 4.3). Compared to ns-2 simulation, our model slightly overestimates the throughput in this region for the Basic access method. When comparing this transition phenomenon in both access methods, the Basic access method (Figures 4.2 and 4.4) is more sensitive to the hidden station effect than the RTS/CTS access method (Figures 4.2 and 4.4). The overshoot in RTS/CTS access method is much smaller than that in the Basic access method except in the scenario of with hidden stations.

(III) ***Saturation Condition*****:** The throughput remains at a steady-state value even as the offered load keeps increasing. The throughput calculated by our analytical model also matches that obtained by ns-2 simulation very well in this condition. As the number of the hidden station increases, the saturated throughput decreases in all scenarios. In the Basic access method, the saturated throughput decreases about 50%, 75% and 86% in the ring-topology case with 1, 3 and 5 hidden stations, respectively (Figure 4.2). In this saturation region, the RTS/CTS access method also outperforms the Basic access method in all scenarios except for the case with no hidden stations. In the scenario with no hidden stations, the saturated throughput in the Basic access method is higher than that in RTS/CTS access method about 27%. In contrast, the saturated throughput in RTS/CTS access method is higher than that in the Basic access method about 30%, 120% and 240% in the ring-topology case with 1, 3 and 5 hidden station, respectively (Figures 4.2 and 4.3). In the random topology, the average saturated throughput of the RTS/CTS access method is higher than that of the Basic access method if the number of mobile stations is more than 1 (Figures 4.4 and 4.5).

Based on our study of the performance of the wireless network with an access point, the RTS/CTS access method outperforms the Basic access method in most scenarios except the scenario with no hidden stations even when using a short data payload of 250 bytes. Our recommendation is to use the RTS/CTS access method instead of the Basic access method in this environment. However, this result is quite different from the setup in most wireless devices that choose the Basic access method as the default method. In general, a wireless networking device running the 802.11 protocol will choose the RTS/CTS access

method if the data frame size is longer than the RTS/CTS threshold. This adjustable threshold ranges between 0 to 2347 octets in most wireless devices and most vendors turn off the RTS/CTS access method or set a very high RTS/CTS threshold, 1500 octets or a higher value [16]. If we adopt the RTS/CTS threshold setup as is used in most 802.11 wireless devices, a station should choose the Basic access method to transmit short frames, such as 250-byte frames used in our simulations. However, our findings show that the RTS/CTS access method is a better choice in this situation.

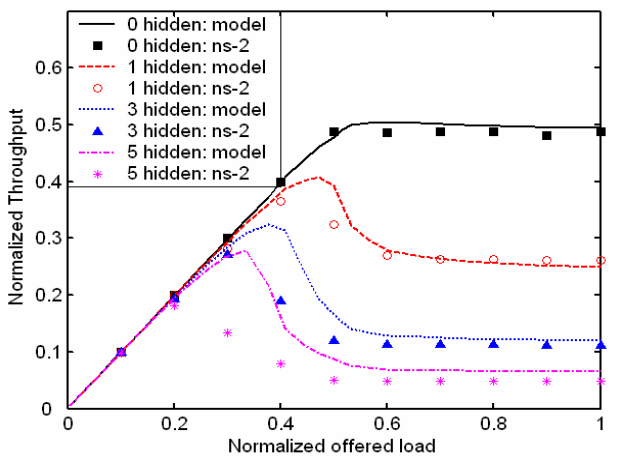
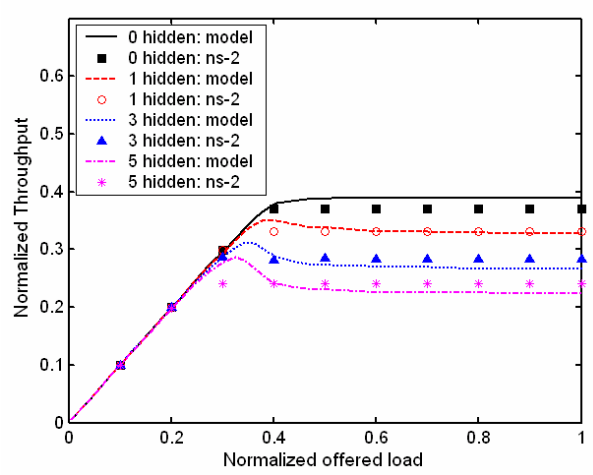


Figure 4.2: Throughput of the ring topology network with 8 stations: Basic access method.



Fgure 4.3: Throughput of the ring topology network with 8 stations: RTS/CTS access method.

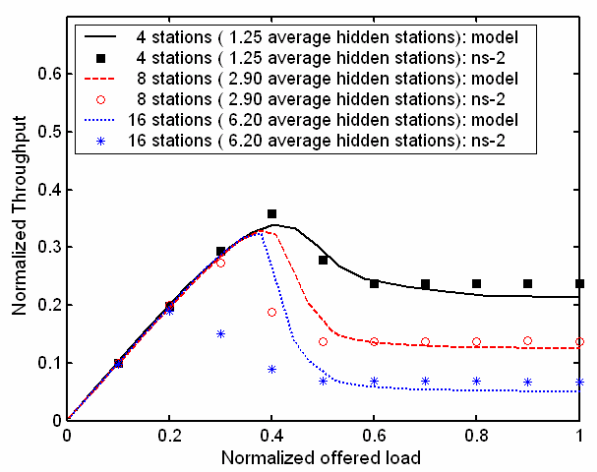


Figure 4.4: Throughput of the random topology network: Basic access method.

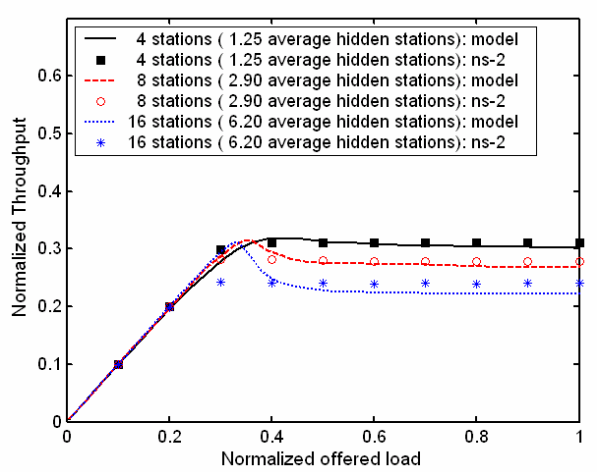


Figure 4.5: Throughput of the random topology network: RTS/CTS access method.

In next section, we further study the hidden station effect on the performance of the 802.11 DCF in a saturation condition by adjusting parameters such as data length, the number of mobile stations and contention window size. We set the initial value of these parameters as follows: (i) the data payload is 500 Bytes; (ii) the number of mobile stations in the ring topology is 32; (iii) the size of the initial contention window W_0 is 32. The throughput of our analytical model is very close to the simulation results obtained by ns-2 in both the Basic and RTS/CTS access method. Our study can be summarized as follows:

(a) The throughput highly depends on the number of hidden stations, rather than the total number of stations in the network. The throughputs are almost horizontal lines regardless of the total number of stations increasing in the network except for the throughput in the scenario with no hidden stations (Figures 4.6 and 4.7). In the Basic access method, the throughput decreases about 50% because of just one hidden station and loses about 80% and 90% of throughput in the presence of 3 and 5 hidden stations, respectively. A hidden station can significantly decrease the throughput because the collision probability between the source and a hidden station is much higher than that between the source and a covered station. Compared to the Basic access method, the RTS/CTS access method only loses about 10%, 20% and 30% throughput in the presence of 1, 3 and 5 hidden stations, respectively. The RTS/CTS access method is more robust to the hidden-station effect in this scenario. The RTS/CTS access method outperforms the Basic access method because it decreases the collision probability between the source and hidden stations by reducing the vulnerable period (relative to a hidden station) from the length of a DATA frame to the length of a RTS frame and a SIFS time (Figure 3.4).

(b) As the length of the data frame increases, the throughput in the RTS/CTS access method also increases; however, the throughput in the Basic access method does not always increase. This result is based on a MAC layer viewpoint because we do not consider the presence of channel errors in this study. In the Basic access method with no hidden stations (Figure 4.8), the throughput increases monotonically. With hidden stations, the throughput reaches a maximum value and then gradually decreases to zero as the payload size increases. The maximum throughput is also reached sooner as the number of hidden stations increases. These throughput curves in the Basic access method (Figure 4.8) represent a tradeoff between the packet collision probability and bandwidth efficiency. On one hand, transmitting a longer data frame means that the source has a longer vulnerable period to hidden stations in the Basic access method because the vulnerable period between the source and a hidden station equals the length of a data frame (Figure 3.3). If the packet arrival rate on each station is constant regardless of non-saturation or saturation condition, then transmitting a longer data frame by the source will cause a higher packet collision probability between the source and a hidden station, which reduces the throughput. On the other hand, transmitting a shorter data frame means using a higher percentage of time to transmit the overhead, and this reduces the throughput. In the RTS/CTS access method, the vulnerable period is fixed to the sum of a RTS frame and a SIFS time (Figure 3.4). The vulnerable period and the packet collision probability are independent of the data-frame size. Increasing the data frame size in RTS/CTS access method reduces the fraction of channel resource wasted on transmitting the overhead, without increasing the packet collision probability. Hence, the aggregate throughput increases as the data frame size increases, as shown in Figure 4.9.

(c) As the size of the initial contention window (also called the minimum contention window) increases, the throughput of the Basic access method also increases (Figure 4.10). It is not obvious that the throughput of the RTS/CTS access method changes significantly with the initial contention window size (Figure 4.11). The throughput curves for both access methods represent a tradeoff between the packet collision probability and bandwidth efficiency. On one hand, the use of a longer initial contention window implies that a station will transmit packets with a lower probability in a unit of time because, on average, it will wait a longer backoff period before transmitting a packet. This will decrease the packet collision probability between the source and hidden stations, which in turn will increase the throughput because of a decreased transmission probability within a vulnerable period. On the other hand, the use of a shorter initial contention window implies that a station will spend shorter period of time, on average, in the backoff procedure. The throughput can be increased by reducing the percentage of the channel resource wasted in the idle state. In the Basic access method, the best initial contention window size for the throughput is in the range from 512 to 1024 slots. Comparing the throughput values between $W_0 = 32$ and $W_0 = 512$ in Figure 4.10, the throughput increases by about 20%, 65%, 220% and 500% in the cases with 0, 1, 3 and 5 hidden stations. In the RTS/CTS access method, the initial contention window size that yields the highest throughput is around 255 slots. Conversely, adjusting the initial contention window does not change significantly the throughput in the RTS/CTS access method.

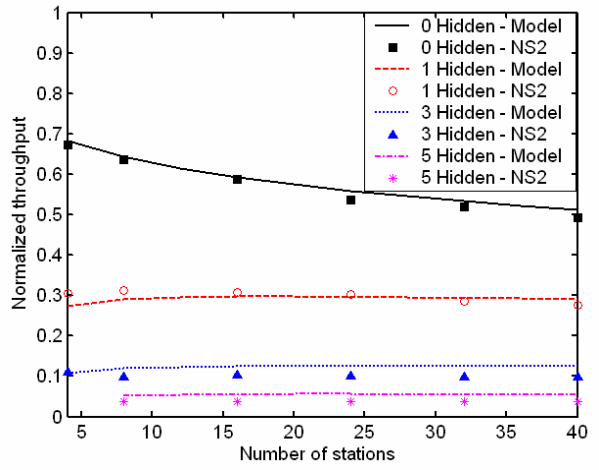


Figure 4.6: Throughput versus number of stations: Basic access method.

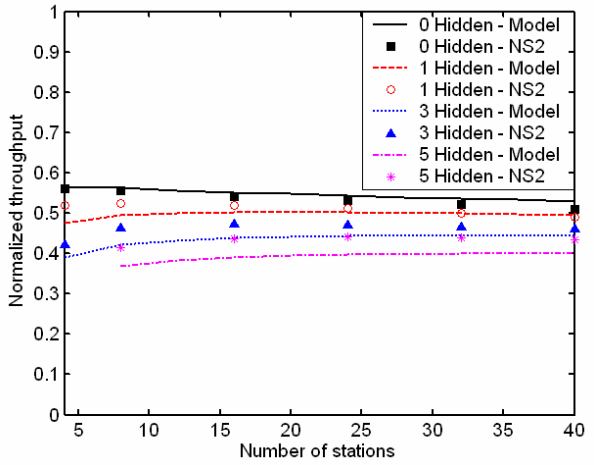


Figure 4.7: Throughput versus number of stations: RTS/CTS access method.

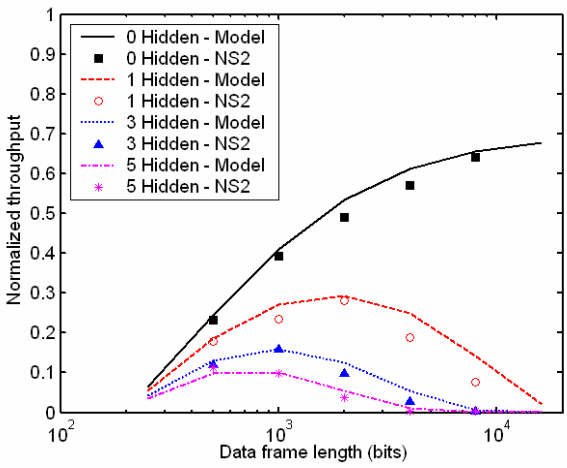


Figure 4.8: Throughput versus data frame length: Basic access method.

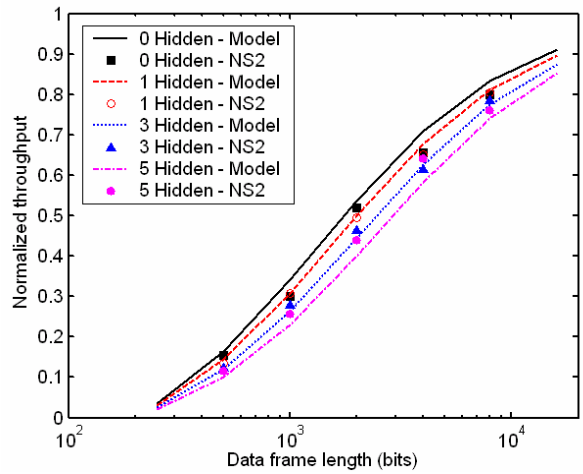


Figure 4.9: Throughput versus data frame length: RTS/CTS access method.

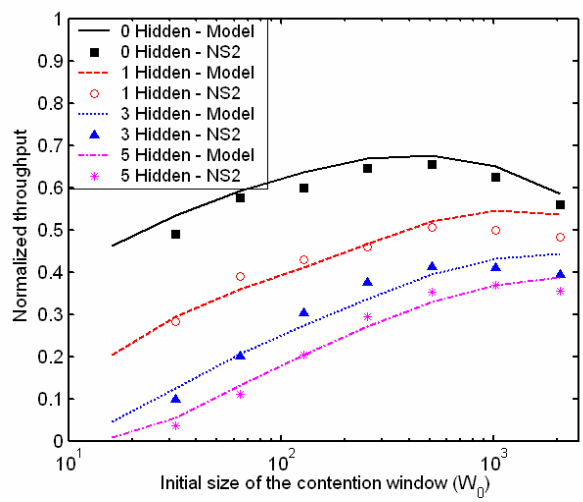


Figure 4.10: Throughput versus initial size of the contention window: Basic access method.

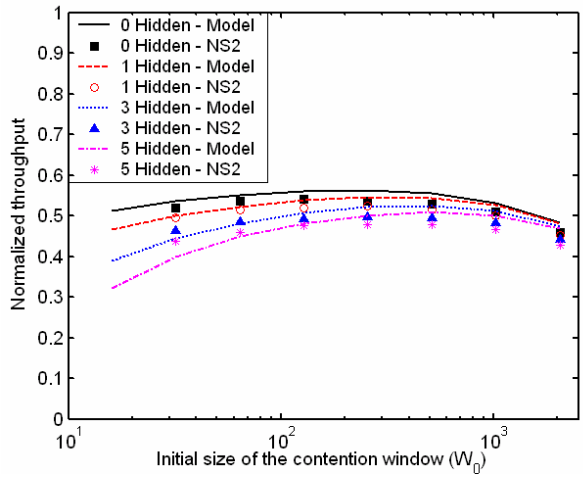


Figure 4.11: Throughput versus initial size of the contention window: RTS/CTS access method.

Chapter 5

The Hidden Station Effect in Wireless Ad Hoc Networks

In a wireless network, the channel state sensed by the sender is not always same as that sensed by the receiver, which results in the exposed and hidden station effects [3]. The hidden stations are those which should suspend their transmission but fail to do so because they cannot hear the sender's transmission. Their transmission can corrupt the sender's packet reception at the receiver. This problem is due to the fact that the PCS threshold is set too high so the sender and hidden stations fail to detect each other's transmission. If the PCS threshold can be adjusted, decreasing this threshold can alleviate the interference from the hidden stations, which will lead to increased aggregate throughput. However, decreasing the PCS threshold will decrease the spatial reuse and might increase the number of exposed stations, which will decrease the aggregate throughput. The exposed stations defer their transmission when they sense sender's transmission, although their transmission would not interfere with the reception of the sender's packet. As the PCS threshold decreases, the aggregate throughput does not decrease or increase monotonically because the throughput is a tradeoff between the interference and spatial reuse.

The topic of setting the optimal carrier-sensing range has attracted several studies. Ye et al. [19] proposed a spatial reuse index that represents the effectiveness of the virtual carrier-sensing based on the sender-receiver distance. They found that the virtual carrier-sensing threshold is optimal when the transmission range equals the interference range. However, the physical carrier-sensing is ignored in their study. According the path

loss model, Zhu et al. [20] derived the optimal PCS threshold that maximizes the aggregate throughput in mesh networks. Their study showed that a network achieves its maximum throughput when the physical carrier-sensing range equals the interference range. This optimal range is based on two assumptions: (a) the interference range is much larger than the transmission range; and (b) background noise is negligible. However, based on the path loss model and SNIR, the assumption (a) is valid only when the sender-receiver distance is close to the transmission range. Also, these two assumptions are mutually inconsistent. When the sender-receiver distance is close to the transmission range, background noise results in the interference range becoming much larger than the transmission range. Yang et al. [21] showed that the MAC layer overhead has a large impact on the choice of PCS threshold. The MAC layer overhead is mainly determined by the data rate and packet size. However, their simulation results showed that the optimal PCS threshold only slightly changes with the packet size. Their results also showed that the optimal PCS threshold is lower than the SINR value by about 2 to 4 dB for the data rates of 18, 36 and 54 Mbps. Their results also imply that the optimal physical carrier-sensing range is larger than the interference range by about 19% to 41% for the data rates of 18, 36 and 54 Mbps. On the other hand, Zhai et al. [22] proposed that different data rates have a similar optimal PCS threshold. They validated their viewpoint by ns-2 simulation in one-hop and multi-hop wireless ad hoc networks, but they did not derive an analytical model. In addition, their optimal PCS threshold is not practical in real networks, because they set the physical carrier-sensing range lower than the transmission range of most data rates. In real wireless networks, for a given data rate, the physical carrier-sensing range is equal to or greater than the transmission range. Lin & Hou [23] proposed a model that balances the interplay of

spatial reuse and spectrum efficiency. Their analytical model showed that there are two or more optimal physical carrier-sensing ranges where the network throughput reaches its peak value. However, they did not validate the multiple-optima phenomenon though simulation results. The work closest to our analysis is that of Ma et al. [24], they developed an analytical model that determines the optimal PCS threshold for a homogenous wireless network with constant link distances. Their results showed that a close-to-optimal value of the carrier-sensing range is equal to the interference range. However, their model results are not consistent with their simulation results which showed that the optimal carrier-sensing range is larger than the interference range by about 20%.

Prior research attempted to evaluate the optimal setting of the PCS threshold in wireless ad hoc networks through spatial analytical models. However, many of their simulation results show that the optimal physical carrier-sensing range that maximizes the aggregate throughput is larger than the interference range by up to 30%. They do not explain why the optimal value occurs in this interval. To answer this question, we introduce the concept of semi-hidden stations as the stations that could corrupt the reception of the receiver's acknowledgement at the sender. These stations sometimes act as exposed stations and at other times act as hidden stations. This effect has not been addressed in the previous work. In this paper, we will show that this effect has a significant influence on the aggregate throughput and the selection of optimal physical carrier-sensing range in wireless ad hoc networks. In addition, we propose a spatiotemporal analysis model to study the effectiveness of the physical carrier-sensing mechanism and derive the optimal physical carrier-sensing range in the presence of regular and semi-hidden stations.

In addition to the spatiotemporal analysis of the effectiveness of the physical carrier-sensing mechanism, it is important to build an analytical model that characterizes the influence of this mechanism on the aggregate throughput of wireless ad hoc networks in the presence of regular and semi-hidden stations. Several models have been proposed to describe the performance of wireless networks. Tobagi et al. [3] first proposed a model to evaluate the hidden station effect and showed that hidden stations seriously degrade the performance of the *p*-persistent CSMA method. Cali et al. [25] derived a theoretical throughput bound by approximating IEEE 802.11 with a *p*-persistent model. The work closest to our analytical model of throughput is Zeng et al. [26], who extended the *p*-persistent model [25] to characterize the impact of physical carrier-sensing on the aggregate throughput. However, the *p*-persistent model is not suitable for modeling the exponential backoff procedure used in IEEE 802.11. Bianchi [7] was the first to derive a model for the saturation throughput of 802.11 that incorporates the exponential backoff mechanism as a two dimensional Markov chain. This essentially models the probability that a station will transmit as the probability that the station's backoff counter will reach zero, given an arbitrary initial value. However, Bianchi's work ignored the hidden station effect. We extended this model to evaluate the hidden station effect on the performance of the 802.11 DCF in access-point-based wireless network [10]. In this work, we modify our earlier two-dimensional Markov chain model [10] to include semi-hidden station effect, and we evaluate the influence of physical carrier-sensing mechanism on the aggregate throughput of wireless ad hoc networks. Based on our model, we answer the question why the optimal value occurs in a specified interval; we also determine the optimal value of carrier-sensing range that is up to 30% greater than the interference range in most situation.

5.1 Interference Model

The radio propagation model used in this paper is the path loss model given by

$$P_r = \frac{P_t}{d_t^n} \tag{5-1}$$

where P_r is the received signal strength at the receiver, P_t is the transmission power at the sender, d_t is the distance between the sender and the receiver, and n is the path loss exponent that typically ranges from 2 to 6, depending on the propagation environment. For example, n is equal to 2 in free space and 6 in building between different floors [27]. We assume all stations use a same transmission power P_t. Based on this model and 802.11 protocol, we can define three ranges: transmission range (R_t), carrier-sensing range (R_c) and interference range (R_i) as follows.

(a) Transmission range (R_t) is the maximum distance between a sender and a receiver that the receiver can correctly decode frames from the sender in the presence of noise but no interference. The correct decoding in case of IEEE 802.11b direct sequence spread spectrum (DSSS) means the frame error rate (FER) must be lower than 8×10^{-2} for MAC-layer packets of 1024 bytes if the signal to noise ratio (SNR) at the receiver is higher than a threshold $S_0 = -80$ dBm [1], hence, we have the relationship

$$SNR(d_t = R_t) = S_0 = \frac{P_r(d_t = R_t)}{N} = \frac{P_t / R_t^n}{N} \tag{5-2}$$

where N is the noise power.

(b) Physical carrier-sensing range (R_c) is the maximum distance between a sender and a receiver that the receiver can sense the signal transmitted from the sender but may not be able to correctly decode frames. Based on the clear channel assessment (CCA) of the 802.11 protocol, a station shall report the channel state as busy, if it senses the energy above the energy detection (ED) threshold (≤ –80 dBm for 802.11b DSSS [1]).

(c) Interference range (R_i) is the maximum distance between a second sender (interfering source) and a receiver at which the signal transmitted from the second sender can interfere with the frame reception on the receiver and cause the FER to be higher than the requirement. At this distance, the Signal to Interference and Noise Ratio (SINR) is equal to S_0 and is given by

$$SINR(d_i = R_i) = S_0 = \frac{P_r}{P_i(d_i = R_i) + N} = \frac{(P_t / d_t^n)}{(P_t / R_i^n) + N} \tag{5-3}$$

where P_i is the received interference strength at the receiver, d_i is the distance between the second sender and the receiver. Based on (5-3), the interference range can be represented as [24]

$$R_i = R_t \cdot \left(\frac{S_0}{(R_t / d_t)^n - 1} \right)^{\frac{1}{n}} \tag{5-4}.$$

This range is not fixed and depends on the sender-receiver distance. However, if we ignore the noise power ($N = 0$), then the equation (5-3) can be simplified as Signal to Interference Ratio (SIR)

$$SIR(d_i = R_i) = S_0 = \frac{P_r}{P_i(d_i = R_i)} = \frac{(P_t / d_t^n)}{(P_t / R_i^n)} = \frac{R_i^n}{d_t^n} \tag{5-5}.$$

Based on (5-5), we can have a simplified interference range as:

$$R_i = d_t \cdot (S_0)^{\frac{1}{n}} \tag{5-6}.$$

We use an example to highlight the difference between the models in equations (5-4) and (5-6). Let X_i denote the ratio of the interference range to the sender-receiver distance, that is

$$X_i = \frac{R_i}{d_t} \tag{5-7}.$$

We set the S_0 as 6 dB, the path loss exponent as 4, and the R_t as 1 m. In the situation of no noise, the R_i increases linearly as the d_t increases (dashed line in Figure 5.1), and the ratio X_i keeps a constant as S_0^(1/n) (dashed line in Figure 5.2). On the other hand, if consider the noise power, the R_i increases linearly only when the d_t is less than 0.6 R_t. After the d_t exceeds the 0.6 R_t, the R_i grows quickly and nonlinearly, and its value approaches to infinity when the d_t equals to the R_t (solid line in Figure 5.1). The ratio X_i in this situation is not a constant as previous one and increases rapidly as the d_t approaching to the R_t (solid line in Figure 5.2). So, the simplified interference range model does not represent well the real situation (with noise) when the d_t is near the R_t.

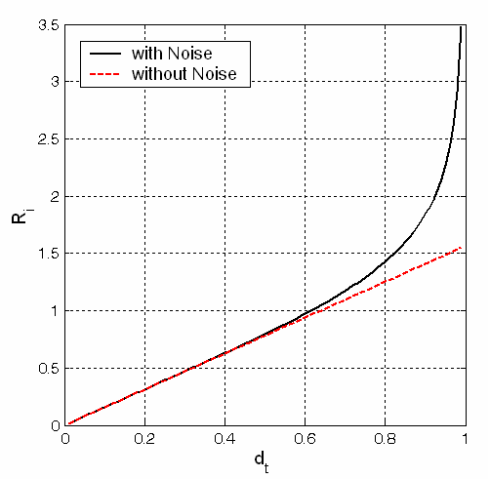


Figure 5.1: The interference range as a function of the sender-receiver distance.

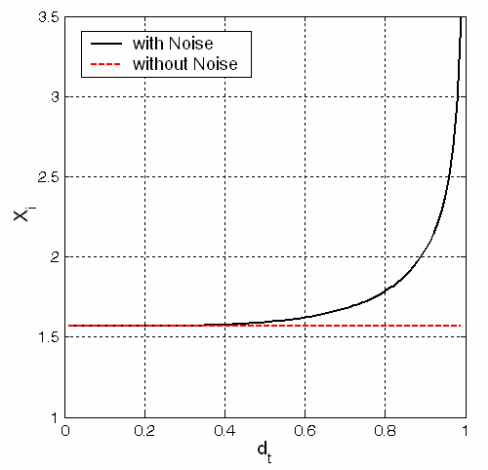


Figure 5.2: The ratio X_i as a function of the sender-receiver distance.

IEEE 802.11 standard defines multiple data rates to support reliable transmission on channels of different quality. In general, a higher data rate requires higher receiver sensitivity and higher SINR to keep the same bit-error-rate (BER) as a lower data rate. Based on the propagation model of (5-1), if a station uses a fixed transmit power for all data rates, than a higher data rate is limited to a shorter transmission range because of requiring higher receiver sensitivity. In order to maximize the throughput, the multi-rate mechanism will use the highest rate among the available rates based on the channel quality between the sender and receiver. For example, according to the receiver sensitivity in Table 5-1, if the received signal is –80dBm, then the 9 Mbps and 6 Mbps rates are available and the 9 Mbps will be selected as the transmission rate. Following this mechanism, the 9 Mbps is used only when the received signal power is between –79 to –81 dBm that is near its receiver sensitivity –81 dBm. This means that each rate will be used near its transmission limit except for the highest rate.

Table 5.1: SINR and receiver sensitivity for standard data rates of IEEE 802.11g [32]. Rt (the rightmost column) was calculated based on (5-1).

Rates (Mbps)	Receiver Sensitivity (dBm)	SINR (dB)	Transmission Range R_t (m)
54	–65	24.56	0.38
48	–66	24.05	0.40
36	–70	18.80	0.50
24	–74	17.04	0.63
18	–77	10.79	0.75
12	–79	9.03	0.84
9	–81	7.78	0.94
6	–82	6.02	1.00

How does the multi-rate mechanism affect the interference range? We set the transmission range of the 6 Mbps rate as 1 meter and calculate the transmission ranges of the other data rates in Table 5-1. According to equations (5-4), (5-6), (5-7) and SINR values in Table 5-1, the interference range and the ratio X_i in the multi-rate mechanism are shown in Figures 5.3 and 5.4. The curves in both figures are discontinuous where the multi-rate mechanism switches the data rate. If we ignore the noise power, as the sender-receiver distance increases, the interference range also linearly increases except for the jumping points (dashed line in Figure 5.3), On the other hand, if we consider the noise power, the interference range increases rapidly as the sender-receiver distance approaches the transmission limit and it jumps down suddenly after switching to a lower data rate (solid line in Figure 5.3). Based on the result in Figure 5.3, the interference range is larger than the transmission range when the sender-receiver distance is larger than 0.2 m regardless of whether we are considering noise power. This means that the interference range is always larger than the transmission range except for the highest data rate of the multi-rate mechanism. According to the result in Figure 5.4, when noise is considered, the ratio X_i is greater than 2.2. This implies that in most scenarios of the multi-rate mechanism, the interference range is more than double the size of the transmission range. In this section, we show that both the Basic and RTS/CTS access methods are ineffective in suppressing most of the interference in wireless ad hoc networks, because the interference range is much larger than the transmission range in most scenarios. Therefore, in the next section we will study the effectiveness of both access methods using a spatiotemporal model.

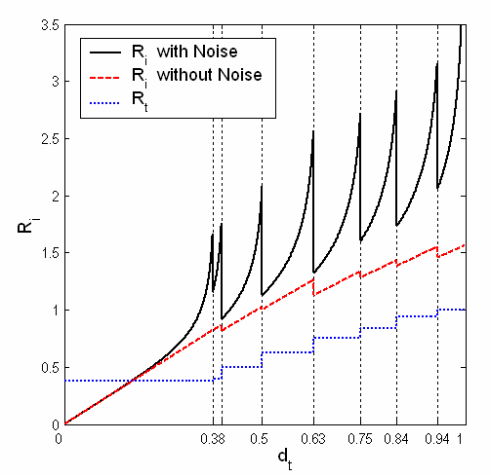


Figure 5.3: The interference range in the 802.11g multi-rate mechanism as a function of the sender-receiver distance.

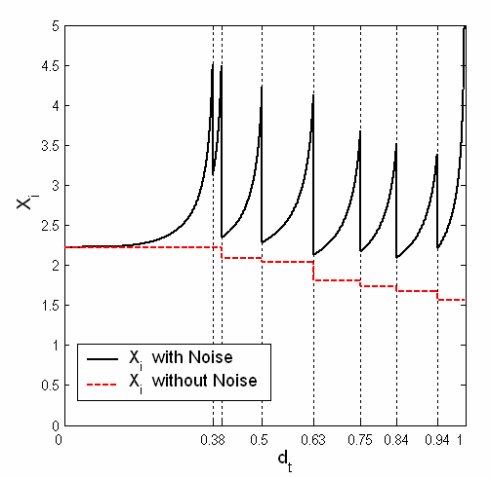


Figure 5.4: The ratio X_i in the 802.11g multi-rate mechanism as a function of the sender-receiver distance.

5.2 Spatiotemporal Analysis of the Basic and RTS/CTS Access Method

DCF provides the physical carrier-sensing mechanism as a fundamental scheme and the virtual carrier-sensing mechanism as an optional one. The former is used in the Basic access method, and the later is used in the RTS/CTS method. In this section, we compare the effectiveness of these two carrier-sensing mechanisms in alleviating the packet collisions resulting from the interference in wireless ad hoc networks.

We first analyze the effectiveness of the Basic vs. RTS/CTS access methods from the spatial viewpoint. Because the interference range is not a fixed distance and is a function of the sender-receiver distance, we classify all scenarios into three spatial configurations based on the size of the interference range as follows. The following assumptions are used in our analysis: (i) the transmission range, carrier-sensing range and interference range are all circular in shape; (ii) the channel between any two stations is identical; (iii) the transmit power of all stations is identical; and, (iv) the physical carrier-sensing range is adjustable and can be much larger than the transmission range.

Configuration 1: $R_i < (R_t - d_t)$

When the sender-receiver distance plus the interference range is smaller than the transmission range, the whole interference range of the receiver is within the transmission range of the sender (Figure 5.5(a)), the sender-receiver distance is given by

$$0 \le d_t < R_t/(1+X_i) \qquad (5\text{-}8).$$

For example, setting the SINR as 6.02 dB, the interval of the sender-receiver distance in Configuration 1 is

$$0 \le d_t < 0.38R_t \qquad (5\text{-}9).$$

There is no hidden station to the sender in this situation because all potential hidden stations can decode the transmitted packet from the sender. The stations outside the interference range but inside the transmission range are the exposed stations. The Basic access method in this configuration is completely effective with respect to the interference. Obviously, the RTS/CTS method is redundant in this configuration because it covers the same interference range as the Basic method but more area of the exposed stations.

Configuration 2: $(R_t - d_t) \le R_i < R_t$

When the interference range is larger than in Configuration 1 but smaller than the transmission range (Figure 5.5(b)), the sender-receiver distance is given by

$$R_t/(1+X_i) \le d < R_t/X_i \qquad (5\text{-}10).$$

If the SINR is set as 6.02 dB, the interval of the sender-receiver distance in Configuration 2 is

$$0.38R_t \le d_t < 0.62R_t \qquad (5\text{-}11).$$

The sender's transmission range covers only part of the interference area, but the receiver's transmission range still covers the whole interference area. The hidden station area increases in the Basic access method as the transmitter-receiver distance grows. However, the RTS/CTS method provides the complete coverage of the interference area through broadcasting of the RTS frame, but it covers slightly larger exposed-station area than the

Basic method. In Configuration 2, the RTS/CTS access method is more effective than the Basic access method.

Configuration 3: $R_i > R_t$

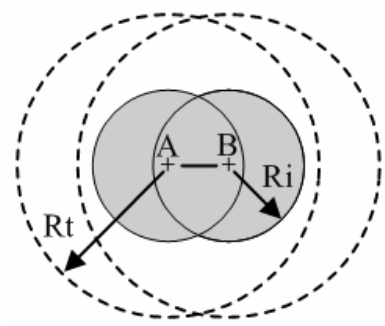
When the interference range is larger than the transmission range (Figure 5.5(c)), the sender-receiver distance is given by

$$R_t / X_i \le d \le R_t \qquad \text{(5-12).}$$

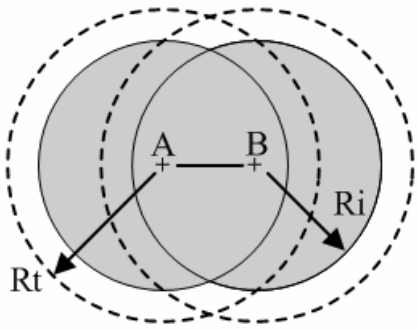
If the SINR is 6.02 dB, the interval of the sender-receiver distance in Configuration 3 is

$$0.62R_t \le d_t < R_t \qquad \text{(5-13).}$$

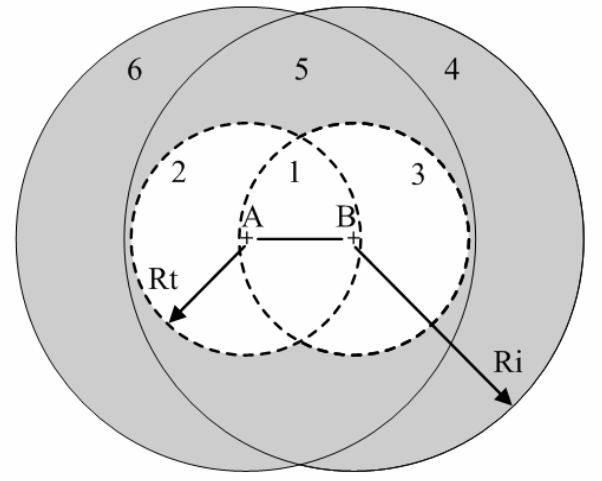
In this configuration, both the transmission ranges of the sender and receiver cover only part of the interference range. Both access methods provide low spatial coverage of the interference range, though the RTS/CTS access method covers more interference range than the Basic access method. Unfortunately, this configuration is the most common situation in wireless ad hoc networks. Based on our study, from Figures 5.3 and 5.4, we can see that this configuration appears almost always, except for part of the scenario where the stations use the highest transmission rate, which is very rare. Therefore, we limit our further study the effectiveness of the Basic and RTS/CTS access methods to Configuration 3.



(a) Configuration 1



(b) Configuration 2



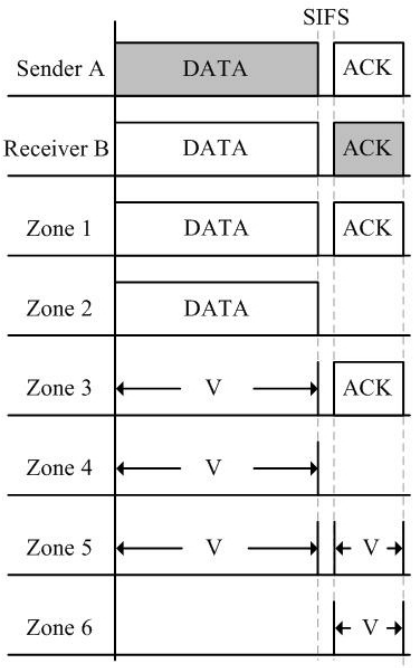
(c) Configuration 3

Fig 5.5: Spatial analysis for the Basic and RTS/CTS access methods (shaded areas represent the interference ranges). Also labeled in (c) are the zones that will be used in the temporal analysis in Figure 5.6.

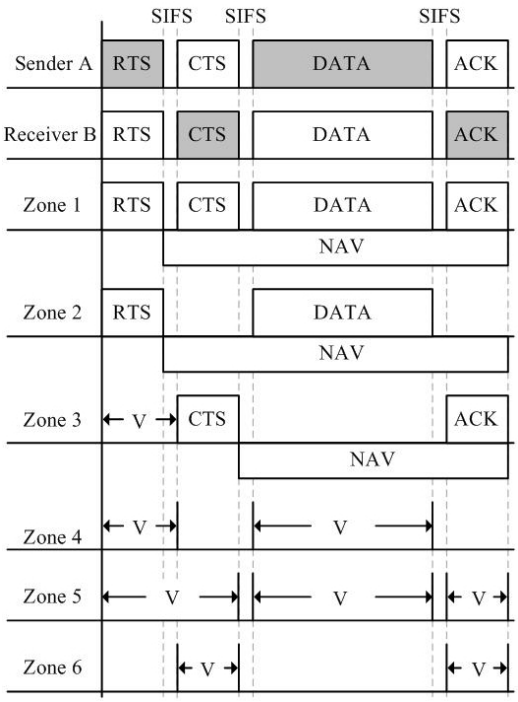
Next, we study the effectiveness of the Basic vs. RTS/CTS access methods from a temporal viewpoint, but only limited to Configuration 3 (Figure 5.5(c)). In the Basic access method (Figure 5.6(a)), when the sender A transmits a data frame to the receiver B, the stations inside zones 1 and 2 can decode this frame and suspend their transmission until they sense the channel is idle again. However, the stations inside zones 3, 4 and 5 are hidden stations to the sender A because they are inside the interference range of receiver B but cannot sense data frame transmitted from sender A. The hidden stations could transmit their packets simultaneously and interfere with the reception of A's data frame on receiver B. The vulnerable period (V) in Figure 5.6 is defined as the period of time when collision is possible between the hidden stations and the sender A or receiver B. If receiver B successfully receives A's data frame, it will reply with an ACK frame to sender A. During this period of time, the stations inside zones 5 and 6 are hidden stations to receiver B and could interfere with sender A's receiving of this ACK frame. If the physical carrier-sensing range is equal to the transmission range, the Basic access method is not effective in alleviating collisions in Configuration 3 because the two-way handshaking mechanism can prevent simultaneous transmissions (interference) only from zones 1 and 3. Based on the multi-rate mechanism, if the interference range is twice the transmission range, then the area of zones 1 and 3 is less than 25% of the entire interference range area.

On the other hand, the RTS/CTS access method is designed to alleviate the hidden station effect in wireless LANs by a four-way handshaking mechanism (Figure 5.6(b)). When sender A transmits a packet (RTS-CTS-DATA-ACK) to receiver B, the stations inside zones 1 and 2 can decode this packet and suspend their transmission by each updating their

network allocation vector (NAV) for the duration of this transmission. During the period of transmitting RTS frame, the stations in zone 3 are potential hidden stations with respect to sender A until they receive the CTS frame and then freeze their transmission. So, the vulnerable period with respect to the stations in zone 3 is the length of an RTS frame and a SIFS time. Comparing the vulnerable period in both access methods, the RTS/CTS access method reduces the vulnerable period relative to the stations in zone 3, from the length of a data frame to the length of an RTS frame plus a SIFS time. However, the RTS/CTS access method does not suppress simultaneous transmissions by the hidden stations in zones 4, 5 and 6 because they cannot sense a transmission by sender A. The vulnerable period with respect to the stations in zone 4 is the length of an RTS, plus a SIFS time and data frame, which is even longer than the vulnerable period in the Basic access method, which is the length of a data frame. In zones 5 and 6, the situation is similar. Unfortunately, the interference range is more than double the size of the transmission range in Configuration 3 (Figure 5.4). The effectiveness of the RTS/CTS access method is also low in Configuration 3.



V = Vulnerable period, (a) Basic access method.



V = Vulnerable period, (b) RTS/CTS access method.

Figure 5.6: Temporal analysis for the Basic and RTS/CTS access methods in Configuration 3, assuming that Rcs = Ri. Zones are labeled in Figure 5.5(c).

According to our spatiotemporal study of the Basic and RTS/CTS access methods, neither method is effective in Configuration 3, which is the most frequent scenario in wireless ad hoc networks. It appears that the IEEE 802.11 DCF is not designed for wireless ad hoc networks. However, the effectiveness of the Basic access method can be improved by increasing the physical carrier-sensing range because this method relies on the physical carrier-sensing mechanism to initiate or suspend transmission. As for the RTS/CTS access method, the issue is if we can increase the physical carrier-sensing range to improve the effectiveness of the virtual carrier-sensing range. We will study this issue in next section.

5.3 Can Physical Carrier-sensing Improve the Effectiveness of Virtual Carrier-sensing?

In this section, we will explore whether we can improve the effectiveness of the RTS/CTS method in alleviating interference in Configuration 3 by increasing the physical carrier-sensing range. We keep using the notation from Figure 5.5(c) but we enlarge the physical carrier-sensing range up from the transmission range to equal the interference range. From the spatial viewpoint, after sender A and receiver B exchange RTS and CTS frames, all potential hidden stations are covered by either the physical carrier-sensing range of A or that of B, and can sense the transmitted signal that will determine the channel as busy. The RTS/CTS access method seems effective to suspend simultaneous transmissions from hidden stations after the RTS-CTS handshake and reduce the vulnerable period of the hidden station in all zones. Nevertheless, if we study this scenario from a temporal viewpoint (Figure 5.7), the enlarged physical carrier-sensing range does not obviously improve the effectiveness of the virtual carrier-sensing mechanism in this

situation. The Carrier Sensed (CS) period in Figure 5.7 represents the time interval during which the stations can sense the carrier signal but cannot decode the transmitted frame. For example, in zone 4, although the stations can sense the transmitted signal and determine the channel as busy after receiver B replies with the CTS frame, these stations just sense the transmitted signal and cannot decode the CTS frame to for setting their NAV and freezing their transmission. After the end of the CTS frame plus a DIFS time, they will determine the channel state as idle again, and could transmit a data frame that will collide with the frame transmitted by sender A. By comparing the temporal analysis of the RTS/CTS access method in Figure 5.6(b) and Figure 5.7, we can see that the vulnerable period of the stations in zone 4 is not reduced significantly even when the physical carrier-sensing range covers these stations in Figure 5.7. Moreover, this problem also occurs with the stations in zone 6.

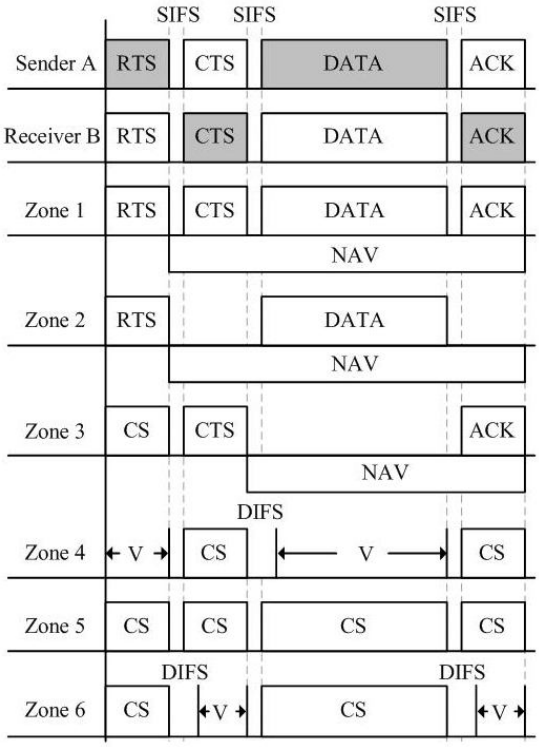
Our spatiotemporal analytical model shows that enlarging the physical carries-sensing range does not improve the effectiveness of the RTS/CTS access method in wireless ad hoc networks. We validate this finding by an ns-2 simulation that compares the hidden station effect of zone 4 across the scenarios in Figure 5.6(b) and Figure 5.7 as follows.

Consider two independent links, AB and CD, in a wireless network (Figure 5.8). Sender A transmits packets only to receiver B and sender C transmits packets only to receiver D. Sender A is a hidden station in zone 4 with respect to link CD, so it is inside the interference range of receiver D but outside of this range for sender C. On the other hand, sender C is a hidden station in zone 4 with respect to link AB. We design three cases:

Case 1: The physical carrier-sensing ranges of both senders cover each other.

Case 2: The physical carrier-sensing range of all stations equals the transmission range and the temporal analysis is same as in Figure 5.6(b).

Case 3: The physical carrier-sensing range is enlarged to equal the interference range and the temporal analysis is same as in Figure 5.7.



CS = Carrier Sensed only (cannot decode the received signal), (b) RTS/CTS access method

Figure 5.7: Temporal analysis for the Configuration 3 assuming that Rcs = Ri.

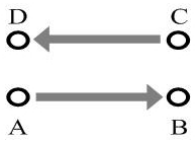


Figure 5.8: Example network to analyze the hidden station effect of zone 4 in Figure 5.6(b) and Figure 5.7.

The result of ns-2 simulation is shown in Table 5.2. In Case 1, two links share a common channel bandwidth and there is no hidden station effect. In Case 2, the results show the hidden station effect on the aggregate throughput. Compared to case 1, the throughput loss in Case 2 is about 50%. In Case 3, we increase the physical carrier-sensing range of all stations so sender C can sense the signal transmitted from receiver B. Of course, sender C still cannot decode the CTS and ACK frames transmitted from receiver B. The throughputs in Case 3 are slightly higher than in Case 2 (by about 7%). This result indicates that in Case 3 the two links still suffer from the hidden station effect. And, enlarging the physical carrier-sensing range does not improve the effectiveness of the RTS/CST access method in preventing the hidden station effect.

Table 5.2: Throughput (bps) of the network in Figure 5.8 using RTS/CTS as achieved by ns-2 simulation averaged over 10 runs.

	Link AB	Link CD
Case 1	1,107,840	1,152,000
Case 2	1,152,480	1,154,400
Case 3	2,344,960	2,353,440

This example shows that the default RTS/CTS access method does not work well in wireless ad hoc networks even when combined with the adjustable physical carrier-sensing range. The reason for this is because the RTS/CTS access method requires that stations can decode the RTS or CTS frame to update their NAV and defer transmission for a predefined period of time (based on information in the RTS or CTS frame). However, the physical carrier-sensing mechanism provides only the channel state, idle or busy, which is not enough for the virtual carrier-sensing mechanism to operate effectively. Therefore, we

focus on the optimal carrier-sensing range for the Basic access method in the rest of this paper.

5.4 Optimal Carrier-sensing Range

If the physical carrier-sensing range is adjustable, what are the reasonable lower and upper bounds of the physical carrier-sensing range in wireless ad hoc networks? And what is the optimal physical carrier-sensing range that achieves a maximum network throughput?

We use the following assumption in this section: the transmissions of all stations are independent, so the hidden and exposed station effects are proportional to the number of the hidden and exposed stations in the network.

A. Lower Bound

If a receiver can correctly decode a frame, then it must be able to sense this frame's transmission. This implies that the physical carrier-sensing range must be larger than or equal to the transmission range, that is

$$R_c \geq R_t \qquad \text{(5-14)}.$$

B. Upper Bound

When the sender-receiver distance is equal to the transmission range, the corresponding interference range reaches its maximum value, defined as R_{i_max}. The largest distance between sender A and any point inside the interference range of receiver B is $R_t + R_{i\_max}$. If the physical carrier-sensing range is equal to this maximum distance, $R_t + R_{i\_max}$, then the

physical carrier-sensing range covers the entire interference range and there are no hidden stations relative to sender A. However, if the physical carrier-sensing range is larger than this maximum distance, then it covers more exposed stations but does not cover more hidden stations (because all hidden stations are already covered at R_{i_max}). There is no advantage to increase the physical carrier-sensing range beyond this maximum distance. So, this maximum distance is a reasonable upper bound for the physical carrier-sensing range, given according to

$$R_c \le R_t + R_{i\_\max} = R_t + R_i(d_t = R_t) \qquad \text{(5-15).}$$

C. Optimal Physical Carrier-sensing Range

Selecting a physical carrier-sensing range that maximizes the network throughput is achieved through a tradeoff between the interference and channel reuse. A larger physical carrier-sensing range could increase the network throughput by reducing the interference from hidden stations but it also could decrease the network throughput by reducing the spatial reuse because of covering more exposed stations. Similarly, a smaller physical carrier-sensing range does not necessarily increase the network throughput. Because the hidden and exposed station effects result in a decrease of network throughput, maximization of network throughput is equivalent to minimization of the number of hidden and exposed stations in the network. However, how do we decide if a station is a hidden or exposed station in a wireless ad hoc network?

Consider the link between sender A and receiver B (Figure 5.9). We define the following three station types based on the coverage of the interference and physical carrier-sensing ranges.

(i) The *covered stations* are inside both the interference range of receiver B and physical carrier-sensing range of sender A as those in zone 5 in Figure 5.9.

(ii) The *hidden stations* are inside the interference range of receiver B but outside the physical carrier-sensing range of sender A as those in zone 4 in Figure 5.9.

(iii) The *exposed stations* are inside the physical carrier-sensing range of sender A but outside the interference range of receiver B, such as those in zones 6 and 7 in Figure 5.9. Previous work considered stations in zone 6 as exposed stations. However, these stations are exposed stations only when sender A is transmitting a frame to receiver B, but they are also hidden (to B) when sender A is receiving the ACK frame. Therefore, we call these stations in zone 6 *semi-hidden stations* or *semi-exposed stations*. A key question is whether their impact on the aggregate throughput is closer to the regular hidden or exposed stations.

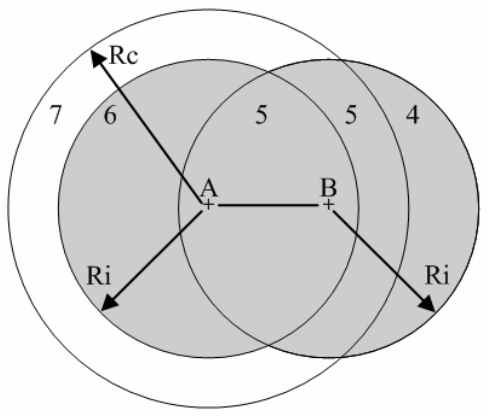


Figure 5.9: Definitions of zones for different types of interfering stations. Unlike Figure 5.5(c), the carrier-sensing range is greater than the interference range.

To answer this question, we use a simple example (Figure 5.10) and ns-2 simulation. Consider two independent links, AB and CD, in a wireless network (Figure 5.10). Sender A transmits packets only to receiver B and sender C transmits packets only to receiver D. Because sender A is inside the interference range of sender C but outside of this range for receiver D, sender A could be a *semi-hidden* or *semi-exposed station* of zone 6 relative to link CD. On the other hand, sender C could be a *semi-hidden* or *semi-exposed station* of zone 6 with respect to link AB. We will determine whether they are *semi-hidden* or *semi-exposed stations* by varying the physical carrier-sensing range and comparing their performance with regular exposed stations. We design four scenarios:

Case 1: Both senders are inside zone 7 of one another, and can sense each other's transmissions.

Case 2: The topology is the same as in Case 1 but senders cannot sense each other's transmissions.

Case 3: Both senders are inside zone 6 of one another, and can sense each other's transmissions.

Case 4: The topology is the same as in Case 3 but they cannot sense each other's transmissions

Figure 5.10: Example network to analyze the semi-hidden station effect of zone 6 in Figure 5.6(b) and Figure 5.7.

The results of an ns-2 simulation are shown in Table 5.3. First, we consider the *exposed station* effect on the aggregate throughput by comparing the result in Cases 1 and 2. In Case 1, the result represents the exposed station effect on the aggregate throughput. Two senders A and C cannot interfere with each other's ACK frame reception, but they share a common channel bandwidth. In Case 2, we reduce the physical carrier-sensing range so two senders cannot sense each other's transmissions. The throughputs in this case are twice higher than in Case 1 because each link uses one independent channel bandwidth.

Table 5.3: Average throughput (bps) of the Basic method under exposed and semi-exposed station effect, obtained by ns-2 simulation.

	Link AB	Link CD
Case 1	2,536,000	2,536,485
Case 2	4,909,280	4,908,860
Case 3	2,526,400	2,495,280
Case 4	1,750,720	1,758,080

Second, we consider the *semi-hidden* or *semi-exposed station* effect on the aggregate throughput by comparing the results in Cases 3 and 4. In Case 3, the result shows that two links share a common channel bandwidth. The scenario and throughput in this case are similar to those of Case 1. In Case 4, we also reduce the physical carrier-sensing range to the point where the two senders cannot sense each other's transmissions. However, they can interfere with each other's reception of the ACK frame. The throughput in Case 4 is lower than in Case 3 by 40%. This result shows that the influence of the stations in zone 6 resembles more the *hidden station* effect than the *exposed station* effect. Although the vulnerable period of senders relative to one another is short (ACK frame length) and the

spatial reuse time relative to one another is long (DATA frame length), the throughput increase from spatial reuse cannot compensate the throughput loss from interference. Therefore, we redefine the stations in zone 6 as *semi-hidden stations* and the hidden stations in zone 4 as (*regular*) *hidden stations*.

In this section, our goal is to select an optimal physical carrier-sensing range that maximizes the network throughput. This goal is equivalent to adjusting the physical carrier-sensing range of the sender to cover fewer *exposed stations* and more *hidden* and *semi-hidden stations*. When the physical carrier-sensing range reaches its optimal value, the total number of the *hidden*, *semi- hidden* and *exposed stations* is at a minimum.

$$\begin{aligned} &\max \textit{Throughput}\, f(R_c) = \min f(R_c) \\ &\text{where } f(R_c) = n_{\text{hidden}} + n_{\text{semi-hidden}} + n_{\text{exposed}} \end{aligned} \tag{5-16}$$

where n_{hidden}, $n_{\text{semi-hidden}}$, and n_{exposed} are the numbers of the *hidden*, *semi-hidden* and *exposed* stations, respectively.

Consider a special case where all stations are distributed uniformly in a wireless network, at a fixed density. Theoretically, the numbers of the *hidden*, *semi-hidden* and *exposed stations* are proportional to shaded areas in Figure 5.9, so the function $f(R_c)$ can be represented as

$$f(R_c) \propto area_{\text{hidden}} + area_{\text{semi-hidden}} + area_{\text{exposed}} \tag{5-17}$$

where the *hidden*, *semi- hidden* and *exposed stations* are located.

As the physical carrier-sensing range increases, the change in the area of *hidden*, *semi-hidden* and *exposed stations* can be classified into three cases (Figure 5.11) described below:

(i) $R_c < (R_i - d_t)$

In this case, as the physical carrier-sensing range increases, only the zone with *hidden stations* gets smaller; the zone with the *exposed stations* remains zero and that with the *semi-hidden stations* is fixed in size because the interference ranges of both the sender and receiver cover the whole physical carrier-sensing range (Figure 5.11(a)). The area of the zone with hidden, semi-hidden and exposed stations can be represented as

$$area_{\text{hidden}} = \pi R_i^2 - \pi R_c^2 \tag{5-18}$$

$$area_{\text{semi-hidden}} = \pi R_i^2 - R_i^2\left[2\theta_1 - \sin(2\theta_1)\right]$$

$$area_{\text{exposed}} = 0$$

where $\theta_1 = \cos^{-1}(d_t / 2R_i)$ and d_t is the distance between the sender and the receiver as given in (5-1).

(ii) $(R_i - d_t) < R_c < R_i$

In this case, as the physical carrier-sensing range increases, both zones with *hidden* and *semi-hidden stations* get smaller, but the zone with *exposed stations* still remains zero because the interference range of the sender still covers the whole physical carrier-sensing range (Figure 5.11(b)). The area of the zone with *hidden*, *semi-hidden* and *exposed stations* can be represented as

$$area_{\text{hidden}} = \pi R_i^2 - \tfrac{1}{2} R_i^2 \left[2\theta_3 - \sin(2\theta_3)\right] - \tfrac{1}{2} R_c^2 \cdot \sin(2\pi - 2\theta_2) - \tfrac{1}{2} R_c^2 (2\theta_2) \qquad (5\text{-}19)$$

$$area_{\text{semi-hidden}} = \pi R_i^2 - R_i^2 \left[2\theta_1 - \sin(2\theta_1)\right] - \pi R_c^2$$

$$+ \tfrac{1}{2} R_i^2 \left[2\theta_3 - \sin(2\theta_3)\right] + \tfrac{1}{2} R_c^2 \cdot \sin(2\pi - 2\theta_2) + \tfrac{1}{2} R_c^2 (2\theta_2)$$

$$area_{\text{exposed}} = 0$$

where

$$\theta_2 = \cos^{-1}\left(\frac{R_c^2 + d_t^2 - R_i^2}{2R_c d_t}\right), \qquad \theta_3 = \cos^{-1}\left(\frac{R_i^2 + d_t^2 - R_c^2}{2R_i d_t}\right)$$

(iii) $R_c > R_i$

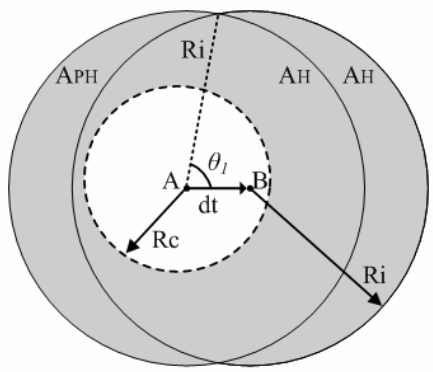
In this case, as the physical carrier-sensing range increases, the zone with *hidden stations* gets smaller, but the zone with *semi-hidden stations* becomes zero and that with *exposed stations* grows because the physical carrier-sensing range is larger than the interference range of the sender (Figure 5.11(c)). The area of the zone with *hidden*, *semi-hidden* and *exposed stations* can be represented as

$$area_{\text{hidden}} = \pi R_i^2 - \tfrac{1}{2} R_c^2 \left[2\theta_2 - \sin(2\theta_2)\right] - \tfrac{1}{2} R_i^2 \cdot \sin(2\pi - 2\theta_3) - \tfrac{1}{2} R_i^2 (2\theta_3) \qquad (5\text{-}20)$$

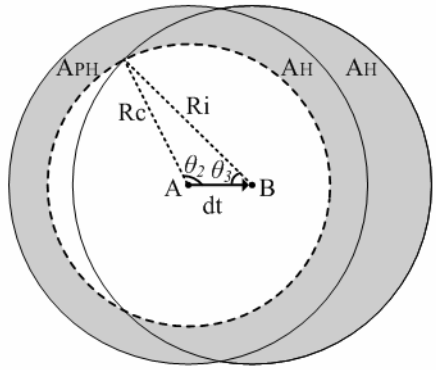
$$area_{\text{semi-hidden}} = 0$$

$$area_{\text{exposed}} = \pi R_c^2 - \tfrac{1}{2} R_c^2 \left[2\theta_2 - \sin(2\theta_2)\right] - \tfrac{1}{2} R_i^2 \cdot \sin(2\pi - 2\theta_3)$$

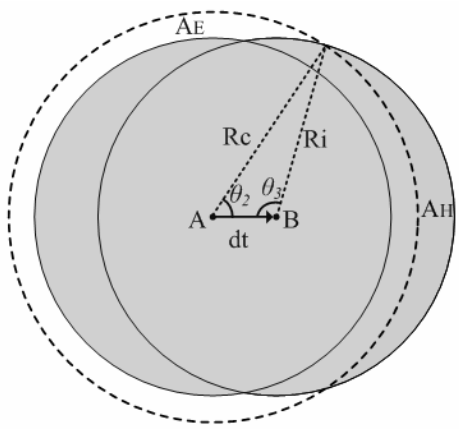
$$- \tfrac{1}{2} R_i^2 (2\theta_3) - \pi R_i^2 + R_i^2 [2\theta_1 - \sin(2\theta_1)].$$



A_H = zone with hidden stations
A_{PH} = zone with semi-hidden stations
(a) Case 1



A_H = zone with hidden stations
A_{PH} = zone with semi-hidden stations
(b) Case 2



A_H = zone with hidden stations
A_E = zone with exposed stations
(c) Case 3

Figure 5.11: Variation of the areas of the zones with hidden, semi-hidden and exposed stations as a function of increasing physical carrier-sensing range.

The optimal physical carrier-sensing range R_c can be obtained by substituting (5-18 to 5-20) into (5-17) and deriving the minimum value of function $f(R_c)$

$$\frac{\partial}{\partial R_c} f = 0 \quad \Rightarrow \quad R_c(optimal) = R_i \tag{5-21}.$$

When the physical carrier-sensing range R_c equals the interference range, the function $f(R_c)$ in (5-17) reaches its minimum:

$$f(R_c = R_i) = \pi R_i^2 - R_i^2[2\theta_1 - \sin(2\theta_1)] \tag{5-22}.$$

However, (5-17) works in this special case, but not in most practical cases because of two reasons. First, the stations in real wireless networks are not always uniformly distributed, and the numbers of *hidden*, *semi-hidden* and *exposed stations* are not always proportional to their zone areas. Second, the value of the function f in (5-17) is continuous with respect to the physical carrier-sensing range. Therefore, the corresponding numbers of *hidden*, *semi-hidden* and *exposed stations* are also continuous and fractional. However, in real wireless networks the number of stations is an integer. Hence, in practical conditions the optimal physical carrier-sensing range is not always equal to the interference range. The optimal value in real wireless networks should be modified according to (5-16). We will compare the optimal values obtained by (5-16) and (5-17) in Chapter 6, and validate them by means of network throughput evaluation obtained by ns-2 simulation [15]

Chapter 6

Performance Analysis of the 802.11 DCF in Mobile Ad Hoc Networks

In addition to the spatiotemporal analysis, we also use an analytical model to evaluate the effect of the physical carrier-sensing mechanism on the performance of the 802.11-based wireless ad hoc networks. To determine the collision probability, we derive a two-dimensional Markov chain model based on the existing models [7, 10]. We will explain below the modifications introduced here compared to the existing models. First, in Section A we derive the Markov chain model, then in Section B we derive the network average throughput.

6.1. Markov Chain Model of Station Transmissions

In this analysis, we assume the following: (a) ideal channel condition, i.e., no channel error due to noise; (b) constant and mutually independent collision probability for packets transmitted by each station, regardless of the number of collisions already suffered; and (c) fixed number n of contending stations in the network.

Let the station's backoff state $b(t)$ be a stochastic process representing the randomly chosen value of the backoff countdown timer. As already stated, we assume that the probability p of a transmitted packet colliding with another packet is independent of the station's backoff stage $s(t)$. This is only approximately true for relatively large contention windows and large number of stations. So, the two-dimensional process $\{s(t), b(t)\}$ can be modeled as a discrete-time Markov chain (Figure 6.1).

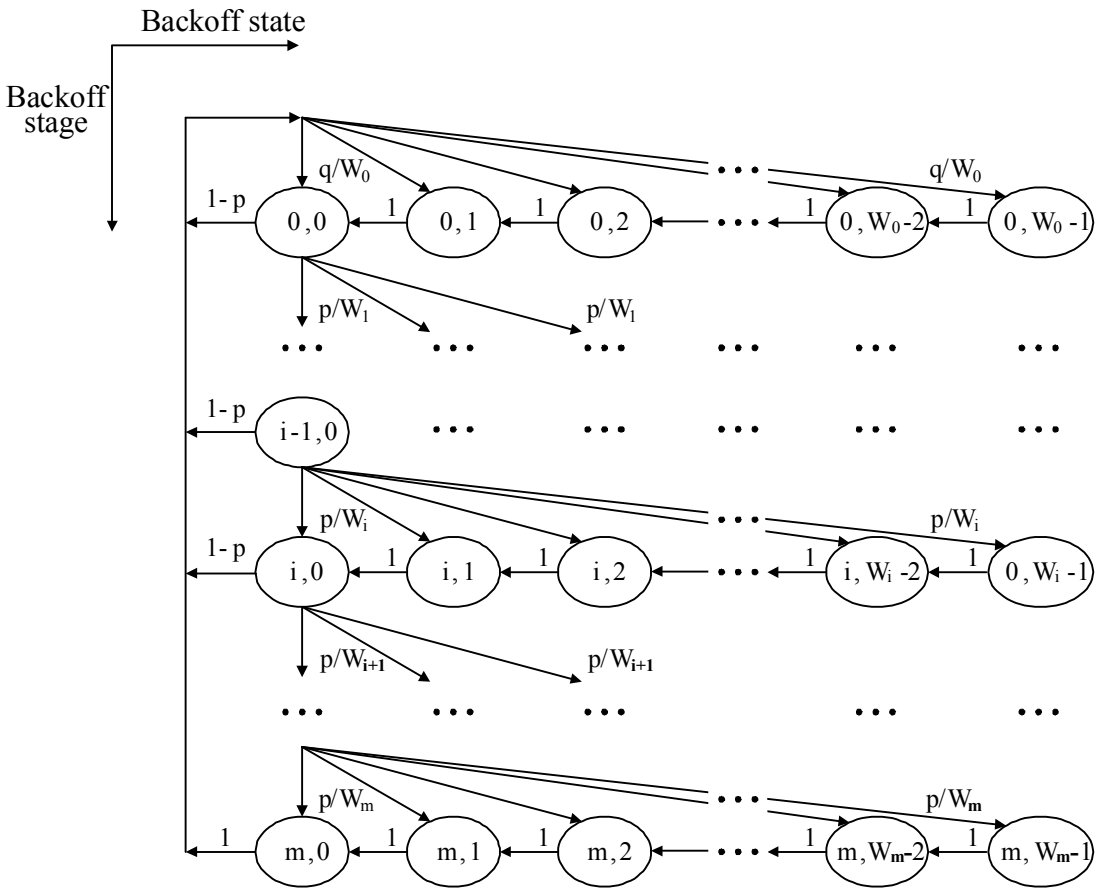


Figure 6.1: Markov chain model for backoff procedure.

Based on the IEEE 802.11 Standard [1], the size of the contention window, also called backoff window, increases exponentially from the minimum contention window, W_0, to the maximum contention window, W_{max}. It can be represented as

$$W_i = \begin{cases} 2^i W_0 & , 0 \le i < m' \\ 2^{m'} W_0 = W_{\max} & , i \ge m' \end{cases} \tag{6-1}$$

where m' is the backoff stage at which the contention window reaches the maximum value, W_{max}, and remains at W_{max} after this stage (known as truncated exponential backoff). Let m

denote the maximum backoff stage, where $m' \le m$. Without loss of generality, in this dissertation we assume that $m = m' = 5$.

In this Markov chain, the transition probabilities are given by

$$\begin{aligned} &P(i,k-1 \mid i,k) = 1 && 1 \le k \le W_i - 1, \quad 0 \le i \le m \\ &P(0,k \mid i,0) = (1-p)/W_0 && 0 \le k \le W_0 - 1, \quad 0 \le i \le (m-1) \\ &P(0,k \mid m,0) = 1/W_0 && 0 \le k \le W_0 - 1 \\ &P(i,k \mid i-1,0) = p/W_i && 0 \le k \le W_i - 1, \quad 1 \le i \le m \end{aligned} \tag{6-2}$$

Let $b_{i,k} = \lim_{t\to\infty} P\{s(t)= i, b(t)= k\}$, $i \in (0,m)$, $k \in (0,W_i - 1)$ be the stationary distribution of the Markov chain. By using the normalization condition for a stationary distribution, we have:

$$1 = \sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} b_{i,k} \tag{6-3}$$

Based on the chain regularities, we can obtain the probability $b_{0,0}$ in (6-4) and the probability τ_1 in (6-5). The probability $b_{0,0}$ represents that the station will be in the state where it is about to transmit and has not experienced collisions; the stationary probability τ_1 represents that a covered station will transmit in a randomly chosen time slot and collide with the frame transmitted by the sender

$$b_{0,0} = \frac{2q(1-p)(1-2p)}{2(1-p)(1-2p) + q(1-2p)(1-p^{m+1}) + qW_0(1-P)[1-(2P)^{m+1}]} \tag{6-4}$$

$$\tau_1 = \sum_{i=0}^{m} b_{i,0} = \frac{1-p^{m+1}}{1-p} \cdot b_{0,0} \tag{6-5}$$

In addition to the probability τ_1, we define several more stationary probabilities. First, for *hidden stations* in zones 3, 4, or 5, we define the probability τ_j, that a *hidden station* in zone j will transmit during the vulnerable period V_j, for j = 3, 4, 5, and collide with the frame transmitted by the sender. Second, for *semi-hidden stations* in zone 6 we define the probability τ_6 that a semi-hidden station will transmit during the vulnerable period V_6 and collide with the frame transmitted by the sender. These probabilities can be represented as

$$\tau_j = \sum_{i=0}^{m} \sum_{k=0}^{V_j} b_{i,k} = \tag{6-6}$$

$$= \begin{cases} \left[(V_j+1) \cdot \left(\frac{1-p^{m+1}}{1-p} \right) - \left(\frac{V_j(V_j+1)}{2W_0} \right) \cdot \left(\frac{1-\left(\frac{p}{2}\right)^{m+1}}{1-\frac{p}{2}} \right) \right] \cdot b_{0,0} & , V_j < W_0 \\ \left[\frac{1}{2} \cdot \left(\frac{1-p^{X_j}}{1-p} \right) + \frac{W_0}{2} \cdot \left(\frac{1-(2p)^{X_j}}{1-2p} \right) + (V_j+1) \cdot \left(\frac{p^{X_j} - p^{m+1}}{1-p} \right) - \left(\frac{V_j(V_j+1)}{2W_0} \right) \cdot \left(\frac{\left(\frac{p}{2}\right)^{X_j} - \left(\frac{p}{2}\right)^{m+1}}{1-\frac{p}{2}} \right) \right] \cdot b_{0,0} & , W_{X_j-1} < V_j < W_{X_j} \\ & , 1 \le X_j \le m \\ 1 & , V_j > W_m \end{cases}$$

where $j = \{3, 4, 5, 6\}$, is the zone number of the *hidden* and *semi-hidden stations*, and V_j is the vulnerable period length of the stations in zone j that is represented in the units of backoff slots. X_j is the backoff stage of the stations in zone j for which the associated vulnerability period V_j size falls between the contention window sizes W_{X_j-1} and W_{X_j}. For

example, for stations in zone 3, if the vulnerable period $W_1 < V_3 \leq W_2$, then use $X_3 = 2$ in (6-6).

In the stationary state, the collision probability p is the probability that at least one covered station will transmit in the same backoff slot as the source, or at least one *hidden station* in zone 3 will transmit in the vulnerable period V_3, or at least one *hidden station* in zone 4 will transmit in the vulnerable period V_4, or at least one *hidden station* in zone 5 will transmit in the vulnerable period V_5, or at least one *semi-hidden station* in zone 6 will transmit in the vulnerable period V_6. Thus, p can be expressed as

$$p = 1-(1-\tau_1)^{n_C-1}(1-\tau_3)^{n_{H3}}(1-\tau_4)^{n_{H4}}(1-\tau_5)^{n_{H5}}(1-\tau_6)^{n_{PTH6}} \quad (6\text{-}7)$$

where n_C is number of the covered stations inside the physical carrier-sensing range that includes the sender itself, n_{H3} is the number of hidden stations in zone 3, n_{H4} is the number of hidden stations in zone 4, n_{H5} is the number of hidden stations in zone 5, n_{PTH6} is the number of semi-hidden stations in zone 6. We solve the nonlinear equations (6-4) – (6-7) using a numerical iteration method to obtain τ_1, τ_3, τ_4, τ_5 and τ_6.

6.2. Throughput Analysis

Let P_{tr} be the probability that there will be at least one transmission in a given time slot.

$$P_{tr} = 1-(1-\tau_1)^{n_C} \quad (6\text{-}8).$$

The probability of a successful transmission, Ps, is the probability that exactly one station will transmit on the channel, conditioned on having at least one station transmit. This probability can also be viewed as the probability of having one station transmit and none of

the covered stations transmit in the same time slot, as well as having none of the hidden and part-time exposed stations transmit in the vulnerable period. Then, the probability of a successful transmission is

$$P_S = \frac{n_C \tau_1 (1-\tau_1)^{n_C-1} (1-\tau_3)^{n_{H3}} (1-\tau_4)^{n_{H4}} (1-\tau_5)^{n_{H5}} (1-\tau_6)^{n_{PTH6}}}{P_{tr}} = \frac{1-n_C p}{P_{tr}} \quad \text{(6-9).}$$

Analogy to the throughput inside the transmission range of a single access-point [7], for an ad hoc network we consider the throughput inside the physical carrier-sensing range of both the sender and receiver. The normalized system throughput S can be determined as

$$S = \frac{P_S P_{tr} E[Payload]}{(1-P_{tr})\sigma + P_S P_{tr} T_S + (1-P_S) P_{tr} T_C} \quad \text{(6-10)}$$

where the $E[Payload]$ is the average length of the packet payload and σ is the duration of an empty backoff slot. The T_S and T_C are the average times the channel is sensed busy because of a successful transmission or a collision, given by

$$\begin{aligned} T_S &= H + E[Payload] + \delta + SIFS + ACK + \delta + DIFS \\ T_C &= H + E[Payload] + \delta + ACK\_Timeout \end{aligned} \quad \text{(6-11)}$$

where $H = PHY\_Header + MAC\_Header$. The δ is the propagation delay and the $ACK\_Timeout = SIFS + ACK + DIFS$.

Our study shows that semi-hidden stations could degrade the performance by corrupting the ACK frames at the sender. This problem is common in wireless ad hoc networks but it is not common in access-point-based wireless networks. Our previous work [10] considered only the regular (full-time) hidden station effect at the receiver. In this paper,

we also model the semi-hidden station effect on the sender, in addition to the regular hidden station effect on the receiver. These hidden stations have different vulnerable period with respect to the receiver and sender. We extend the two-dimensional Markov chain model and throughput model so that the extended model characterizes the network throughput in the presence of both the regular and semi-hidden stations.

6.3 Simulation Setup

The system simulation is performed using the ns-2 simulator software package [15]. The physical layer parameters follow the 802.11g specifications. The required SINR and receiver sensitivity is listed in Table 5.1. The transmission range is set as 100m. The simulation topology is a ring with 20 evenly distributed stations (Figure 6.2). Each station sends frame to its right neighbor. The traffic is set to be saturated so that each station always has a packet ready for transmission.

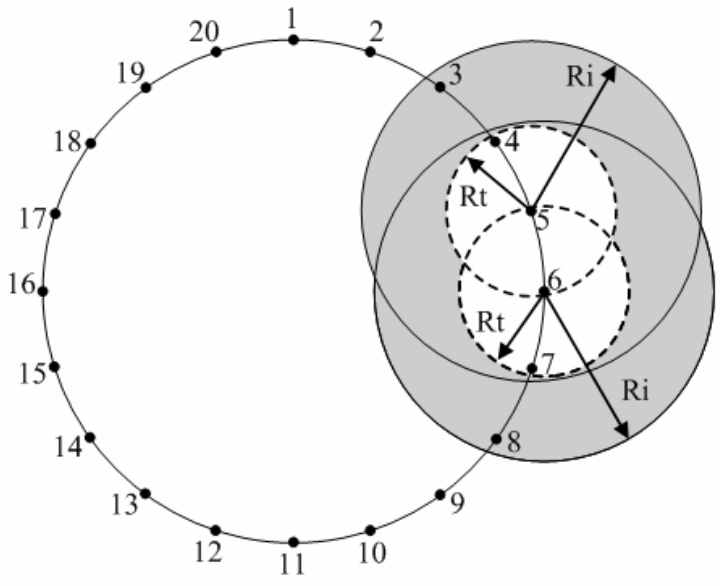


Figure 6.2: Ring topology with 20 stations.

We also use an extension of ns-2 to calculate SINR, which compares the received signal with the aggregate interference (the original ns-2 only considers the individual interference). We use the ring topology because it is symmetric in all directions and always gives homogeneous throughput at all stations. There is no throughput unfairness problem in a ring topology, so we can focus on the impact of interference on the performance.

6.4 Simulation Results and Discussion

We study the most frequent scenario where the interference range is much larger than the transmission range (Configuration 3 in Chapter 5.2). We set the distance between two adjacent stations at 95m so the interference range is about 227m, according to (5-4). The smallest value of the physical carrier-sensing range is set equal to the transmission range based on the lower bound definition in Chapter 5.3. In Figure 6.3(a), the throughput obtained by our analytical model is consistent with that obtained by ns-2 simulation. As the physical carrier-sensing range increases from the lower bound up to 276m, the aggregate throughput also increases quickly and reaches its maximum (Figure 6.3(a)). Then it decreases gradually as the physical carrier-sensing range exceeds 276m. The optimal physical carrier-sensing range in this scenario equals 276m.

This result is corroborated by simple counting the number of the exposed, full-time and semi-hidden stations, given by (5-16). Figure 6.4(a) shows the qualitative shape of the function $f(R_c)$ obtained both by counting the number of exposed and hidden stations as in (5-16) as well as by the total area of the zones containing exposed, full-time and semi-hidden stations as in (5-17). In case of counting the function f reaches the minimum

when the physical carrier-sensing range equals 276m. In case of the area calculation, f reaches the minimum when the physical carrier-sensing range equals the interference range, at 227m. The optimal physical carrier-sensing range using (5-16) is larger than the interference range by about 22% because the areas of the zones with exposed, full-time and semi-hidden stations do not accurately represent the numbers of the stations in these zones. Considering the link between stations 6 and 5 (Figure 6.2), when the physical carrier-sensing range equals the transmission range, stations 3 and 4 are full-time hidden station; station 6 is a semi-hidden station; and there are no exposed stations. So, the value of the function f equals 3 in this situation.

When the physical carrier-sensing range increases to 188m, station 3 is the only full-time hidden station and there are no semi-hidden and exposed stations, so now the value of the function f equals 1. As the physical carrier-sensing range increases to 276m, station 9 is the only exposed station and there are no full-time or semi-hidden stations, so the value of the function f again equals 1. When the physical carrier-sensing range falls in the interval from 188m to 276m, the total number of exposed, full-time and semi-hidden stations reaches the minimum value. So, the optimal physical carrier-sensing range is close to but rarely equal to the interference range in real wireless networks.

In Configuration 2 (Figure 5.5(b)), the distance between two adjacent stations in the ring topology (Figure 6.2) is set at 61.5m so the interference range equals 100m, according to (5-4). As the physical carrier-sensing range increases from the transmission range to 119m, the aggregate throughput increases and reaches its maximum value (Figure 6.3(b)). After

the physical carrier-sensing range exceeds 119m, the aggregate throughput decreases (Figure 6.3(b)). The optimal physical carrier-sensing range is 119m, which is larger than the interference range by about 19%. This result is in agreement with the value of the function f obtained by (5-16), which reaches its minimum when the physical carrier-sensing range is set at 119m (Figure 6.4(b)). Unlike this, the curve of the function f obtained by (5-17) reaches its minimum value when the physical carrier-sensing range equals the interference range, at 100m (Figure 6.4(b)). Therefore, the area-based method based on (5-17) does not accurately represent the optimal physical carrier-sensing range in real wireless networks.

In Configuration 1 (Figure 5.5(a)), we set the distance between two adjacent stations on the ring at 30m so the interference range is 47m, based on (5-4). In this configuration, the throughput obtaining by our analytical model agrees with that produced by ns-2 simulation (Figure 6.3(c)). As the physical carrier-sensing range increases, the aggregate throughput decreases monotonically. When the physical carrier-sensing range equals its lower bound (the transmission range, 100m), the aggregate throughput is at the maximum, and the function f reaches its minimum value (Figure 6.4(c)). Both results agree that the optimal physical carrier-sensing range in Configuration 1 equals the transmission range. In our simulation, we do not consider physical carrier-sensing ranges below 100m, because this would violate the lower bound of the physical carrier-sensing range, which equals the transmission range, 100m. This is the reason why in this case the optimal physical carrier-sensing range is more than double the interference range, 47m.

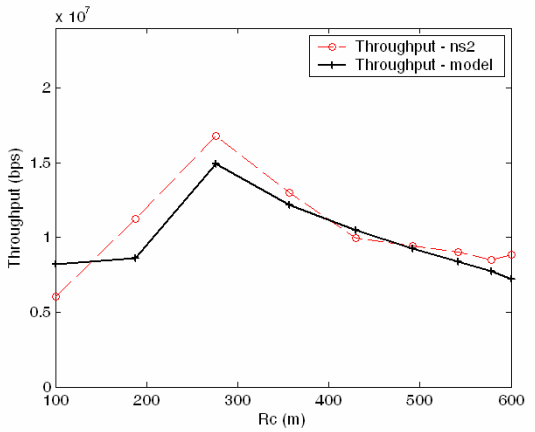


Figure 6.3 (a): Throughput for Configuration 3.

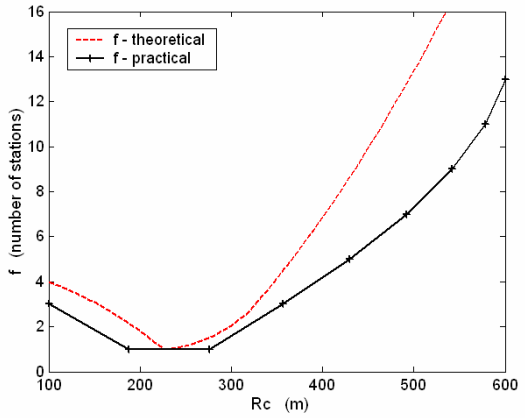


Figure 6.4 (a): Function *f* of Configuration 3.

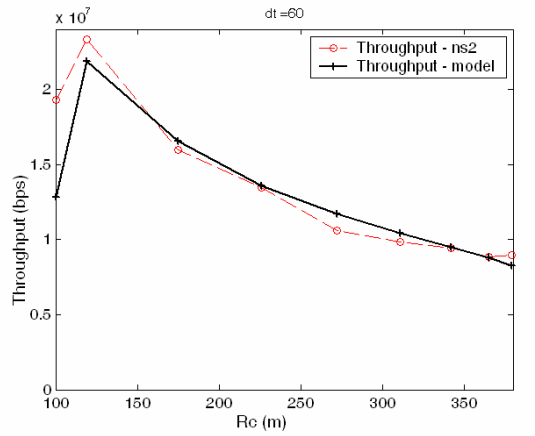


Figure 6.3 (b): Throughput for Configuration 2.

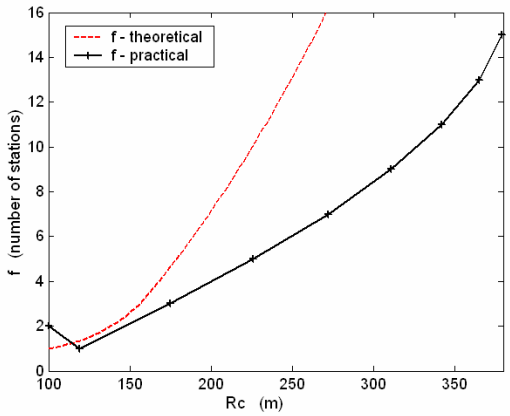


Figure 6.4 (b): Function *f* of Configuration 2.

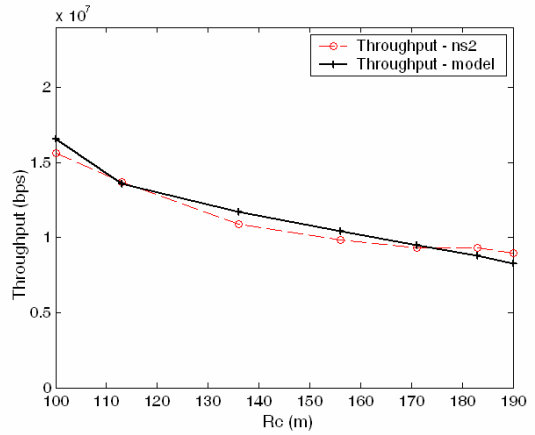


Figure 6.3 (c): Throughput for Configuration 1.

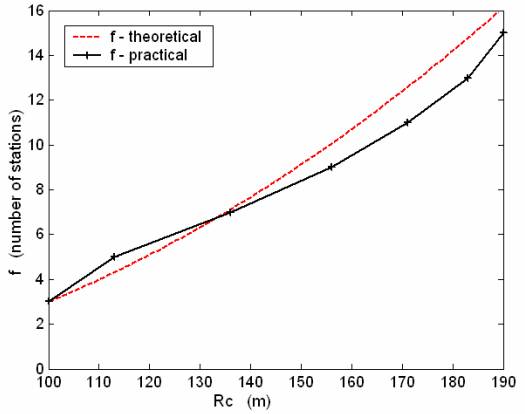


Figure 6.4 (c): Function *f* of Configuration 1.

Ma et al. [24] proposed that a close-to-optimal value of the physical carrier-sensing range equals the interference range. Our derivation of (5-21) shows that the true optimal physical carrier-sensing range equals the interference range only if the areas of the zones with all stations accurately represent the number of stations inside these zones. However, in most scenarios the areas of the zones do not accurately represent the number of stations inside these zones, as described in the discussion of (5-17). Therefore, we propose a modified method according to (5-16), which derives the optimal physical carrier-sensing range more accurately by counting the numbers of exposed, full-time and semi-hidden stations.

The previous work studied optimal physical carrier-sensing range based on the area of the zone covered by the stations. We improved this method by counting the number of stations in those zones. Setting the optimal physical carrier-sensing range yields the minimum total number of exposed and hidden stations in the network. We also derived a Markov chain model that links the number of different station types to the network throughput. The evaluation of our model on a ring topology shows that the optimal throughput coincides with the minimum total number of exposed and hidden stations, and both appear at the optimal physical carrier-sensing range.

Previous studies investigated setting the optimal physical carrier-sensing range, but not how the throughput varies for non-optimal values of physical carrier-sensing range. Our Markov chain model of throughput shows how the network throughput changes with changing physical carrier-sensing range and, linked with it, a changing total number of hidden and exposed stations.

Chapter 7

Conclusions

In this dissertation**,** the performance of IEEE 802.11DCF in wireless network in the presence of hidden stations was studied. This chapter summarizes the main contributions of this research work in the first section. Next, several suggestions for future research directions are presented.

7.1 Contribution of the Thesis

In the access-point-based wireless network, we derived an analytical model to compute the non-saturation and saturated throughput of the IEEE 802.11 DCF in the presence of hidden stations for both the Basic and RTS/CTS access methods. The proposed model is in good agreement with ns-2 simulations in most condition and, thus, can be used to estimate the network throughput. Our model generalized the existing models and they can be considered as special cases of our model, with zero hidden stations.

Based on our study of the performance of 802.11 DCF in the presence of the hidden stations, the best policy to increase the throughput for the Basic access method is by increasing the initial contention window size, and the second best option is by decreasing the data frame size. On the other hand, adjusting the initial contention window size does not change significantly the throughput in RTS/CTS access method. If we do not consider the channel error, using the longest possible data frame is the best policy for this access method.

The RTS/CTS access method outperforms the Basic access method in access-point-based wireless LANs. First, the throughput in the former is higher than that in the latter method, except for the scenario when transmitting short data frames in the environment with no hidden stations. However, the probability of no hidden stations in a wireless LAN is low, particularly when many mobile stations try to connect to a single access point. Furthermore, the Basic access method is very sensitive to the hidden station effect. If there are no hidden stations, the throughput of the Basic access method is slightly higher than that of the RTS/CTS method in the scenario when sending short data frames. However, the throughput of the Basic access method is much worse than that of the RTS/CTS access method in the presence of hidden stations.

We present a spatiotemporal model that characterizes the effectiveness of the physical and virtual carrier-sensing mechanism in wireless ad hoc networks. Both the Basic and RTS/CTS access methods are not effective to alleviate the hidden station problem in the configuration that the interference range is larger than the transmission range. However, this configuration is the most frequent happened scenario in wireless ad hoc network; and the default multi-rate mechanism of IEEE 802.11 makes this configuration occurring more frequently.

In wireless ad hoc network, the hidden station effect not only occurs when a receiver is accepting a RTS or DATA frame but also when a sender is accepting an ACK frame. We define the semi-hidden stations that were previously considered as exposed stations,

because their impact on the aggregate throughput is similar to that of regular hidden stations. Our analytical results show that the semi-hidden station effect significantly influences the aggregate throughput and selection of optimal physical carrier-sensing range.

Optimal physical carrier-sensing setting can significantly improve wireless network performance. However, increasing the physical carrier-sensing range does not always increase the network performance. An optimal physical carrier-sensing setting is a tradeoff between the spatial reuse and hidden station effect. Our study shows that choosing the physical carrier-sensing range as the interference range is a theoretically optimal setting, if network topology and traffic are uniformly distributed.

We also present a modified Markov chain model that describes the aggregate throughput of 802.11-based wireless ad hoc networks in the presence of hidden and semi-hidden stations. Combining our spatiotemporal and modified Markov chain model, our analytical result provides an insight into the relationship between the physical carrier-sensing range and the aggregate throughput.

7.2 Future work

Besides the hidden station effect, channel noise is another important parameter that results in packet loss in wireless networks. Incorporating the effect of channel error into performance model would increase the accuracy of the model. If consider the packet loss due to channel error, the throughput in the RTS/CTS access method as discussed in chapter

4 will not increase monotonously as the data frame increases; and an optimal data frame length will be a tradeoff between packet error rate and channel utilization.

An optimal physical carrier-sensing range is significantly depended on the interference range. However, the interference range is related to many parameters, such as path loss exponent, transmit power, data rate, etc. An adaptive physical carrier-sensing mechanism would be helpful to approach the optimal physical carrier-sensing setting in different wireless channel and scenario.

References

[1] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ISO/IEC 8802-11, 1999(E), August 1999.

[2] A. S. Tanenbaum, *Computer Networks*. 4th Edition, Prentice Hall, Upper Saddle River, NJ, 2004

[3] L. Kleinrock and F. Tobagi, "Packet switching in radio channels, Part II—The hidden terminal problem in carrier sense multiple access and the busy tone solution," *IEEE Transactions on Communications*, vol. COM-23, no. 12, pp. 1417-1433, December 1975

[4] K. Huang and K. Chen, "Interference analysis of nonpersistent CSMA with hidden terminals in multicell wireless data networks," *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communication*, pp. 907-911, September 1995

[5] H. S. Chhaya and S. Gupta, "Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol," *Wireless Networks*, vol. 3, pp. 217-234, August 1997

[6] Y. Wang and J. J. Garcia-Luna-Aceves, "Performance of collision avoidance protocols in single channel ad hoc networks," *Proc. IEEE ICNP*, pp. 68-78, November 2002

[7] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535-547, March 2000

[8] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma, "Performance of reliable transport protocol over IEEE 802.11 wireless LAN: Analysis and enhancement," *Proc. IEEE INFOCOM*, vol. 2, pp. 599-607, June 2002

[9] E. Ziouva and T. Antonakopoulos, "CSMA/CA performance under high traffic conditions: Throughput and delay analysis," *Computer Communications (Elsevier)*, vol. 25, no. 3, pp. 313-321, February 2002

[10] F. Hung, S Pai and I. Marsic, "Performance Modeling and Analysis of the IEEE 802.11 Distribution Coordination Function in Presence of Hidden Stations," *IEEE/AFCEA MILCOM,* October 2006

[11] K. Sakakibara, S. Chikada and J. Yamakita, "Analysis of unsaturation throughput of IEEE 802.11 DCF," *Proc. ICPWC-2005*, pp. 134-138, January 2005

[12] K. Duffy, D. Malone and D. Leith, "Modeling the 802.11 Distributed Coordination Function in Non-saturated Conditions," *IEEE Comm. Letters*. vol. 9, no. 8, pp. 715-717, August 2005

[13] P. E. Engelstad and O.N. Østerbø, "Non-Saturation and Saturation Analysis of IEEE 802.11e EDCA with Starvation Prediction," *Proc. ACM MSWiM 2005*, pp. 224-233, October 2005

[14] S. Y. Ni, Y. C. Tseng, Y. S. Chen and J. P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Proc. ACM/IEEE MobiCom '99*, pp. 151-162, August 1999

[15] The ns Manual, URL: http://www.isi.edu/nsnam/ns/ns-documentation.html

[16] J. Geier, "Improving WLAN Performance with RTS/CTS," on http://www.wi-fiplanet.com, 2002

[17] S. Xu, and T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?" *IEEE Commun. Magazine*, vol. 39, no. 6, pp. 130-13, June 2001

[18] K. Xu, M. Gerla, and S. Bae, "How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks?" *Proc. of IEEE Globecom*, pp. 72-76, November 2002

[19] F. Ye, S. Yi and B. Sikdar, "Improving spatial reuse of IEEE 802.11 based ad hoc networks," *Proc. of IEEE Globecom*, pp. 1013-1017, December 2003

[20] J. Zhu, X. Guo, L. L. Yang, W. S. Conner, S. Roy, and M. M. Hazra, "Adapting physical carrier-sensing to maximize spatial reuse in 802.11 mesh networks," *Wiley J. Wireless Commun. Mob. Comput*., vol. 4, issue 8, pp. 933-946, December 2004

[21] X. Yang and N. H. Vaidya, "On the physical carrier sense in wireless ad hoc networks," *Proc. of IEEE INFOCOM*, pp. 2525-2535, March 2005

[22] H. Zhai and Y. Fang, "Physical carrier sensing and spatial reuse in multirate and multihop wireless ad ho networks," *Proc. of IEEE INFOCOM*, pp. 1-12, April 2006

[23] T.Y. Lin and J. C. Hou, "Interplay of spatial reuse and SINR determined data rates in CSMA/CA-based, multi-hop, multi-rate wireless networks," *Proc. of IEEE INFOCOM*, pp. 803-811, May 2007

[24] H. Ma, R. Vijaykumar, S. Roy and J. Zhu, "Optimizing 802.11 mesh networks performance using physical carrier-sensing," accepted for publication in *IEEE/ACM Trans. on Networking*

[25] F. Cali, M. Conti, and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit," *IEEE/ACM Trans. on Networking*, vol. 8, no. 6, pp. 785-799, December 2000

[26] Z. Zeng, Y. Yang, and J. C. Hou, "How physical carrier sense affects system throughput in IEEE 802.11 wireless networks," *Proc. of IEEE INFOCOM*, pp. 1445 - 1453, April 2008

[27] T. S. Rappaport, *Wireless Communications, Principles and Practices*, 2nd Edition, Prentice Hall, Upper Saddle River, NJ, 2002

[28] J. Yee and H. Pezeshki-Esfahani, "Understanding wireless LAN performance trade-offs," CommsDesign.com, November 2002. URL: http://www.commsdesign.com/story/OEG20021101S0015

Curriculum Vitae

Fu-Yi Hung

Education

2009	Doctor of Philosophy in Electrical and Computer Engineering Rutgers, The State University of New Jersey New Brunswick, New Jersey
2001	Master of Science in Electrical Engineering State University of New York (SUNY), Buffalo Buffalo, New York
1993	Master of Science in Mechanical Engineering National Central University Chungli, Taiwan
1991	Bachelor of Science in Mechanical Engineering National Central University Chungli, Taiwan

Publications

2007 F.-Y. Hung and I. Marsic, "Access Delay Analysis of IEEE 802.11 DCF in the Presence of Hidden Stations," *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2007)*, pp. 2541-2545, Washington, DC, November 2007.

2007 F.-Y. Hung and I. Marsic, "Effectiveness of Physical and Virtual Carrier Sensing in IEEE 802.11 Wireless Ad Hoc Networks," *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2007)*, pp. 143-147, Hong Kong, March, 2007.

2007 F.-Y. Hung and I. Marsic, "Analysis of Non-Saturation and Saturation Performance of IEEE 802.11 DCF in the Presence of Hidden Stations," *Proceedings of the IEEE 65th Vehicular Technology Conference (VTC-2007-Fall)*, pp. 230-234, Baltimore, MD, September 2007.

2006 F.-Y. Hung, S. Pai and I. Marsic, "Performance Modeling and Analysis of the IEEE 802.11 Distributed Coordination Function in Presence of Hidden Stations," *Proceedings of the Military Communications Conference (MILCOM 2006)*, pp. 1-7, Washington, DC, October 2006.