BU

Bournemouth
University

School of Design, Engineering & Computing

Report on Wi-Fi

File Name	Report Wi-Fi.docx
Revision	V1
Date	April 2011
Author	Keith Amoah

5 Contents

5 Wi-Fi

5.1 Background

Wi-Fi is the name given to short-range wireless broadband technology. In Europe, the maximum power of the transmitter is limited to 100mW in 2.4 and 5 GHz bands.

The IEEE 802.11 standard defines the standards for Wireless Local Area Networks. [501]

Wi-Fi is the commercial name for this class of systems. The Wi-Fi Alliance is an industry-led, not-for-profit organization which has the goal of driving the adoption of a single worldwide standard for high-speed wireless local area networking. [502]

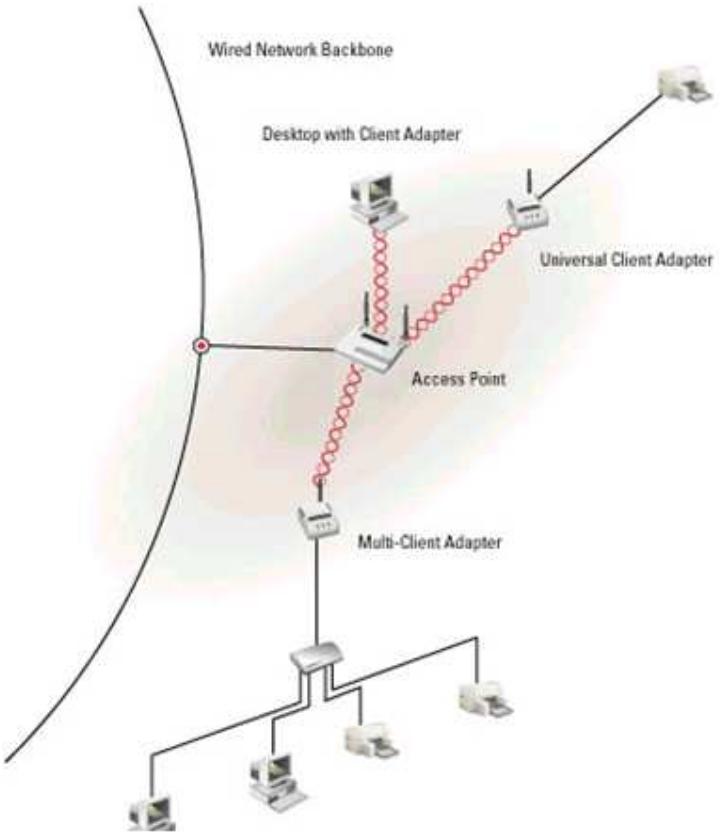

Fig 1 Wireless LANs Source www.bournemouth.ac.uk

5.2 History

In 1985, the Federal Communications Committee (FCC) opened up the frequency 900Hz, 2.4 and 5.8HHz for use without a government licence. These frequencies were known as the "garbage bands" as they were used for things other than just communications i.e. Microwave ovens etc.

In 1988, the company NCR wanted to use the unlicensed band to link its cash registers together. They approached the IEEE about creating a standard similar to 802.3. A new group 802.11 was set up. In 1997, the first basic specification was agreed on and it allowed transfer speeds of 2mbits. Two variants of the standard, 802.11a and 802.11b, were ratified in December 1999 and January 2000 respectively.

Today, the latest standard is 802.11n which, when using 40 MHz of bandwidth with 4 spatial streams, allows for speeds up to 600 $Mbits^{-1}$

5.2.1 Fixed Access

Wi-Fi Standard	Frequency	Bandwidth	Speed
802.11a	5GHz	20Mhz	Up to $54Mbits^{-1}$
802.11b	2.4 GHz	20 MHz	Up to $11Mbits^{-1}$
802.11g	2.4 GHz	20 MHz	Up to $54Mbits^{-1}$
802.11n	2.4, 5 GHz	20 or 40Mhz	Up to $600Mbits^{-1}$

Table 1 802.11 details

5.3 Wi-Fi

5.3.1 Simple Installations

Wireless LAN comprises of

- Wireless Access Points
- Wireless Clients

In the UK, Ofcom limits the maximum equivalent isotropically radiated power (EIRP) from a 2.4GHz Access Point to 100mW [504]. This gives a range in free air of about 100 metres within a building. With walls and furnishings, this is considerably less.

Therefore, single wireless access points are really designed to provide coverage to a small area. In a domestic dwelling, normally the access point is also a router. The range of this access point can be extended by using repeaters near the edge of the range of the primary access point/router.

Wireless Networks can be configured as

- Independent Basic Service Set (often referred to as adhoc , peer to peer relationship)
- Basic Service Set (often referred to as infrastructure, all wireless clients attach to a wireless access point that is broadcasting a SSID)
- Extended Service Set. (this is where multiple APs share the same SID) Clients are able to move seamlessly from one AP to another. Multiple Wireless APs are used where larger coverage or resilience is required.

.

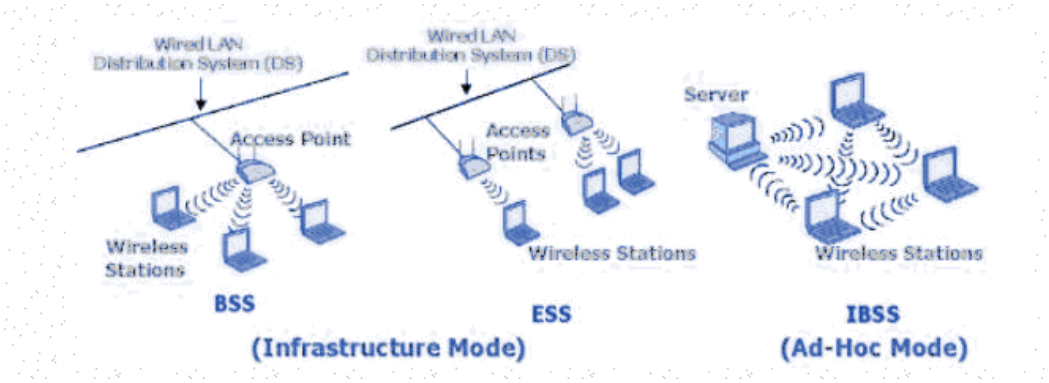

Fig 2 Wireless LAN configurations BSS, ESS and IBSS
Source: www.bournemouth.ac.uk

5.3.2 Sharing the Medium

Wireless is a shared medium so an algorithm called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is required. This means that wireless stations all listen and if all is quiet, back-off for a further random time before transmitting data.

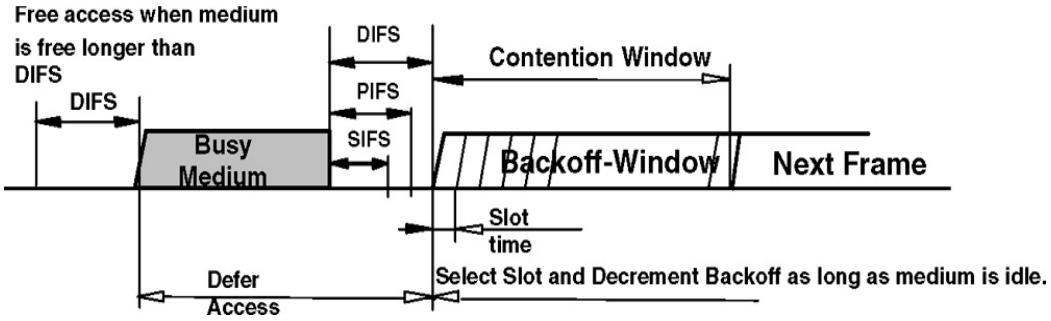

Fig 3 IEEE 802.11 inter-frame space (Prasad and Prasad 2005)

5.3.3 Spectrum

Wi-Fi can operate in 2.4GHz and 5GHz. (5.8GHz). As stated before, it is an unlicensed spectrum.

In Europe, there are 13 overlapping channels in the 2.4 GHz band starting from Channel 1 at 2.412GHz in 5MHz stepping up to Channel 13 at 2472Ghz. (America only uses channels 1->11).

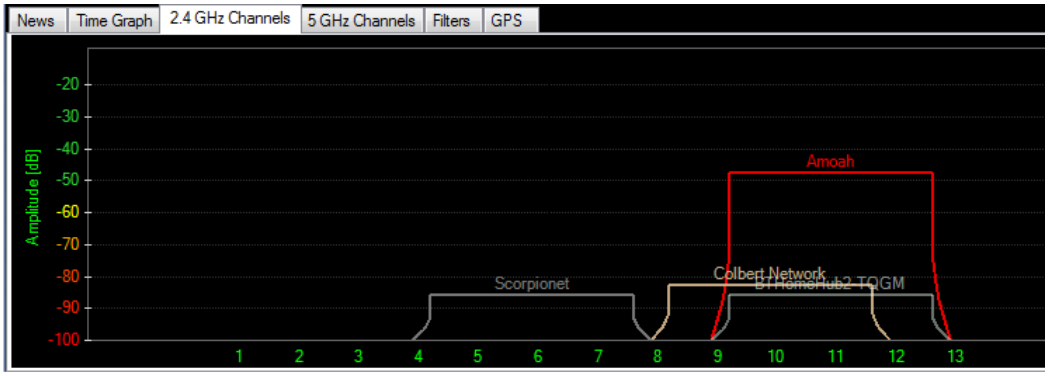

Fig 4 showing 2.4 GHz band with APs using 20 MHz bandwidth

In the UK, the 2.4 GHz Spectrum is more widely used domestically than the 5 GHz spectrum (see figures 1 & 2).

In the 5 GHz band, Europe uses Channels 36, (5.180GHz), 40(5.200 GHz), 44, 48, 52, 56, 64(5.320GHz), 100(5.500GHz), 104, 116, 120, 124, 128, 132, 136(5.680GHz).

Fig 5 showing the 5GHz bandwidth 40 MHz band with AP using channels 36+40

5.3.4 Modulation and Performance

Performance of Wi-Fi depends on

- Whether the equipment is 802.11a, 802.11b, 802.11g, 802.11n

- Signal strength and Quality
  - Distance Wireless Access Point
  - 2.4 or 5GHz (5 GHz less interference but higher attenuation)
- MIMO (spatial Multiplexing)
  - 1x1, 2x2, 4x4

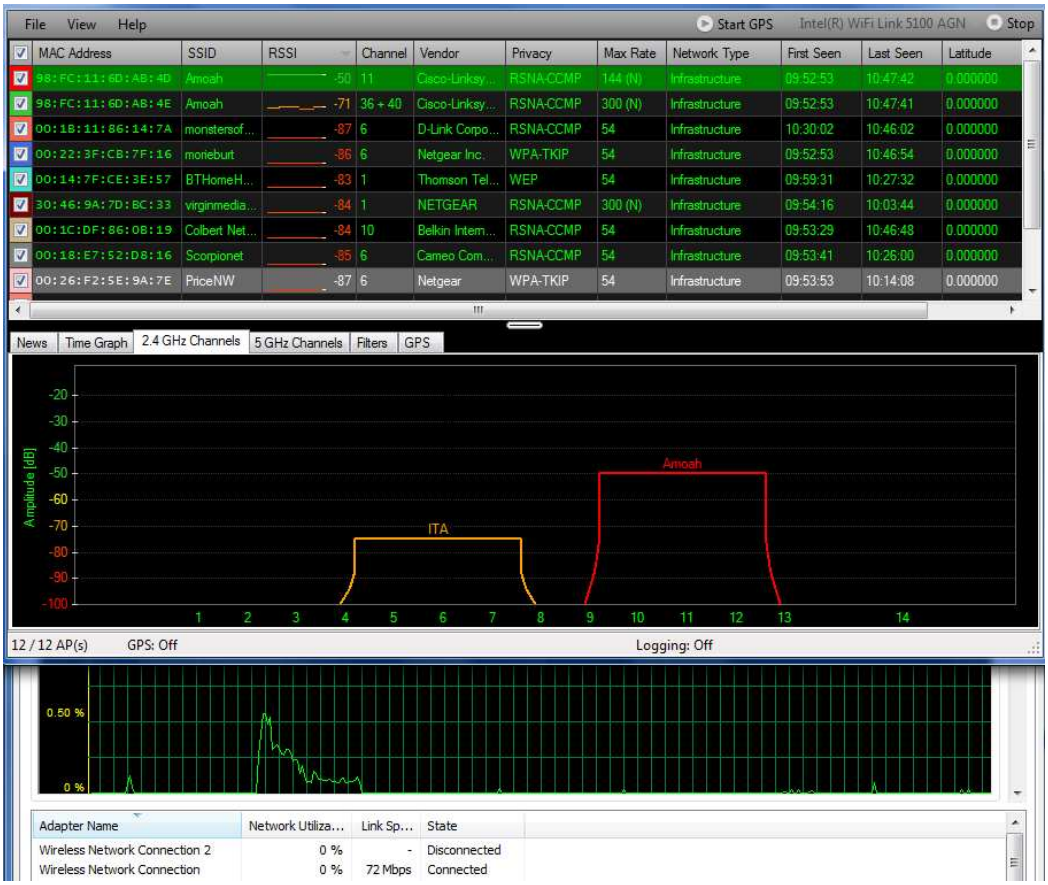

Fig 6 shows connection to WAP Amoah at 72Mbits

Adaptive Modulation

Wi-Fi uses adaptive modulation dynamically adjusting the modulation type of a communication channel based on specific criteria (e.g. signal quality – signal strength, interference and noise), dropping down from 64QAM near the wireless access point down to BPSK at the edge of the access points range.

MIMO

802.11n can use Multiple Input Multiple Output to either increase the throughput through spatial multiplexing or to improve the signal to noise ration.

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1 / 2	1	6.50	7.20	13.50	15.00
1	QPSK	1 / 2	1	13.00	14.40	27.00	30.00
2	QPSK	3 / 4	1	19.50	21.70	40.50	45.00
3	16-QAM	1 / 2	1	26.00	28.90	54.00	60.00
4	16-QAM	3 / 4	1	39.00	43.30	81.00	90.00
5	64-QAM	2 / 3	1	52.00	57.80	108.00	120.00
6	64-QAM	3 / 4	1	58.50	[illegible]	121.50	135.00
7	64-QAM	5 / 6	1	65.00	72.20	135.00	150.00
8	BPSK	1 / 2	2	13.00	[illegible]	27.00	30.00
9	QPSK	1 / 2	2	26.00	28.90	54.00	60.00
10	QPSK	3 / 4	2	39.00	43.30	81.00	90.00
11	16-QAM	1 / 2	2	52.00	57.80	108.00	120.00
12	16-QAM	3 / 4	2	78.00	86.70	162.00	180.00
13	64-QAM	2 / 3	2	104.00	115.60	216.00	240.00
14	64-QAM	3 / 4	2	117.00	130.00	243.00	270.00
15	64-QAM	5 / 6	2	130.00	144.40	270.00	300.00
16	BPSK	1 / 2	3	19.50	21.70	40.50	45.00
...	...	...	...	...	...	...	...
31	64-QAM	5 / 6	4	260.00	288.90	540.00	600.00

Table 2 Modulation schemes Source 802.11n Wireless LAN standard.

From the example in Fig 6 and table 2, it can be seen that the laptop is communicating with the Wireless Access Point using 64-QAM, coding rate 5/6, with 1 spatial stream and 20 MHz Channel.

5.3.5 Security

There are several steps that can be taken to improve the security of wireless LAN.

1. Access List of allowed clients (based MAC address wireless clients)
2. Suppress the broadcasting of the Wireless APs SSID
3. Reduction of Transmit Power (this reduces the range of coverage by AP)
4. Encryption.

Encrypting the communication stream is the main security measure in wireless LANs. In a small wireless network, identical encryption keys are typed in to Wireless Access Point and the user end equipment.

Wired Equivalent Privacy **(WEP)** was the security scheme that was introduced with the original 802.11 standard in 1999. 64-WEP relies on a 40 bit key concatenated with 24 bit initialisation vector to create 64bits. This is passed through an RC4 encrypting algorithm to generate a traffic key. This traffic key is then "exclusively or" with the bit stream to create an encrypted stream.

Unfortunately, WEP had some flaws and can now be compromised so Wi-Fi Protected Access (WPA) was developed. This also used RC4 encryption algorithm so could be deployed with most existing Wi-Fi equipment with a firmware upgrade. WPA introduced temporal Key Integrity Protocol (TKIP) which mixes the Key with the initialisation vector rather than just carrying out concatenation as is the case in WEP.

WPA2, which is more secure than WPA, uses a more secure encryption algorithm AES.

Description	WEP	WEP	WPA-PSK	WPA2-PSK	WPA2-PSK
Key length	64bit	128bit	128bit	128bit	256bit
Encryption Algorithm	RC4	RC4	TKIP+RC4	AES	AES
Level of security					

Figure 7 Domestic Security

The Wi-Fi Alliance which certifies new wireless equipment only wishes to support WPA2 from 2013 [508, 509]. This means if your Wireless Access Point goes faulty and you have to replace it, it will only support WPA2. If your wireless clients do not support this, they will have to be replaced also.

Description	WEP	WEP	WPA-PSK	WPA2-PSK	WPA2-PSK
Key length	Dt	128bit	128bit	128bit	256bit
Encryption Algorithm	RC4	RC4	TKIP+RC4	AES	AES
Level of security	WEP and WPA will no longer be supported in new equipment from 2013			Only supported form of encryption for new equipment from 2013	

Fig 8 Retirements of WEP and WPA

5.3.6 Enterprise Installations.

Even with high gain antennae the range of wireless AP is limited. In order to cover large factory floors and to provide resilience a large number of APs are required.

By way of example, Cisco has a scheme of Controller based wireless LANs which used Wireless Service Module (WiSM) to control light weight wireless access points [509]. Each light weight wireless access point is connected to two WiSM (see figure below). The wireless access points are installed with a 40% overlap. If a wireless access point fails, the WiSM boosts the transmitting power of the surrounding wireless access points to maintain coverage. Failures can be mathematically modelled to ensure the building always has adequate coverage.

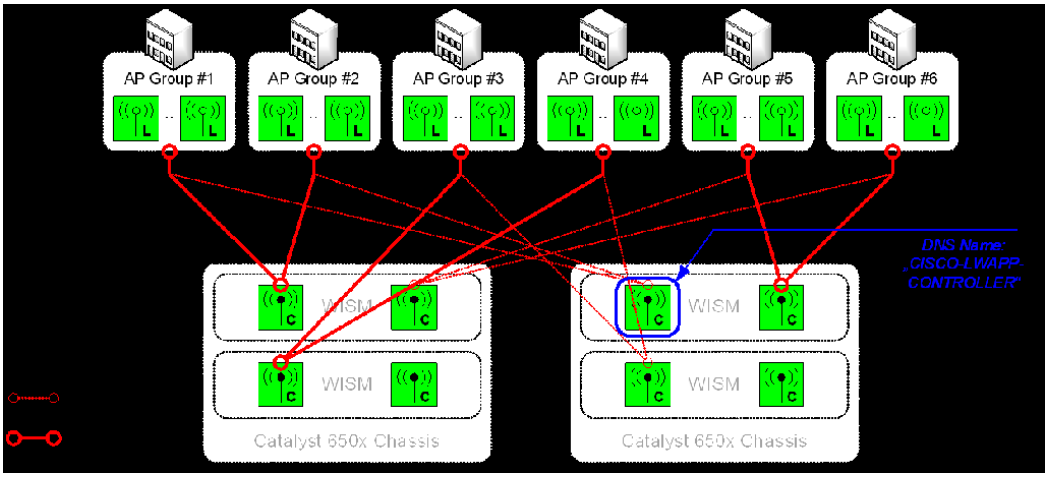

Fig 9 Enterprise Wireless LAN. [510]

Security

In larger organisations, RADIUS servers with Protected Extensible Authentication Protocol (PEAP) are used to authenticate Wireless Clients and to pass keys through tunnels between Wireless Access Point and Clients.

Description	Legacy LEAP	Legacy PEAP	WPA Enterprise LEAP	WPA Enterprise PEAP	WPA2 Enterprise PEAP
Auithentification	IEEE 802.1x w/ LEAP	IEEE 802.1x w/ PEAP	IEEE 802.1x w/ LEAP	IEEE 802.1x w/ LEAP	IEEE 802.1x w/ LEAP
Encryption	Dyn WEP	Dyn WEP	WPA/TKIP	WPA2/TKIP	WPA2/AES
Level of security					

Fig 10 Enterprise Security

5.4 Wi-Fi Meshes

My local Borough Council of Swindon in Wiltshire has teamed up with a digital technology firm aQovia to set up a company called Digital City UK, to install a wireless (Wi-Fi) broadband mesh of 1,400 access points covering the whole borough with internet access to 186,000 citizens. [506]

The pilot for this project was in the town of Highworth. Unfortunately, this project was suspended in March 2011.

I did try to contact Mr Riki Hunt the director of Digital City on his choice of technology. I personally tested the system in Highworth before its suspension. I was not able to hold a connection as I walked around Highworth and I did not get positive feedback from the businesses in the High Street that I interviewed, Brooks Café and the Kebria Tandoori Restaurant. The local inhabitants interviewed were also disparaging of the “unreliable internet service that was always losing connection”.

5.5 References - Wi-Fi

[501] Economist, Jun 10th 2004. *A brief history of Wi-Fi.* from The Economist print edition. Available from: http://www.marcus-spectrum.com/documents/economist.pdf [Accessed: 02 March 2011]

[502] IEEE, 2009. *IEEE 802.11n-2009 Wireless Local Area Networks.* Available from: http://standards.ieee.org/getieee802/download/802.11n-2009.pdf [Accessed: 02 March 2011]

[503] Wi-Fi Alliance, N/A. *Wi-Fi Alliance Organisation.* Available from: http://www.wi-fi.org/organization.php [Accessed: 02 March 2011]

[504] Ofcom, N/A. *UK Fixed Wireless Access, Wireless LAN and Wi-Fi frequency bands.* Available from: http://stakeholders.ofcom.org.uk/market-data-research/telecoms-research/bbresearch/wireless_update/wirelessbroadband/bwuAnnex1 [Accessed: 11 March 2011]

[505] Gast, M.S, 2006, 802.11 Wireless Networks The Definitive guide , 2nd ed, O'ReillyMedia Inc and Southeast University Press

[506] Which on-line Consumer Magazine, November 2009: *Swindon: the UK's first broadband 'Wi-Fi town'£1m network of Wi-Fi hotspots form 'Swindon mesh'* . Available from: **http://www.which.co.uk/news/2009/11/swindon-the-uks-first-broadband-wi-fi-town-188857/** [Accessed: 15 March 2011]

[507] Air Magnet Inc, 2005, *802.11n Primer.* Available from: http://www.airmagnet.com/assets/whitepaper/WP-802.11nPrimer.pdf [Accessed: 12 March 2011]

[508] ZDNET, Kingsley-Hughes, A, June 2010. *Wi-Fi Alliance to dump WEP and TKIP ... not soon enough.* Available from: http://www.zdnet.com/blog/hardware/wi-fi-alliance-to-dump-wep-and-tkip-not-soon-enough/8677 [Accessed: 01 April 2011]

[509] WNN Wi-Fi Net News, Fleishman, G., June 2010. *Say Goodbye to WEP and TKIP*. Available from: http://wifinetnews.com/archives/2010/06/say_goodbye_to_wep_and_tkip.html [Accessed: 01 April 2011]

[510] Cisco Systems, Inc. 2007. *WiSM configuration Guide.* Available from: .http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ContCG40-Oct.pdf [Accessed: 01 April 2011]