Encyclopedia of Internet Technologies and Applications

Mario Freire
University of Beira Interior, Portugal

Manuela Pereira
University of Beira Interior, Portugal

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Sara Reed
Copy Editor: Larissa Vinci and Mike Goldberg
Typesetter: Amanda Appicello and Jeffrey Ash
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of Internet technologies and applications / Mario Freire and Manuela Pereira, editors.
p. cm.
Summary: "This book is the single source for information on the world's greatest network, and provides a wealth of information for the average Internet consumer, as well as for experts in the field of networking and Internet technologies. It provides the most thorough examination of Internet technologies and applications for researchers in a variety of related fields"--Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-59140-993-9 (hardcover) -- ISBN 978-1-59140-994-6 (ebook)
1. Internet--Encyclopedias. I. Freire, Mário Marques, 1969- II. Pereira, Manuela.
TK5105.875.I57E476 2007
004.67'803--dc22
2007024949

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Wi-Fi Technology

Antonios Alexiou
Research Academic Computer Technology Institute and University of Patras, Greece

Dimitrios Antonellis
Research Academic Computer Technology Institute and University of Patras, Greece

Christos Bouras
Research Academic Computer Technology Institute and University of Patras, Greece

INTRODUCTION

Wi-Fi, short for "wireless fidelity," is a term for certain types of **wireless local area network (WLAN)** that use specifications in the 802.11 family. In general, the wireless technologies are used for the replacement or the expansion of the common wired **networks**. They possess all the functionality of wired LANs but without the physical constraints of the wire itself. The wireless nature inherently allows easy implementation of broadcast/multicast services. When used with portable computing devices (e.g., notebook computers), wireless LANs are also known as cordless LANs because this term emphasizes the elimination of both power cord and network cable (Tanenbaum, 2003).

Wi-Fi sprang into existence as a result of a decision in 1985 by the Federal Communications Commission (FCC) to open several bands of the wireless spectrum for use without a government license. To operate in these bands though, devices would be required to use "spread spectrum" technology. This technology spreads a **radio signal** out over a wide range of frequencies, making the signal less susceptible to interference and difficult to intercept. In 1990, a new IEEE committee, called 802.11, was set up to look into getting a standard started. It was not until 1997, that this new standard was published (though pre-standard devices were already shipping).

Two variants were ratified over the next two years—802.11b, which operates in the Industry, Medical, and Scientific (ISM) band of 2.4 GHz and 802.11a, which operates in the Unlicensed National Information Infrastructure bands of 5.3 GHz and 5.8 GHz. Wi-Fi's popularity really took off with the growth of high-speed broadband Internet access in the home. It was, and remains, the easiest way to share a broadband link between several computers spread over a home. The growth of hotspots, free and fee-based public access points, have added to Wi-Fi's popularity. The latest variant was 802.11g (WiFi-Forum, 2006).

The first version of **IEEE 802.11** provides data rates up to 2 Mbps, while now there is a set of relevant protocols such as IEEE 802.11a, IEEE 802.11b, IEEE 802.11e, IEEE 802.11f, IEEE 802.11g, and IEEE 802.11i. The most popular of these are the 802.11b and the 802.11g that use the frequency of 2.4 GHz, and the 802.11a, which uses the frequency of 5GHz. Additionally, the 802.11b specification provides a bandwidth rating of 11 Mbps, while 802.11a and 802.11g offer higher performance, providing a maximum bandwidth of 54Mbps, almost five times that of 802.11b. Furthermore, the performance of both the 802.11 families decreases as the distance from the antenna increases.

The 802.11 standard specifies wireless connectivity for fixed, portable, and moving clients in a limited geographic area. Specifically, it defines an interface between a wireless client and an access point, as well as among wireless clients. As in any 802 LAN standard, such as 802.3 (Ethernet) and 802.5 (Token Ring), the 802.11 standard specifies data rates of at least 1 Mbit/s and defines only the **physical (PHY)** and **medium access control (MAC) layers**, which correspond to the first two layers of the Open System Interconnect (OSI) network hierarchy. However, the 802.11 MAC layer also performs functions that are usually associated with higher-layer protocols. These additional functions allow the 802.11 MAC layer to conceal the unique characteristics of the wireless PHY layer from higher layers.

BACKGROUND

As Wikipedia LAN (2006) refers, a local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings, such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology, running at 10 to 10000 Mbit/s. The defining characteristics of LANs, in contrast to WLANs, are: (a) much higher data rates, (b) smaller geographic range—at most a few kilometers—and (c) the fact that they do not involve leased telecommunication lines. "LAN" usually does not refer to data running over local analog telephone lines, as on a private branch exchange (PBX).

Additionally, in the wireless LANs (WLANs), there is the opportunity for the wireless transfer of the data. More specifically, as Wikipedia WLAN (2006) mentions, a wireless LAN, or WLAN, is a wireless local area network that uses radio waves as its carrier: The last link with the users is wireless, to give a network connection to all users in the surrounding area. Areas may range from a single room to an entire campus. The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network.

As mentioned above, the Wi-Fi is one of the technologies that are used in the WLANs. Therefore, the three most popular protocols of the 802.11 technology have a number of differences that are presented in Table 1.

WI-FI TECHNOLOGY

Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels: the OSI model, the Physical Layer, and Data Link Layer (Figure 1). Any LAN application, network operating system, or protocol will run on an 802.11-compliant WLAN as easily as they run over Ethernet (IEEE 802.11 (2006)).

The 802.11-based networks consist of the following logical units:

- **Access point (AP):** The AP functions as a gateway between the wired and the wireless network.
- **Distribution system (DS):** The distribution system merges the APs of the network and users that are served from different APs and are reachable by the entire network.
- **Wireless medium:** Many physical layers have been assigned that use microwaves for the transmission of the packets among the APs.
- **Stations:** The stations that exchange information through the wireless network are mostly mobile devices.

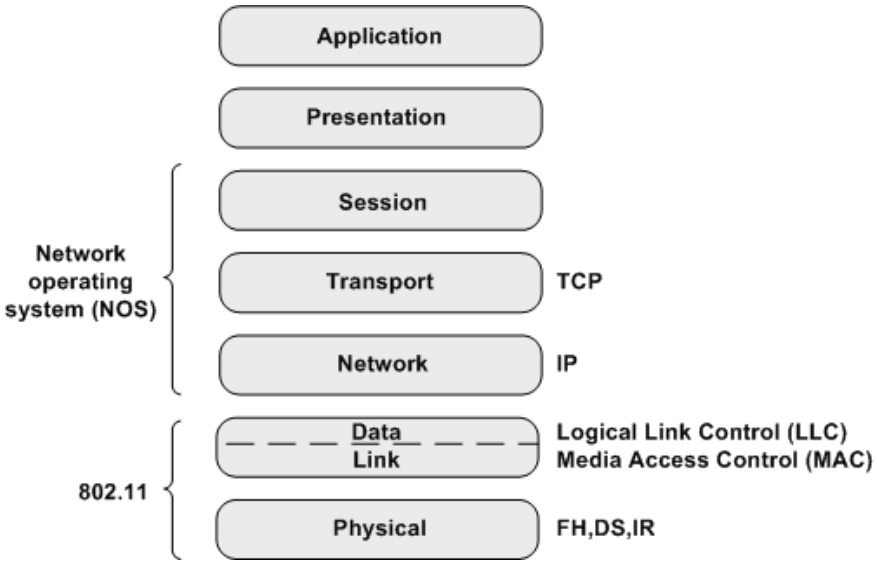
More specifically, when two or more stations come together to communicate with each other, they form a basic service set (BSS). The minimum BSS consists of two stations; 802.11 LANs use the BSS as the standard building block. A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS), or is referred to as an ad-hoc network. An ad-hoc network is a network where stations communicate only peer-to-peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-hoc or IBSS networks are characteristically limited, both temporally and spatially (Wikipedia Wi-Fi Technology (2006)).

When BSSs are interconnected, the network becomes one with infrastructure. The 802.11 infrastructure has several elements. Two or more BSSs are intercon-

Table 1. Comparison of Wi-Fi technologies

Wireless Standard	802.11b	802.11g	802.11a
Max speed	11 Mbps	54 Mbps	54 Mbps
Max encryption	128 bit WEP	128 bit WEP	152 bit WEP 256 bit AES
Discrete channels	3	3	8
Max range full throughput	~30 ft.	~20 ft.	~10 ft.
Natively compatible	802.11b, 802.11g	802.11b, 802.11g	802.11a
Potential user	Entry level and home networks	Larger networks, small business	Large businesses concerned with security

Figure 1. IEEE 802.11 and the OSI model



nected using a distribution system (DS). This concept of a DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of access points. An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points. Creating large and complex networks using BSSs and DSs leads us to the next level of hierarchy, namely extended service set (ESS). The interesting point in the ESS is that the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSSs transparently to the LLC.

Unless adequately protected, a Wi-Fi network can be susceptible to access by unauthorized users who use the access as a free Internet connection. The first, and most commonly used, wireless encryption standard, wired equivalent privacy (WEP), has been shown to be easily breakable even when correctly configured. Most wireless products now on the market support the Wi-Fi protected access (WPA) encryption protocol, which is considered much stronger, though some older access points have to be replaced to support it. The adoption of the 802.11i standard (marketed as WPA2) makes available a rather better security scheme—when properly configured. The new versions of the popular operating systems support the WPA2. While waiting for better standards to be available, many enterprises have chosen to deploy additional layers of encryption (such as VPNs) to protect against interception. Some report that interference of a closed or encrypted access point with other open access points on the same or a neighboring channel can prevent access to the open access points by others in the area. This can pose a problem in high-density areas, such as large apartment buildings where many residents are operating Wi-Fi access points (Wi-Fi Technology, 2006).

WI-FI NETWORK SECURITY

Much attention has been focused recently on the **security aspects** of existing 802.11b wireless LAN systems. This occurs because unlike cables, radio signals are easily exposed and cannot be physically contained. Additionally, the broadcast nature of wireless LANs makes it difficult to protect such LANs from unauthorized access. Thus, many ways to prevent unauthorized access are applied (Benny, 2002).

Service Set Identifier (SSID)

One commonly used wireless LAN feature is a naming handle called a service set identifier (SSID), which provides a primitive level of access control. More specifically, before associating with a particular access point (AP), users are required to enter the AP's SSID together with a password. Unfortunately, the SSID is regularly broadcast by the AP and can easily be detected. Thus,

better approaches to the issue of the wireless networks' security have been adopted (Tan & Bing, 2003).

Wired Equivalent Privacy (WEP)

WEP is part of the IEEE 802.11 standard ratified in September 1999. It uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Standard 64-bit WEP uses a 40-bit key, to which a 24-bit initialization vector (IV) is concatenated to form the RC4 traffic key. At the time that the original WEP standard was being drafted, U.S. Government export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, all of the major manufacturers eventually implemented an extended 128-bit WEP protocol using a 104-bit key size. A 128-bit WEP key is almost always entered by users as a string of 26 Hexadecimal (Hex) characters (0-9 and A-F). Each character represents four bits of the key (4 * 26 = 104 bits). Adding the 24-bit IV brings us what we call a "128-bit WEP key." A 256-bit WEP system is available from some vendors, and as with the above-mentioned system, 24 bits of that is for the IV, leaving 232 actual bits for protection. This is typically entered as 58 Hexadecimal characters (58 * 4 = 232 bits) + 24 IV bits = 256 bits of WEP protection (Wikipedia WEP (2006)).

Key size is not the major security limitation in WEP. Cracking a longer key requires interception of more packets, but there are active attacks that stimulate the necessary traffic. There are other weaknesses in WEP, including the possibility of IV collisions and altered packets that are not helped at all by a longer key. Thus, WEP is said to be easily broken, although a substantial amount of data have to be collected before a wireless network can be cracked successfully. Note, however, that using readily-available and downloadable tools, WEP networks can be cracked within minutes (Webopedia WEP, 2006).

Wi-Fi Protected Access (WPA)

Certifications for implementations of WPA started in April 2003 and became mandatory in November 2003. The full 802.11i was ratified in June 2004. WPA is designed for use with an 802.1X authentication server, which distributes different keys to each user; however, it can also be used in a less secure "pre-shared key" (PSK) mode (Wi-Fi Alliance, 2006). The newer version of WPA is the WPA2, whose product certification is available through the Wi-Fi Alliance certifying wireless equipment as being compatible with the 802.11i standard. The goal of WPA2 certification is to support the additional mandatory security features of the 802.11i standard that are not already included for products that support WPA.

In WPA, data are encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit IV. One major improvement in WPA over WEP is the temporal key integrity protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger IV, this defeats the well-known key recovery attacks on WEP. In addition to authentication and encryption, WPA also provides vastly improved payload integrity. The cyclic redundancy check (CRC) used in WEP is inherently insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key.

WPA was formulated as an intermediate step towards improved 802.11 security for two reasons: first, 802.11i's work lasted far longer than originally anticipated, spanning four years, during a period of ever-increasing worries about wireless security; second, it encompasses as a subset of 802.11i-only elements that were backwards compatible with WEP for even the earliest 802.11b adopters. WPA firmware upgrades have been provided for the vast majority of wireless network interface cards shipped; 802.11 access points sold before 2003 generally needed to be replaced. By increasing the size of the keys and IVs, reducing the number of packets sent with related keys, and adding a secure message verification system, WPA makes breaking into a wireless LAN far more difficult (Wi-Fi Planet, 2006).

FUTURE TRENDS

Even with the progress in the wireless technology, what has been missing is a universal wireless technology with the performance to connect consumer electronic multimedia products. To actually deliver on consumer expectations, wireless technologies need to be significantly faster than what is currently available today, while at the same time managing to be power-efficient during operation (UWB Forum, 2006).

To meet these demands, pioneers in the industry, working through the IEEE, turned to **ultra wideband**

(UWB) technology. Scalable in performance from 100Mbps to over 2Gbps, certain UWB systems will deliver secure wireless connections between high-quality multimedia products that are not susceptible to interference and breaks in performance. The usefulness of UWB will not just end with high-quality multimedia. Its raw high-speed performance will enable wireless to finally deliver on true device synchronization. Unlike conventional wireless systems which use narrowband modulated carrier waves to transmit information, UWB transmits over a wide swath of radio spectrum, using a series of very narrow and low-power pulses. The combination of broader spectrum, lower power, and pulsed data means that UWB causes significantly less interference than conventional narrowband radio solutions while safely coexisting with other wireless technologies on the market (Intel UWB, 2006).

Another technology that is related to the Wi-Fi technology and is currently evolved is the **WiMAX** technology. From a technical perspective, WiMAX and Wi-Fi are two different things. Unlike Wi-Fi, WiMAX requires a network plan and sites for base-station antennas. Additionally, WiMAX offers not only more range, but also more bandwidth. While Wi-Fi solutions can broadcast up to 100 meters (330 feet) with a maximum of 54 megabits per second (Mbps), WiMAX has a range of up to 50 kilometers (30 miles) with a transmission speed of about 70 Mbps—under certain conditions. WiMAX is a shared medium, which means that the capacity is spread over all users in a radio cell. The speed also drops as the user's distance from the base station increases.

CONCLUSION

In this article, the Wi-Fi technology was presented. As has been shown, wireless technologies are used for the replacement or the expansion of the common wired networks. The first version of IEEE 802.11 provides data rates up to 2 Mbps, while there is a set of available relevant protocols such as IEEE 802.11a, IEEE 802.11b, IEEE 802.11e, IEEE 802.11f, IEEE 802.11g, IEEE 802.11i. The most popular of these are the 802.11b and the 802.11g that use the frequency of 2.4 GHz, and the 802.11a, which uses the frequency of 5GHz (IEEE 802.11, 2006).

Additionally, much attention has been focused recently on the security aspects of existing 802.11 wireless LAN systems. This occurs because unlike cables, radio signals are easily exposed and cannot be physically contained. One commonly used wireless LAN feature is a naming handle called a service set identifier (SSID), which provides a primitive level of access control. Unfortunately, the SSID is regularly broadcast by the AP and can easily be detected. Similarly, the wired equivalent privacy (WEP) is unsecured, and hence the Wi-Fi protected access (WPA) was designed so as to improve the security of the wireless networks. As was presented, the future of the wireless networks is the WiMAX and the ultra wideband (UWB) technology, which aims to provide from 100Mbps to over 2Gbps secure wireless connections between high-quality multimedia products that are not susceptible to interference and breaks in performance.

REFERENCES

Bing, B. (2002). *Wireless local area networks: The new wireless revolution.* John Wiley & Sons.

IEEE 802.11 (2006). The working group setting the standards for wireless LANs. Retrieved March 15, 2006, from http://www.ieee802.org/11/Wikipedia

Local Area Network (LAN) (2006). Retrieved March 11, 2006, from http://en.wikipedia.org/wiki/LAN/

Tan, T.K., & Bing, B. (2003). *World wide Wi-Fi: Technological trends and business strategies*. John Wiley & Sons.

Tanenbaum, A.S. (2003). *Computer networks* (4th ed.). Prentice Hall.

UWB (2006). Retrieved March 9, 2006 from, http://www.intel.com/technology/comms/uwb/

UWB Forum (2006). Retrieved March 10, 2006, from http://www.uwbforum.org/Intel

Webopedia WEP (2006). Retrieved March 15, 2006 from, http://www.webopedia.com/TERM/W/WEP.html

WiFi-Forum (2006). Retrieved March 9, 2006, from http://www.wifi-forum.com/Wikipedia Wireless

Wikipedia Wired Equivalent Privacy (WEP) (2006). Retrieved March 10, 2006 from, http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Wi-Fi Alliance (2006). Retrieved March 15, 2006, from http://www.wi-fi.org/

Wi-Fi Planet (2006). Retrieved March 15, 2006, from http://www.wi-fiplanet.com/tutorials/article.php/1368661

Wi-Fi Technology (2006). Retrieved March 10, 2006, from http://www.wi-fitechnology.com/

Wikipedia Wi-Fi Technology (2006). Retrieved March 11, 2006 from, http://en.wikipedia.org/wiki/WiFi/

KEY TERMS

IEEE 802: Standards for the interconnection of LAN computer equipment. They deal with the Data Link Layers of the ISO Reference Model for OSI.

IEEE 802.11: 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

LAN: A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college.

Ultra Wideband (UWB): Ultra wideband (UWB) systems transmit signals across a much wider frequency than conventional systems and are usually very difficult to detect.

WEP: Wired-equivalent privacy (WEP) protocol was specified in the IEEE 802.11 standard and attempts to provide a wireless LAN (WLAN) with a minimal level of security and privacy comparable to a typical wired LAN. WEP encrypts data transmitted over the WLAN to protect the vulnerable wireless connection between users (clients) and access points (APs).

Wi-Fi: Abbreviation of wireless fidelity, standard technology for wireless access to local networks.

WiMAX: The Worldwide Interoperability for Microwave Access (WiMAX) is a certification mark for products that pass conformity and interoperability tests for the IEEE 802.16 standards. IEEE 802.16 is working group number 16 of IEEE 802, specialising in point-to-multipoint broadband wireless access.

WPA: WiFi protected access (WPA) is a fairly new standard for wireless networks and is more secure than WEP.