Wireless LANs and Regional Networking

Jouni Ikonen and Janne Oksanen
Lappeenranta University of Technology, Laboratory of Telecommunications, P.O. Box 20, FIN-53851 Lappeenranta, FINLAND

Email: {jikonen, joksanen}@lut.ji

Key words: Wireless local area network, public access

Abstract: The spread of the internet accelerated rapidly in mid 90's due to the invention of the web. Home Internet connections were slow due modems, and so faster methods were provided for urban areas e.g. cable TV, xDSL, leased telephone lines, wireless, etc. In the city of Lappeenranta all of the previously mentioned technologies are available, but not everywhere, and they do not support mobility. However, net access is not common for home users and the success of local services requires a high user take-up. Many net users have learned to use the net at work or at school and require access from home also. In this paper a case where continuous Internet access is being planned for the citizens of Lappeenranta is presented. Access is being designed to use a dense WLAN (Wireless Local Area Network) network. A backbone network is planned to overlay multiple different organization networks to save costs. The network is being designed to be an independent non-profit making organization to provide users with low cost net access. Connection to the Internet can be made via a wide selection of ISPs (Internet Service Providers), which have been given access to the Lappeenranta network. Co-operation of ISPs is needed to optimise the frequency of use and to maximize performance.

1. INTRODUCTION

The popularity of wireless LAN technologies has surged due the IEEE 802.11 standard. The price of wireless LAN equipment has become reasonable for end users and WLAN technology has become widely accepted. In particular, in areas which are hard to install cable in or where a connection is only needed temporarily, wireless solutions are popular.

Compatibility problems between different vendors have lead to the founding of the Wireless Ethernet Compatibility Alliance (WECA), which is formed by organizations producing IEEE 802.11 equipment and software [WEC]. Products of organizations belonging to WECA are supposed to be compatible with each other. Compatible products are given WIFI (standard for wireless fidelity) recommendation. In practice, WIFI compatibility is limited to basic features. Vendors tend often to add their own features to the products to make their products "better" than the standard and to stand out from the crowd.

Originally, IEEE 802.11 provided three transmission methods [IEE]: frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS) and infrared. Both IEEE 802.11 FHSS and DSSS have been widely used, but infrared failed to become widely accepted. Both radio technologies provided a 2 megabits per second communication rate, which is sufficient for many uses to meet the challenges of modern society.

In European countries (excluding Spain and France) both FHSS and DSSS operate in the 2.400 – 2.4835 GHz frequency range. The DSSS system utilizes "sets" of frequencies in a sequential progression and uses "channels". In Europe (ETSI) there are 13 channels available in the spectrum, but each uses frequencies such that about three channels can coexist without much overlapping.

FHSS can overcome moderate signal interference better than DSSS [MID]. FHSS can suffer packet loss on several of the frequency hops with no need to retransmit packets. The IEEE 802.1 1 standard and the FHSS has redundant data built into its methodology that allows for radio packet loss without loss of the data being sent and the need to retransmit that data.

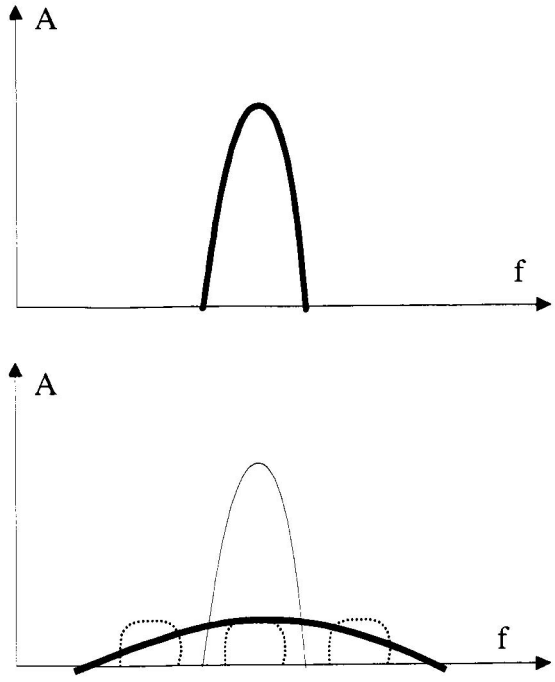

Figure 1. In DSSS signal is spread over larger spectrum. Narrow band interference does not interrupt communications

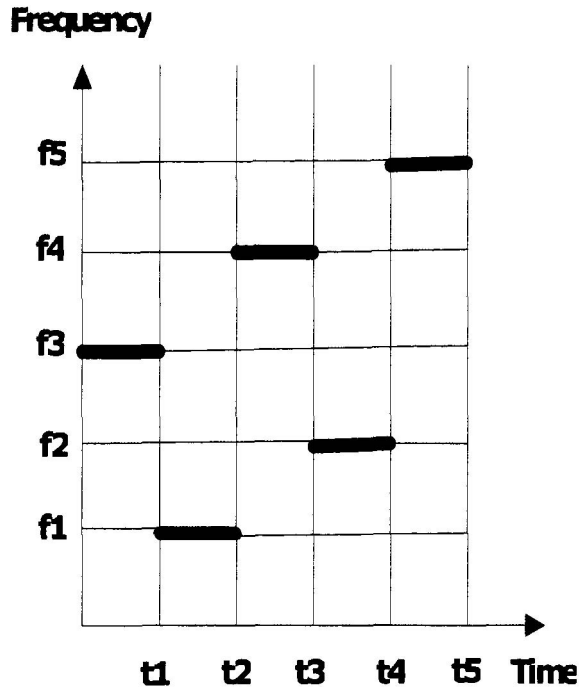

Figure 2. In FHSS narrow band is used for communication, but used frequency is changed in fast pace. Interference on a frequency can be overcome by error coding

Figure 1 presents the basic idea behind direct sequence spread spectrum WLAN technology. In traditional radio communications the signal is transmitted on a frequency band sufficient to carry the message. In DSSS the signal is spread over a wide frequency and an actual message can be seen as background noise to traditional narrow beam communications. On the receiving end- transmission is reconstructed from the wide band transmission and the effect of narrow band interference is diminished. In Figure 2 a frequency hopping approach is visualized. Transmission is carried out using multiple frequency channels, which are changed in a pattern known to the receiver and transmitter.

IEEE 802.11b was published in 1999 [IEb]. The standard supports only direct sequence spread spectrum transmission methods. The communication rate was increased to support speeds of up to 5.5 and 11 Mbit/s and that is the reason why FHSS technology failed to become more common. Spread spectrum has been promoted by using arguments like inherent transmission security, resistance to interference from other radio sources, redundancy,

resistance to multi-path and fading effects. SS-technology can be used to overlay existing radio systems without interrupting their operation. [BREI However, in practice, channels used in neighbouring WLAN cells should be chosen far enough from each other to maximize the signal noise ratio. In practice, measured TCP/IP traffic throughput is about half that of named maximal throughput .

One of the reasons behind the popularity of WLAN products is that they use a licence free radio band. Its licence- free operation has also made the 2.4 GHz (2.4000 – 2.4835 GHz) band very popular and there are many products using this frequency. The down side is the limited frequency band. Anyone can develop their own products-/-networks to use the ISM (Industrial, Science and Medical) band, and many systems will interfere with each other. Besides the licence -free ISM band there are also licensable bands available, that can be used, for example, as a WLAN wireless backbone. For example, products on 2.5GHz, 2.6GHz and 3.5GHz frequencies require licences. The good news for licensed frequencies is the regulation of the users so that interference can be controlled. Down-sides are licence costs, more expensive devices, the number of available licences, and also the limited number of licensable frequencies [BRE]. On the other hand there are also considerable costs on licensed bands also.

Development of wireless methods has not stopped here, and IEEE 802.1 la [IEa] is under development. It is supposed to allow speeds of up to 54 Mbit/s and realize basic quality of service (QoS) methods. IEEE 802.1la compliant products operate on a 5 GHz (5.15-5.25; 5.25-5.35; 5.725-5.825) licence -free frequency.

HiperLAN (High Performance Radio LAN) is one of the new wireless network standards developed by ETSI (European Telecommunication Standardization Institution). It operates on 5.15-5.3 GHz and 17.1-17.3 GHz. HiperLAN is not compatible with IEEE standards as it uses different protocols. A simple HiperLAN network can be constructed from two HiperLAN -capable devices. No wired infrastructure is required. If communicating devices are out of range from each other, a third device can relay the messages. The range in HiperLAN is approximately 50 m. Both synchronous and asynchronous traffic are supported. HiperLAN type 1 provides a 20 Mbit/s communication rate, and HiperLAN type 2 up to 54 Mbit/s [ET1, ET2].

Security plays a very important part in wireless network environments and no FHSS or DSSS access technologies are sufficient protection by

themselves. Originally WLAN technology was developed for military purposes where it is easy to think that technology is safe to use. Multiple security solutions have been developed for WLAN. One of the approaches is WEP (wired equivalent privacy) [WEP]. It is based on shared keys and network names [PRA]. This is a sufficient approach for most home usage. WEP is not invented to be a complete end-to-end security solution. WEP only protects the wireless link between the client machines and the access points. WEP has known security problems and there are methods to break the security regardless of whether 64 or 128 bit encryption has been used. Security can be improved by using other existing methods like VPN (virtual private network). There are good standardized VPN solutions, like IPSec (IP security protocol) [IPS]. Many vendors also offer their own solutions, like Microsoft [MIC], but these solutions often have compatibility problems.

Usage of WLAN networks differs notably depending on the geographical area, where system is used. In the USA 1 W transmission power can be used, where 100 mW is maximum in Europe. The effect on operation range is notable and makes a big difference when using WLAN technology in outdoor environments. Power limitation requires dense access point networks and very careful frequency planning. Roaming is much more needed feature with small cells. The idea of roaming is to enable the user to move from the area of one access point to the area of another without the user noticing anything. However, roaming is a problem in WLAN outdoor networks as vendors expect users to move inside a subnet, which can be difficult in a MAN network. Another feature, which must be considered, is broadcast traffic. Normally in LANs there are number of applications using broadcast messages. These messages should be limited so that they cannot block the limited capacity of a radio network. The solution for broadcasts is often to divide the network to small sub-networks. Many vendors provide the possibility of blocking broadcasts in access points. Limiting traffic only to IP is often a good approach.

Many applications requires a fixed IP address. However, this is difficult in wireless and mobile environments. A mobile IP has been offered as a solution to this problem. With a mobile, an IP user can have the same identification regardless of his location in the network. There are, however, problems that still make the use of a mobile IP difficult. One of the problems is lack of mobile IP clients for different platforms. This situation is expected to change in the near future, as there are many organizations that are tackling the same problem. There are also alternative approaches to a mobile IP.

Management of network and users becomes very important as the size of the network and the number of users increases. Many vendors offer network management tools but their interoperability is open to question. Wireless access points can be configured via SNMP, but it is still difficult to manage a large network. Things get much more difficult if many tools are used for management. One of the network management key tasks is to monitor the network, to check for bottlenecks of traffic, and misusage of the network, and to solve problems before they arise.

1.1 Case Wireless Lappeenranta

Internet access in homes has become very popular. One of the driving forces seems to be the children in the families, who learn to use the Internet at school and demand access at home also. As local telephone calls in Finland are charged by according to the time used, the phone bill in a family with a several youngsters might be notable. Parents and children are led to search for other net access methods. Fixed Internet connections via cable TV network or wireless LAN access are popular choices as they have fixed cost and continuous Internet access.

In Lappeenranta there are a wide selection of Internet access methods available. Modem, ISDN and cable TV are popular, but xDSL is not gaining many users as it is quite a new access method and still too expensive for most home users. Fixed Internet access cost is considered quite high for beginner net users and often difficult to justify by teenagers to the parents, until the phone bills start exceeding the cost of other methods.

As there are already many access technologies, why introduce yet another into the same area? There are many reasons for wireless Internet access, as listed below. Not all the reasons concern wireless access, but involve aerial connectivity via multiple access methods.

Basic ideas behind the Lappeenranta network:

- Mobile Internet usage
- Generation of large number of regional network services
- Small threshold to join network
- Obtain high regional Internet penetration
- Research of wireless LAN to suite the needs of the MAN network.
- Research of new applications
- Co-existence of Internet operators in an access network

- Optimize radio frequency use

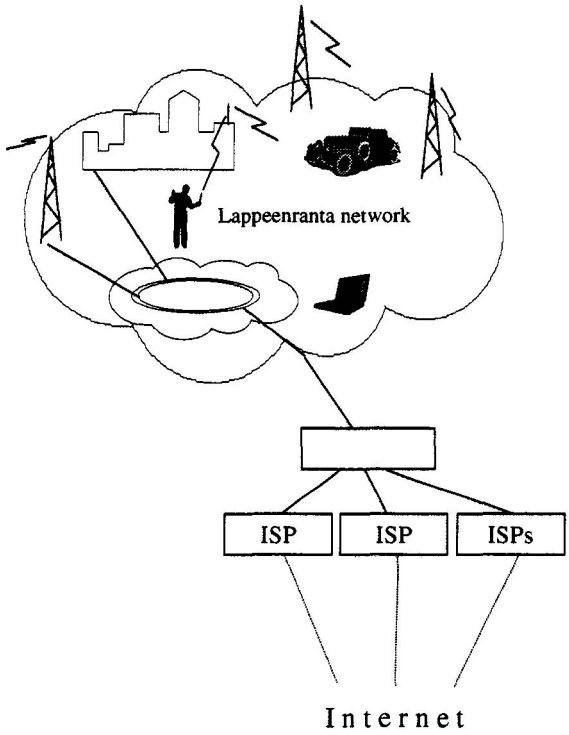

Figure 3. Structure of the Lappeenranta network

One of the basic ideas behind the Lappeenranta network is to provide local services to local users. To enable a large user base, the cost to use and join the network must be kept low. The object is to provide free local network usage and charge for Internet access. Internet access is provided via Internet service providers (ISPs). The user can choose an ISP, that will provide the best cost / performance / service to the user's needs. The basic structure of the network is proposed in Figure 3.

Low cost or free access is targeted to attract users to use the local services. In the early days of the network there are only a limited number of services available and Internet services attract the users. At a later stage a large user base will attract more services into joining the network. If the services available are good this will attract even more users.

The network is open to different ISPs and they are on a par in the network. By providing one network to be used by all ISPs, the frequency usage can be optimized in this area. If multiple ISPs were to build their own 2.4 GHz WLAN access networks into this area, the frequencies available would not be sufficient and interference would reduce the network capacity. Also, building multiple networks is more expensive.

Mobile users are currently quite rare. A laptop and a WLAN card can be considered a wireless mobile device. A laptop is, however, difficult to carry around and use, for example, at a bus stop to check the bus timetable. Smaller WLAN -capable mobile devices are under development. Currently, Compaq *iPaq* [COM] is one example of what WLAN -capable device might look like. Phones supporting WLAN directly are envisioned. Symbol has produced a *NetVision Data Phone* [SYM], which supports H.323 calls on WLAN. However, IP call standardization is a problem. Many vendors are using their own solutions and interoperability problems slow down the spread of VoIP technology. Also lack of quality of service aspects in current WLAN standards is seen as a big problem.

A wireless backbone on 2.4 GHz is not suitable, as usable frequencies are limited. Another choice is to build a wireless backbone by using licensed frequencies. The option of installing a new cable is expensive, but optical cables can provide the necessary capacity far into the future. The choice in the Lappeenranta network was to use existing cables and to install as few new cables as possible. This is realized by using networks owned by participating organizations, e.g. the city of Lappeenranta, to build the backbone and connect wireless access points to the network. Use of networks of other organizations always raises security considerations and this must be taken into careful consideration at the planning stage.

2. SERVICES AND TECHNOLOGY

Closed private networks have been disappearing due the popularity of and demand for the public Internet. Since Internet services are available via ISPs, what does the local network have to offer? The idea is that Lappeenranta network offers local services, that are related to geographical place. These services could include:

- Lunch ordering services. There is no point in ordering from a neighbouring city as it is out of delivery range.
- Local timetables
- Local events and ticket reservation

- Location based information

Many services publicly available on the Internet can be adapted to the local network to minimize outbound network traffic. These services could include multiplayer gaming sites, newspapers, chat services, etc. Development of new services is difficult to predict and is dependent on the development of mobile terminal devices, and public acceptance of the network.

Many obstacles lie in the way of a successful network. The technology used must be widely available and reasonably prized. This is the reason for selecting the 802.11b standard, as there are many vendors. Many of the principles of fixed network development apply to a mixture of wired and wireless networks. Planning the network from scratch is probably easier than using existing organizations' networks, but the cost of a new-wired infrastructure can be excessive.

3. CONCLUSION AND FUTURE WORK

Originally, WLAN technology was developed for office networks. However, the same technology has been used for extraneous environments because of the availability of low cost equipment and license -free operation. Success in public networks has varied and technology has mainly been used to connect buildings and home PCs. In our experiments this has been a feasible approach since the number of wireless links between access points has been kept low. If possible, existing wired infrastructure should be used to connect access points to the backbone network. Use of a license -free frequency is not always a good idea, as other networks can interfere at any time.

An important aspect of building an aerial WLAN network is co-operation with other parties using the same technology. This is to minimize radio interference and maximize throughput. Our approach is to build one public access WLAN network that is open to all parties. This can bring consensus to "free" ISM frequencies, however the fact that WLAN is not the only technology using the same frequency must be kept in mind.

The Lappeenranta network is still at the beginning stage. The first year of the project involves a small part of the city and during this time many problems in the network must be solved. Wireless network are still missing

suitable terminal devices, and their development will show whether WLAN technology in an extraneous environment will be a success or failure.

REFERENCES

[BRE] BreezeCom
www. breezecom.com/Materials/PDFFiles/fhvsds.PDF
[COM]Compaq *iPaq*
http://athome,compaq.com/showroom/static/iPaq/handheld.asp
[ET1] ETSI HiperLAN/1 standard
http://www,etsi.org/technicalactiv/hiperlan1 .htm
[ET2] ETSI HiperLAN/2 standard
http://www.etsi.org/technicalactiv/hiperlan2.htm
[IEE] IEEE 802.11 standard
www.ieee.org
[IEa] IEEE 802.11a standard
www.ieee.org
[IEb] IEEE 802.11 b standard
www.ieee.org
[IPS] IP Security Protocol
http://www.ietf.org/html.charters/ipsec-charter.html
[MIC] Microsoft VPN
http://www.microsoft.com/ISN/whitepapers/
microsoft_virtual_pr_952.asp
[MID] Midcoast Wireless
www.midcoast.net/wirelessfaq.html
[PRA] Anand R. Prasad, Henri Moelard and Jan Kruys: Securify *Architecture for Wireless LANs: Corporate & Public Environment,* VTC2000, 2000, pp. 283-287.
[SYM]Symbol *Net Vision Data Phone* http:J/www.symbol.com/
products/wireless/wireless_sp24_netvisionappli_d.html
[WEC] WECA
www. wi-fi.org
[WEP]WEP, Wired Equivalent Privacy
www.wi- fi.org/pdf/Wi-FiWEPSecurity.PDF