Global Information Assurance Certification Paper

SANS GIAC GSEC PRACTICAL
Timothy Peter Davis, Sydney Australia
June 23, 2004

GSEC Practical V1.4 – Option 1

Bluetooth versus WiFi – A Comparison

Table of Contents

Abstract

Bluetooth™ and 802.11b (WiFi, Wireless Fidelity) are both wireless technologies that of recent have both proliferated so rapidly that they they have become well established in both the enterprise and the consumer electronic market. Bluetooth has been widely deployed in mobile phones & headsets as a cable replacement whilst WiFi has been widely accepted by laptop computer manufacturers allowing consumers to work with less restriction due to cables and the legacy Local Area Network attributes previously encountered.

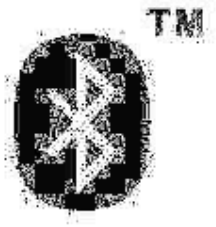
This document will give a brief history and technical overview of the two technologies and seeks to illustrate the differences and the commonalities between Bluetooth™ and WiFi (802.11b), the security features and risks applicable to each technology, ways in which to mitigate the risks involved when using either. It will explain how the two technologies can co-exist and why one and not the other may be better suited to some applications.

History – The origins of each technology.

Bluetooth

The term “Bluetooth” is rapidly becoming a commonly known label that has been given to Short Range Wireless Radio technology, the following describes how the name came to be courtesy of its inventors.

> How did Bluetooth™ get its name? In 1997, one of the Bluetooth™ inventors from Ericsson met with his Intel contact at a bar in Canada. They started talking about Scandinavia and the Vikings and the Ericsson inventor gave his Intel contact a book on the subject called "Röde Orm". When he had read it, he called the Ericsson Inventor. What about "Bluetooth?" Harald Bluetooth was the Viking king that joined two Scandinavian kingdoms peacefully. Bluetooth™ was to similarly join telecommunications and computing. [1] *Ericsson*
> The logo itself was originally designed by a Scandinavian firm at the time the trade association was announced to the public. Keeping to the traditions of the name, the logo combines the runic alphabetic characters "H" which looks similar to an asterisk and a "B". Look carefully you can seen both represented in the logo. [6] *Bluetooth.org*



> Telefonaktiebolaget LM Ericsson is the sole legal owner of the Bluetooth brand, and has assumed the responsibility to protect its name and mark

through trademark registration. However Ericsson does not own the Bluetooth specification. [14] *Palo Wireless*

Bluetooth is an open standard as such there is large quantities of information about the standard on the internet. www.bluetooth.org being a principal source for information.

Bluetooth™ uses the 2.4Ghz radio frequency band to provide wireless connectivity to many electronic devices currently in use by consumers today such as Mobile phones & Headsets, Personal Digital Assistants (PDAs) and Laptop computers, Many other commonly found devices also uses this frequency range such as microwave ovens and cordless phones. The 2.4GHz band is known as the Industrial, Scientific & Medical (ISM) frequency range. No license is required for devices in this range. The limitations are 1 watt of output power and only spread spectrum modulations are allowed. The amount of spectrum is limited, and as each band eventually fills up it will force new users to use higher bands, i.e. such as 802.11a which uses the 5.15 – 5.825GHz spectrum.

History of WiFi, (802.11b)

Many years ago , on the eve of World War II, a well-known actress of the day Hedy Lamarr and George Antheils, an avant-garde American composer, while at a dinner party, thought up an interesting scheme to control armed torpedoes over long distances without the enemy detecting them or jamming their transmissions. While they had the foresight to patent their invention, the term of the patent lapsed without either of them realizing any money from their invention, which formed the basis of what was to later become spread-spectrum communications.

This invention becomes even more incredible when you consider that it came before the invention of digital electronics.. however, it makes very substantial use of several key digital concepts. Yes, the term "ahead of it's time" would apply here, because over 50 years later, as high-speed microprocessors become inexpensive, spread-spectrum communications- Hedy Lamarr and George Antheils ' secret communications system ' - adapted to use today's ultrafast microprocessors- is coming into it's own as a effective and inexpensive way to communicate over long distances, privately and efficiently. Spread-spectrum forms the basic principle that enables the simultaneous multi-channel operation of modern digital cellular telephony. The same characteristics that made their technique jam-proof, also, through a mathematical phenomenon which can easily be documented, creates an extraordinary efficiency of transmission such that extremely low-power transmitters can be used over extraordinary distances, and many transmitters and receivers can occupy the same band of frequencies at the same time. This extrordinary efficiency is enabling inexpensive wireless access to high-bandwidth TCP-IP telecommunications, frequently radically altering the economics of setting up Internet-connected LANs for community organizations. [5] *Beaumont, C.*

Technical Overview – Bluetooth

Bluetooth is by now a well established communications standard for short-range wireless links. Its main use today is for replacing proprietary cables from each manufacturer with a standard universal radio link connecting technology such as mobile phones & headsets, personal digital assistants PDAs and laptops but its future applications could spread much wider such as increased use in vehicles and home automation, printers & fax's, the possibilities are endless. It can also be used as a mechanism to form small ad-hoc groups of connected devices without the usual infrastructure requirements.

Radio Specifications

The bandwidth is limited to 1Mb (~700kbps realistically), but it does make up by being a robust, low complexity RF architecture – Frequency Hopping Spread Spectrum (FHSS) when compared to WiFi's Direct-Sequence Spread Spectrum (DSSS), low power and low cost wireless solution. More information about the two RF technologies is provided later in the document in the comparison section page 13.

It can operate in noisy frequency environments, as it uses a fast acknowledgement and frequency hopping scheme to make the link robust. Bluetooth radio modules operate in the unlicensed ISM band at 2.4GHz, and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. Compared with other systems in the same frequency band, the Bluetooth radio hops faster and uses shorter packets.

- 2.4 MHz freq range - It has 1600 hops/s over 79 1-MHz freq. channels
- 1Mbps, actual data throughput ~700kbps
- Signals can be transmitted through walls and briefcases etc, eliminating the need for line-of-site.
- Signal is omni-directional, devices do not need to be pointing towards each other.
- Governments worldwide have regulated it, so you can utilize it wherever you travel.

Transmission Power -

Power Class 1: is designed for long range (~100m)
Power Class 2: for ordinary range devices (~10m)
Power Class 3: for short range devices (~10cm)
[9] *Palo Wireless*

Class 2 devices are most commonly deployed and include devices such as phones and headsets. The receiver device must be classed identically to the sender where the distance is exceeded for either party for it to work obviously.

The Bluetooth Protocol Stack

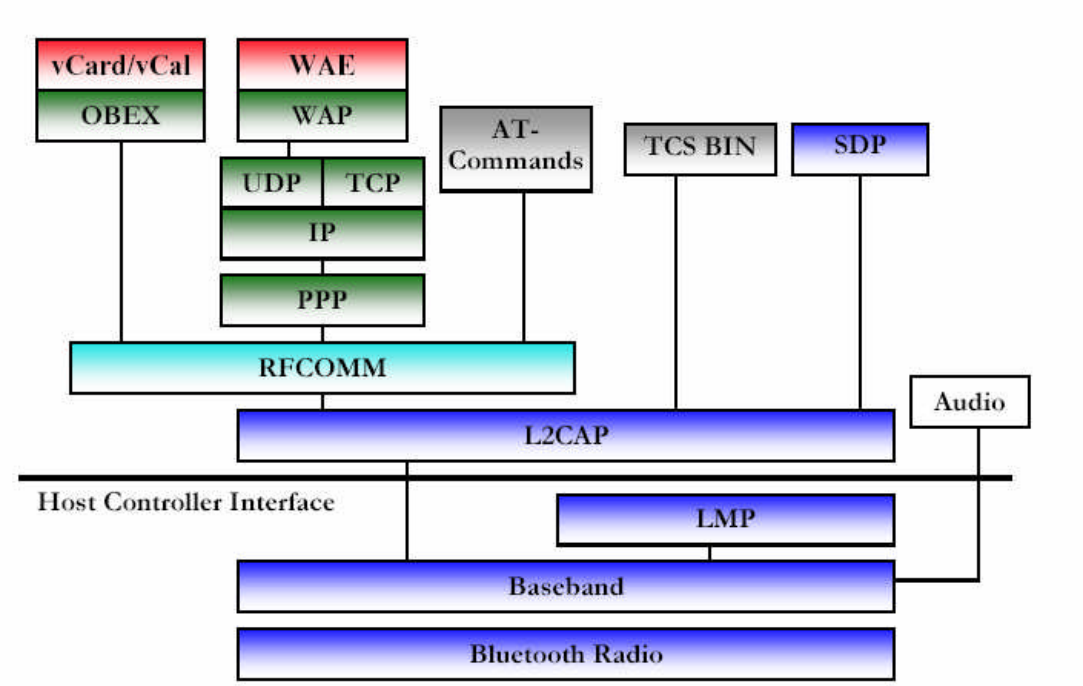


Figure 1 Bluetooth Protocol Stack

Table 1 [8] *Mettala, R.*

The Bluetooth Protocol Stack Explained

The Blue boxes are those protocols that are relevant to Bluetooth only.

The Bluetooth radio converts the digital baseband data to and from a 2.4GHz analog signal using Gaussian Frequency Shift Keying (GFSK) modulation. Further detail provided in the comparison section – page 13.

Baseband is responsible for constructing and decoding packets, encoding and managing error correction, encrypting and decrypting for secure communications, calculating radio transmission frequency patterns, maintaining synchronization, controlling the radio, and all of the other low level details necessary to realize Bluetooth communications.

Link Manager Protocol (LMP) - The Link Manager protocol is responsible for managing all the parameters for Bluetooth connections. The following is a list of operations that are incurred by the LMP layer.

General Response
Authentication
Pairing
Change Link Key
Change the Current Link Key
Encryption
Slot Offset Request
Clock Offset Request
Timing Accuracy Information Request
LMP Version
Supported Features
Switch of Master-Slave Role
Name Request
Detach
Hold Mode
Sniff Mode
Park Mode
Power Control
Channel Quality-Driven Change
Quality of Service
SCO Links
Control of Multi-Slot Packets
Paging Scheme
Link Supervision
Connection Establishment
Test Mode
Error Handling
[9] *Palo Wireless*

Service Discovery Protocol (SDP) - This is the protocol that provides a means by which devices discover and recognize each other and the services that can be used with these particular discoveries. This changes dynamically based on the RF proximity of devices in motion. [9] *Palo Wireless*

Basically when two devices both Bluetooth enabled come within an operating range they can then discover each other, then browse each other in order to exchange information about each devices services using SDP for one of a number of functions.

Logical Link Control and Adaptation Protocol (L2CAP) **–** This layer exists above the Baseband layer in the Bluetooth protocol stack and in the data link layer when referencing the OSI model.

This protocol controls all the parameters for each connection, it controls encryption options, the exchange of Quality Of Service (QoS) information, It also formats the data - Re-assembly occurs for data packets that are received from baseband layer as the baseband has a smaller MTU than the L2CAP layer

and when sending data the L2CAP must segment the data so as to again be supported by the smaller baseband MTU limit.

Bluetooth Security Overview

> The Bluetooth specification includes security features at the link level. It supports authentication (unidirectional or mutual) and encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key a pairing procedure is used when the two devices communicate for the first time. [15] *Mulker, T.*

There are four parts to security within Bluetooth devices ;

1>Bluetooth device address (BD_ADDR), which is a 48-bit address that is unique for each Bluetooth device.
2>Private authentication key, which is a 128-bit random number used for authentication purposes.
3>Private encryption key, 8-128 bits in length that is used for encryption.
4>Random number (RAND), which is a frequently changing 128-bit random or pseudo-random number that is made by the Bluetooth device itself.

Bluetooth security has three modes.

> Security mode 1 (non-secure): A device will not initiate any security procedure. [15] *Mulker, T.*

Basically the device is in discovery mode looking for any other Bluetooth devices, when one is in proximity no authentication or access approval is required before service access is granted. It is obviously not recommended to use this mode ever.

> Security mode 2 (service-level enforced security): A device does not initiate security procedures before channel establishment at L2CAP level. This mode allows different and flexible access policies for applications,especially running applications with different security requirements in parallel. [15] *Mulker, T.*

Broadcast traffic is not encrypted, but individually addressed traffic is encrypted.

> Security mode 3 (link level enforced security): A device initiates securityprocedures before the link set-up at the LMP level is completed. [15] *Mulker, T.*

Security, both encryption and authorization is enforced prior to the link being created by LMP layer – unlike mode 2, all traffic is encrypted.

Trust Levels - devices can be configured as either trusted or un-trusted, once a device has been paired successfully it can be configured as trusted and it has a fixed relationship and it can pair without re-authenticating using the information gained on a previous pairing and it has unrestricted access to all services. This is has some security concerns as the access or privileges then resides with the device and not the user, should the device be stolen, the trusts that it holds with other devices goes along with it. The data with which the trust is formed on is kept in non-volatile memory.

The BD_ADDR is a unique IEEE 48bit address allocated to each device, similar to a MAC address on a Network Interface Card (NIC).

The untrusted device obviously has no fixed relationship and access to services is restricted.

Link Keys

There are four types of link keys;

The 'initialization key' is used for key exchange only in installation where other keys are not yet used and a link key is being built. It is derived from the PIN and post creation it's discarded.

The 'unit key' is created in the device when it is installed and is kept in non-volatile memory. It is sometimes used as a link key. It is semi-permanent.

The 'combination key' is created from the contributions from the pair of devices and for each new pair – most common. It is also semi-permanent.

The 'master key' is the only temporary key which is used in PICONET type situations where information is being sent to multiple recipients.

Encryption Keys

The 'Encryption key' is generated from the current link key. And is configurable between 8-128 Bits. When the Link Manager activates the encryption, the encryption key is generated. It is automatically changed every time the Bluetooth device enters the encryption mode. As well as the link key playing a role in the encryption key there is also a 96-bit Ciphering Offset Number (COF) and a 128-bit random number. The COF is based on the Authenticated Ciphering Offset (ACO), which is generated during the authentication process along with the sres result as mentioned below in the challenge response exchange diagram.

Authentication - the process of verification. The Bluetooth authentication system uses a challenge response system to check whether the other party knows the

secret key. This method uses symmetric keys, i.e. both participants share the same key.

The challenge response exchange ;

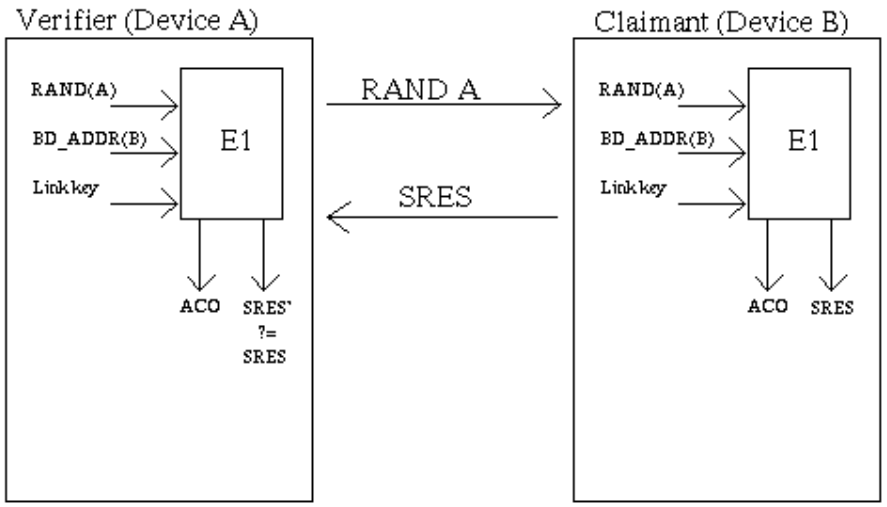


Table 2 [7] *Vainio, J. T.*

- claimant and verifier share the same symmetric secret/private key (i.e. PIN)
- claimant's knowledge of the secret key checked by a 2-move protocol
- verifier generates a random number, RAND_A
- sends RAND_A as the challenge to the claimant
- both verifier and claimant compute a function E1 (a 64-bit block cipher)
- a function of RAND_A, device address BD_ADDR, and the link key
- claimant returns first 32 bits of result of E1 computation, SRES, to verifier
- verifier checks SRES is the same as its own computation
- if both SRES results are equal – authentication was successful.

Technical Overview – 802.11b (WiFi)

For the purpose of this document, all references to WiFi should be assumed as 802.11b unless stated otherwise.

802.11b, or IEEE 802.11b, is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers). The 802.11 committee is the

group responsible for developing the standards for wireless local area networks (WLAN).

Within the 802.11x standard there are a number of additional specifications;

802.11b or WiFi (wireless fidelity) 2.4GHz spectrum, bandwidth max is 11Mbps
802.11a Operates in the 5 GHz spectrum, bandwidth max is 54Mbps
802.11g (draft standard) 2.4Ghz, bandwidth maximum of 54Mbps
802.11i WiFi Protected Access – WPA, specifications for security enhancements for the 802.11x technologies, intended to replace Wired Equivalent Privacy (WEP), by using technologies such as TKIP – Temporal Key Integrity Protocol. Further information about TKIP in Mitigation section.

A wireless 802.11b LAN network functions just like a regular Ethernet LAN in that it utilizes Carrier Sense Multiple Access / Collision Detection (CSMA/CD) at the MAC sub-layer of the Data Link/Network layer - This technology allows a transmitting node to detect a collision and retransmit. The difference being the physical layer consists of Direct Sequence Spread Spectrum RF technology using Radio waves via a radio tower a.k.a. Wireless Access Point (AP) or wireless gateway instead of using unshielded twisted pair (UTP) cabling or other existing mediums patched to a hub or a switch. For the purpose of this document I will not go into detail about CSMA/CD and associated topics, but rather discuss the technical details that relate specifically to 802.11 (wireless).

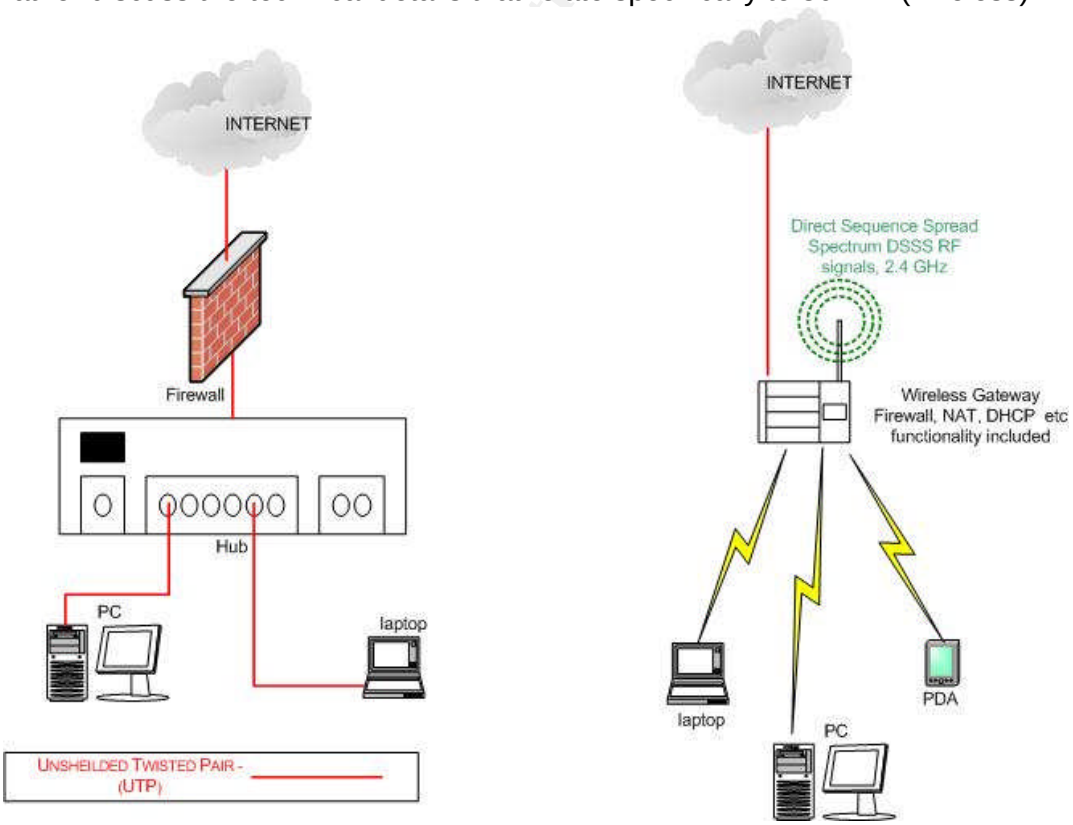


Table 3. Traditional wired LAN vs. WiFi gateway.

A WiFi access point differs from a WiFi gateway as it lacks the functionality that is encompassed by the gateway such as DHCP/NAT/VPN support/firewall

NB: Devices must be capable of 802.11b, i.e. fitted with WiFi compatible hardware, usually internal or on-board a PCMCIA / PCI card.

Radio Specifications – The physical layer

Direct Sequence Spread Spectrum is the chosen Radio Frequency (RF) method for 802.11x, it operates in the 2.4Ghz spectrum also though it does have notable differences to FHSS – the technical details are listed below in 'Similarities & a Comparison – RF architectures'

Some details specific to DSSS are;

> DSSS systems spread the signal energy across a relatively wide band by increasing the occupied bandwidth. A DSSS transmitter converts a bit stream into a symbol stream, in which each symbol represents a certain number of bits, depending on the phase shift keying (PSK) modulation technique.
>
> The symbol information is converted into a complex-valued signal that is fed to the spreader. The spreader multiplies its input signal with a pseudo noise sequence, called a chip sequence. This multiplication creates a signal with a wider bandwidth. The inphase and quadrature components of the spreader output signal are fed to a quadrature modulator.
>
> The transmitter front end provides filtering, conversion to a higher RF, and power amplification. The channel center frequencies are 2.412 Mhz, 2.417 Mhz, 2.422 Mhz, 2.462 Mhz, 2.467 Mhz and 2.472 Mhz. [19] *Rathod, M.*

DSSS allows operation of WiFi with distances from the AP or gateway up to 255ft (office environment) , the average throughput of 802.11b is 4-5Mbps. It has 11 channels that can be utilized where WiFi networks are functioning in parallel to minimize interference. Typically you would not want to say use the same channel as your neighbour as interference and unintendedly a Denial Of Service could occur.

Security Overview - WiFi

Wired Equivalent Privacy (WEP) Protocol
Encryption is 40-128bits.

Manual key management is a tedious process and does not scale for enterprise purposes. Because the keys have to be changed manually they are usually left for weeks maybe months and possibly years. This leaves the network wide open for hackers.

802.11b uses Wired Equivalent Privacy (WEP) algorithm, it is a pseudo random number generator (PRNG) initialized by a shared secret key. The PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet which is combined with the outgoing/incoming packet producing the packet transmitted in the air. Eavesdropping is meant to be prevented by the use of WEP. , access control (authentication) and data integrity (checksum) are also included in WEP.

The risks associated with WEP are listed in the section "Security Issues and Mitigation methods"

SSID – Service Set Identifier, The SSID provides a means to "segment" a wireless network into multiple networks serviced by one or more AP's. Each AP is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must have the correct SSID configured – this acts like a password required to become part of the SSID segment.

MAC address Filtering – AP's can be programmed with a list of VALID MAC address's acting as a basic access list. This too does not scale well at the enterprise level as the list must be kept up to date.

Similarities & A quick Comparison

1a) RF Architectures

2.4 GHz - this is a very commonly used frequency band. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth & WiFi devices, all work within the 2.4 GHz frequency band. It is known as the Industrial, Scientific & Medical (ISM) frequency band. [3] No License is required.

Within the 2.4Ghz spectrum the two technologies work with two different RF methods, but both are what's known as 'spread spectrum' methods.

Bluetooth FHSS compared to WiFi DSSS

Bluetooth uses the Radio Frequency RF-method of FHSS (Frequency Hopping Spread Spectrum).

> One might make the point as too why Bluetooth doesn't use Direct sequence spread spectrum (DSSS) – this is the RF method used by WiFi, which is more powerful in multipath rejection, throughput etc. There is one simple reason as to why FHSS is used in place of DSSS : FHSS is simpler:

Mostly the difference is in the baseband, DSSS has to run on a much more powerful Digital Signal Processing (DSP) chip since DSSS uses chip rate (many times higher than the symbol rate) while FHSS only need to run at the symbol rate, so the power consumption for FHSS is much lower and the complexity is lower too.

In the RF part, FHSS use Frequency Shift Keying (FSK) which is relatively easy to build and the noise immunity is better while DSSS usually use Quadrature Phase Shift Keying (QPSK)(for IEEE 802.11 2 Mbps) or CCK (in IEEE 802.11b 11Mbps) which are more complex and the noise immunity is inferior to FSK.

However, one major disadvantage of FHSS is that it is slower than DSSS, mostly due to the fact that FSK need a frequency synthesizer (to hop frequency) and if you need a greater spread spectrum advantage, it has to be fast but this is not easy to implement. [4] *Palo Wireless*

1b) Reliability

The whole spectrum used by each technology varies. It is 83.5MHz in FHSS (Bluetooth), the whole ISM band. While for DSSS it is only 20MHz (one of the sub-bands). This basically means that the chances of having an interference covering a range of 20MHz is greater than the chance of having an interference covering 83.5MHz. A 20MHz wide interference could potentially deny or block a DSSS connectivity while it will only block 25% of the hops in a FHSS system. An FHSS system can still function in these conditions at 75% capacity – it will still work where as a DSSS system will not work at all. In this perspective the FHSS RF method is more robust.

1c) Speed

Bluetooth can operate at about ~700kbps
WiFi ~11Mbps

802.11b is roughly ten times faster and can operate at ten times the distance approximately with similar costs for each technology, though Bluetooth consumes much less energy, hence its wide use in mobile phones and PDA's.

From this we can say that Bluetooth is going to be too slow for video transfers & still images as we move towards >6MegaPixel cameras in the mass consumer market not just 'prosumer', this transfer will remain the domain of Firewire™ and USB v2.0 and possibly WiFi.

As a wireless LAN solution Bluetooth is not going to have the required bandwidth for deployment in the enterprise space and the constraints around each piconet/scatternet does not allow for scalability.

A Piconet (Pico meaning very small) is a group of devices connected via Bluetooth, it consists of 1 master and up to 7 slaves. All devices have the same physical channel defined by the master device parameters (clock and BD_ADDR) [11] BD_ADDR is a 48Bit MAC address similar to those used on Network Interface cards. Several piconets can join to form a scatternet, each piconets maintains independence. These are sometimes referred to as PAN's or PLAN's Personal Local Area Networks.

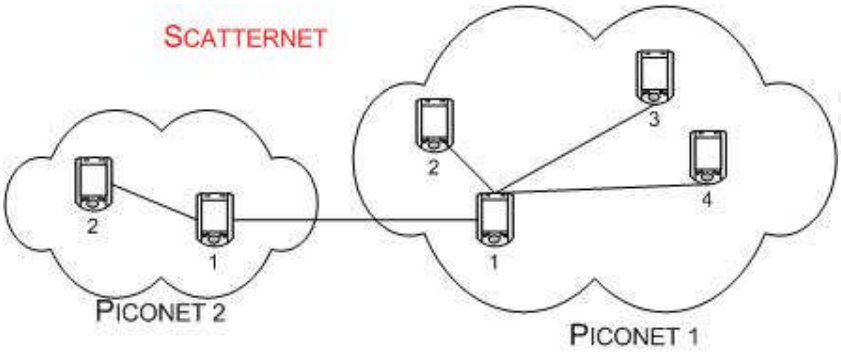


Table 3
Device number 1 in each cloud is master, Devices labeled 2-4 are all slaves.

1d) Applications

Bluetooth is primarily a cable replacement and was initially designed to connect devices point-to-point whereas 802.11b is primarily applied to a LAN access function.

Though it has had widespread acceptance, Bluetooth is not a matured network technology, it does allow LAN access or dial-up networking using only point-to-point (PPP) protocol , there is no support for general IP networking as exists for 802.11x. , as the 'Table 3' above shows , it simply would not scale well.

Bluetooth consumes less power than WiFi making it a better choice for deployment in smaller devices such as mobile phones which are powered by batteries not mains power.

Security Risks and Methods for Mitigation

1) Bluetooth

Man-in-the-middle

Bluetooth uses 4 digit pins when initialising, this is a weakness. This can be exhausted and broken. This is only compounded by the fact that it is common place for users to pick one common code out of the 10000 possibilities – that being '0000'. One way to work around this weakness is to pair in locations that are secure, the working distance of most Bluetooth devices is ~10m, less when solid walls etc. are involved.

Denial of service Attacks

As mentioned earlier in the document the Bluetooth and WiFi technology operate in the unlicensed and heavily used 2.4 GHz frequency spectrum. This makes it open to Denial of Service attacks from devices creating interference, devices such as microwaves and portable phones , and although both technologies use frequency hopping RF methods they are not immune to noise which could thus create a DOS attack.

Battery Exhaustion Attack

Other types of attacks that have been listed are 'battery exhaustion attacks' where retransmission repeatedly will cause battery exhaustion and hence DOS attack. A measure of limiting the attempt rate when throttling and possibly disabling that particular source for a grace period during attack would resolve this issue.

Bluejacking

'Drive-by messaging' a.k.a 'Bluejacking' is a new craze where users can send anonymous and unsolicited messages to other Bluetooth devices in the working range as business cards. This could be to simply 'freak out' other Bluetooth users in a small area or in a much larger commercial sense the same method could be deployed on customers passing a store and being targeted for marketing purposes. A privacy debate waiting to happen I'm sure.
There are web pages dedicated to this form already ; http://www.bluejackq.com/

2) WiFi – 802.11b

Eavesdropping or 'man in the middle' attacks – WEP key cracking, 802.11b

WEP uses a stream cipher based on the RSA's RC4 cipher which is reasonably strong but its use in a wireless packet network where physical intrusion may not be required to 'listen' to or 'sniff' packets has been questioned. These type of attacks are called 'parking lot attacks' or man-in-the-middle attacks, where it is possible that an attacker could use the parking lot outside of the intended victim's residence/business boundaries to become close enough that signal strength was sufficient to sniff the perceived internal network. The perimeter of the network is that point where the signal stops not the physical boundary's of the building with which the Wireless Access Point/ gateway has been installed.

Where I work we can pick up a strong signal from two building's that run parallel to ours, one broadcasting SSID with no security in place, open to all forms of attack.

More on WEP and its vulnerabilities – this from Berkley University USA;

We have discovered a number of flaws in the WEP algorithm, which seriously undermine the security claims of the system. In particular, we found the following types of attacks:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

Our analysis suggests that all of these attacks are practical to mount using only inexpensive off-the-shelf equipment. We recommend that anyone using an 802.11 wireless network not rely on WEP for security, and employ other security measures to protect their wireless network.

Note that our attacks apply to both 40-bit and the so-called 128-bit versions of WEP equally well. They also apply to networks that use 802.11b standard (802.11b is an extension to 802.11 to support higher data rates; it leaves the WEP algorithm unchanged).
[17] *Shipley, P.M.*

Whilst it discourages 'script kiddies' and regular users from attempting to crack it, it fails to prevent serious hackers from penetration.

Organizations and to a degree home/small office users should consider upgrading to TKIP – Temporary Key internet Protocol, some times referred to as WEP2.
TKIP shares a 'temporal key' amongst the clients and AP's , it combines the temporal key with the clients MAC address then adds a 16-octet initialization vector to produce the key that will encrypt the data. TKIP uses the RC4 algorithm to encrypt the data as does WEP but it changes temporal keys every 10000 packets. Most WEP devices can be upgraded to TKIP with only firmware / software upgrades. It is thought to be a temporary solution only with stronger encryption still needed

DOS attacks

Just like Bluetooth WiFi is susceptible to DOS using generated noise in the 2.4 GHz RF spectrum – as mentioned above in the Bluetooth DOS paragraph. Another DOS attack that AUScert discovered as listed as trivial but affective low-cost attack on 802.11;

> "an attacker using a low-powered, portable device such as an electronic PDA and a commonly available wireless networking card may cause significant disruption to all WLAN traffic within range, in a manner that makes identification and localization of the attacker difficult."
>
> The specific vulnerability is with the medium access control (MAC) function in the 802.11 protocol. "WLAN devices perform Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which minimizes the likelihood of two devices transmitting simultaneously. Fundamental to the functioning of CSMA/CA is the Clear Channel Assessment (CCA) procedure, used in all standards-compliant hardware and performed by a Direct Sequence Spread Spectrum (DSSS) physical (PHY) layer," says AusCERT.
>
> This attack simulates, in essence, an "always busy" signal for CCA, thus "preventing the transmission of any data over the wireless network."
> [18] *Schwartz, M*

Other forms of attack on WiFi

- ARP poisoning via man-in-the-middle, conquered and defended in the wired world some time ago, now an issue again in the wireless realm.

Parking Lot Attacks & Wardriving

To reduce the risk of 'parking lot attack' or man-in-the-middle attacks.
make sure that the access point or gateway is placed in the centre of your physical room or building, this minimizes the distance that the signal possibly breach's your location. You should survey your site to actually ascertain how far your signal really does transmit at usable levels, you could be transmitting further than was calculated or expected.

There is actually a name given to locating 802.11 networks whilst driving in a vehicle 'wardriving'. It was invented in (1999-2000) by Peter M Shipley (USA) who admits he wasn't the first person to actually go out and search for open wireless LANS but the first person to automate it with dedicated software and GPS unit. He noted that WEP usage was at 15% when he started the project and after going public usage is now 33% - a rate which all in the security fraternity would agree is still highly unacceptable.
[17] *Shipley, P.M.*

Disable Service Set Identifier (SSID) broadcasting. An SSID is a unique identifier included in the header of packets sent over a WLAN that acts as a password when a mobile or WiFi enabled device tries to join the network, they differentiate one WLAN from another. It can be sniffed in plain text from a packet – it offers no real security, it is essentially just a network name.
By disabling the SSID broadcast you effectively closing your network.

Change the default password that most wireless network devices ship with. Hackers are obviously going to be able to find all the default passwords and use them. Along with changing the default password, change the default network name – again, hackers will know of these defaults.

Use Media Access Control (MAC) tables on your wireless access point. These act like an extended Access Control List on a router, each WiFi network interface card has a MAC address just like a regular Ethernet NIC would. These MAC address's can be 'permitted' on your WLAN with all others denied.

Use of Virtual Private Network's are always excellent methods for ensuring data integrity and security across public and private networks, if your WiFi access point is IPSEC / IKE compliant it will be able to pass the VPN traffic through your WAP from your laptop/desktop and via possibly the internet to your company's network for example. For the device to be compliant it must understand IP Protocol's – 50 ESP (Encapsulating Security Protocol) 51 AH (authentication header) both portless protocols. The IKE (internet key exchange) protocol exchanges keys, while IPSec encrypts and signs packets.

> No more WEP – WiFi, TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named *Michael*, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all WEP's known vulnerabilities [16] *Grimm, C.B.*

Can they Coexist ? 'Blue802'

One question that is being asked amongst technical folk who understand the workings of the two technology is "Can they coexist ?", as both Bluetooth™ and WiFi operate in the 2.4GHz spectrum. Will each cause enough interference that neither can function simultaneously.

The answer in short is yes, but performance could be degraded. Some manufacturers have described the degradation as 'elegant' or 'graceful' and that most home users would not notice, while others have said network traffic will come to a near standstill.

> Several companies are working on this problem and HP's iPAQ Pocket PC h4150 and iPAQ h4350 ship short-range Bluetooth and mid-range 802.11 WiFi capabilities, the chip/hardware is made by Texas Instruments.
>
> The Texas Instruments Bluetooth/802.11 coexistence package (Table 2) was designed for mobile devices like PDAs and

handsets, where the interference problem is magnified by the close proximity of the chips. TI's design criterion was that that no RF radio isolation should be required. The design features a coexistence bus that runs between the WLAN and Bluetooth chips, running in real time on the MAC Layer which dynamically adjusts to the traffic patterns on the devices. At the same time, TI designed the chips to use as little power as possible, particularly when in standby mode, another crucial issue for handhelds, in which the life of the small batteries can make or break a product. [12] *Kuchinskas, S.*

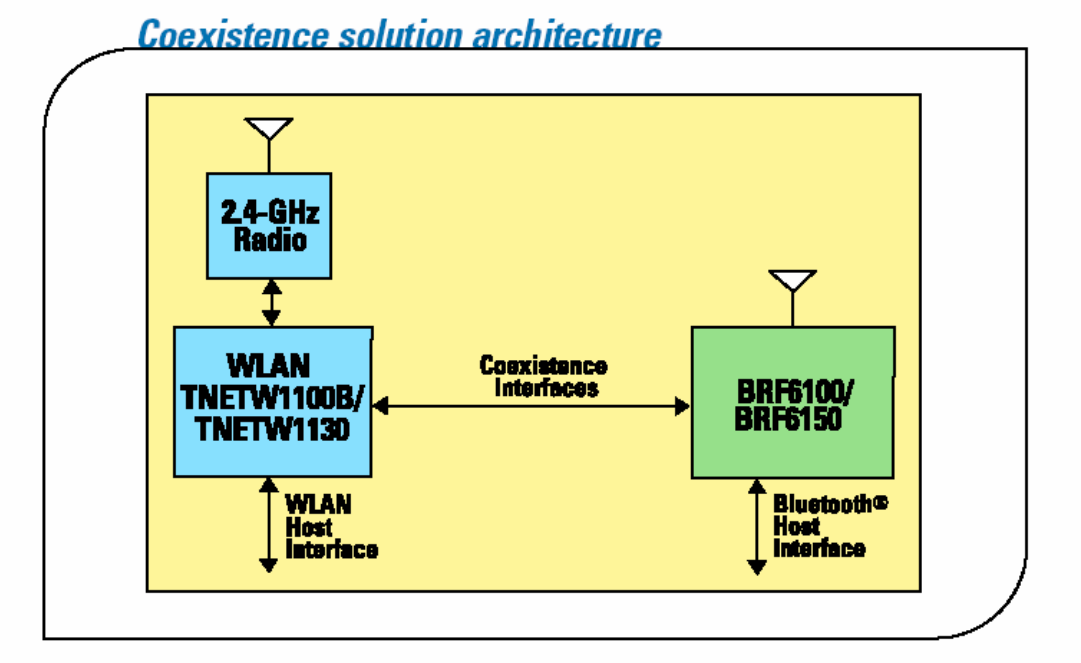


Table 2 [13] *Texas Instruments*

For Bluetooth this means the BASEBAND layer will be manipulated and for 802.11b the MAC layer to allow the two technologies to work in tandem.

Summary

I feel Bluetooth's deployment and acceptance will continue to grow with its current mode of use in mind – a cable replacement in general and possibly a personal local area network (PLAN) technology.

I see 802.11x (WiFi) continuing it's massive growth for all LAN uses but to a lesser extent in the corporate market place due to current throughput and security reasons that have not yet been addressed fully but hopefully in the near future 802.11i security methods will be practiced widely and there is talk of GiFi with which theoretically 2Gbps can be achieved at frequencies of 56Ghz - Glenn Fleishman (2003), "Gi-Fi?", (Wi-Finetnews.com).

It is extremely important that in both technologies, users and administrators alike use all the security functionality that has been provided to them correctly. That being done all but the most hardcore of hackers will be kept at bay. It is just as easy to configure the equipment correctly as it is wrong with just a little research and thought prior to implementation. In the current Information Technology climate that we live in security is paramount.

References

[1] 'Milestones In the Bluetooth Advance'
(Last Published March 22, 2004) Ericsson Web Site
URL - http://www.ericsson.com/bluetooth/companyove/history-bl/

[2] Web Page – wi-fialliance.org
Open Section FAQ's (2004)
URL - http://www.wi-fialliance.org/OpenSection/FAQ.asp?TID=2#80211b

[3] NTIA – Office of Spectrum Management
Frequency Allocation Chart (Oct 2003)
URL - http://www.ntia.doc.gov/osmhome/allochrt.html

[4] Palo Wireless Resource Centre (2000, July 19)
Original Post: why FHSS ? (SIG Forum)
URL - http://www.palowireless.com/infotooth/knowbase/othernetworks/57.asp

[5] Beaumont, C. (nd)
The Fascinating Story of the Lamarr/Antheil spread spectrum patent
URL - http://www.ncafe.com/chris/pat2/index.html

[6] What's in a name ?, the story of Bluetooth (no date)
URL - https://www.bluetooth.org/bluetooth/landing/btname.php

[7] Vainio, J. T. (2000, 25th May)
Bluetooth Security
URL - http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[8] Mettala, R.(1999, Aug 25)
Bluetooth Protocol Architecture. PDF document
URL - https://www.bluetooth.org/foundry/sitecontent/document/whitepapers_presentations

[9] Palo Wireless Resource Centre (no date)
URL - http://www.palowireless.com/infotooth/tutorial.asp

[11] Palo Wireless Resource Centre (no date)
URL - http://www.palowireless.com/infotooth/glossary.asp

[12] Kuchinskas, S. (2003, October 13)
TI Behind Wi-Fi, Bluetooth Convergence
URL - http://www.wi-fiplanet.com/news/article.php/3091311

[13] Texas Instraments Product Bulletin (2003)
Wireless performance optimization solutions:Bluetooth and 802.11 coexistance
http://focus.ti.com/pdfs/vf/wireless/coexistencebulletin.pdf

[14] Palo Wireless Resource Centre (2000, August 22)
Original Post: Various Posts (SIG Forum)
URL - http://www.palowireless.com/infotooth/knowbase/general/97.asp

[15] Mulker, T.(1999, July 15)
Bluetooth Security Architecture. PDF document Page 8
URL - https://www.bluetooth.org/foundry/sitecontent/document/whitepapers_presentations

[16] Grimm, C.B. (2002, October 31)
Overview – WiFi Protected Access, WiFi Alliance web page
URL - http://www.wi-fialliance.org/opensection/pdf/wi-fi_protected_access_overview.pdf

[17] Shipley, P.M. (n.d)
Personal Web Page
URL - http://www.dis.org/shipley/

[18] Schwartz, M (2004, May 26)
Security Briefs: WiFi Attacks, Enterprise Systems WEB page.
URL - http://www.esj.com/news/article.asp?EditorialsID=986

[19] Rathod, M. (n.d.)
Local Area Networks Sans Wires
URL - http://www.networkmagazineindia.com/200102/focus1.htm