ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Wireless LAN: An Overview on Different Technologies and Issues

Prachi R. Narkhede

Assistant Professor, Dept. of Electronics and Telecommunication, PRMIT&R, Badnera, Amravati, India

ABSTRACT: Wireless communication is a rapidly expanding application of science and technology. It offers numerous advantages as compared to wired communication networks. Wireless communication is an ever developing field, and the future holds many possibilities in this area. Wireless LAN is a dominant means of supporting wireless communication capabilities. The paper provides introduction to the wireless LAN along with brief information about different technologies used in Wireless LAN like IrDa, Bluetooth, HomeRF and IEEE 802.11. The paper also discusses the issues and security threats in the wireless LAN that should be focused on in the future.

KEYWORDS: Wireless LAN, IrDa, Bluetooth, HomeRF, IEEE 802.11

I. INTRODUCTION

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using wireless distribution method within a limited area. This enables user to move around within a local coverage area and still be connected to the network and can provide a connection to the wider Internet. A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air.

The increased demands for mobility and flexibility in our daily life led the development from wired LANs to wireless LANs (WLANs). Today a wired LAN can offer users high bit rates to meet the requirements of bandwidth consuming services like video conferences, streaming video etc. With this in mind a user of a WLAN will have high demands on the system and will not accept too much degradation in performance to achieve mobility and flexibility. This will in turn put high demands on the design of WLANs of the future.

- **WLAN components**

The physical architecture of WLAN is quite simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NICs)/client adapters [8].

1. Access Points :
   Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. An AP operates within a specific frequency spectrum and uses 802.11 standard specified modulation techniques. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.
2. Network Interface Cards :
   (NICs)/client adapters Wireless client adapters connect PC or workstation to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with APs (will be discussed in the following section). Available in PCMCIA (Personal Computer Memory Card International Association) card and PCI (Peripheral Component Interconnect), it connects desktop and mobile computing devices wirelessly to all network resources. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. It is coupled to the PC/workstation operating system using a software driver. The NIC enables new employees to be connected instantly to the network and enable Internet access in conference rooms.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

II. WLAN ARCHITECTURE

The WLAN components mentioned above are connected in certain configurations. There are three main types of WLAN architecture: Independent, Infrastructure, and Microcells and Roaming.

A. Ad Hoc Networks:

The independent mode or the ad hoc mode is used if there are no Access Points (APs) in the network. In this mode, Stations (STAs) form an Ad hoc network directly with each other as shown in Fig. 1. An ad hoc network, such as a packet radio network, is one without a fixed topology. A wireless host can freely communicate with another host directly whenever the receiver is in its transmission coverage.

The major advantage of this configuration is flexibility. An ad- hoc network can be built easily, without the need of any pre-set and fixed infrastructure. The network failure is less likely as the network does not depend on a single host.

However, there are some drawbacks for ad hoc networks. First, it is much more difficult and complex to perform routing in ad hoc networks because of frequent changes in the network topology due to host mobility. Second, it is more difficult to control or coordinate properoperation of an ad hoc network, since each wireless host may have its own algorithms to perform activities such as time synchronization, power management, and packet scheduling [6].

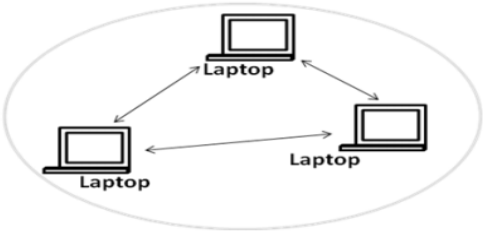

Fig.1.Independent WLAN [6]

B. Infrastructure WLAN

Infrastructure WLAN consists of wireless stations and access points. Access Points combined with a distribution system (such as Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility. The access points not only provide communications with the wired network but also mediate wireless network traffic in the immediate neighbourhood. This network configuration satisfies the need of large-scale networks arbitrary coverage size and complexities [8]. Figure 2 shows the architecture of Infrastructure WLAN.

The malfunction of a base station may partition an infrastructure network, blocking the communication between all wireless hosts connecting to the failed base station and all other hosts in the network.

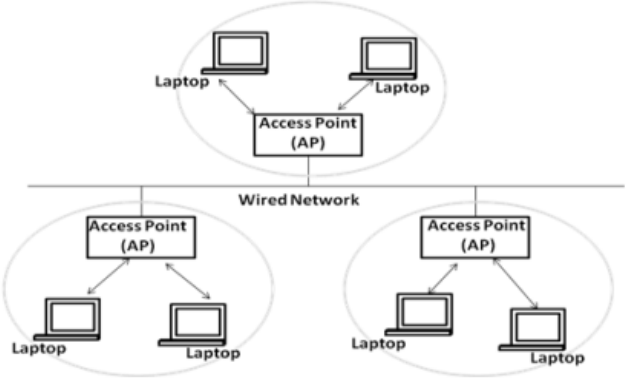

Fig.2.Infrastructure WLAN [6]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

C. Microcells and Roaming

The area of coverage for an access point is called a "microcell'. The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access. One of the main benefits of WLAN is user mobility. Therefore, it is very important to ensure that users can move seamlessly between access points without having to log in again and restart their applications. Seamless roaming is only possible if the access points have a way of exchanging information as a user connection is handed off from one access point to another. In a setting with overlapping microcells, wireless nodes and access points frequently check the strength and quality of transmission. The WLAN system hands off roaming users to the access point with the strongest and highest quality signal, in accommodating roaming from one microcell to another. Figure 3 shows the architecture of Microcells and Roaming [8].

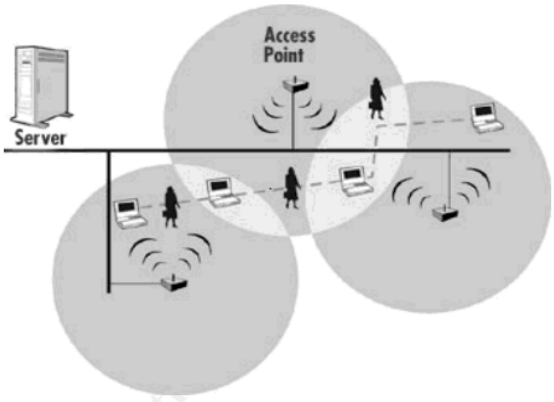

Fig.3.Microcells and Roaming [8]

III. ESTABLISHMENT OF CONNECTION BETWEEN ACCESS POINT AND WIRELESS STATION

In the infrastructure topology, wireless stations (STAs) communicate wirelessly to a network access point (AP) which is connected to the wired network, this setup forms a WLAN. The establishment of connections between STAs and AP goes through three phases (as shown in Fig. 4.):

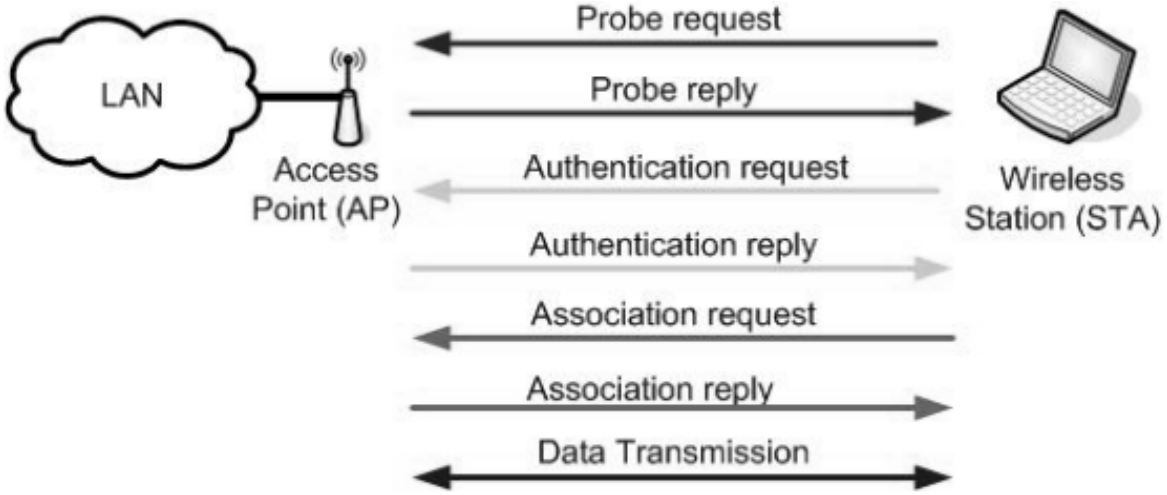

Fig.4. Establishment of connection between access point and wireless station [2]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

a. Probing: In probing phase, the STA can either listen passively to AP signals and automatically attempts to join the AP or can actively request to join an AP.

b. Authentication: Next is the authentication phase, the STA here is authenticated by the AP using some authentication mechanisms.

c. Association: After successfully authenticating, the STA will send an association request to the AP, when approved, the AP adds the STA to its table of associated wireless devices. The AP can associate many STAs but an STA can be associated to one AP only at a time [2].

Advantages of WLAN

a. Mobility
Wireless LAN can provide connection to the network even if the users are movable. In such cases, the use of cables or wired LANs becomes impractical.

b. Ease of installation
As cabling is not required, the wireless LAN network is easy to install and thus the cost of installation is also reduced.

c. Portability
Wireless system is much easier to move from one location to other as compared to wired system thus offering advantages of portability and flexibility.

d. Use of license free spectrum
Wireless LANs are designed to operate in license-free frequency bands (like ISM band) thus the operaion and maintenance costs are less as compared to Cellular and PCS networks. The use of license free spectrum increases the risk of interference and security threats.

IV. WIRELESS LAN TECHNOLOGIES

The different wireless technologies used for industry support, enterprise home and public WLAN needs are IrDa, Bluetooth, HomeRF and IEEE 802.11. These technologies are briefly explained below:

1. Infrared (IrDa)

Wireless infrared communications refers to the use of free space propagation of light waves in the near infrared band as a transmission medium for communication (Carruthers, 2002).The Infrared Data Association (IrDA) is another trade association, which defined standards for infrared communication for many years. It has some advantages notably that it is cheap and there are many devices which already include infrared including most laptops and PDAs as well as some printers. Before the advent of radio frequency LANs people were building infrared LANs, with some success. (irda.org, 2011)

The wavelength band between about 780 and 950 nm is presently the best choice for most applications of infrared wireless links, due to the availability of low-cost LED's and laser diodes (LD's), and because it coincides with the peak responsively of expensive, low-capacitance silicon photodiodes (Rancourt,, 1993).

It provide a useful complement to radio-based systems, particularly for systems requiring low cost, light weight, moderate data rates, and only requiring short ranges(Carruthers, 2002).

However, this radiation cause problem relates to eye safety; it can pass through the human cornea and focused by the lens onto the retina, where it can potentially induce thermal damage (Kahn & Barry, 1997). To achieve eye safety with an LD user can employ a thin plate of translucent plastic. Such diffusers can achieve efficienciesof about 70%, offering the designer little freedom to tailor the source radiation pattern. Computer generated holograms (Smyth et al, 1995) [1].

2. Bluetooth

Bluetooth wireless standard was created by Ericson in Lund, Sweden in 1994. Bluetooth devices communicate via radio transceivers encoded onto microprocessor chips. The Bluetooth system operates in the 2.4 GHz ISM band. The Bluetooth transceiver applies TDD scheme, i.e. it alternately transmits and receives in synchronous manner. All Bluetooth devices use FHSS. There are 79 frequency slots of 1MHz and the signal hops 1600

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

times a second. The Bluetooth standard also specifies link manager software for enabling Bluetooth devices to communicate.

In February 1998, Nokia, Ericsson, Toshiba, IBM and Intel together form a special interest group (SIG). Since organization of SIG, Bluetooth becomes a single, unifying approach providing support. The Bluetooth wireless technology allows users to make almost instant connections between various communication devices. It provides efficient transmission and ensures safety from interference and security of data. Bluetooth supports point-to-point as well as point-to-multipoint connections. Currently Bluetooth supports up to seven simultaneous links within a radius of 10 meters.

One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of 1 milliwatt. Thelow power limits the range of a Bluetooth device to about 10 meters, cutting the chances of interference between a computer system and a portable telephone or television [9]. The range is increased when a scatternet is used because each unit only has to be within 10 meters of one other unit. The range can also be increased if the data is transmitted in a high power mode which offers transmissions up to 100 meters [1].

3. HomeRF

It was developed in 1998 by the Home Radio Frequency Working Group, a consortium of mobile wireless companies that included Proxim Wireless, Intel, Siemens AG, Motorola, Philips and more than 100 other companies. HomeRF is an open industry specification developed by Home Radio Frequency Working Group (Wireless Networking Choices for the Broadband Internet Home., 2001) that defines how electronic devices such as PCs, cordless phones and other peripherals share and communicate voice, data and streaming media in and around the home [1].

HomeRF-compliant products operate in the license-free 2.4 GHz frequency band and utilize frequency-hopping spread spectrum RF technology for secure and robust wireless communications with data rates of up to 1 Mbps (HomeRF1) [9].

Unlike Wi-Fi, HomeRF already has quality-of service support for streaming media and is the only wireless LAN to integrate voice. In the year 2001, the Working group unveiled HomeRF 2.0 that supports 10 Mbps (HomeRF 2.0) or more.

4. IEEE 802.11

The institute of electrical and electronics engineering (IEEE) formed a committee to develop a standard for wireless LAN in 1990. IEEE released the 802.11 standard for wireless local-area networking in June 1997. It can use direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) modulation techniques [4]. This standard defines wireless LAN with either fixed or mobile stations operating at 2.4 GHz and provides data rate of 1 and 2 Mbps. This standard was not compatible with Ethernet which operates at 10Mbps.

Thus higher rate was added to existing standard and IEEE 802.11b standard was developed which could provide two data rates of 5.5 Mbps and 11 Mbps [3] in September 1999. It operates at 2.4 GHz. In the same year another standard IEEE 802.11a was developed which operates at 5GHz with maximum data rates of 54 Mbps.

V. ISSUES IN WIRELESS LAN

1. Data rate

The future requirement of wireless LAN is providing multimedia services. Thus the wireless LAN must improve the current data rate. The data rate depends on various factors like data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol.

The current compression methods used in multimedia application can give compression ratio of about 75 to 100. To improve the data rate of the system the compression ratio should be improved but the quality of audio or video should not be adversely affected.

One more issue with the compression algorithm is highly compressedmultimedia data is more sensitive to network errors. Hence efficient error control mechanism is needed for establishing a reliable network.

Data rate can also be enhanced by using intelligent data transfer protocols which can adapt to the varying nature of wireless LAN.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

2. Power

The mobile devices in the wireless LAN network are small in size and are generally battery operated. Due to this the power limitation is prominent in these devices as compared to the fixed devices. The power limitation leads to limit the range and throughput of the wireless LAN.

The power requirement depends on the complexity and modulation techniques used in the wireless LAN technology. It is observed that direct sequence spread spectrum (DSSS) based implementation requires less power as compared to the frequency hopping spread spectrum (FHSS) implementation.

To conserve the energy, the mobile device should be able to transmit and receive in intelligent manner to minimize number of transmissions and receptions for particular communication operation.

3. Mobility

Without the constraints imposed by the wired connections among devices, all devices in a wireless network are free to move. To support mobility, an ongoing connection should be kept alive as a user roams around. In an infrastructure network, a handoff occurs when a mobile host moves from the coverage of a base station or access point to that of another one. A protocol is therefore required to ensure seamless transition during a handoff. This includes deciding when a handoff should occur and how data is routed during the handoff process.

In an ad hoc network, the topology changes when a mobile host moves. This means that, for an ongoing data communication, the transmission route may need to be recomputed to, cater for the topological changes. Since an ad hoc network may consist of a large number of mobile hosts, this imposes a significant challenge on the design of an effective and efficient routing protocol that can work well in an environment with frequent topological changes.

4. Signal fading

The main problem that exists for indoor environments is that the signal propagated from the transmitter antenna will experience many different signal transformations and paths with a small portion reaching the receiver antenna. The propagated electromagnetic signal in theindoor environment can undergo reflection, diffraction, scattering along with different path losses. Thus the strength of the transmitted signal reduces with the increased distance from the transmitting antenna.

The transmitted signal can reach the receiving antenna in more than one path, thus giving rise to multipath. Thus, the resultant signal after summing up all dispersed signals may have been significantly distorted and attenuated when compared with thetransmitted signal. The receiver may not recognize the signal and hence the transmitted data cannot be received. This unreliable nature of the wireless medium causes a substantial number of packet losses.

5. Radio signal interference

A radio-based LAN, for example, can experience inward interference either from the harmonics of transmitting systems or from other products using similar radio frequencies in the local area. Microwave ovens operate in the S band (2.4GHz) that many wireless LANs use to transmit and receive. These signals result in delays to the user by either blocking transmissions from stations on the LAN or causing bit errors to occur in data being sent. Newer products that utilize Bluetooth radio technology also operate in the 2.4GHz band and can cause interference with wireless LANs, especially in fringe areas not well covered by a particular wireless LAN access point. The other issue, outward interference, occurs when a wireless network's signal disrupts other systems, such as adjacent wireless LANs and navigation equipment on aircraft [9].

6. Security

Security is a principal consideration when planning, designing, implementing, and managing a network infrastructure[7]. This is especially true for wireless LANs, which presentsaunique set of challenges to IT and security professionals [5].

The important security threats in wireless LAN are Denial of Service, Spoofing, and Eavesdropping [8].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

a. Denial of Service

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. By using a powerful enough transceiver, radio interference can easily be generated that would make WLAN unable to communicate using radio path. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attack.

b. Spoofing

This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN.

c. Eavesdropping

This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation.

VI. CONCLUSION AND FUTURE WORK

This paper provides an overview on basic design of wireless LAN. The paper initially discusses basic components and architecture of wireless LAN along with its advantages. The paper also provides brief details about different technologies that can be used for implementation of wireless LAN. Then it presents the overview of different issues in operation of wireless LAN including data rate, power, mobility, signal fading, radio signal interference and security threats. As the popularity of wireless network is growing enormously, it is a challenge that these issues should be addressed properly in order to develop and maintain the efficient and reliable networks in the future.

REFERENCES

1. Ibrahim Al Shourbaji, "An Overview of Wireless Local Area Networks (WLAN)", International Journal of Computer Science and Information Security, Vol. 11, No. 2, 2013.
2. Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen,"IEEE 802.11 Wireless LAN Security Overview",IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, pp.138-156, 2006.
3. "IEEE 802.11b Wireless LANs : Wireless Freedom at Ethernet Speeds", a Technical Paper, 3Com Corporation.
4. Qiang Ni*, Lamia Romdhani, Thierry Turletti, "A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN", Journal of Wireless Communications and Mobile Computing, WileyVolume 4, Issue 5: pp.547-566, 2004.
5. "Wireless LAN Security: Enabling and Protecting the Enterprise", A White Paper, Symantec Enterprise Security.
6. Raj Kumar Singh, Dr.A.K.Jain, "Research Issues in Wireless Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, pp. 115-119, 2012.
7. Abu Taha Zamani, Javed Ahmad, "Wireless LAN Security : IEEE 802.11g & VPN", International Journal of Advanced Research inComputer Science and Software Engineering, Volume 4, Issue 2, pp. 523-530, 2014.
8. "Wireless LAN: Security Issues and Solutions", SANS Institute InfoSec Reading Room.
9. Vijay Chandramouli, "A Detailed Study on Wireless LAN Technologies", URL: https://www.uta.edu/oit/policy/ns/docs/wireless-paper-vijay.pdf.

BIOGRAPHY

Prachi R. Narkhede is an Assistant Professor in the Electronics and Telecommunication Department, PRMIT&R, Badnera, Amravati. She received Master of Engineering (Electronics Engineering) degree in 2015 from Yeshwantrao Chavan College of Engineering, Nagpur, MS, India.