Study of Wireless Local Area Networks

Dr. Joginder Singh Cheema
HOD, Department of Computer Applications,
Baba Budha College, Bir Sahib, Tarntaran.

Abstract: Wireless Local Area Networks (WLANs) have moved quickly to the mainstream and are now found in many educational institutions, homes, businesses and public areas. Organisations and consumers have been keen to take advantage of the flexibility adding wireless networks can offer. A recent report from In-Stat predicts that the wireless market will grow from 140 million wireless chipsets a year in 2005 to 430 million in 2009[1]. The emergence of new security standards has also increased confidence in WLANs. Users are becoming more familiar with the technology and are increasingly expecting wireless access to be available. There is a wide range of products and standards involved in WLAN technology and more continue to emerge. This paper will focus on wireless LANs and the issues surrounding their implementation.

Keywords: WLAN, PDAs, LANs

I. INTRODUCTION

A wireless local area network (WLAN) is two or more computers joined together using radio frequency (RF) transmissions. This differs from a wired LAN, which uses cabling to link together computers in a room, building, or site to form a network. Although WLANs can be independent they are more typically an extension to a conventional wired network. They can allow users to access and share data, applications, internet access or other network resources in the same way as wired networks[1][2].

Currently, Wireless LAN technology is significantly slower than wired LAN. Wireless LANs have a nominal data transfer rate of between 11 and 54 Megabits per second (Mbps) compared to most wired LANs in schools which operate at 100Mbps or 1000Mbps. Wireless LANs are typically used with wireless enabled mobile devices such as notebook computers, PDAs and Tablet PCs. This allows users to take advantage of the flexibility, convenience and portability that WLANs can provide. Wireless networking is also appearing on other devices such as mobile phones, digital cameras, handheld games consoles and other consumer electronics. The term Wi-Fi (Wireless Fidelity) is often used to refer to 802.11 wireless networks. It comes from the testing and certification programme run by the Wi-Fi Alliance (see below) to ensure wireless products from different manufacturers comply with standards and are interoperable.

II. HOW DOES A WLAN WORK?

[3][4]To access a wireless network all devices will need to have a wireless network interface card (NIC) either built in, or installed separately. Wireless NICs are available in various forms and with different interfaces to suit different devices e.g. PCMCIA and PCI cards; CF (Compact Flash) and SD (Secure Digital) cards; and USB wireless network adaptors. In all cases the necessary software drivers may also need installing. Increasingly, portable devices are being sold with wireless LAN connectivity as a standard feature. Most new laptop and tablet PC models for example have in-built wireless and this is also now included on many PDAs. Built-in wireless adapter cards have now overtaken external wireless adapter cards in the market.

There are two main types of wireless network configuration: ad-hoc mode and infrastructure mode.

Ad-hoc networks are the simplest form of wireless network created by two or more wireless enabled computers communicating with each other directly. These types of WLANs are useful for creating small dynamic networks. However, these ad-hoc networks have similar limitations as wired peer to peer networks and are only really suitable for occasional, small networks of a few computers. Ad-hoc networks cannot provide the same security as properly implemented infrastructure mode networks.

Infrastructure mode requires one or more access points (APs) through which the network cards communicate. In a typical wireless LAN, a transmitter/receiver (transceiver) device, called an access point, is normally physically connected to the wired network using standard Ethernet cabling. It acts as a bridge between the wired network and the remote computer(s). At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure, using radio frequencies to transmit data to each user.

Access points can have a varying amount of intelligence and functionality built-in. There are two main types of AP. “Thick” APs are fully functional and can handle all processes. “Thin” APs only include radios and antennas and rely on controllers (WLAN switches/appliances) for other functionality including managing APs, security and authentication. There is also a third hybrid category with some limited radio frequency management functionality, but that still need controllers to function fully.

The vast majority of WLANs use fully functional (thick) APs in a decentralised architecture. The APs are usually deployed in stand-alone mode, but in larger networks where the communication between APs poses an unacceptable load, a controller can be used to handle load balancing and roaming. There is a management overhead in configuring and managing each access point, although overlay management tools are available (see Managing WLANs)[5].

Centralised architectures are less common. In these networks all traffic passes through the controllers (WLAN switches/WLAN Appliances), which handle load balancing and other management functions. The APs deal with RF access and often enforce policies set by the controller. Various manufacturers balance the functionality between controllers and APs differently. Centralized networks are generally considered easier to manage than decentralized networks. They can also allow seamless roaming of users across subnets. However, these tend to be single vendor solutions and the increased cost of centralized equipment is usually only justified in larger, complex or multi-site deployments.

III. ADVANTAGES OF A WLAN

[6][7]A wireless LAN has some specific advantages over wired LAN:

- Access to the network can be from anywhere in the school within range of an access point, giving users the freedom to use ICT where and when it is needed.

• It is typically easier and quicker to add or move devices on the network (once in place, a wired LAN can be difficult to move and expensive to change.) Increasing the overall network coverage of the wireless LAN can often be achieved by adding further access points.
• Small dynamic ad hoc networks can be created very quickly and relatively easily.
• It is typically easier and quicker to provide connectivity to the network in areas where it is difficult or undesirable to lay cable or drill through walls. Instances might be:-
-where a school is located on more than one site or is made up of several buildings.
-when implementation is anticipated to be temporary or semi-permanent
-when only one device is required at a remote part of a building or site
-in historic buildings where traditional cabling would be difficult to install or inappropriate
• Where wireless enabled laptop computers are used, any classroom in range of an access point(s) can become a 'computer suite', potentially increasing the use of ICT across the curriculum
• While the initial investment required for wireless LAN hardware can be similar to the cost of wired LAN hardware, installation expenses can be significantly lower
• Wireless provides increased flexibility for teachers. A teacher with a wireless enabled laptop can access the wireless network to show students work, share resources, obtain information from the internet from anywhere within range of an AP, without being tied to a wired PC. This flexibility is further enhanced when combined with a wireless projector.
• Portability. They allow computer devices to move around the school with the pupil rather than the pupil going to a specific place to use a device. This allows for outdoor field work and work in non-classroom spaces (common areas, library, canteen, gymnasium/sports hall, playground).

IV. DISADVANTAGES OF A WLAN

A wireless LAN has some specific Disadvantages over wired LAN:

• The current data rates of wireless networks means that high bandwidth activities are better done on wired networks
• As the number of devices using the network increases, the data transfer rate to each device will decrease accordingly.
• As wireless standards change, it may be necessary, or at least desirable, to upgrade to higher specifications of wireless which could mean replacing wireless equipment (wireless NICs, access points etc). Currently, wireless standards are changing more quickly than wired standards.
• Security is more difficult to guarantee.
• Devices will only operate at a limited distance from an access point, with the distance largely determined by the standard used. Obstacles between the access point and the user, like walls, glass, water, trees and leaves can also determine the distance of operation. Poor signal reception has been experienced around reinforced concrete school buildings; these may require higher numbers of access points which in turn increases overall cost.
• In practice, a wireless LAN on its own is not a complete solution and will still require a wired LAN to be in place to provide a network backbone.
• Data speeds drop as the user moves further away from the access point
• It is generally easier to make a wired network 'future proof' for future requirements
• As the number of people using wireless devices increases, there is the risk that certain radio frequencies used for wireless will become congested and prone to interference; particularly the 2.4GHz.frequency.

V. SPECIFICATIONS FOR WLANS

These specifications are taken from *Functional Specification - Institutional Infrastructure,* which sets out the functional requirements for institutions to aim to achieve[8][9].

1. Secure wireless networks *shall* complement rather than replace an institution's wired network

While wireless technologies allow a high degree of flexibility in accessing the institution's network, they are still widely viewed as technologies that support the institution's wired network. It is anticipated that in the medium term, media-rich applications and services that place high demands on the institution's network will be best met via a wired network.

2. Institutions should provide secure wireless access to curriculum and administration resources from a wide range of work spaces in the institution

In order to achieve complete flexibility of working within the institution, a learner or educator needs to be able to gain access to networked resources from all work spaces. To allow flexible access to the institution's ICT services, it is anticipated that a wide area of wireless coverage of the institution will be needed. Wireless networking technologies allow access to networked resources when fixed access to the network is not possible, practical or even desirable. Careful planning of what areas need wireless coverage will be required to ensure that flexible working via wireless technologies is achieved.

VI. IMPLEMENTING A WLAN

[10][11]Following are the steps to implement WLAN:

Planning: As wireless network technology has matured there has been a proliferation in manufacturer offerings of both equipment and management tools. There are various factors that need to be considered before deploying a wireless network. These include what it is to be used for, the requirements for applications intended to be run on the network, the number of users and the size and location of the area to be covered. It is also important to have a good understanding of the technologies and standards involved. It is recommended that a small pilot wireless network is set up to test applications and use before widespread deployment. *WLANs vary in their size and complexity.* Schools may decide to cover a small area such as a classroom/classrooms or to have blanket coverage over a wide area or entire site. The amount of coverage can be increased over time, but clearly defined aims need to be set out at the start of any *WLAN project.* Alternatively, many schools use "mobile" APs instead of fixed APs. These are usually fitted to a laptop trolley, which can be wheeled into a classroom and connected to a free network port. This provides an inexpensive way of delivering wireless connectivity to a suite of laptops, which can be moved around the school. However, it does not provide the flexibility of "blanket" wireless coverage and relies on there being fixed wired network ports in classrooms.

Site survey: To determine the location of access points for infrastructure networks, it is recommended that a site survey is undertaken by a specialist. A site survey will also determine the number of access points required to give the desired coverage, the range of each access point, and its channel designation, signal strength and the presence of interference.

Before a site survey is undertaken, it is advisable to prepare a floor plan to show where coverage is required. Precise details should be sought from suppliers of 'network coverage' and 'data transfer rates' particularly towards the edge of the coverage area. You should specify the level of coverage you require, as a supplier's definition may be as low as 1Mbps. It is also a good idea, if possible, to ensure that the site survey is carried out with the equipment anticipated to be used in the school. It is also advisable to build in some redundancy to provide better performance and reliability. This can be achieved with extra access points or by moving access points closer together. For schools upgrading from an existing 802.11b wireless network, a further site survey may be required since the coverage is likely to be different when compared to 802.11b.

Positioning Aps: The access point, or the antenna attached to the access point, will usually be mounted high in a classroom or in the ceiling space However, an access point may be mounted anywhere that is practical as long as the desired radio coverage is obtained. Larger spaces generally require more access points. APs will also need a power supply and this needs to be taken into consideration when planning the location and cost of installations. It is advisable for electrical installations to include remote power switches, so that APs in awkward locations can be easily powered down or rebooted.

Power over Ethernet (PoE): Many enterprise class access points now support Power over Ethernet. Power over Ethernet (PoE) is a network standard (IEEE 802.3af) for sending DC power over data cabling to provide power for networked devices. The standard allows for 15.4 W, but only 12.95 W is available at any device. PoE allows for greater flexibility in WLAN deployment as access points can be installed in places away from power outlets and easily moved to meet requirements. Another key consideration is potential cost savings on installation and management. Using PoE devices reduces the financial and time costs of employing a qualified electrician to install mains sockets and cabling. The reduction in wiring and lack of mains voltage can also improve safety. Although PoE can be used over existing fast Ethernet Cat 5 and Cat 6 cabling, the costs of mid-span PoE expansion modules, UPS, power supply units (PSU) and air conditioning to cope with the extra heat are not insignificant. PoE is not yet a widely used technology and the costs are a barrier to take up. However, it could be considered for larger WLAN deployments.

A new emerging standard for PoE, known as PoE Plus, is in development as IEEE 802.3at. It should offer higher power throughput (somewhere between 30 W and 60 W) and therefore should support a wider variety of devices. It should be backwards compatible with IEEE 802.3af. The new standard is not expected to be ratified until late 2007/8.

Network Management: Schools will need to allocate resources for network management in the same way as they would for a wired network. Tasks such as configuring MAC and IP addresses, changing security keys, managing radio strength, monitoring network performance, upgrading access points and generally ensuring system integrity, will need to be undertaken on a relatively regular basis. Most access points will allow a certain amount of configuration, usually via a browser interface. In networks of more than a handful of access points, manual configuration of APs can become unmanageable. Enterprise class APs provide some management tools and will often allow some remote management using Simple Network Management Protocol (SNMP) via Management Information Bases (MIB). However, these management tools are proprietary and rely on all APs being from the same vendor. Alternatively, third party management and WLAN monitoring tools that can work with products from a variety of manufacturers are increasingly available. The Wi-Fi Alliance is considering introducing a new certification for Wi-Fi equipment to make setting up secure wireless networks easier. Imposing easy to use setup schemes on Wi-Fi equipment is seen as important for the increasing number of non-technical users using the technology. Some vendors have already introduced proprietary set-up solutions. The WFA has set up a working group to look at the problem.

VII. WLAN ISSUES

[12]Following are the WLAN Issues:

1. Security

Wireless LAN security problems have been widely publicised and have been a key barrier to take up. Security is always a balance between perceived risks and costs. Various factors need to be considered including the vulnerability of the network, the threat of attack, the value of the data to be secured and the costs involved. Securing WLANs, as with all networks, needs to be seen as a continuous process rather than a one-off step. Any security solution needs to be consistently and properly implemented with regular monitoring.

Anyone with a compatible wireless device can detect the presence of a wireless LAN, however if appropriate security mechanisms are put in place, this does not mean that they can access any data. The wireless LAN should be configured so that anyone trying to access the wireless LAN has at least the same access restrictions as they would if they sat down at a wired network workstation. Schools should be implementing a comprehensive security policy and incorporating standards like WPA/WPA2. However, there are a number of other security measures that can be taken.

All the suggestions below are practical steps that institutions can put in place to improve wireless LAN security. An institution can:

- ensure that the devices with WEP security are upgraded to WPA/WPA2 where possible and that the encryption is enabled. WPA provides a high level of security for a wireless network. If an upgrade to WPA is not possible, schools should ensure that WEP is enabled.
- educate users about security and implement an organisation wide policy. Ensure that users know not to plug in their own access points that could leave the network open
- restrict access to the Wireless network by only permitting devices with a recognised MAC (Media Access Control) address. Every computer has an individual alphanumeric identifier known as a MAC address. Within the software accompanying the access point, there is an Access Control List (ACL), which as its name suggests, controls access to the network. The access point can be configured to only permit recognised devices. This only gives an additional layer of security to the network; it is not a secure solution in itself as MAC addresses can be easily "spoofed". It should be noted that the management of these ACLs can become burdensome in larger networks.
- Change default settings on access points. The default usernames and passwords on access points are widely known and should be changed.
- change the default Service Set Identifier (SSID or network name) (SSID is the method wireless networks use to identify or name an individual wireless LAN.) Access points may be set to broadcast the SSID, this should be turned off where possible. This only

adds an additional layer of security and is not a solution in itself. On access points where this is not possible, the network name can be made less recognisable by including non alphanumeric characters (like _*# etc).

- avoid wireless accessibility outside buildings where it is not required; directional aerials can be obtained to restrict the signal to 180° or 90° from the access point.
- switch off the power to the access point(s) 'out of hours' making the wireless LAN unavailable at those times.
- make sure that the network is regularly checked to ensure that only legitimate wireless access points and devices are connected to the network. This can be done by walking around with a wireless device and software tools like Netstumbler.
- put the Wireless LAN into its own DMZ so that all wireless nodes pass though a firewall to access the educational network.
- The security measures a school would consider for a standard LAN implementation can also be incorporated in to a WLAN (e.g. installing a firewall, using a DMZ, administrator file restrictions etc)
- Implement firewalls on client devices
- Regularly update the firmware of all wireless equipment
- Set an appropriate maximum number of clients that can associate with an AP
- Disable the ability to manage APs over the WLAN
- incorporate a Virtual Private Network (VPN). A VPN is a secure (encrypted) private network created over a public network. Anyone wishing to access files on the WLAN would first need to log on to the network via the VPN using a user name and password. Data sent between the client device and the network is secure as it is encrypted / decrypted using VPN encryption. Most VPN solutions entail installing VPN software on the client devices. A VPN for wireless would provide a relatively high level of security for a school. Users would need to ensure they use sensible (i.e. not obvious) password and log-on details otherwise this level of security is easily compromised.

Several companies now offer third party security tools and management systems. These can provide various functions such as intrusion detection systems (IDS) that actively monitor airwaves for rogue access points/devices and disable any found. Some systems can limit the area from which devices are allowed to connect to the network using location based technology. These solutions add to the cost of WLAN deployment.

2. Performance

It is important to remember that transmission speeds for all wireless LANs vary with file size, number of users, distance from the access point, the environment and any interference present.

As the distance from the access point increases, the nominal data rate for 802.11a and 802.11g standard equipment drops from 54Mbps to 48, 36, 24, 18, 12, 9, or 6 Mbps. 802.11b standard equipment drops from 11Mbps to 5.5Mps, 2Mbps or 1Mbps. It is possible to boost the range of some access points by installing specialized antennae.

Wireless clients will only send data when other devices are not transmitting. Interference from other wireless signals can cause clients to wait before sending data or cause dropped packets that have to be retransmitted, slowing down the network.

The environment of a WLAN can also affect the range and throughput. Buildings with many girders, thick walls, and concrete will often shorten the effective range and there may be areas that are effectively 'dead zones'. Water, glass and paper can also reduce a network's range.

3. Prices

The cost of access points depends on the quality and on built-in functionality, and includes:

- the quality of the antennae
- antennae directionality
- encryption included in the access point
- whether the access point has DHCP (Dynamic Host Configuration Protocol – allows automatic assignment of IP addresses to new devices on the network) built in
- DSL access (which allows internet access direct from the access point) this is designed for small home network or small business use
- the number of user devices that can be listed in the Access Control Lists; is the number limited and if so is it sufficient for your network?
- the ability to centralise the control and management of access points over the network
- whether the access point can act as a bridge between other access points and the network
- support for Power over Ethernet (PoE)

Enterprise class access points are significantly more expensive than consumer/SOHO class devices. They tend to include more features, more robust radios and better support and management tools.

VIII. CONCLUSION

The future of wireless local-area networking is now, and it is the solution for communication problems in organizations or any place that need a wide spread of internet connection , interoperability became reality with the introduction of the standards and protocols and prices have dramatically decreased. These improvements are just a beginning. Organizations who use WLANs networks can eliminate many of wireless LAN's security risks with careful education, planning, implementation, and management. WLAN brings out not only advantages, but also some Specific security problems, although development of wireless standards and security protocols may enhance the WLAN security. We know that hackers will never go away, so we bear the burden to provide the best 'locks' we can to protect our WLANs. Finally, whatever the outcome, wireless LANs will survive and are here to stay even if the technology has a new look and, or feel in coming years.

IX. FUTURE WORKS

Future work should focus on the following issues:

• Lack of method to detect a passive sniffer: An attacker usually first collects data traffic before launching an intrusion. This type of passive sniffing is quite dangerous, but there is nothing to do in this direction except to use the proper protection through encryption.

• To think about how to reduce and eliminate the risks attacks that can be happened on WLAN networks such as Man-in-the Middle attacks , Denial of Service (DoS) attacks and Identity theft (MAC spoofing)
• Authentication is the key: The most significant vulnerability of wireless LANs is the fact that, at the physical level, by definition they enable access to anyone, authorized or not, within a WLAN access point's radius of useful signal strength.

REFERENCES

[1] Khatod, Anil, (2004). Five Steps To WLAN Security A Layered Approach. AirDefense Inc. November 4, 2004 12:00 PM ET, http://www.computerworld.com/s/article/97178/Five_Steps_T o_WLAN_Security_A_Layered_Approach
[2] Wireless LAN Security802.11b and Corporate Networks. An Technical White Paper, 2001, Internet Security Systems, Inc.
[3] Bidgoli, Hossein, (2006). Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management. Volume 3, Wily, 2006.
[4] Securing Wireless Local Area Networks. A VeriSign/Soltrus White Paper 2003 VeriSign, Inc. All rights reserved.
[5] Wireless Networking Basics, NETGEAR, Inc. October 2005, v1.0, October 2005
[6] Goldsmith, Colin, (2004). Wireless Local Area Networking For Device Monitoring, Master thesis, University of Rochester Rochester, New York
[7] Lansford, J., (2000). HomeRFTM/SWAP: A Wireless Voice and Data System for the Home. Intel Communications Architecture Labs, Hillsboro, Oregon, 2000
[8] O'Hara, B. & Petrick, A., (1999). IEEE 802.11 Handbook: A Designer's Companion, Standards Information Network, IEEE Press, New York, New York, 1999.
[9] The Wireless LAN Standard. Cisco Systems, 2000.
[10] 802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard., White Paper, 2002, www.proxim.com
[11] Wireless Networking Choices for the Broadband Internet Home., White Paper, 2001. www.homerf.org
[12] Wireless LAN Security. Symantec Corporation, 2002.