

forward

a future of reliable wireless ad hoc networks of roaming devices

Interoperability Challenges for Wireless Communications

March 31, 2003

Record of Changes

Date	Version	Comment
31-03-2003	1.0	First Issue

Authorisation

Dr. Sadie Creese
FORWARD Steering Committee Member

Date

Authors

Chris Cant, QinetiQ, c.cant@eris.qinetiq.com

Sadie Creese, QinetiQ, s.creese@eris.qinetiq.com

Helen Roscoe, QinetiQ, h.roscoe@eris.qinetiq.com

Michael Anthony Smith, QinetiQ, m.a.smith@eris.qinetiq.com

Executive summary

This report forms deliverable D1 of the FORWARD project. It is the first and only deliverable of Work Package 3 *Interoperability of Wireless Comms*. The purpose of Work Package 3 is to informally assess the current level of interoperability in the area of wireless communications both between multi-vendor products, and between wireless technology and other spectrum users.

A resume of current mainstream wireless technologies is presented, focusing on Bluetooth and IEEE 802.11, although HomeRF, ZigBee and UltraWideBand (UWB) are also discussed.

The current state of interoperability of Bluetooth and IEEE 802.11 wireless devices is examined. This was achieved through a survey of wireless technologies, interviews with technicians with direct experience of using such technologies and reference to previous QinetiQ experience in military applications in this area. The perceived areas of concern by the market is highlighted, and the steps that have been taken to increase interoperability between different vendors' solutions are outlined.

The issue of Bluetooth/ IEEE 802.11 co-existence is discussed along with the problems of wireless technology co-existing with other spectrum uses. The current state of wireless implementations with respect to the vision of all pervasive computing is discussed.

An overview of security issues pertinent to interoperability of wireless communications is presented. Two key interoperability issues which could result in security compromises are outlined: Backwards Compatibility and Under-specification of Standards.

Finally, the report draws some conclusions:

Conclusions on the current state of interoperability between wireless devices:

- The current wireless standards are some way short of being perfect in support of interoperability. The exact scale of the problem is disputed.
- The recent entry of Microsoft into the Bluetooth market is seen as a positive step for interoperability, vendors will be forced by Microsoft's weight to inter-operate with them (and so by implication with each other).
- In the rush to get products to market, vendors are implementing draft specifications. This policy may lead to short term interoperability problems.
- Shortcomings in the specifications have led to vendors implementing differing solutions. This has resulted in interoperability problems, even when implementations have been shown to conform to the standards. Interoperability is demonstrated through comprehensive testing between specific devices / systems.

Impact on the development of Next Wave technologies and markets:

- Pervasive computing environments cannot be achieved with the current levels of interoperability between devices.
- The testing strategies adopted in order to achieve device interoperability are both commercially expensive, leading to compromise that short changes the consumer, and not optimal since they are not scalable. It would be in-feasible to conceive of every device vendor performing tests with millions of other devices it may be required to interact with, and that the testing will cover every possible set of communications the device could possibly enter into.

Advice for current use of wireless equipment:

- When currently purchasing wireless equipment users should be careful to choose products that have been explicitly tested for interoperability.

Contents

- 1 Introduction** **1**
 - 1.1 Purpose 1
 - 1.2 The Next Wave Technologies and Markets vIRC 1
 - 1.3 Pervasive Computing 1
 - 1.4 The objectives of FORWARD 1
 - 1.5 Structure of the Document 2

- 2 Current Wireless Technologies** **3**
 - 2.1 Performance issues of wireless technologies 3
 - 2.2 Bluetooth 3
 - 2.3 IEEE 802.11 6
 - 2.4 HomeRF 7
 - 2.5 ZigBee 7
 - 2.6 UWB 8

- 3 Wireless Interoperability** **9**
 - 3.1 Interoperability Problems 9
 - 3.2 Perceived areas of concern 11
 - 3.3 Interoperability initiatives 12

- 4 Wireless Interference** **14**
 - 4.1 Interference Issues 14
 - 4.2 A practical wireless infrastructure 15
 - 4.3 Potential impact of malicious interference 15

- 5 Security and Interoperability** **16**
 - 5.1 Security 16
 - 5.2 Key interoperability issues for security 17

- 6 Conclusions** **19**

- References** **19**

- List of Abbreviations** **22**

This page is intentionally blank

1 Introduction

1.1 Purpose

This report forms deliverable D1 of the FORWARD project. It is the first and only deliverable of Work Package 3 *Interoperability of Wireless Comms*.

The purpose of Work Package 3 is to informally assess the current level of interoperability in the area of wireless communications. This was achieved through a survey of wireless technologies, interviews with technicians with direct experience of using such technologies and reference to previous QinetiQ experience in military applications in this area.

The insight gained in Work Package 3 will underpin the research performed in Work Package 4: *Enabling Interoperability of Bluetooth Devices*.

1.2 The Next Wave Technologies and Markets vIRC

The FORWARD project is part of the DTI sponsored Next Wave Technologies and Markets programme¹. The aim of the programme is to ensure that UK business is structured and equipped to exploit the new information and communications technologies offered by the pervasive computing paradigm (described in Section 1.3 below). In addition, the programme aims to foster viable markets with confident consumers so that U.K. citizens can enjoy the benefits offered by such future technology environments. The programme achieves this by supporting seven themed virtual interdisciplinary research centres (vIRC), integrating and disseminating the research via a knowledge transfer club. The FORWARD project is part of the *City and Buildings Virtual Research Centre*, whose focus is challenges in mobile appliance design, infrastructure integration, delivery architectures and interaction design.

1.3 Pervasive Computing

The pervasive computing paradigm foresees communicating and computational devices embedded in all parts of our environment, from our physical selves, to our homes, offices, streets and so forth. Humans will be surrounded by intelligent, intuitive, interfaces capable of providing information and communication facilities efficiently and effectively. Systems will recognise the presence of individuals, perhaps even their mood, in an unobtrusive manner, modifying their functionality according to the users changing needs. The prolific amount of communicating devices will provide and enable multiple dynamic networks at any one location. The systems created from the integration of these large, complex networks will provide many new ubiquitous services, *nu-services*. In order that users may take advantage of the *nu-services*, users and their autonomous agents will be able to traverse these networks passing seamlessly from one to another, coexisting in many at a single point in time. So creating a truly ubiquitous computing environment capable of supporting ambient intelligence.

1.4 The objectives of FORWARD

Trust is at the heart of all successful business relationships, both in the physical world and on-line, ensuring their longevity and stability. User confidence is essential to the development of Next Wave technologies and markets; if people do not believe that the technologies will deliver the desired functionality, then they will not purchase them.

The users of Next Wave technologies will have to be able to rely on them to not only secure their data, protecting it from unwanted eyes, but also to deliver a certain quality of desired basic functionality and services. However, the inevitable complexity of Next Wave technologies and environments means that this will be extremely challenging to achieve. First, there will be more information to secure. In order to take advantage of next wave technologies companies and individuals will not only increasingly store information electronically, but their Cyber-actions (digital behaviour) may also be

¹ www.nextwave.org.uk

recorded by third parties. In some cases the stored information will be extremely valuable, perhaps a key business asset or sensitive personal data.

Second, the required communications infrastructures will be far more complex. Dynamic networks, networks that are mobile and can be created in an ad hoc manner, are core to the pervasive computing paradigm. The devices that populate such networks will have to be capable of interaction. The protocols and mechanisms for establishing such forms of communication will have to be scalable, and the infrastructures reliable and re-configurable. Designing systems formed from such networks will be challenging. It is unlikely that a human will be capable of even imagining all of the possible configurations such a system might be in. Such complex systems may possess emergent properties not conceived of in their design, the result of combining many components. These properties may be undesirable, impacting upon the integrity of the system and possibly the trust of the user. Techniques will have to be developed which support the design and implementation of high-integrity systems, capable of evaluating emergent properties, and enabling the assessment and validation of the technologies the systems use. Relevant standards will have to evolve to capture new types of behaviour and interactions.

The aim of project FORWARD is to enable the development of trustworthy flexible, ambient intelligent environments. It will achieve this by systematically investigating core issues in the development of trustworthy wireless communications protocols and devices, delivering a methodology based on rigorous tools and techniques. Interoperability between devices is one of these core concepts. If we cannot achieve reliable interoperability then we will not be able to deliver ambient intelligence and ubiquitous computing, nor the accompanying *nu-services*.

1.5 Structure of the Document

This report is structured as follows. Section 2 introduces the current mainstream wireless technologies and standards, focusing on Bluetooth and IEEE 802.11(a,b,g). Section 3 discusses the state of wireless interoperability, whilst Section 4 describes interference issues, and Section 5 discusses the potential implications interoperability problems may have on information security. Finally, Section 6 presents conclusions on the current state of interoperability of wireless communications devices.

2 Current Wireless Technologies

2.1 Performance issues of wireless technologies

Wireless technology differs in one important respect from wired technology. The communications medium is the *ether* (e.g. air) rather than copper wire or fiber optic cable. The transmissions are made using Radio Frequency (RF) propagation² rather than sending signals down a wire or cable. This rather obvious distinction has a number of impacts on the performance of the technology. Figures usually quoted for wireless technologies express performance in terms of range and bandwidth (data throughput). These figures are idealised, since the exact performance of any device, group of devices or wireless network will depend on the environment into which it is deployed. This is not the case (generally) for wired technologies, where modern cabling is shielded.

As an example, the throughput and range of wireless devices will depend on a number of external factors. These include: the construction of the building into which they are deployed and the presence of competing RF sources (especially microwave sources). Even the climate into which the devices are deployed could affect performance. As with wired networks, the best performance of the network is limited by the performance of the weakest component.

Current mainstream wireless technologies use a specific part of the RF spectrum. The 2.4 GHz band is unregulated, meaning that users are free to use it for any purpose without restriction. RF radiation in this band is readily absorbed by water molecules and as a result this frequency has been chosen as the optimum frequency at which microwave ovens should operate.

The water absorption properties of this part of the RF spectrum allow the range of the wireless technologies to be intentionally limited. As a result, the range depends on the power output of the transmitters. This allows the operation of distinct networks in relatively small spaces that do not interfere with each other. The downside of the water absorption property is that for very humid conditions, the range of the devices may be very seriously degraded. Given the effect of environmental factors on the performance of wireless technologies, the performance figures quoted below should only be taken as indicative rather than definitive (there is no guarantee that a particular installation would be able to achieve them).

2.2 Bluetooth

2.2.1 Background

The Bluetooth technology is named after the Danish king Harald Blåtand (Bluetooth) born AD908, who was responsible for uniting his country under Christianity. Originally the standard was developed by an Ericsson led consortium including IBM, Intel, Nokia and Toshiba. This consortium was joined by a newly formed organisation the Bluetooth Special Interest Group (SIG). The Bluetooth SIG has rapidly expanded to around 2000 members, with the original consortium joining it in 2000 to form a Promoter group responsible for leading the SIG's activities.

2.2.2 Wireless range and frequencies

Bluetooth is designed to connect devices over a relatively short range. The short range is dictated by two major requirements. First, the need for many Bluetooth interactions to coexist within closely located physical spaces. An open plan office, for example, might be home to a number of independent Bluetooth networks that must form separate mini- networks without interfering with one another. Second, the requirement for Bluetooth to be deployed in small portable (or indeed wearable) battery powered devices means that the power available to Bluetooth transmitters must be kept to an absolute minimum.

As a result of these requirements, the range for Bluetooth devices is usually quoted as around 10m, however, experience in QinetiQ has achieved successful communication at distances of 100m.

² Here the term RF propagation is being used to represent communications over the entire electromagnetic spectrum.

The data throughput provided by Bluetooth is low, around 433Kbps working in symmetric mode or 732Kbps and 56kbps for asymmetric mode. Note that this figure is unlikely to actually be realised by user data, due to protocol overheads.

Up to 8 Bluetooth enabled devices can be connected simultaneously into a small network known as a piconet. Overlapping piconets can form a scatternet.

In recognition that the frequency chosen for Bluetooth would be subject to external interference, Bluetooth devices employ frequency hopping techniques. Obviously, to communicate effectively, this frequency hopping must be synchronised between devices.

The Bluetooth SIG controls the standard and associate intellectual property. In order to sell Bluetooth technologies, vendors have to be a member of the Bluetooth SIG and their products must have undergone the Bluetooth Qualification Programme. The program seeks to test implementations against all aspects of the specification. In addition the qualification programme seeks to test a candidates interoperability with other implementations.

Version 1.0 of the specification also suffered from a lack of international harmonisation regarding the use of the RF spectrum. In some countries, for example France and Spain, part of the 2.4 GHz band was already being used for non-commercial purposes. There was a need to avoid using these parts of the spectrum when Bluetooth performed its frequency hopping and so the number of distinct frequencies that a Bluetooth device could hop to was limited to 23 rather than the 79 used by the rest of the world. This specification amendment was released as version 1.0b. As a result of this change, devices using Version 1.0b of the specification are not compatible with devices using Version 1.0 (or indeed later versions).

As a result of negotiations, the 23 hop option of 1.0b was removed for Version 1.1 of the specification and all devices conforming to the 1.1 version of the specification should use 79 hops.

The current version of the specification is 1.1. This version has tightened up many areas of the specification so that implementations from different vendors are more likely to communicate. However, problems still remain and Version 1.2 of the specification is expected later in 2003. Notable changes to be included in Version 1.2 are changes to ensure co-existence with IEEE 802.11b.

2.2.3 Overview of Application Areas and Profiles

Bluetooth can be applied to a number of application areas. The Bluetooth specification is arranged into a number of profiles. These profiles are arranged hierarchically, with generic profiles providing base services to high layer application profiles. The higher layer profiles, determine how Bluetooth devices should perform in specific application areas. Currently, 13 profiles are defined, although more are expected.

General Access Profile (GAP) – This profile defines how Bluetooth devices find and connect to each other. Security protocols are also defined in this profile. To ensure that basic interoperability is achieved, all Bluetooth devices must conform to at least the GAP.

Service Discovery Application Profile – This profile defines the features and procedures for an application in a Bluetooth device to discover services that are registered in other Bluetooth devices and to retrieve any desired available information that is vital to these services. Most applications require this profile.

Generic Object Exchange Profile (GOEP) – This profile defines the requirements for Bluetooth devices necessary for the support of object exchange activities. The objects exchanged include synchronisation data or simple binary file transfers. The profile includes the use of a server by a client to either push or pull data.

As well as the generic profiles, a number of specialisation groups of protocols exist. For example, the Serial Profiles are concerned with host computer and peripheral communications. The Mobile Telephony and Networking Profiles address the mobile phone and computer networking arenas respectively.

Serial Profiles:

Serial Port Profile – This profile defines the protocols and procedures to be used by devices to set up and connect virtual serial ports. For tasks such as data transfer and printing, this serial port emulation can then be used.

Object Push Profile – This profile is used for the exchange of small objects between devices, such as business cards. This profile makes use of the GOEP to define the interoperability requirements for the protocols needed by the applications.

File Transfer Profile – The application requirements for Bluetooth devices necessary for the support of file transfers are defined by this profile. This profile uses the GOEP as a base profile to define the interoperability requirements. The most common devices using this profile would be (but are not limited to) PCs, notebooks, and Personal Digital Assistants (PDAs).

Synchronisation Profile – This profile defines the requirements for the protocols and procedures to be used by the devices performing synchronisation functionality, for example between diaries on a PDA and a desktop PC. This profile also uses the GOEP.

Mobile Telephony Arena Profiles:

Headset Profile – This profile defines the protocol and procedures used by devices to implement the usage model called 'Ultimate Headset'. Devices would include headsets and personal computers. The headset can act as the devices audio input and output mechanism, providing full duplex audio, whilst being wirelessly connected.

Cordless Telephony Profile – This profile is used by devices implementing the so called '3-in-1 phone'. The '3-in-1' phone concept means that the same phone could act as a portable phone in the home to a fixed line, as a cell phone on the move and as an intercom between headsets. This profile can also be applied more generally to wireless telephony in a residential or small office environment. A separate profile (the Intercom Profile) implements the 3-in-1 phone concept of intercom functionality.

Current safety drives in the UK to ban the use of mobile phones whilst driving may seriously curtail the uptake of devices utilising the Cordless Telephony Profile.

Networking Functionality Profiles:

LAN Access Profile – This profile defines how Bluetooth-enabled devices can access the services of a Local Area Network (LAN) using Point to Point Protocol (PPP), and also shows how the same PPP mechanisms are used to form a network consisting of two Bluetooth-enabled devices.

Fax Profile – This profile is implemented by those devices implementing the fax part of the usage model called 'Data Access Points, Wide Area Networks', for example a mobile phone being used by a computer as a wireless fax modem to send or receive a fax message.

Dial-Up Networking Profile – This profile defines the protocols and procedures used by devices implementing the usage model, 'Internet Bridge', for example modems and mobile phones.

The explanations of the Bluetooth profiles given above illustrate that many of the higher level profiles, for example the File Transfer Profile, build on the lower levels such as the GOEP or GAP. As a result, implementation incompatibilities at lower layer profiles have a far more drastic effect than discrepancies at the higher layers. An implementation discrepancy in the GAP profile, for example, may mean that two devices do not inter-operate at all. A discrepancy at a high profile layer could result in two devices inter-operating in some areas of functionality but not all.

2.3 IEEE 802.11

2.3.1 Overview

This standard is aimed primarily at providing a replacement for cabled networks. In buildings where it is impractical to lay cables, perhaps for local planning control reasons, wireless technologies can be used instead to form a Wireless Local Area Network (WLAN).

WLAN technology operates around the principle of an access point. The access point is the interface between the wireless and wired world, as well as the hub through which wireless-enabled hosts communicate. Since the WLAN access point is static, installed in a fixed location within a building, the power it can consume is typically limited by the mains voltage rather than scarce battery power. Similarly, host computers within a fixed installation such as a building are free to draw on mains power. The range for WLAN technology is normally quoted at 100m. This range allows wireless networks to be formed on the scale of a building or individual floor (rather than intra-office for Bluetooth).

2.3.2 Standard Variants

The data throughput for IEEE 802.11 depends on the particular variant, however, it is in the order of a few Mbits/s rather than the Kbits/s of Bluetooth. The network speed is considered sufficient for current requirements, although there is some doubt that it is future-proof.

The original IEEE 802.11 standard was published in 1999 and provided for data rates up to 2Mbps again using the 2.4 GHz band. Like Bluetooth, IEEE 802.11 employs frequency hopping techniques to limit the impact of interference, although the rate of hopping is slower than for Bluetooth. There are a number of different variants to the standard, the main ones are described below.

IEEE 802.11a: This variant of the specification uses the 5 GHz band and transmits data on multiple sub-carriers within the communications channel, to provide data rates up to 54Mbps. The 5 GHz band is a relatively uncluttered part of the RF spectrum, and so there is space within the spectrum for 12 non-overlapping channels.

Whilst the bands are less prone to interference than those in the 2.4 GHz bands, the increased absorption of RF radiation in the 5 GHz band by walls and other solid objects causes signals to be more greatly attenuated. As a result of this attenuation and the increased data rates, the range of 802.11a is reduced over the base standard. This may, however, be an advantage since it will limit the leakage outside of a building or industrial site if antenna placement is considered carefully.

The modulation technique employed by 802.11a Orthogonal Frequency Division Multiplexing (OFDM) consumes significantly more power than other modulation techniques.

Since IEEE 802.11a operates on a separate frequency band to the other 802.11 standards, interoperability between 802.11a and other variants is only possible via a gateway, which converts between the two formats.

IEEE 802.11b: This variant operates in the same 2.4 GHz band as Bluetooth and is capable of supporting 5.5Mbps and 11Mbps. The standard was adopted by the Wireless Ethernet Compatibility Alliance (WECA) in 1999 and trademarked under the name WiFi. This standard also defines how wireless networks can implement the Wired Equivalent Privacy (WEP) standard to achieve data security. The WEP standard has been the subject of much attention from the computer security and hacking communities and has been shown to provide inadequate levels of security against a competent attacker.

IEEE 802.11g: Currently, this standard is in draft form, although it is due for final ratification sometime in 2003. The standard provides high-speed extensions to IEEE 802.11b, with data rates up to 54Mbps. This throughput is comparable with 802.11a, however, since the 802.11g standard uses the 2.4 GHz band, the two are not inter-operable without gateway technology.

Other standards in the 802.11 family include:

IEEE 802.11c: this standard sought to address WLAN bridging issues and has been folded into the 802.11 standard.

IEEE 802.11d: addresses deployment issues in developing countries.

IEEE 802.11e: addresses quality of service issues.

IEEE 802.11i: this standard seeks to address the failings of WEP and propose new security extensions. Due for publication sometime in 2003.

IEEE 802.11f: this standard seeks to allow communications between access points from different vendors so that users can roam from network to network dynamically.

The IEEE 802.11f standard has not been seen as a vital part of WLAN technology by vendors and users alike. Users are tempted (and encouraged) to buy solutions from a single source (i.e. all CISCO equipment) and vendors are unwilling to support anything that may hand market share to their competitors.

However, for future ubiquitous computing requirements to be satisfied, the IEEE 802.11f standard must be agreed upon and fully implemented (or a successor or alternative proposed). On the positive side, this standard, in draft form has some support from vendors, notably CISCO, which is implementing a version of the standard.

2.4 HomeRF

This wireless alternative technology again uses the 2.4 GHz frequency and performs frequency hopping in much the same manner as Bluetooth and IEEE 802.11. It is capable of data rates of around 20Mbps/s but crucially is able to support high quality voice traffic as well as data. It has a comparable range to the IEEE 802.11 technologies.

Since the technology is simpler than WiFi, products should be cheaper. Additionally a simpler technology means less components, so the wireless cards to fit in devices can be smaller. HomeRF allows the use of compact flash cards which will fit into handheld devices.

HomeRF is also designed to counter interference by providing more separate channels that allow users to avoid channels that are blocked. Lastly, HomeRF was designed with security in mind and has some significant advantages over IEEE 802.11. Each HomeRF network is separated from other HomeRF networks in such a way as to minimise the risk of devices from an external network intercepting information. In addition to the network separation, HomeRF uses a strong 56bit encryption algorithm devised by Intel. For export control reasons devices will revert to using 40 bit encryption if required.

HomeRF, however, has failed to compete with the WiFi alliance and earlier this year lost all of its major industry backers. From a web news report dated 7th January 2003:

“A consortium of companies promoting a wireless home networking specification to compete with Wi-Fi disbanded at the beginning of the year, representing its commercial end.” [Shi03]

2.5 ZigBee

An upcoming technology is the ZigBee wireless standard, based on IEEE 802.15.4. The standard is capable of operating in three bands: 2.4GHz (worldwide), 868MHz (Europe) and 915MHz (Americas).

The standard is designed for very low power consumption, meaning that battery life is months rather than days or weeks. The data throughput is lower than Bluetooth (20-40Kbps at the 2.4GHz frequency) although the quoted range is slightly better (10-75m). The protocol is much simpler than Bluetooth, since it is designed to support less complex data packets.

This standard has been designed to provide building automation services (both in domestic and industrial settings), with a central master mode and up to 254 slave nodes communicating with it. Most devices on the network would be in sleep mode (not transmitting data) for most of the time. Slave nodes might be building devices such as burglar alarms, lights or heating systems. Whilst most devices are asleep, low latency is a feature of ZigBee, it is claimed that a ZigBee device can wake up and transmit a packet across the network in around 15 milliseconds. As a result of its design, this standard could be seen as a candidate technology in the pervasive vision of wireless networking.

The ZigBee standard is supported by a not-for-profit alliance. The main promoter companies of ZigBee are: Philips, Mitsubishi, Motorola and Invensys with an additional 25 companies providing input and support to the specification as well as implementation of integrated circuits.

Devices are not expected on the market until 2004 at the earliest, so its commercial viability will depend on the ability of Bluetooth and IEEE 802.11 to provide a cost-effective alternative in the meantime.

Interoperability between Bluetooth and ZigBee would be possible only through gateway devices, since the protocols are completely different. One could envisage the master device (the main building control centre) being Bluetooth enabled to allow communication with a PDA for the collection of statistics or for configuration tasks.

2.6 UltraWideBand (UWB)

A further technology to join the wireless market is UWB, operating in the 3.1 - 10.6 GHz frequency range. This is not an exclusive frequency allocation and so UWB technology has to be designed from the outset to cope with interference from other spectrum users. One major area of concern in the interference area is the Global Positioning by Satellite (GPS) system.

The definition of what constitutes wide-band is somewhat informal, although it is generally taken to be any device that operates across a frequency spread of 25% from a centre frequency (around 1.5GHz).

Whilst UWB technology is not fully developed, data rates of around 100Mbps over a range of 100m are claimed. Due to the way that the frequency band is utilised and the data encoded, the technology is far more resilient to interference from other devices than narrow-band technologies such as IEEE 802.11. This allows UWB to efficiently support a higher density of devices without a serious performance impact. This property, coupled with its relatively high data rates makes it ideal for the domestic environment.

3 Wireless Interoperability

3.1 Interoperability Problems

When studying the area of interoperability, it is difficult to get concrete examples of problems. The lack of hard evidence is partly due to the area being difficult to quantify and partly because companies consider product shortcomings to be sensitive information to be kept from the public domain [Kew03]. Indeed, some vendors even claim that the problem of interoperability has been solved:

“Bluetooth interoperability problems are largely solved now, according to suppliers of the technology.

...

“Interoperability is good, it has certainly improved and is now better than 95 percent.” said Charles Sturman, Bluetooth product manager at system and IP developer TTPCom

...

...the interoperability issues were largely addressed in the latest 1.1 version of the Bluetooth radio specification, which...is the basis of chips and systems now coming onto the market...” [BWea]

Products usually attract user forums on the Internet. In areas of consumer electronics where wireless technology has an impact, such as Personal Digital Assistants (PDAs), the associated user forums are an interesting source of information. Whilst the evidence provided by these forums is not subject to scientific rigour, it can be useful, especially to gain an insight into the end-user perception of the technology and its interoperability problems (see [PPC03] and select the “wireless” forum as an example).

The speed of market advancement in the technology arena means that in a very short time information on specific products becomes of historic interest only. Many commentators have attributed interoperability problems to ambiguities in specifications:

“Bluetooth products are insecure and interoperability is elusive because the specification allows vendors to select default security settings, and the implementation process ensures only low-level compatibility. What you need to know Gartner believes [is that] Bluetooth vendors will not offer adequate interoperability or security for more than single-vendor point solutions through year-end 2005. Even when vendor offerings mature, legacy Bluetooth devices will create opportunities for malicious activities in the near future, even if the Bluetooth SIG or a small set of major vendors creates an enterprise-grade set of Bluetooth products...” [Cla02]

As a result of the incomplete specifications, vendors are forced into testing programs not only to claim conformance with the Bluetooth specification, but also to ensure that their implementation inter-operates with the implementations of other major players:

“Tality Corporation, a subsidiary of Cadence Design Systems, Inc. (NYSE:CDN) – today announced that it has established and verified stable interoperability between its Bluetooth Development System and products from Cambridge Silicon Radio, Ericsson, Philips Semiconductors and Texas Instruments – leading providers of Bluetooth silicon platforms. The interoperability was demonstrated in an open forum – the Bluetooth World Congress 2001.” [Tal01]

Given the number of vendors and the number of defined profiles within the Bluetooth specification set (not to mention different versions), to devise a comprehensive testing strategy is non-trivial and performing the testing is time consuming. The impact of the need for such comprehensive testing is increased production cost and time delays to the vendors. For users it can result in a lack of market choice.

The problem of vendors implementing slightly differing solutions is compounded by the fact that, certainly for Bluetooth devices, the configuration is seen as confusing and insufficiently well documented:

“If you have ever tried to get two Bluetooth devices to operate with each other you know this type of effort is important. First you start the discovery process. After the devices have discovered each other you need to “bond” the devices together. Every device does it a different way. It is extremely difficult to figure out what to do and then actually do it. Bluetooth’s potential is blunted and delayed until this problem is solved. PalmSource and Sony Ericsson have wisely gotten together to fix the problem for their products. However, both companies will need to make these one-off deals with every other company they want their devices to work together. This will take a long time and a lot of effort.” [OM01]

Cross-vendor interoperability problems leave the end-user with a stark choice: either risk devices from multiple vendors not communicating or purchase only a mix of the devices that the vendors have explicitly stated will work together (which narrows the options considerably):

“In practice, Bluetooth-enabled devices don’t work as advertised. Examples from attempts to use Bluetooth-enabled devices make the point, as noted:

...

It is difficult to find and recognise specific devices in an environment where a number of Bluetooth-enabled devices are turned on. Your devices could discover another device that does not have security turned on.

...

Piconets don’t work in an uncontrolled environment. Point-to-point connections work only when the devices are certified for use with each other.

...

Gartner Dataquest has asked the Bluetooth SIG for examples of cases in which interoperability has been demonstrated in an open environment. The SIG was unable to provide any.

...

The current qualification system is inadequate. It does not ensure the level of interoperability required to accomplish even the simple tasks normally expected from Bluetooth-enabled devices. As a result, companies that make products using Bluetooth must provide customers with a list of recommended products that will work with their product. Such an arrangement is an unsatisfactory substitute for open interoperability.” [Gar02]

Additionally, since the interfaces to Bluetooth enabled devices may be low functionality (for example, a telephone headset with a minimal set of buttons, rather than a full-function computer keyboard), troubleshooting problems when they do arise is complicated and time-consuming:

““When you encounter a Bluetooth interoperability problem without some in-depth visibility of what is happening, you have no idea which component is at fault. It’s like sitting at the end of a five-mile traffic jam trying to figure out what’s causing the holdup,” said consultant Jennifer Bray at Cambridge Silicon Radio (CSR).” [Lon02]

In common with Bluetooth, the IEEE 802.11 standards have been devised by a vendor-based forum. The members of the forum each have their own agendas and established technology. As a result, the standard produced is a compromise.

“Certification happens late in the development process, but the roots of interoperability reach back to the earlier stages of product design and development when each manufacturer (or silicon supplier) adds value by optimising its designs in unique ways. It’s

a good approach, but one that can translate into different (but in-spec) behaviour in transmitters and receivers, and may leave your own devices working well together but not with devices from other makers.” [Blu]

The IEEE 802.11a standard uses a separate frequency (5 GHz) to the other IEEE 802.11 standard (b & g) and as a result, is only capable of inter-operating with networks or devices of the other standards through a gateway device.

In theory it is possible to get IEEE 802.11b and g variants of the specification to inter-operate. The IEEE 802.11g standard provides for equipment to inter-operate with IEEE 802.11b equipment by switching to the lower speed standard. However, current problems with the IEEE 802.11g specification have raised the fear that, rather than co-operating with the IEEE 802.11b devices, IEEE 802.11g devices may just force their slower cousins off air by blocking their signals.

The latest standard, IEEE 802.11g, is currently only in the design stage, however, products are starting to appear, claiming conformance to the draft specification:

“Of even more concern, however, is the prospect of interoperability problems among draft-802.11g products. My test results from mixing Linksys and BuffaloTech products – both of which use Broadcom’s ‘54g’ technology – were not conclusive, but they weren’t encouraging either.” [Hig03]

Another example a product being introduced to the market ahead of the standards is the Apple Airport Extreme system [Mac03].

3.2 Perceived areas of concern

The market perception of Bluetooth has possibly been damaged by the over-hyping of original expectations. As a result, it may take a period of time before users wholeheartedly embrace the technology:

“Mass use of Bluetooth for short-range wireless communications is years away. The technology’s backers hyped Bluetooth and, back in reality, now predict that it will be eight years before Bluetooth is as commonly used as a mobile phone is today. “We did overheat it a lot,” said Mike McCamon, executive director of the Bluetooth Special Interest Group.” [Eve02]

One concern to business adopters of the technology is the cost to them in support terms of Bluetooth interoperability problems. Bluetooth and other wireless technologies should give businesses a cost and operational advantage over using wired technologies, however, simply deploying systems that are Bluetooth enabled is not the end of the story:

““Bluetooth technology will cost businesses and consumers worldwide an additional \$5.6 billion annually as a result of added support and usage costs necessary to use the technology”, according to analyst firm Gartner. Security flaws and interoperability problems will make Bluetooth-enabled devices inadequate for use without additional spending to correct the problem areas, says the analyst firm, which also predicts that more than 560 million Bluetooth-enabled devices will be purchased by businesses and consumers.

“Bluetooth deployment costs will be higher than other wireless technologies because of limited interoperability and the need to implement policies to safeguard against data corruption and theft,” said Bill Clark, research director for Gartner. “Although manufacturers must have products certified by Bluetooth prior to sale, the certification does not make high-level security and interoperability between products a requirement. Therefore, the user interfaces, default configurations and usability choices are left to the individual manufacturers’ to decide upon.”” [Sun02].

In addition to the issues previously mentioned, there is also concern over the usage of specifications that have yet to be ratified by the standards bodies. Devices are currently being sold claiming to adhere to Bluetooth version 1.2, when this specification is still only in draft form (c.f. the IEEE 802.11 market).

The result of implementing draft specifications may be further interoperability problems. Any remaining inconsistencies in the draft specifications may surface in products, which could result in the need for software upgrades or even the complete replacement of a product. In addition, devices that correctly implement the fully published specification may not completely inter-operate with the early-to-market devices.

With IEEE 802.11, vendors are also producing devices that claim to conform to a draft standard. As with the Bluetooth 1.2 case, devices are emerging which follow the 802.11g standard, that is still in draft form.

“More disturbingly, however, is the interim introduction of 802.11g-draft chipsets from several companies. These chipsets, while following the current draft proposal for 22 Mbps and 54 Mbps in the 2.4 GHz band, as well as backwards support for 802.11b’s several speeds, could produce a near-term market confusion. The WiFi Alliance won’t be testing for 802.11g interoperability for some time – possibly not until 2004 according to some reports.” [Wi02]

“...the 802.11g wireless Local Area Network (LAN) standard is supposed to deliver on the promise of seamless interoperability by ensuring that compliant equipment from different manufacturers will work together. Now, in an ironic twist, some vendors are claiming it could actually cause those interoperability problems

...

There are actually two concerns about 802.11g. Concern No. 1 is whether the technology will work with legacy 802.11b clients; the big fear is that legacy 802.11b clients could be knocked off the air in favour of 802.11g kit in crowded networks. Concern No. 2: whether all 802.11g products will be able to inter-operate, particularly with the number of pre-standard products being announced.” [Uns03]

“You can, today, buy an 802.11g (pre-standard) device. This story was written on a PC connected over a Linksys WRT54G “Wireless-G” broadband router. It really is running at 54 megabits a second, giving a pretty good working approximation of 20 megabits per second throughput. And, the good news: it will work fine with my old WiFi cards on the 11b standard too, even though it slows down to 11 megabits (5 megabits throughput) to do so.

...

So why is this bad news? The answer is that since it works, in a one-off situation like this, people will, quite naturally, buy it. And then, the fun will begin; because there’s no guarantee of compatibility with other 11 ‘pre-g’ standards.” [Kew03].

3.3 Interoperability initiatives

The difficulty in setting up Bluetooth devices to allow them to communicate has been acknowledged by the Bluetooth Special Interest Group (SIG) as a major impediment to user take-up. As a result, the Bluetooth SIG launched its – 5-Minute Ready initiative, in December 2002. This initiative has a number of strands, among them educating the public into the benefits of Bluetooth and its application. However, the two major strands of the initiative are aimed squarely at its vendor membership

To quote the Bluetooth SIG press release [BWeb], initiatives include:

- A Bluetooth Designer Handbook with information on best practises and recommended methodologies for Bluetooth implementations;

- Reference platforms against which manufacturers can test their products;
- Establishment of an independent testing facility for device interoperability at the University of Kansas, sponsored by the Bluetooth SIG.

Microsoft has, until recently, resisted implementing Bluetooth support within its operating systems, possibly due to the immaturity of the technology. However, Window XP Service Pack 1 now comes with native support for Bluetooth version 1.1. It remains to be seen what influence Microsoft will have on the Bluetooth market, however, their involvement is seen by many to be a positive step towards interoperability improvements. Since Microsoft has such a large share of the desktop market and many PDA's run Windows operating systems, the need for other vendors to inter-operate seamlessly with the Microsoft solution will be crucial.

A number of consulting companies are offering Bluetooth testing services and it may be that the smaller vendors will utilise the experience and expertise of these companies to reduce costs and time to market. Examples of companies that do testing and development are given at [RFI03, WF03, CTC03, BTS03].

In the 802.11 area, the Wireless Ethernet Compatibility Alliance (WECA) organisation controls the use of the WiFi trademark and only allows vendors to badge their products with the WiFi mark if their product passes a number of conformance and interoperability tests. Unfortunately, these tests are limited in scope to basic functionality levels, which means that a device can be certified as WiFi compliant and yet still not inter-operate with other vendors' devices.

Currently, the testing is limited to IEEE 802.11a and b. Vendors pay a fee to join the WECA organisation and then pay per product to have them certified (currently \$15000). Testing of upgrades is, however, free. The WECA organisation has not yet announced any plans to perform interoperability testing on IEEE 802.11g products.

Other organisations run IEEE 802.11 testing facilities to extend the test coverage from that which is offered by the WECA certification process. An example of one such organisation is the University of New Hampshire InterOperability Lab [IOL03].

4 Wireless Interference

4.1 Interference Issues

4.1.1 Between IEEE 802.11 and Bluetooth

The exact functionality and performance of equipment will depend on the relative positions of both building structure and IEEE 802.11 / Bluetooth devices. One study [LSN01] produced a simulation of interference between Bluetooth and IEEE 802.11 and then corroborated its findings using experiments. A further study [Cha01] illustrated the effects of interference between Bluetooth and IEEE 802.11 using configurations of components found in typical office environments, including the use of computers that are both Bluetooth and IEEE 802.11 enabled. Both [LSN01] and [Cha01] found that the interference between Bluetooth and IEEE 802.11 caused increased error rates and reduced data throughput. However, the problems were not insurmountable and the studies were able to suggest technical resolutions to the problems.

Wireless Local Area Network (WLAN) access points and Bluetooth devices, while not entirely blocking each others transmissions, may reduce effective ranges and data throughput. It should be noted that due to differing use of frequency hopping techniques, Bluetooth is likely to interfere more with a WLAN than a WLAN is to interfere with Bluetooth. One reason for this is due to the fact that whilst Bluetooth hops 1600 times a second, IEEE 802.11 only hops around 50 times and so will continue to attempt to use a blocked frequency for longer. Both studies at [Fen01] and [FHS] used a combination of analytical and experimental approaches to show the effect of interference on the error rates of a wireless technology. Both studies found that the relatively long packets and slow rate of frequency hopping used by IEEE 802.11 meant that interference caused higher error rates in IEEE 802.11 than in Bluetooth.

4.1.2 With other spectrum users

Due to the use of the unregulated portion of the Radio Frequency (RF) spectrum, Bluetooth and IEEE 802.11 occupy the same frequency ranges as a number of other devices. Primary examples of these are digital cordless phones and microwave cookers.

These present two different types of interference. Digital phones use the 2.4 GHz band in much the same way as the wireless networking technologies, i.e. the handset(s) and the base station use RF waves to communicate information. On the other hand, a microwave cooker uses a high power (approx 800W) microwave source to heat food. Any microwave energy that leaves the microwave cooker is a side effect of the devices main function.

There is anecdotal evidence that both digital phones and microwave cookers interfere with wireless computing technologies [Moh03]. The study at [Lee99] investigated the error rate suffered by a IEEE 802.11 network when a microwave oven was operating in the proximity. Various configurations were tried which took into account the relative placement of wireless technology, microwave oven and building components such as walls. The study concluded that microwave ovens were indeed a problem if they were not sympathetically located. Within an office environment, interference from microwave cookers can be minimised by placing such devices away from wireless computing networks. Unfortunately, the same is not true of digital phones (as one of their features is that they can be relocated whilst in use). As a result, the use of digital mobile phones may cause network interference resulting in reduced network throughput or severed connections.

Other QinetiQ experience includes interference problems between an Apple Airport base-station and a BskyB satellite television receiver. When the devices were in close proximity dropped connections and reduced throughputs were incurred. However, when the devices were sufficiently separated (approximately 10 feet), the problems were removed. This highlights the point that interference with wireless technology may not come from the most obvious sources (since the satellite television receiver would not as such be considered to be a transmission source) and that placement of devices is crucial.

With regards to the domestic environment and the vision of ubiquitous computing, it must be realised that the presence of devices such as microwave cookers in the home may hamper the vision of all pervasive networks. Space restrictions within the domestic setting mean that scope for sympathetic placement of wireless devices may be limited or not possible. As a result, the wireless technology will have to be robust enough to cope with intermittent interference if it is to fulfil the ubiquitous role.

4.2 A practical wireless infrastructure

Consider an example company SmallCo which runs its operations from a single two story building. The company has Internet access with a local Internet Service Provider (ISP) using a 2Mbyte Asymmetric Digital Subscriber Line (ADSL) always on connection. Due to local planning regulations concerning listed buildings, the large scale modification of the building for cable runs has proved infeasible.

As a result, SmallCo has opted to use wireless networking solutions. On each floor of the building, a WLAN access point provides a hot-spot for network access. The WLAN access points are connected to the company ISP to allow onward connection to the Internet. Within each floor of the building are a number of offices. Each office is equipped with WLAN enabled PCs and laptops. Each office has shared facilities for scanning documents and for printed output. These devices are connected to via an office Bluetooth network. The number of WLAN access points required will depend on the propagation characteristics of the building.

Users regularly synchronise their Personal Digital Assistants (PDAs) with their desktop machines to keep calendars and diaries updated. Again these connections are implemented using Bluetooth. This functionality to support the wireless office exists now and can be rolled out as currently exists in the marketplace.

However, there are a number of associated potential interoperability problems. The interference problems previously highlighted would manifest itself in a number of ways at an application level. Users would have difficulties where there was a particularly high density of wireless devices.

Problems would include:

- Initiating connections to wireless devices may be unreliable. This unreliability would be caused by the negotiation sequence between devices either being interfered with or blocked totally.
- Connection throughput would be variable, with some transactions taking place at an acceptable rate, but others such as printing (where there is a large amount of data to transfer) taking a very long time. The slow throughput would result from packets being lost due to interference and therefore having to be retransmitted.
- Connections may be lost completely. If the interference is too high, then the association between devices may be destroyed.

All of these effects are likely to add to end user frustration with wireless technology.

4.3 Potential impact of malicious interference

The use of a relatively low power microwave source (in the order of 400W) in the vicinity of a WLAN can potentially disable the wireless receivers in wireless access points or connected hosts.

Simple equipment comprising a directional aerial and any device capable of generating radio frequency interference on the correct wavelength, would be sufficient to cause the targeted receivers to burn out.

In an area of high wireless use, such an attack could be used to disable a large number of systems in a very short time. A defence against this type of attack would be to physically shield sensitive systems from external attack, although this is likely to be an expensive exercise.

5 Security and Interoperability

5.1 Security

5.1.1 Generic Concepts

Issues of security and privacy will be core to the wide scale acceptance of ubiquitous computing. Unfortunately, the very principles that next wave technologies are built on, such as dynamic networking, interoperability between diverse components, and services built upon disjoint business offerings, impose constraints in terms of connectivity, computational power and energy availability. These constraints will make ensuring security harder, because they place real limits on the hardware and software utilised, whilst the security challenges become more complex.

To understand the interaction between security and interoperability it is important to define clearly what is meant by security. Classically, security is defined as comprising three key elements: confidentiality, integrity and availability.

- **Confidentiality** concerns the control of access to information. Confidentiality is preserved when authorised users, and programs operating on their behalf, are permitted only appropriate access to the information controlled by a system.
- **Integrity** concerns the accuracy of information processed by a system. Unauthorised users should not be able to alter information held on a system.
- **Availability** concerns the ability of an authorised user to access information when required and in a timely fashion.

More recently non-repudiation has been added to the list:

- **Non-repudiation** concerns the inability of a user who sends a message to later deny that they sent it. Non-repudiation protocols are designed to provide evidence which protects honest users from other cheating users.

All aspects of security presuppose the ability of the system to be able to authenticate and authorise users. The identification process will usually take the form of a challenge and response dialogue involving the exchange of credential information.

5.1.2 Wireless Comms

The security of wireless communications is likely to be harder to achieve than for wired networks because information is exchanged between system components using Radio Frequency (RF) signals over the ether. This presents elements wishing to compromise the system with a greater interface with which to eavesdrop on communications than would be possible in a wired network. Such activity could compromise the confidentiality of the system. In addition to eavesdropping, traffic could be either modified (threatening the integrity of the system) or replayed (allowing the identification process to be compromised). Securing the availability of service / data will also be much harder. As recent Internet attacks have shown, it is very hard to defend against Denial of Service (DoS) attacks, especially when an array of sources are used (such as in the Tribe Flood Network 2000 Distributed DoS (DDoS) attack). In the wireless arena, as well as the "normal" DoS attacks against application and transport layer services, the physical layer can be attacked. Such attacks would include jamming the parts of the RF spectrum used by wireless devices or seeking to overload receivers by using high energy levels of RF radiation directed against them.

To counter threats to confidentiality and integrity, wireless technology has adopted cryptographic techniques. The Wired Equivalent Privacy (WEP) standard, supported by standards for key management and distribution such as IEEE 802.1X were supposed to provide cryptographically secured

communications between wireless system components to prevent eavesdropping, tampering and replay. Unfortunately, the security of some of these measures, for example WEP [BGW], have been exposed as being inadequate. The weaknesses in the cryptography underlying WEP allow an attacker to employ cryptanalysis techniques to decrypt traffic on the network, given approximately one days worth of traffic on a network with average load. Current approaches to countering threats to availability in a wireless environment include standard (and not very effective) techniques from the wired world, such as filtering and bandwidth control, and physical shields (effective but expensive and so often restricted to critical systems).

5.2 Key interoperability issues for security

It is clear that interference is a great risk to information security, as discussed above. This section outlines two other key concerns related to the impact of interoperability issues on security.

5.2.1 Backwards compatibility

The rapid advancement of computing technology, both software and hardware, leaves behind a legacy of old systems. Such systems often represent a substantial investment, in terms of both financial cost and deployment time. Hence, there is pressure on new technology to be compatible with the existing technologies.

Often new technologies are built to be “backwards compatible” with some of the existing technologies. This means that they are able to interact with the existing technologies using the existing communication algorithms and formats, in addition to any new ones that they may incorporate. Such backwards compatibility can lead to what is known as the “lowest common denominator” solutions, which negates some of the benefit from the newer solutions. In other words, in order for different products to inter-operate they must use common communication standards; hence the communication standard chosen ought to be the best – most secure – standard that all the participating products support. It is possible that the only common communication standard is not very secure at all, or that the communication standard search order goes from least secure to most secure. Both of these situations could result in interoperability negotiations agreeing on an insecure standard. Having said this, with time – as the older technology – gets “sufficiently” phased out, the lowest common denominator rises.

Example: The original security provided by the IEEE 802.11 Wireless Local Area Network (WLAN) technology was considered to be poor, by the wireless technology community. Therefore, the IEEE 802.11 committee setup a working group to consider these issues and propose solutions; one of the results of this has been the development and adoption of the IEEE 802.1X security standard. It provides a framework for authentication and key management that may provide a platform for addressing some of the identified security issues, such as the secure generation and distribution of keys, for use with the framework’s associated security products [GBCC⁺03].

However, possibly due to the desire for backwards compatibility, the IEEE 802.1X standard mandates that any completely compliant solution must offer at least the “MD5 authentication” scheme, which is known to suffer from a man-in-the-middle (MITM) attacks; that is where communications between the two authenticating parties go via an intruder, who is capable of reading, modifying and generating messages. It is worth noting that some manufactures are ignoring this, possibly unnecessary, requirement – as old systems may have, or could be provided with, a different authentication scheme.

5.2.2 Under-specification of Standards

In general a standard (specification) or protocol is designed to be flexible so that it is applicable to the greatest variety of implementations, and is thus open to a variety of interpretations. However, this

flexibility in the specification may cause security vulnerabilities. This is because devices conforming to the same standard, but with differing valid implementations, may have (perhaps subtle) differences in behaviour. They will expect to receive certain messages from each other. However, due to their differences it is possible that a device sends messages which other devices do not expect to receive. When devices receive unexpected messages they may move into a insecure state; a lack of defensive programming against unexpected messages can lead to an unauthorised user gaining access to otherwise secured information or superuser (administrator) privileges, or to catastrophic failure potentially enabling an attacker to take control of, for example, a network router. In some extreme cases, such a difference in implementation may prevent different devices from communicating at all, and thus essentially implementing a permanent denial of service attack.

The necessary proliferation of these standards and protocols throughout network architectures makes the potential impact of such vulnerabilities a much greater risk; if they are faulty then associated vulnerabilities are likely to exist throughout the system.

Example: Implementations of the Simple Network Management Protocol (SNMP), from different vendors, were tested using malformed messages, and found to have security vulnerabilities, including buffer overflows, leading to superuser (administrator) access and denial of service attacks.

Common failures, in different implementations, suggest that the problem was due to underlying specification issue; it is very unlikely that they all suffer from the same accidental coding errors.

6 Conclusions

Conclusions on the current state of interoperability between wireless devices:

- The current wireless standards are some way short of being perfect in support of interoperability. The exact scale of the problem is disputed.
- The recent entry of Microsoft into the Bluetooth market is seen as a positive step for interoperability, vendors will be forced by Microsoft's weight to inter-operate with them (and so by implication with each other).
- In the rush to get products to market, vendors are implementing draft specifications. This policy may lead to short term interoperability problems.
- Shortcomings in the specifications have led to vendors implementing differing solutions. This has resulted in interoperability problems, even when implementations have been shown to conform to the standards. Interoperability is demonstrated through comprehensive testing between specific devices / systems.

Impact on the development of Next Wave technologies and markets:

- Pervasive computing environments cannot be achieved with the current levels of interoperability between devices.
- The testing strategies adopted in order to achieve device interoperability are both commercially expensive, leading to compromise that short changes the consumer, and not optimal since they are not scalable. It would be in-feasible to conceive of every device vendor performing tests with millions of other devices it may be required to interact with, and that the testing will cover every possible set of communications the device could possibly enter into.

Advice for current use of wireless equipment:

- When currently purchasing wireless equipment users should be careful to choose products that have been explicitly tested for interoperability.

References

- [BGW] Nikita Borisov, Ian Goldberg, and David Wagner. Security of the wep algorithm. <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>.
- [Blu] Ensuring interoperability. <http://www.get.agilent.com/bluetooth/rand/interop.shtml>.
- [BTS03] Bluetooth testing, qualification and certification services web site. <http://www.thewirelessdirectory.com/Bluetooth-Development/Bluetooth-Testing.htm>, 2003.
- [BWea] Official bluetooth in the news site. <http://www.bluetooth.com/news/news.asp?A=2&PID=112>, March.
- [BWeb] Official bluetooth in the news site. <http://www.bluetooth.com/news/news.asp?A=2&PID=336>.
- [Cha01] M.V.S. Chandrashekar et al. Evaluation of interference between ieee802.11b and bluetooth in a typical office environment. In *IEEE Personal, Indoor and Mobile Radio Communications Symposium 2001*, 2001.
- [Cla02] William Clark. Article on gartner's position on bluetooth. http://www.mobileinfo.com/News_2002/Issue42/Bluetooth_Gartner.htm, November 2002.
- [CTC03] Centro de tecnologia de las comunicaciones web site. <http://www.cetecom.es>, 2003.
- [Eve02] Joris Evers. Why we're still waiting for bluetooth. <http://www.pcworld.com/news/article/0,aid,101942,00.asp>, June 2002.
- [Fen01] Wang Feng et al. Performance of a bluetooth piconet in the presence of ieee802.11 wlans. In *IEEE Personal, Indoor and Mobile Radio Communications Symposium 2001*, 2001.
- [FHS] Throughput of ieee802.11 fhss networks in the presence of strongly interfering bluetooth networks.
- [Gar02] Bluetooth poised to achieve potential; interoperability could kill market, July 2002. Hardcopy of the Gartner Dataquest Product Analysis.
- [GBCC⁺03] Richard Gover, Casper Boden-Cummings, Richard Case, Simmon Cannon, and Kamran Azeem. Vulnerabilities and security solutions for ieee 802.11 based wlans. Technical Report QinetiQ/KI/COM/TR030149/1.1, QinetiQ, March 2003.
- [Hig03] Tim Higgins. Linksys instant wireless-g access point (wap54g). <http://www6.tomshardware.com/network/20030117/wireless-12.html>, January 2003.
- [IOL03] Interoperability lab web site. <http://www.iol.unh.edu/>, 2003.
- [Kew03] Guy Kewney. New wireless 11g 'standard' ends in tears. <http://www.theregister.co.uk/content/59/29250.html>, February 2003.
- [Lee99] Yang-Han Lee et al. The effects of microwave oven over the ieee802.11 fhss wireless lan card, 1999.
- [Lon02] MArk Long. Tackling the bluetooth interoperability issue? <http://www.e-insite.net/index.asp?layout=article&articleid=CA222285>, June 2002.

- [LSN01] Jim Lansford, Adrian Stephens, and Ron Nevo. Wifi (802.11b) and bluetooth: Enabling coexistence. *IEEE Network*, Sept/Oct 2001.
- [Mac03] Apple mac's official airport site. <http://www.apple.com/airport/>, 2003.
- [Moh03] Doug Mohney. The cons and pros of 2.4ghz wireless connections. <http://www.theinquirer.net/?article=7235>, January 2003.
- [OM01] Outlook4mobility news articles. <http://www.outlook4mobility.com/NewsAnalysis/oct2102.htm>, October 2001.
- [PPC03] Pocket pc thoughts forum index. <http://www.pocketpcthoughts.com/forums>, 2003.
- [RFI03] Radio frequency investigations ltd website. <http://www.rfi-wireless.com>, 2003.
- [Shi03] Richard Shim. Homerf working group disbands. http://news.com.com/2100-1039-979611.html?tag=cd_mh, January 2003.
- [Sun02] Jorgen Sundgot. Grim picture painted for bluetooth. <http://www.infosync.no/show.php?id=2304>, September 2002.
- [Tal01] Tality demonstrates bluetooth interoperability with leading silicon platforms. http://www.cadence.com/company/pr/pr01-bluetooth_interop.html, 2001.
- [Uns03] Interop woes smite 802.11g. http://www.unstrung.com/document.asp?doc_id=27440, January 2003.
- [WF03] Wireless futures, testing facility the blue labs, web site. <http://www.wirelessfutures.co.uk/>, 2003.
- [Wi02] Wi-fi networking news. <http://80211b.weblogger.com/2002/11/21>, November 2002.

List of Abbreviations

ADSL	Asymmetric Digital Subscriber Line
DDoS	Distributed DoS
DoS	Denial of Service
GAP	General Access Profile
GOEP	Generic Object Exchange Profile
GPS	Global Positioning by Satellite
ISP	Internet Service Provider
LAN	Local Area Network
MITM	man-in-the-middle
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistant
PPP	Point to Point Protocol
RF	Radio Frequency
SIG	Special Interest Group
SNMP	Simple Network Management Protocol
UWB	UltraWideBand
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network