RTT TECHNOLOGY TOPIC
August 2004

WiFi PHY

In last month's Hot Topic, we discussed the evolution of radio physical layers, showing how radio bearers were becoming more flexible with the ability to support multiple simultaneous data streams per user, variable data rates for each data stream and different types of service (side by side delivery of best effort and time bounded services).

In this month's Hot Topic, we look specifically at the WiFi physical layer (PHY) and related changes being made to the Medium Access Control (MAC) layer.

WiFi Devices
WiFi chip sets costing 100 dollars in 2000 now cost less than 10 dollars. This is driving the trend towards embedding WiFi connectivity into laptop and desk top computers (local networking), PDA,s and phones (Nokia's 9500 being a recent example). Intel's promotion of their Centrino chip set has helped to consolidate this trend. WiFi devices are also going into a broad cross section of consumer devices including audio products (WiFi HiFi), video (including 802.11 based CCTV), voice products and (in the US) automotive products. This implies a broadening of the WiFi application 'form factor' which in turn implies some substantial changes in the WiFi PHY, WiFi MAC and higher layer protocols.

The WiFi PHY
One issue to date has been how to get 802.11 to work at the same time as Bluetooth. In a larger form factor device (ie a lap top PC) one option is to provide as much separation as possible between the Bluetooth and WiFi antennas with the use of near field antennas providing some additional separation. Alternative techniques depend on arbitrating access at the MAC layer or relying on adaptive frequency hopping to 'hide the problem'. Probably a better alternative is just to recognise that when Bluetooth and 802.11 are used together, particularly in small form factor devices, it just makes more sense to use the 5 GHz band for 802.11 (now possible thanks to the availability of low cost dual band transceiver chip sets).

The 5GHz band has the additional advantage of additional bandwidth and more flexibility in terms of having more non-overlapping channels than the 2.4 GHz band. For example, at 2.4 GHz, only Channel 1, 7 or 13 or 1, 6 and 11 are used (or occasionally 4 channels across a multi-site system). At 5 GHz, there are either 12 x 20 MHz non-overlapping channels (US) or up to 19 channels in Europe with each channel sub-divided into 64 sub carrier data channels of which 48 can be data channels. The 5GHz PHY is therefore inherently more flexible when supporting multiple per user data streams than the 2.4 GHz PHY.

The data rate can change depending on the modulation used. DBSK supports 6-9 M/bit/s, DQPSK supports 12-18 M/bit/s, DBSK with QAM supports 25 to 38 M/bit/s

and DQPSK with QAM supports 48 to 54 M/bit/s. Some products are also available which offer 108 M/bit/s by bonding two channels together. The alternative of course is to use 802.11a side by side with 802.11g at 2.4 GHz though probably not a great idea to use Bluetooth as well in this type of device. 802.11g and 802.11a both use an OFDM multiplex so there is good commonality across these two physical layers and the inter-working is to an extent pre specified within 802.11j

The WiFi MAC
Figure 1 shows the physical layer options (a, b and g) and MAC layer work items (e,f,h,I,j,k,n,s).

Figure 1 802.11 Task Groups and Work Items

a	b				e	f	g	h	i	j	k	n	s
5 GHz	2.4 GHz						2.4GHz						
6-54 M/bit	1M/bit	2M/bit	5.5M/bit	11M/bit			6-54 M/bit						
	Basic rate	Extended rate	Enhanced rate										
OFDM	DBPSK	DQPSK	QPSK										

A reminder of why these work items exist.

802.11 e QoS and prioritisation
802.11 has always traditionally been a connectionless contention based access protocol. The traditional bandwidth allocation mechanisms, primarily the distributed co-ordination function and point co-ordination (PC) functions are not well adapted to and were never intended for time bounded services such as real time voice and/or video.

Figure 2 shows the changes proposed for the QoS and prioritisation mechanisms.

Figure 2 QOS and prioritisation

Bandwidth management/Parametized QOS					
Traditional					
CSMA/CA					
DCF					
PCF/PC					
New					
EDCA	Extended data channel access Wireless media extension	Background	Best Effort (Replaces DCF)	Video TXOP Video transmission opportunity	Voice TXOP Voice transmission opportunity
HCCA	Hybrid Controlled	HCCA establishes 8 queues in the Access Point			

	Channel Access Point co-ordinator (PC)replaced with a hybrid coordinator(HC)	(AP) designated by their traffic specification

The traditional bandwidth allocation mechanisms used in 802.11 b (distributed co-ordination function and point co-ordination function using a point co-ordinator) are supplemented with two new protocols specified by the 802.11 e work groups based on traffic prioritisation (802.11 d). The new functions are EDCA - extended data channel access also known as the Wireless Media Extension. This establishes four prioritisation levels, background, best effort (equivalent to existing DCF capabilities), video and voice, Video and voice data streams are given dedicated transmission opportunities known as TXOP. HCCA - hybrid controlled channel access, replaces or rather supplements the existing point co-ordination functions with the point co-ordinator replaced by a hybrid co-ordinator. The hybrid co-ordinator establishes 8 queues in the Access Point ingress and egress ports, which can then treat individual data/traffic streams in accordance with their traffic specification (TSPEC). 802.11e is not ratified yet but pre standard chip sets will be available from Atheros later this year targeted at the home networking market.

802.11 f Handover
802.11 has always worked on the principle of 'break before make' rather than 'make before break'. Simply put, if acknowledgement packets stop coming back, the device will channel scan and look for another beacon. The time taken to do this is typically about 70 milliseconds. If you were walking from access point to access point within an office using WiFi for voice this would be annoying. A fast roaming study group is looking at reducing these roaming delays to less than 50 milliseconds. As with 802.11 e, pre-standard devices are being shipped with these capabilities already enabled, Spectralink being one example.

The question then arises as to the degree of mobility being supported and whether the base station/access point or the user's device should take the handover decision. Seamless 'make before break' handover protocols (used in cellular voice networks) imply substantial amounts of measurement reporting and a rework of the beacon structure (see 802.11 k below).

802.11 h Power Control
If measurement reporting is used then it makes sense to introduce power control. Power control improves the battery life/duty cycle of the user device and should generally help to reduce the noise floor, which in turn should deliver some capacity and coverage benefits. Power control however implies a rework of the beacon structure (see 802.11k below).

802.11 i Authentication and encryption
802.11 i (ratified in June 2004) addresses the replacement of the existing (semi-secure) authentication and encryption procedures known as Wireline Equivalent Privacy (WEP) with WiFi Protected Access (WPA). This adds in the user authentication missing in WEP and makes it easier to implement SIM based access - effectively bringing WiFi together with existing cellular authentication procedures.

802.i also describes a Temporal Key Integrity Protocol, a combination of WPA and AES, the American encryption standard for streamed media. The challenge here is to keep configuration simple and to minimise any impact on header overheads and end to end latency budgets.

802.11 j Interworking
Originally established to address issues of 802.11a and Hiperlan interworking, additional work items include handover between 802.11 b, g and a and in the longer term, handover between WiFi and cellular (or alternative 802.16 /802.20 wide area systems.)

802.11 k Measurement reporting
802.11k measurement reporting introduces many of the techniques presently used in cellular (including GSM MAHO mobile assisted handoff). Measurements collected and sent to the MIB Management Information Base) would include data rate, BER, SNR and a neighbour graph. One proposal is to use beacon compression to take out redundant information in persistent sessions and therefore release beacon bandwidth for measurement reporting. This would be known as a Resource Management Beacon (RRM beacon) and is covered by recent Nokia contributions to the 802.11k work groups

802.11 n Stream Multiplexing
802.11n is intended as a protocol for managing multiple HDTV channel streams with additional space for simultaneous voice and data. The standard is going to mandate the use of MIMO (multiple input/multiple output) techniques to get throughputs of =>100M/bit/s.There is an as yet unresolved dispute between two interest groups with different ideas of how to implement MIMO. The TGn sync group backed by Agere, Intel, Toshiba and Cisco supports a 40 MHz rather than 20 MHz channel with a 2x2 antenna configuration. The headline data rate for two adjacent 'bonded' 40 MHz channels is 250 Mbit/s. The MAC overheads bring this down to about 175Mbit/s

The World Wide Spectrum Efficiency organisation (WWise) backed by TI, ST, Broadcom and Conexant supports the retention of the existing 20 MHz channel and a 4x4 antenna approach which offers similar headline rates. Final ratification of the standard is expected by end 2006.

802.11 s Mesh Networking
And finally (for the moment), 802.11s addresses mesh networking and ad hoc network protocols. This potentially brings WiFi into much more direct competition with Bluetooth based personal area networks (PANS) and Device Access/Device Area Networks (DANS) and paves the way for possible future integration with UWB based PAN/DAN solutions. Mesh networking protocols will also facilitate a whole new generation of wearable WiFi products both for consumers and professional users.

Summary
The rapid decrease in WiFi chip prices has opened up new consumer and professional applications. This increase in 'application bandwidth' has required substantial changes to be made to the WiFi PHY and MAC. Effectively as application bandwidth increases protocol bandwidth increases. QoS, handover, authentication, encryption, inter-working, measurement reporting and mesh network protocols all

absorb bandwidth and absorb power. Even power control absorbs power and certainly absorbs bandwidth. Additional functionality always has a cost in terms of MAC overhead. At the same time, higher layer protocols (TCP/IP and SIP for example) introduce additional header overhead and (to use an IETF term) good put (the ratio of user data rate to channel data rate) goes down. Given the large amount of bandwidth now available when you add the b, g and a physical layers together, this probably does not matter though it does have power budget and delay budget implications. In addition, the contention based protocols that have been always been the basis for Ethernet and 802.11 wireless LAN are becoming more connection oriented in order to support an increase in the time bounded traffic mix. Connection oriented protocols buy bandwidth at the expense of other users and therefore introduce more variability at the PHY and MAC level (A small but significant percentage of users tend to absorb a disproportionate amount of bandwidth). Headline data rates should therefore be treated with caution when considering the likely application performance that can be achieved when multiple users are accessing a common bandwidth bearer.

About RTT Technology Topics

RTT Technology Topics reflect areas of research that we are presently working on.

We aim to introduce new terminology and new ideas to clarify present and future technology and business issues.

Do pass these Technology Topics on to your colleagues, encourage them to join our Push List and respond with comments.

Contact RTT

RTT, the Shosteck Group and The Mobile World are presently working on a number of research and forecasting projects in the cellular, two way radio, satellite and broadcasting industry.

If you would like more information on this work then please contact

geoff@rttonline.com

00 44 208 744 3163