INCLUDES

NEWNES ONLINE MEMBERSHIP

WIRELESS NETWORKING

know it all

- A comprehensive overview from our best-selling authors
- Explains the theory, concepts, design, and implementation of 802.11, 802.16, and 802.20
- Includes discussion of indoor networks, signal propagation, and network security

Chandra • Dobkin • Bensky
Olexa • Lide • Dowla

Wireless Networking

Newnes Know It All Series

PIC Microcontrollers: Know It All
Lucio Di Jasio, Tim Wilmshurst, Dogan Ibrahim, John Morton,
Martin Bates, Jack Smith, D.W. Smith, and Chuck Hellebuyck
ISBN: 978-0-7506-8615-0

Embedded Software: Know It All
Jean Labrosse, Jack Ganssle, Tammy Noergaard, Robert Oshana, Colin Walls, Keith Curtis,
Jason Andrews, David J. Katz, Rick Gentile, Kamal Hyder, and Bob Perrin
ISBN: 978-0-7506-8583-2

Embedded Hardware: Know It All
Jack Ganssle, Tammy Noergaard, Fred Eady, Creed Huddleston, Lewin Edwards,
David J. Katz, Rick Gentile, Ken Arnold, Kamal Hyder, and Bob Perrin
ISBN: 978-0-7506-8584-9

Wireless Networking: Know It All
Praphul Chandra, Daniel M. Dobkin, Alan Bensky, Ron Olexa,
David A. Lide, and Farid Dowla
ISBN: 978-0-7506-8582-5

RF & Wireless Technologies: Know It All
Bruce Fette, Roberto Aiello, Praphul Chandra, Daniel M. Dobkin,
Alan Bensky, Douglas Miron, David A. Lide, Farid Dowla, and Ron Olexa
ISBN: 978-0-7506-8581-8

For more information on these and other Newnes titles visit: www.newnespress.com

Wireless Networking

Praphul Chandra
Daniel M. Dobkin
Alan Bensky
Ron Olexa
David A. Lide
Farid Dowla

ELSEVIER

AMSTERDAM • BOST ON • HEIDELBERG • LONDON
NEW YORK • O XFORD • P ARIS • SAN D IEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • T OKYO

Newnes is an imprint of Elsevier

Cover image by iStockphoto
Newnes is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Library of Congress Cataloging-in-Publication Data
A catalogue record for this book is available from the British Library.

British Library Cataloguing-in-Publication Data

Chandra, Praphul.
Wireless networking / Praphul Chandra, Ron Olexa, Alan Bensky.
p. cm. -- (The Newnes know it all series)
Includes index.
ISBN-13: 978-0-7506-8582-5 (pbk. : alk. paper) 1. Wireless communication systems. I. Olexa, Ron. II. Bensky, Alan, 1939- III. Title.
TK5103.2.C447 2007
621.384--dc22

2007029327

ISBN: 978-0-7506-8582-5

For information on all Newnes publications
visit our Web site at www.books.elsevier.com

07 08 09 10 10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

Contents

This page intentionally left blank

About the Authors

Alan Bensky, MScEE (Chapters 4, 5, 6, and 15), is an electronics engineering consultant with over 25 years of experience in analog and digital design, management, and marketing. Specializing in wireless circuits and systems, Bensky has carried out projects for varied military and consumer applications. He is the author of *Short-range Wireless Communication, Second Edition*, published by Elsevier, 2004, and has written several articles in international and local publications. He has taught courses and gives lectures on radio engineering topics. Bensky is a senior member of IEEE.

Praphul Chandra (Chapters 10, and 11) works as a Research Scientist at HP Labs, India in the Access Devices Group. He joined HP Labs in April 2006. Prior to joining HP he was a senior design engineer at Texas Instruments (USA) where he worked on Voice over IP with specific focus on Wireless Local Area Networks. He is the author of two books – *Bulletproof Wireless Security* and *Wi-Fi Telephony: Challenges and Solutions for Voice over WLANs*. He is an Electrical Engineer by training, though his interest in social science and politics has prompted him to concurrently explore the field of Public Policy. He maintains his personal website at www.thecofi.net.

Daniel M. Dobkin (Chapter 1, 2, 3, and 9) is the author of *RF Engineering for Wireless Networks*. He has been involved in the design, fabrication, and characterization of devices and systems used in microwave wireless communications for over two decades. He is currently an independent consultant involved in research and teaching related to RFID and other fields in communications. He has taught numerous introductory short courses in RFID technology in the US and Singapore. Dr. Dobkin received his Ph.D. degree from Stanford University in 1985 and his B.S. from the California Institute of Technology in 1976. He is the author of about 30 technical publications, inventor or co-inventor of six U.S. patents, and has written two technical books: Principles of Chemical Vapor Deposition with Michael Zuraw and RF Engineering for Wireless Networks.

Farid Dowla (Chapters 12, 13, and 14) is the editor of *Handbook of RF & Wireless Technologies.* Dowla received his BS, MS, and PhD in electrical engineering from the Massachusetts Institute of Technology. He joined Lawrence Livermore National Laboratory

shortly after receiving his doctorate in 1985. His research interests include adaptive filters, signal processing, wireless communication systems, and RF/mobile communication. He currently directs a research team focused on ultra-widebandRFradar and communication systems. Dowla is also an adjunct associate professor of electrical engineering at the University of California at Davis. He is a member of the Institute of Electrical and Electronic Engineers (IEEE) and Sigma Xi. He holds three patents in signal processing area, has authored a book on neural networks for the U.S. Department of Defense, and has edited a book on geophysical signal processing. He contributes to numerous IEEE and professional journals and is a frequent seminar participant at professional conferences.

David A. Lide (Chapter 11) is the author of *Wi-Fi Telephony*. He currently is a Senior Member of the Technical Staff at Texas Instruments and has worked on various aspects of Voice over IP for the past nine years. Prior to that, he has worked on Cable Modem design and on weather satellite ground systems. He lives with his family in Rockville, Maryland.

Michael R. Moore (Chapter 13) was a contributor to *Handbook of RF & Wireless Technologies*. He is a research and development engineer in the Engineering and Science Technology Division at Oak Ridge National Laboratory. He holds a BS and MS in electrical engineering from Mississippi State University in Starkville, Miss. His current research expertise includes 16 years in RF instrumentation, health effects, and communications. He has several years of experience in shielding, generating, and modeling electromagnetic fields and their effects. He is an active member of IEEE SCC28 committee on the biological effects of RF and the IEEE 1451 committee on sensor networking. He currently directs several projects dealing with software radio technologies, specializing in spread-spectrum receivers, and is a communications analyst for the Army's Future Combat Systems (FCS) network, focusing on system issues, network vulnerability, and combat identification. He has several patents and patents pending in the area of wireless communications.

Asis Nasipuri (Chapter 12) was a contributor to *Handbook of RF & Wireless Technologies*. He is a professor in the department of electrical and computer engineering at the University of North Carolina at Charlotte. He received his BS in electronics and electrical communication engineering from the Indian Institute of Technology in Kharagpur, India in 1987 and his MS and PhD in electrical a computer engineering from the University of Massachusetts at Amherst in 1990 and 1993, respectively. He then joined the Indian Institute of Technology at Kharagpur, India as a faculty member in the Department of Electronics and Electrical Communication Engineering. From 1998 to 2000, he served as a visiting researcher in the Department of Computer Science at the University of Texas at San Antonio. Since 2000, he has been at UNC-Charlotte as an assistant professor of electrical and computer engineering. Nasipuri's research interests include mobile ad hoc and sensor networks, wireless communications, and statistical signal processing. He has published more than 20 research articles on these topics.

Ron Olexa (Chapters 7, 8, and 16) is the author of *Implementing 802.11, 802.16, and 802.20 Wireless Networks*. He is currently President of Horizon Wi-Com, a wireless carrier providing WiMax service to major markets in the Northeast US. He is also the owner of Wireless Implementation LLC, a consulting company that has provided technical support and business planning guidance to project as diverse at satellite communications systems, Cellular network deployments, WiMax and 802.11 hotspot and hotzone implementations. He has previously been CTO at Advanced Radio Telecom and Dialcall, COO of Superconducting Core Technologies, and has held various senior management positions in large wireless communications companies over his 30 year career.

Robert Poor (Chapter 14) was a contributor to *Handbook of RF & Wireless Technologies*. He is chief technology officer for Ember Corporation in Boston.

This page intentionally left blank

CHAPTER 1

Basics of Wireless Communications

Daniel M. Dobkin

1.1 Harmonic Signals and Exponentials

Before we begin to talk about wireless, we briefly remind the reader of a previous acquaintance with three concepts that are ubiquitous in radio engineering: sinusoidal signals, complex numbers, and imaginary exponentials. The reader who is familiar with such matters can skip this section without harm.

Almost everything in radio is done by making tiny changes—modulations—of a signal that is periodic in time. The archetype of a smooth periodic signal is the sinusoid (Figure 1.1), typically written as the product of the angular frequency ω and time t.

Both of these functions alternate between a maximum value of 1 and minimum value of -1; cosine starts at $+1$, and sine starts at 0, when the argument is zero. We can see that cosines and sines are identical except for an offset in the argument (the *phase*):

$$\cos(\omega t) = \sin\left(\omega t + \frac{\pi}{2}\right) \tag{1.1}$$

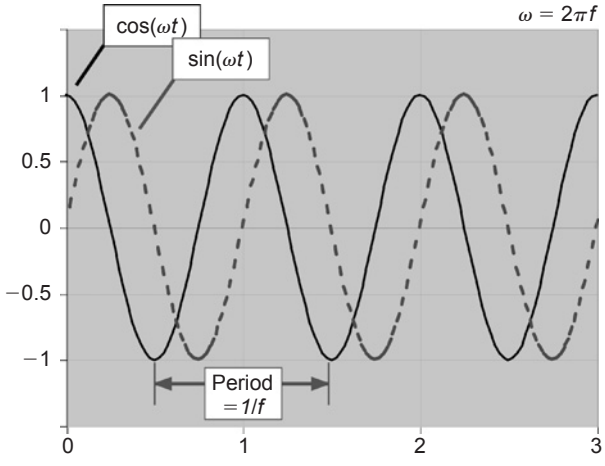

Figure 1.1: Cosine and Sine Functions

We say that the sine lags the cosine by 90 degrees. (Note that here, following common practice, we write angles in radians but often speak of them in degrees.) The cosine and sine are periodic with a period = $(1/f)$, where $f = \omega/2\pi$ is the frequency in cycles per second or hertz.

Let us now digress briefly to discuss complex numbers, for reasons that will become clear in a page or two. Imaginary numbers, the reader will recall, are introduced to provide square roots of negative reals; the unit is $i = \sqrt{(-1)}$. A complex number is the sum of a real number and an imaginary number, often written as, for example, $z = a + bi$. Electrical engineers often use j instead of i, so as to use i to represent an AC; we shall, however, adhere to the convention used in physics and mathematics. The complex conjugate z^* is found by changing the sign of the imaginary part: $z^* = a - bi$.

Complex numbers can be depicted in a plane by using the real part as the coordinate on the x- (real) axis, and the imaginary part for the y- (imaginary) axis (Figure 1.2). Operations on complex numbers proceed more or less the same way as they do in algebra, save that one must remember to keep track of the real and imaginary parts. Thus, the sum of two complex numbers can be constructed algebraically by

$$(a + bi) + (c + di) = [a + c] + [b + d]i \quad (1.2)$$

and geometrically by regarding the two numbers as vectors forming two sides of a parallelogram, the diagonal of which is their sum (Figure 1.3).

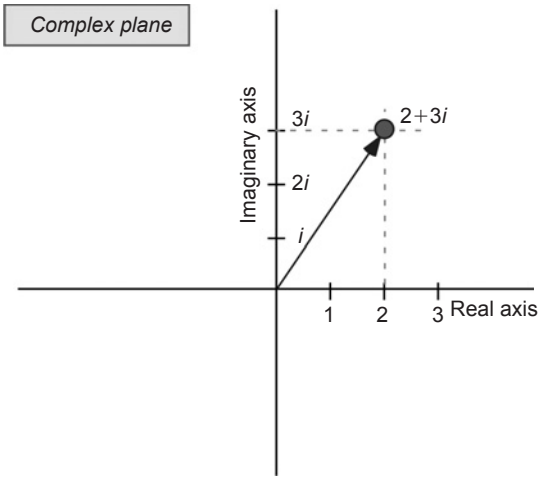

Figure 1.2: Complex Number Depicted as a Vector in the Plane

Multiplication can be treated in a similar fashion, but it is much simpler to envision if we first define the length (also known as the *modulus*) and angle of a complex number. We define a complex number of length 1 and angle θ to be equal to an exponential with an imaginary

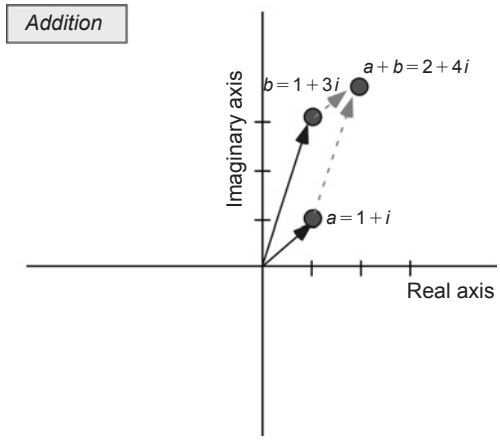

Figure 1.3: Addition of Complex Numbers

argument equal to the angle (Figure 1.4). Any complex number (e.g., *b* in Figure 1.4) can then be represented as the product of the modulus and an imaginary exponential whose argument is equal to the angle of the complex number in radians.

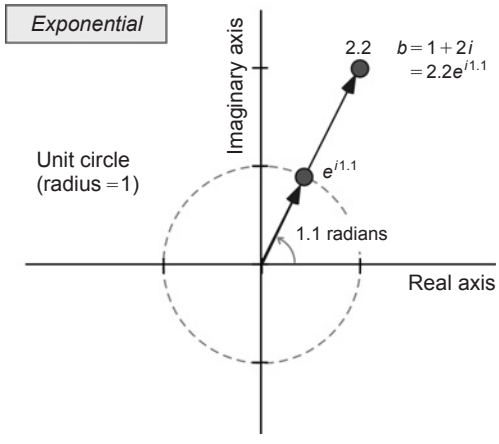

Figure 1.4: Imaginary Exponentials and Complex Numbers

By writing a complex number as an exponential, multiplication of complex numbers becomes simple, once we recall that the product of two exponentials is an exponential with the sum of the arguments:

$$(e^a) \cdot (e^b) = e^{[a+b]} \quad (1.3)$$

The product of two complex numbers is then constructed by multiplying their moduli and adding their angles (Figure 1.5).

$$\left(\rho_1 e^{i\theta_1}\right) \cdot \left(\rho_2 e^{i\theta_2}\right) = \left[\rho_1 \rho_2\right] e^{i[\theta_1 + \theta_2]} \quad (1.4)$$

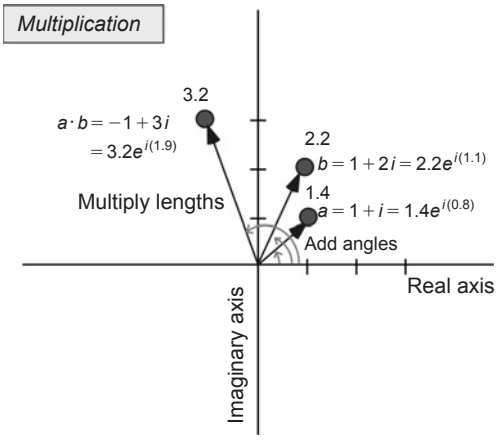

Figure 1.5: Multiplication of Complex Numbers

We took the trouble to introduce all these unreal quantities because they provide a particularly convenient way to represent harmonic signals. Because the *x*- and *y*-components of a unit vector at angle θ are just the cosine and sine, respectively, of the angle, our definition of an exponential with imaginary argument implies

$$e^{i\theta} = \cos(\theta) + i \sin(\theta) \quad (1.5)$$

Thus, if we use for the angle a linear function of time, we obtain a very general but simultaneously compact expression for a harmonic signal:

$$\begin{aligned} e^{i(\omega t + \phi)} &= \cos(\omega t + \phi) + i \sin(\omega t + \phi) \\ &= [\cos(\omega t) + i \sin(\omega t)] \cdot [\cos(\phi) + i \sin(\phi)] \end{aligned} \quad (1.6)$$

In this notation, the signal may be imagined as a vector of constant length rotating in time, with its projections on the real and imaginary axes forming the familiar sines and cosines (Figure 1.6). The phase offset ϕ represents the angle of the vector at $t = 0$.

In some cases we wish to use an exponential as an intermediate calculation tool to simplify phase shifts and other operations, converting to a real-valued function at the end by either simply taking only the real part or adding together exponentials of positive and negative frequency. (The reader may wish to verify, using equations [1.5] and [1.6], that the sum of exponentials of positive and negative frequencies forms a purely real or purely imaginary sinusoid.) However, in radio practice, a real harmonic signal $\cos(\omega t + \phi)$ may also be regarded as being the product of a real carrier $\cos(\omega t)$ and a complex number $\mathrm{I} + i\mathrm{Q} = [\cos(\phi) - i \sin(\phi)]/2$, where the imaginary part is obtained through multiplication with $\sin(\omega t)$ followed by filtering. (Here I and Q denote "in-phase" and "quadrature," that is, 90 degrees out of phase, respectively.) We'll have more to say about the uses of such decompositions when we discuss radios in Chapter 3.

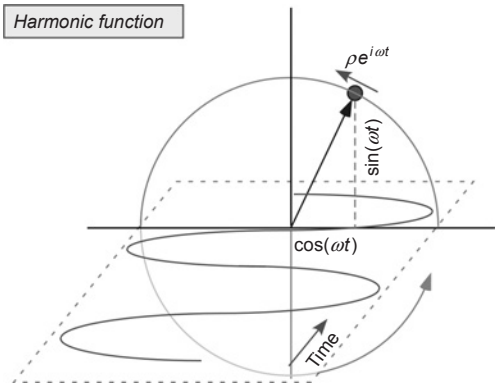

Figure 1.6: An Imaginary Exponential Can Represent Sinusoidal Voltages or Currents

Finally, we note one other uniquely convenient feature of exponentials: differentiation and integration of an exponential with a linear argument simply multiply the original function by the constant slope of the argument:

$$\frac{d}{dx}(e^{ax}) = ae^{ax} \qquad \int e^{ax}\,dx = \frac{1}{a}e^{ax} \quad (1.7)$$

1.2 Electromagnetic Waves and Multiplexing

Now that we are armed with the requisite tools, let us turn our attention to the main topic of our discussion: the use of electromagnetic waves to carry information. An electric current element **J** at some location [1] induces a potential **A** at other remote locations, such as [2]. If the current is harmonic in time, the induced potential is as well. The situation is depicted in Figure 1.7.

The magnitude of the induced potential falls inversely as the distance and shifts in phase relative to the phase of the current. (The reader may wish to verify that the time dependence of **A** is equivalent to a delay by r/c.) The induced potential in turn may affect the flow of electric current at position [2], so that by changing a current **J**[1] we create a delayed and attenuated but still detectable change in current **J**[2]: we can potentially communicate between remote locations by using the effects of the electromagnetic disturbance **A**.

In principle, every current induces a potential at every location. It is this universality of electromagnetic induction that leads to a major problem in using electromagnetic waves in communications. The potential at our receiver, **A**, can be regarded as a medium of communications that is shared by every possible transmitter **J**. How do we detect only the signal we are interested in?

The sharing of a communications channel by multiple users is known as *multiplexing*. There are a number of methods to successfully locate the signals we wish to receive and reject others.

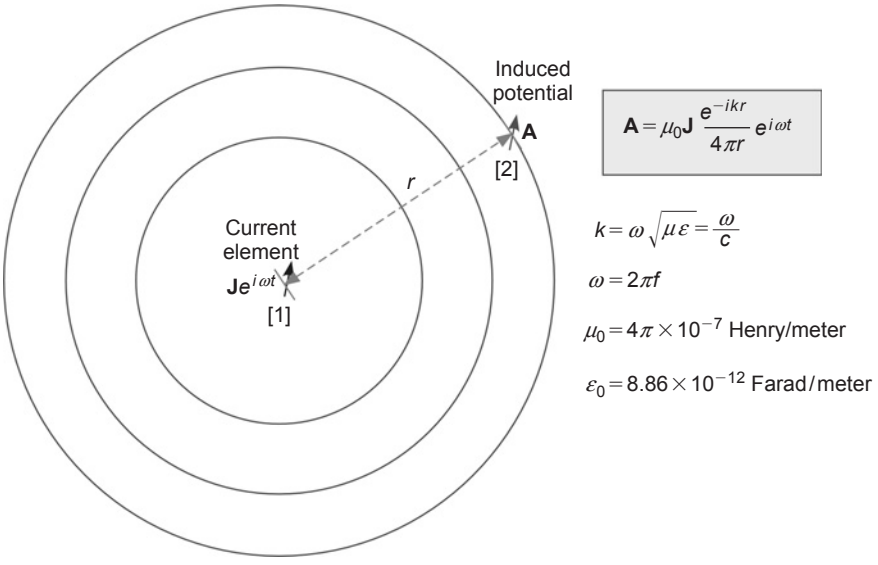

Figure 1.7: A Harmonic Current at [1] Induces a Harmonic Potential at [2]

A few important examples are the following:

- *Frequency-division multiplexing*: only receive signals with a given periodicity and shape (sinusoidal, of course).
- *Spatial multiplexing*: limit signals to a specific geographical area. Recall that induced potentials fall off as (1/distance) in the ideal case, and in practice attenuation of a signal with distance is often more rapid due to obstacles of various kinds. Thus, by appropriate choice of signal power, location, and sensitivity, one can arrange to receive only nearby signals.
- *Time-division multiplexing*: limit signals to a specific set of time slots. By appropriate coordination of transmitter and receiver, only the contents of the desired time slot will be received.
- *Directional multiplexing*: only listen to signals arriving from a specific angle. This trick may be managed with the aid of antennas of high directivity.
- *Code-division multiplexing*: only listen to signals multiplied by specific code. Rather in the fashion that we can listen to a friend's remarks even in a crowded and noisy room, in code-division multiplexing we select a signal by the pattern it obeys. In practice, just as in conversation, to play such a trick it is necessary that the desired signal is at least approximately equal to other undesired signals in amplitude or power, so that it is not drowned out before we have a chance to apply our pattern-matching template.

In real communications systems, some or all of these techniques may be simultaneously used, but almost every modern wireless system begins with frequency-division multiplexing by transmitting its signals only within a certain frequency band. (We briefly examine the major exception to this rule, ultrawideband communications, in section 1.5.) We are so accustomed to this approach that we often forget how remarkable it is: the radio antenna that provides us with music or sports commentary at 105 MHz is also exposed to AM signals at hundreds to around a thousand kHz, broadcast television at various frequencies between 50 and 800 MHz, aeronautical communications at 108–136 MHz, public safety communications at 450 MHz, cellular telephony at 880 and 1940 MHz, and cordless telephones, wireless local area networks (WLANs), and microwave ovens in the 2400-MHz band, to name just a few.

All these signals can coexist harmoniously because different frequencies are *orthogonal*. That is, let us choose a particular frequency, say ω_c, that we wish to receive. To extract only the part of an incoming signal that is at the desired frequency, we multiply the incoming unknown signal $s(t)$ by a sine or cosine (or more generally by an exponential) at the *wanted* frequency ω_c and add up the result for some time—that is, we integrate over a time interval T, presumed long compared with the periodicity $1/f$ (equation [1.8]). The reader may recognize in equation [1.8] the *Fourier cosine transform* of the signal s over a finite domain. A similar equation may be written for the sine, or the two can be combined using an imaginary exponential.

$$\tilde{S}(\omega_c) = \frac{1}{T}\int_0^T s(t)\cos(\omega_c t)dt \quad (1.8)$$

If $s(t)$ is another signal at the same frequency, the integral will wiggle a bit over each cycle but accumulate over time (Figure 1.8).

On the other hand, if the unknown signal is at a different frequency, say $(\omega_c + \delta)$, the test and unknown signals may initially be in phase, producing a positive product, but over the course

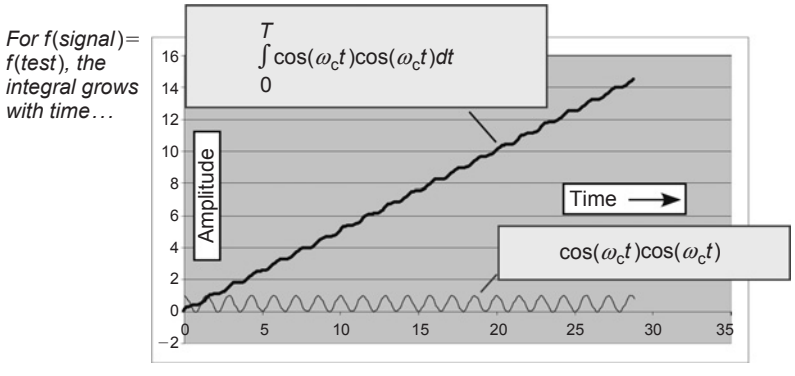

Figure 1.8: Unknown Signal at the Same Frequency as Wanted Signal

of some time they will drift out of phase, and the product will change signs (Figure 1.9). Thus, the integral will no longer accumulate monotonically, at least over times long compared with the difference period ($1/\delta$) (Figure 1.10); when we divide by T and allow T to become large, the value of $S(\omega_c)$ will approach zero.

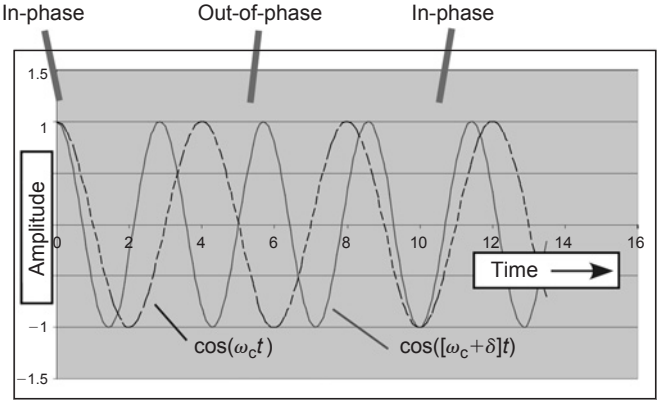

Figure 1.9: Two Signals at Different Frequencies Do Not Remain in Phase

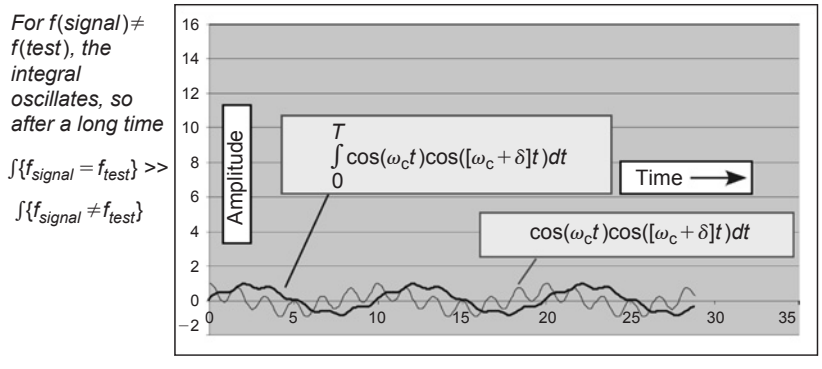

Figure 1.10: Unknown Signal at a Different Frequency from Wanted Signal

Any signal that is periodic in time can be regarded as being composed of sinusoids of differing frequencies: in more formal terms we can describe a signal either as a function of time or as a function of frequency by taking its Fourier transform (i.e., by performing the integration [1.8] for each frequency ω_c of interest.) The orthogonality of those differing frequencies makes it possible to extract the signal we want from a complex mess, even when the wanted signal is small compared with the other stuff. This operation is known generally as *filtering*. A simple example is shown in Figure 1.11. It is generally very easy when the frequencies are

widely separated, as in Figure 1.11, but becomes more difficult when frequencies close to the wanted frequency must be rejected. We examine some of the means to accomplish this task for WLAN radios in Chapter 3.

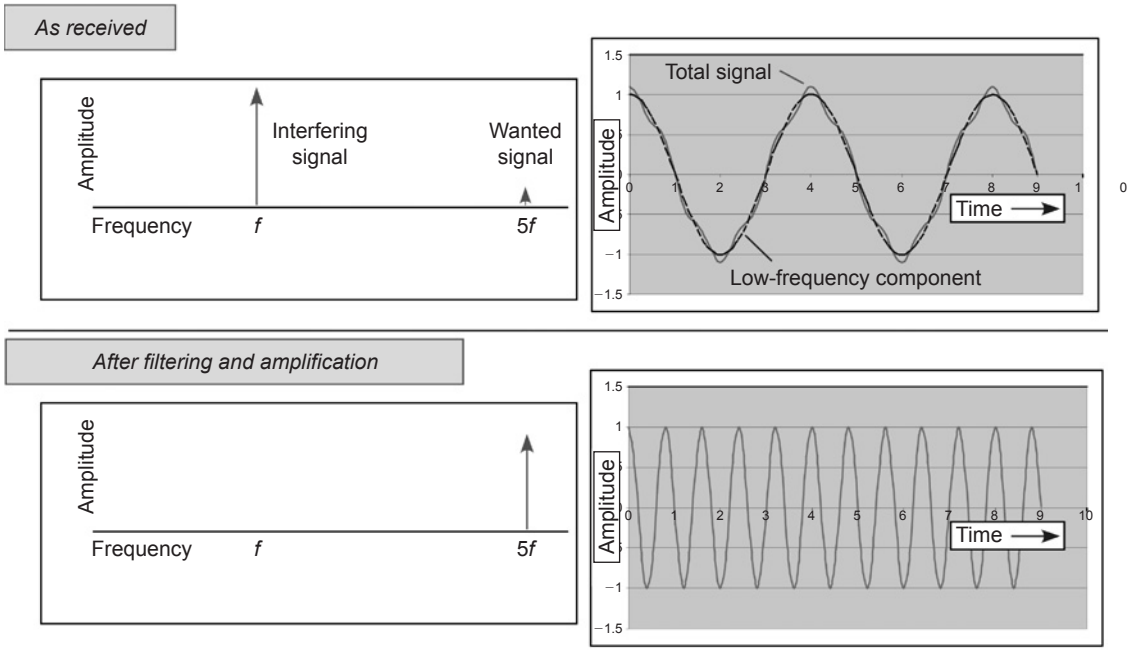

Figure 1.11: Extraction of a Wanted Signal in the Presence of a Large Unwanted Signal

1.3 Modulation and Bandwidth

1.3.1 Simple Modulations

So far the situation appears to be quite rosy. It would appear that one could communicate successfully in the presence of an unlimited number of other signals merely by choosing the appropriate frequency. Not surprisingly, things are not so simple: a single-frequency signal that is always on at the same phase and amplitude conveys no information. To actually transmit data, some aspect of our sinusoidal signal must change with time: the signal must be *modulated*. We can often treat the modulation as a slowly varying function of time (slow being measured relative to the carrier frequency) multiplying the original signal.

"slowly" varying modulation function — sinusoidal vibration at carrier frequency

$$f(t) = m(t)\cos(\omega_c t) \tag{1.9}$$

A simple example of a modulated signal may be obtained by turning the carrier on and off to denote, for example, 1 and 0, respectively: that is, $m(t) = 1$ or 0. This approach is known as *on–off keying* or OOK (Figure 1.12). OOK is no longer widely used in wireless communications, but this simple modulation technique is still common in fiber optic signaling.

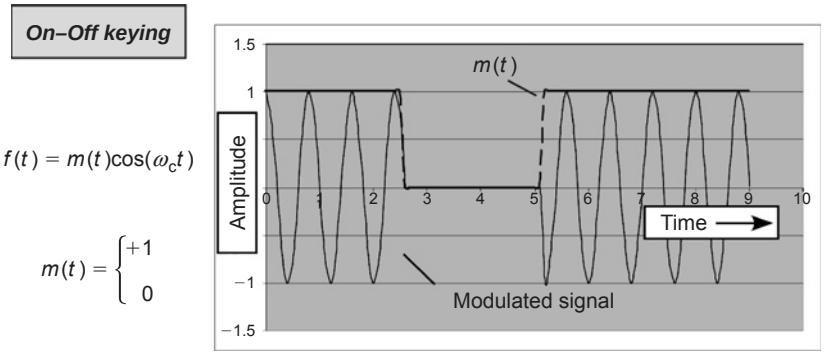

Figure 1.12: Modulation by Turning the Carrier On or Off

A key consequence of imposing modulation on a signal at a frequency ω_c is the inevitable appearance of components of the signal at *different frequencies* from that of the original carrier. The perfect orthogonality of every unique frequency present in the case of unmodulated signals is lost when we actually transmit data. Let us examine how this comes about for the particularly simple case of a sinusoidal modulation, $m = \cos(\omega_m t)$. Recall that the orthogonality of two different frequencies arose because contributions to the average from periods when the two signals are in phase are canceled by the periods when the signals are out of phase (Figure 1.9). However, the modulated signal is turned off during the periods when it is out of phase with the test signal at the different frequency $(\omega_c + \delta)$ so the contribution from these periods no longer cancels the in-phase part (Figure 1.13). The modulated carrier at (ω_c) is now detected by a filter at frequency $(\omega_c + \delta)$.

The astute reader will have observed that this frustration of cancellation will only occur when the frequency offset δ is chosen so as to ensure that only the out-of-phase periods are suppressed. In the case of a periodic modulation, the offset must obviously be chosen to coincide with the frequency of the modulation: $|\delta| = \omega_m$. In frequency space, a modulated carrier at frequency f_c acquires power at sidebands displaced from the carrier by the frequency of the modulation (Figure 1.14).

In the case of a general modulating signal $m(t)$, with Fourier transform $M(\omega)$, it can be shown that the effect of modulation is to translate the spectrum of the modulating or *baseband* signal up to the carrier frequency (Figure 1.15).

We can now see that data-carrying signals have a finite bandwidth around their nominal carrier frequency. It is apparent that to pursue our program of frequency-division multiplexing of

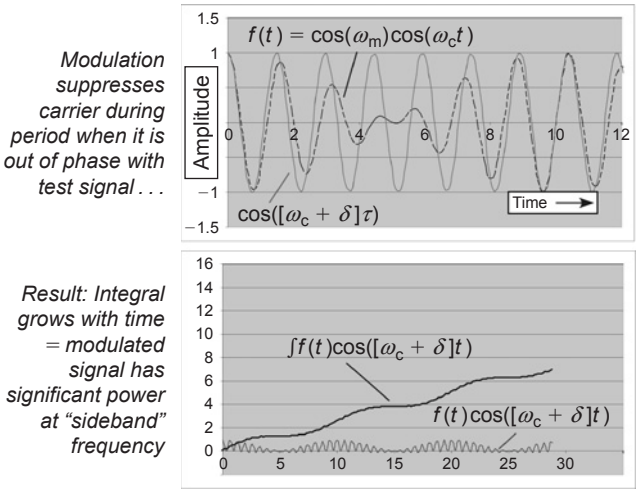

Figure 1.13: A Modulated Signal Is No Longer Orthogonal to All Other Frequencies

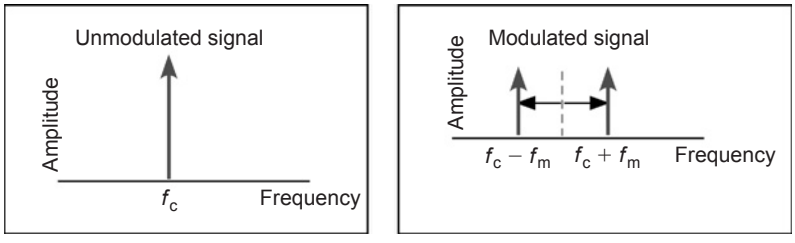

Figure 1.14: Modulation Displaces Power From the Carrier to Sidebands

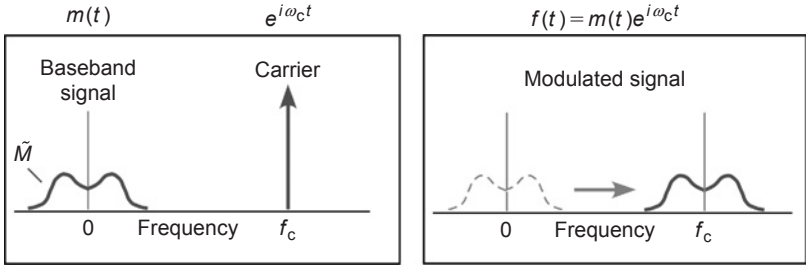

Figure 1.15: The Spectrum of a Carrier Modulated by a General Signal *m*(*t*)

signals, we shall need to allocate bands of spectrum to signals in proportion to the bandwidth those signals consume. Although the spectrum of a random sequence of bits might be rather more complex than that of a simple sinusoid, Figure 1.14 nevertheless leads us to suspect that the faster we modulate the carrier, the more bandwidth we will require to contain the resulting sidebands. More data require more bandwidth (Figure 1.16).

It would seem at first glance that the bandwidth required to transmit is proportional to the data rate we wish to transmit and that faster links always require more bandwidth. However, note

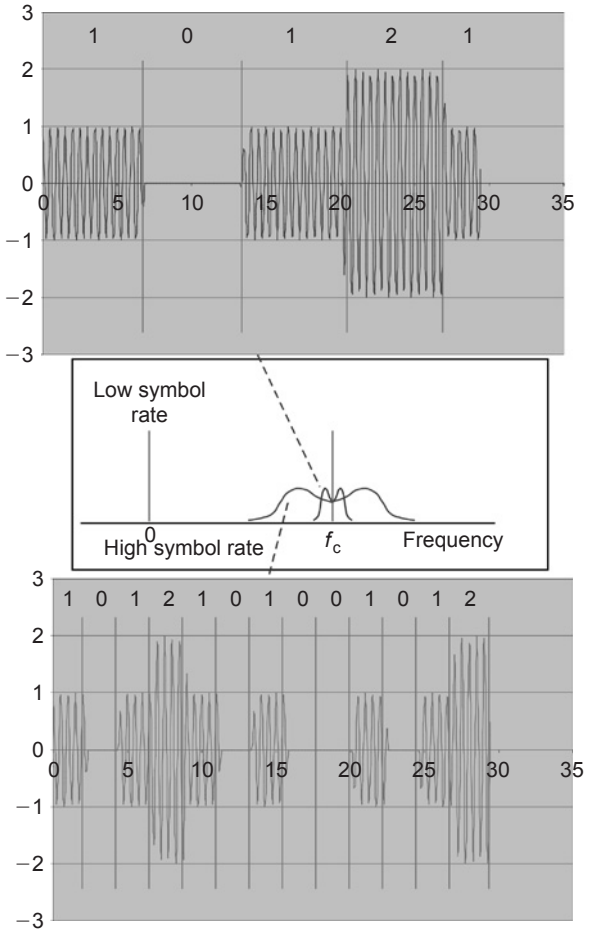

Figure 1.16: Faster Symbol Rate = More Bandwidth

that in Figure 1.16 we refer not to the bit rate but to the *symbol* rate of the transmitted signal. In the case shown, a symbol is one of three possible amplitudes, corresponding to a data value of 0, 1, or 2: this is an example of amplitude-shift keying (ASK), a generalization of OOK. (Note that in this and other examples we show abrupt transitions between different states of the carrier; in practice, the transitions are smoothed to minimize the added sidebands.) Each symbol might be said to contain 3/2 bit. The bit rate is thus 1.5 (symbol rate). More generally, we can envision a number of approaches to sending many bits in a single symbol. For example, we could use more amplitudes: if 8 amplitudes were allowed, one could transmit 3 bits in each symbol. Because the width of the spectrum of the modulating signal is mainly dependent on the rate at which transitions (symbols) occur rather than exactly what the transition is, it is clear that by varying the modulation scheme, we could send higher data rates without necessarily expanding the bandwidth consumed.

We can nevertheless guess that a trade-off might be involved. For example, the use of 8 distinct amplitudes means that the difference between (say) a "3" and a "4" is smaller than the difference between an OOK "1" and "0" for the same overall signal power. It seems likely that the more bits we try to squeeze into a symbol, the more vulnerable to noise our signal will become.

With these possibilities in mind, let us examine some of the modulation schemes commonly used in data communications. The first example, in Figure 1.17, is our familiar friend OOK. Here, in addition to showing the time-dependent signal, we have shown the allowed symbols as points in the phase/amplitude plane defined by the instantaneous phase and amplitude of the signal during a symbol. The error margin shows how much noise the receiver can tolerate before mistaking a 1 for a 0 (or vice versa).

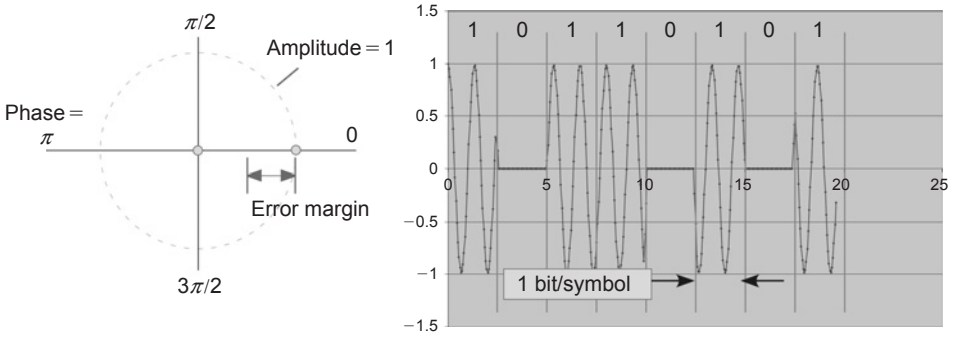

Figure 1.17: On–Off Keying (OOK)

Note that although we have shown the 1 symbol as a single point at a phase of 0 and amplitude 1, a symbol at any other phase—that is, any point on the circle *amplitude* = 1—would do as well. OOK is relatively easy to implement because the transmitter doesn't need to maintain a constant phase but merely a constant power when transmitting a 1 and the receiver needs merely to detect the signal power, not the signal phase. On the down side, OOK only sends one bit with each symbol, so an OOK-modulated signal will consume a lot of bandwidth to transmit signals at a high rate.

As we mentioned previously, we might add more amplitudes to get more data: ASK (Figure 1.18). The particular example in Figure 1.18 has four allowed amplitudes and is denoted 4ASK. Once again we have collapsed the allowed states onto points for clarity but with the understanding that any point on, for example, the 2/3 circle will be received as (10), etc. 4ASK allows us to transmit 2 bits per symbol and would be expected to provide twice the data rate of OOK with the same bandwidth (or the same data rate at half the bandwidth). However, the margin available before errors in determining what symbol has been received (i.e., before symbol errors occur) is obviously much smaller than in the case of OOK. 4ASK cannot tolerate as much noise for a given signal power as can OOK.

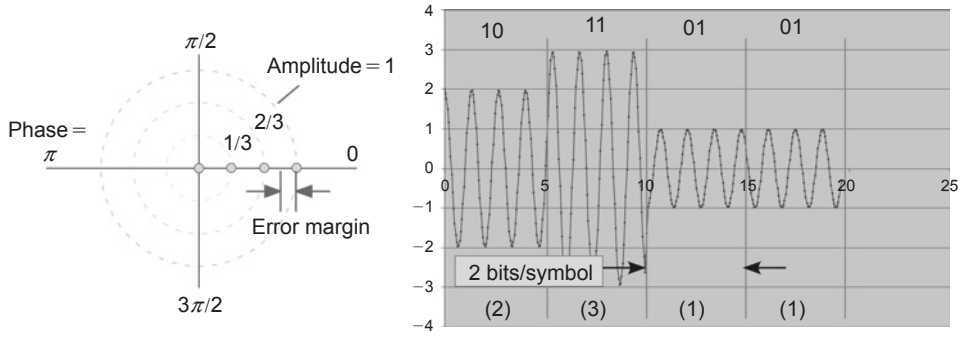

Figure 1.18: 4-Amplitude-Shift Keying (4ASK)

Although it is obviously possible to keep adding amplitudes states to send more bits per symbol, it is equally apparent that the margin for error will decrease in inverse proportion to the number of amplitude states. A different approach to increasing the number of states per symbol might be useful: why not keep track of the phase of the signal?

The simplest modulation in which phase is used to distinguish symbols, binary phase-shift keying (BPSK), is depicted in Figure 1.19. The dots in the figure below the binary symbol values are placed at constant intervals; a 1 is transmitted with the signal peaks coincident with the dots, whereas a 0 has its peaks between dots: 180 degrees or π radians out of phase. In phase-shift keying, the nominal symbols are points in the phase plane rather than circles: the group of points is known as a signal constellation. However, as long as the signal is large enough for its phase to be determined, the signal amplitude has no effect: that is, any received signal on the right half of the phase-amplitude plane is interpreted as a 1 and any signal on the left half is interpreted as 0. The error margin is thus equal to the symbol amplitude and is twice as large as the error margin in OOK for the same peak power. BPSK is a robust modulation, resistant to noise and interference; it is used in the lowest rate longest range states of 802-11 networks.

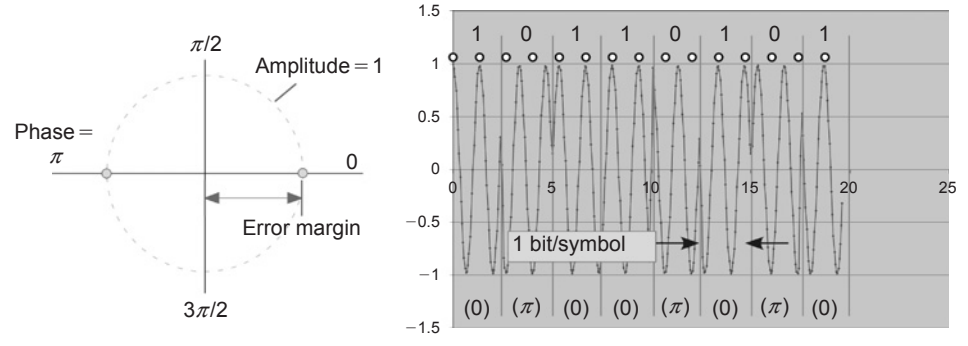

Figure 1.19: Binary Phase-Shift Keying (BPSK)