Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.85 – 93

RESEARCH ARTICLE

An Overview of IEEE802.11 Wireless LAN Technologies

Dr. S.Dhanalakshmi[#1], M. Sathiya[*2]

[#1]Professor & Head Dept of Computer Science & Applications
[*2]M.Phil Full Time Research scholar, Department of Computer Science
Vivekanandha College of Arts and Sciences for Women (Autonomous), Namakkal, TamilNadu, India
[1] vicascshod@gmail.com
[2] sathiya1629@gmail.com

Abstract- ***Wireless Communication is an application of science and technology that has come to be vital for modern existence. Wireless communication is an ever developing field, and the future holds many possibilities in this area. One expectation for the future in this field is that, the devices can be developed to support communication with higher data rates and more security. This paper provides a detailed study of the available wireless LAN technologies and the concerned issues. Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs. Wired Equivalent Privacy (WEP) was the first logical solution to secure WLANs. However, WEP suffered many problems which were partially solved by IEEE802.1x protocol. As the technology continues to move from wired to wireless, the wireless LAN (Local Area Network) has become one of the most popular networking environment.***

Keywords- WLAN, Security, WEP, IEEE802, Mobile Computing

I. INTRODUCTION

Computer technology has rapidly growth over the past decade. Much of this can be attributed to the internet as many computers now have a need to be networked together to establish an online connection. Companies and individuals have interconnected computers with Local Area Networks (LANs).The LAN user has at their disposal much more information, data and applications than they could otherwise store by themselves. In the past all local area networks were wired together and in a fixed location. Wireless technology has helped to simplify networking by enabling multiple computer users simultaneously share resources in a home or business without additional or intrusive wiring. The increased demands for mobility and flexibility in our daily life are demands that lead the development.

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.

Wireless technology has helped to simplify networking by enabling multiple computer users to simultaneously share resources in a home or business without additional or intrusive wiring. These resources might include a broadband Internet connection, network printers, data files, and even streaming audio and video. This kind of resource sharing has become more prevalent as computer users have changed their habits from using single, stand-alone computers to working on networks with multiple computers, each with potentially different operating systems and varying peripheral hardware. U.S. Robotics wireless networking products offer a variety of solutions to seamlessly integrate computers, peripherals, and data. Wireless networking enables the same capabilities and comparable speeds of a wired 10BASE-T network without the difficulties associated with laying wire, drilling into walls, or stringing Ethernet cables throughout an office building or home. Laptop users have the freedom to roam anywhere in the office building or home without having to hunt down a connector cable or available jack. Every room in a wireless home or office can be "connected" to the network, so adding more users and growing a network can be as simple as installing a new wireless network adapter.

Wireless Local Area Networks (WLANs) succeeded in providing wireless network access at acceptable data rates. The Institute of Electrical and Electronics Engineering (IEEE) have set standards and specifications for data communications in wireless environment, IEEE802.11 is the driving technology standard for WLANs. WLANs are deployed as an extension to the existing fixed/wired LANs and due to the fact that the nature of WLANs are different from their wired counterparts, it is important to raise the security of WLANs to levels closer or equal to the wired LANs. In general IEEE802.11 can operate in two network topology modes, Ad hoc and Infrastructure modes.

This paper discusses WLANs in infrastructure mode. 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; probing, authentication and association. 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. Next is the authentication phase, the STA here is authenticated by the AP using some authentication mechanisms described later in the paper. 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. Figure 1 shows the three phases in WLANs.

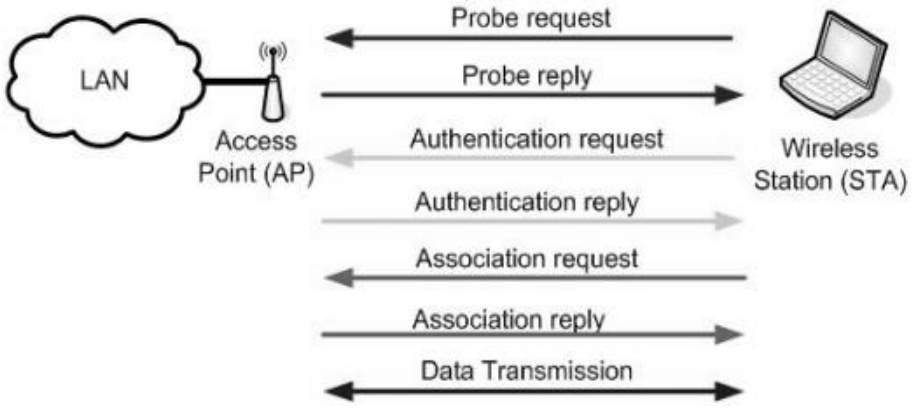

Fig. 1: WLAN establish connections between STAs and AP

A wireless LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Base Service Set or BSS*) is controlled by a Base station (called Access point or AP). Wireless LAN standards that are currently being explored in the field of communications technology are:

1. IEEE 802.11.
    a. 802.11a
    b. 802.11b
    c. 802.11g
2. HiperLAN/2.
3. Bluetooth.
4. HomeRF.

II. HISTORY OF WLAN

In the early 1990's WLANs found almost no success in selling to enterprise or campus environments as wired LAN replacements or enablers of mobility. The WLAN products of that day were far too slow, too expensive, too bulky, and too power hungry. Furthermore, mobile network connectivity was simply not yet a killer application. The "survivor" companies of that age were the ones who focused on adapting WLAN technology to specialty niches such as retailing, hospitality, and logistics. Organizations that went after the "big" market of enterprise networking, and there were many that did, either went bankrupt or became largely scaled back divisions of large companies. By the middle of the 1990's the WLAN industry had mainly consolidated into 4 players, But in the late 1990's the first significant market opportunity for WLANs emerged and it was quite unlike what the WLAN industry to date had largely
envisioned. The opportunity was the sharing of a broadband Internet connection within the home amongst multiple networked devices such as PCs initially, but inevitably also voice over Internet protocol (VoIP) phones, gaming consoles, media streamers and home automation appliances.

WLAN hardware initially cost so much that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (in products using the Wi-Fi brand name). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, it is even more unlikely that it will ever succeed.

Fig.2: 54 Mbit/s WLAN PCI Card (802.11g)

In 2009 802.11n was added to 802.11. It operates in both the 2.4 GHz and 5 GHz bands at a maximum data transfer rate of 600 Mbit/s. Most newer routers are able to utilise both wireless bands, known as **dualband**. This allows data communications to avoid the crowded 2.4 GHz band, which is also shared with Bluetooth devices and microwave

ovens. The 5 GHz band is also wider than the 2.4 GHz band, with more channels, which permits a greater number of devices to share the space. Not all channels are available in all regions.

III. WLAN TECHNOLOGY

As various wireless networking technologies have advanced over time, several WLAN technologies have emerged, including: Narrowband, Spread spectrum, Frequency hopping spread spectrum, and Direct sequence spread spectrum.

a) *Narrowband:* As the name suggests, narrowband technology uses a specific radio frequency (in the range of 50 cps to 64 Kbps) for data transmission.

b) *Spread Spectrum:* Originally developed for military use, spread spectrum technology allows for greater bandwidth by continually altering the frequency of the transmitted signal, thus spreading the transmission across multiple frequencies. Spread spectrum uses more bandwidth than narrowband, but the transmission is more secure, reliable, and easier to detect.

c) *Frequency Hopping Spread Spectrum:* Frequency Hopping Spread Spectrum (FHSS) technology synchronizes the changing frequency of both the transmitter and receiver (using a narrowband carrier) to, in effect, produce a single transmission signal. This frequency "hopping" can occur as often as several times a second; it is constantly changing from one frequency to another, transmitting data for a certain period of time before changing frequency again. Like spread spectrum technology, FHSS technology consumes additional bandwidth, however, this is over the course of multiple carrier frequencies.

d) *Direct Sequence Spread Spectrum:* Direct Sequence Spread Spectrum (DSSS) technology breaks down the transmitted stream of data into small pieces across a frequency channel. A redundant bit pattern (known as a chipping code) is generated for each bit transmitted. Generally, the longer the chipping code, the more likely it is that the original transmitted data will be properly received. DSSS technology uses more bandwidth than FHSS, but DSSS is considered more reliable and resists interference. Because of the chipping code, data can still be recovered without retransmission of the signal, even in the case of damaged data bits. U.S. Robotics wireless networking products utilize DSSS technology.

IV. ISSUES OVER WIRELESS LAN

Since wireless devices need to be small and wireless networks are bandwidths limited, some of the key challenges in wireless networks are:

a. Data Rate Enhancements.
b. Low power networking.
c. Security.
d. Radio Signal Interference.
e. System Interoperability

a) *Enhancing Data Rate:* Improving the current data rates to support future high speed applications is essential, especially, if multimedia service are to be provided. Data rate is a function of various factors.

b) *Low Power Design:* The size and battery power limitation of wireless mobile devices place a limit on the range and throughput that can be supported by a wireless LAN.

c) Security: Security [10] is a big concern in wireless networking, especially in m-commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network.

d) Radio Signal Interference: Interference can take on an inward or outward direction. 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.

e) System Interoperability: With wireless LANs, interoperability is taken as a serious issue. To ensure interoperability with wireless LANs, it is best to implement radio cards and access points from the same vendor, if possible.

V. BENEFITS AND ADVANTAGES OF WLAN

A) Benefits

i) SIMPLIFIED IMPLEMENTATION AND MAINTENANCE

Wireless APs can be placed in the ceiling, where they can accommodate a virtually endless variety of office configurations. Wired LANs, in contrast, consume time and resources to run cables from a network closet to user's desktops and to difficult-to-service areas such as conference room tables and common areas. With a wired LAN, each additional user or modification to the floor plan necessitates adjustments to the cabling system.

ii) EXTENDED REACH

Wireless LANs enable employees to access company resources from any location within an AP's transmission range. This flexibility and convenience can directly improve employee productivity.

iii) INCREASED WORKER MOBILITY

The roaming benefits of wireless LANs extend across all industries and disciplines. The shop foreman can manage logistics from the warehouse as easily as office-based employees move about the building with their laptops or PDAs. And field sales employees can connect to public wireless LANs in coffee shops and airport lounges.

iv) REDUCED TOTAL COST OF OWNERSHIP AND OPERATION

The cumulative benefits of simplified implementation and maintenance, an extended LAN reach, and the freedom to roam minimize expenses and improve organizational and employee productivity. The result is reduced total cost of ownership and operation.

B) Advantages

Wireless LANs designed to operate in license-free bands making their operation and maintenance costs less than contemporary cellular and PCS networks. The use of license-free spectrum, however, increases the risk of network security and in-band interference. The key advantages of wireless networks as opposed to wired networks are mobility, flexibility, ease of installation and maintenance, and reduced cost. (Aziz, 2003).

According to (Symantec , 2002) wireless LANs are less expensive and less intrusive to implement and maintain, as user needs change. Simple implementation and maintenance, extended reach, increased worker mobility and reduce total cost of ownership and operation.

VI. WIRED EQUIVALENT PRIVACY(WEP) PROTOCOL

The IEEE 802.11 standard for wireless LAN communications introduced the WEP protocol in order to address the security problems discussed above and attempted to bring the security of the wireless systems closer to that of wired ones. The main goal of WEP algorithm is to protect wireless communication from eavesdropping. Although unauthorized access to a wireless network is not an explicit goal in the 802.11 standard for wireless communication, it is frequently considered to be a feature of WEP. Unfortunately, the 802.11 provides only limited support for wireless confidentiality through the Wired Equivalent Privacy (WEP) protocol [11]. Difficult security issues such as key management and a robust authentication mechanism are left as open problems by the standards committee. In this section, we first describe the features of WEP and then discuss about the pitfalls in WEP.

The goal of WEP is to provide an equivalent level of privacy as is ordinarily present in an unsecured wired LAN by encrypting transmitted data. WEP has never intended to be an end-to-end security solution. WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The 802.11
Standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks described above but no commercial systems that we are aware of has mechanisms to support such techniques.

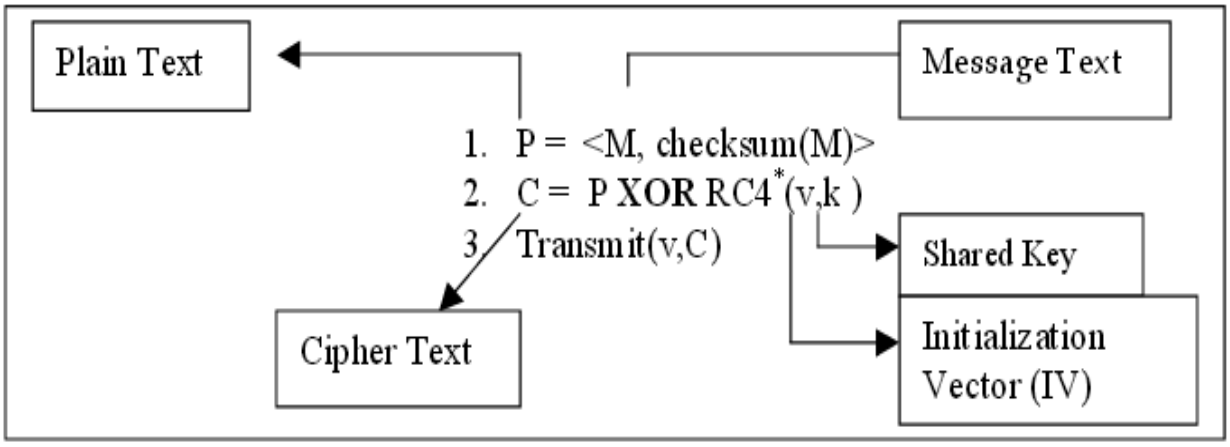

Fig. 3: WEP Protocol Review

VII. AD HOC MODE VS INFRASTRUCTURE MODE

The 802.11 specification defines two types of operational modes: ad hoc (peer-to-peer) mode and infrastructure mode. In ad hoc mode, the wireless network is relatively simple and consists of 802.11 Network Interface Cards (NICs). The networked computers communicate directly with one another without the use of an access point. In infrastructure mode, the wireless network is composed of a wireless access point(s) and 802.11 Network Interface Cards (NICs). The access point acts as a base station in an 802.11network and all communications from all of the wireless clients go through the access point. The access point also provides for increased wireless range, growth of the number of wireless users, and additional network security.

AD HOC MODE

In ad hoc mode, also known as Independent Basic Service Set (IBSS) or peer-to-peer mode, all of the computers and workstations connected with a wireless NIC card can communicate with each other via radio waves without an access point. Ad hoc mode is convenient for quickly setting up a wireless network in a meeting room, hotel conference center, or anywhere else sufficient wired infrastructure does not exist.

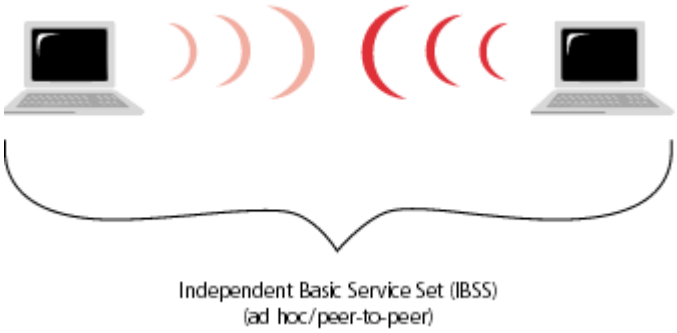

Fig. 4: Ad hoc Mode

INFRASTRUCTURE MODE

In infrastructure mode, all mobile and wireless client devices and computers communicate with the access point, which provides the connection from the wireless radio frequency world to the hard-wired LAN world. The access point performs the conversion of 802.11 packets to 802.3 Ethernet LAN packets. Data packets traveling from the LAN to a wireless client are converted by the access point into radio signals and transmitted out into the environment. A basic wireless infrastructure with a single access point is called a Basic Service Set (BSS).When more than one access point is connected to a network to form a single sub-network, it is called an Extended Service Set (ESS).

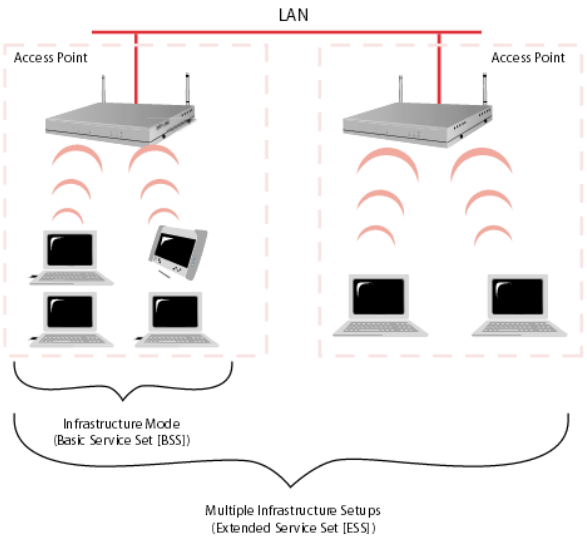

Fig. 5: Basic Service Set (BSS) and Extended Service Set (ESS)

VIII. WIRELESS NETWORK COMPONENTS

Much like a traditional wired LAN, a WLAN is a grouping of computers and peripheral devices that share a common communications backbone. As is implied by the name, a WLAN allows users to connect to the LAN wirelessly via radio transmission. The following are the most common components of a WLAN.

Access Point

The access point is a device that links a wireless network to a wired LAN. It increases the effective range of a wireless network and provides additional network management and security features. Wireless networks of three or fewer PCs do not require an access point for ad hoc networking. Access points are useful for larger networks, and they are particularly well-suited for adding wireless capability to an existing wired network. The U.S. Robotics 22 Mbps Wireless Access Point connects via an RJ-45 cable to a LAN and can support up to 20 wireless users at an effective range of up to 1500 feet in open spaces. It also enables additional security features such as MAC address authentication.

PC Card

A wireless PC card enables laptop users to connect wirelessly to the LAN. U.S. Robotics 22 Mbps Wireless PC Cards allow for ad hoc networking of up to three computers at an effective range of up to 1000 feet in open spaces.

PCI Adapter

Just as a wireless access PC card allows portable and laptop computers access to the LAN, a wireless access PCI adapter allows desktop PC users access to the LAN. U.S. Robotics 22 Mbps Wireless PCI Adapters allow for ad hoc networking of up to three computers at an effective range of up to 1000 feet in open spaces.

Router

A router is a device used for sharing a single Internet connection across multiple computers. This is ideal in the home or office where multiple computers and devices can be online at the same time with only a single Internet connection. The U.S. Robotics 22 Mbps Wireless Cable/DSL Router includes built-in wireless access point capabilities.

IX. 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. Wireless LANs are becoming more and more secure especially with the arrival of IEEE802.11i complaint wireless hardware. Sensitive information and highly secured communications can be transmitted with a higher confident than few years back that no illicit user around can actively or passively tamper with the data transmitted providing a careful, skilled personnel is in charge of configuring and installing the APs. IEEE802.11 was initially designed to interconnect wireless devices to wired networks; the aim was to achieve networking with minimum or no security. Security was not an important issue at that stage, however, with the successful of LANs and the fast adoption of this technology, security became important and achieving security became a primary concern.

ACKNOWLEDGEMENT

We express our sincere thanks to our HoD Dr.S.Dhanalakshmi for their whole hearted and kind cooperation. We extend our thanks to all the faculties of the department of Computer Science and Applications, who were behind throughout the course of study.

REFERENCES

[1] Clark, David, Pogran, Kenneth T. & Wed, David p. (1978). An Introduction to Local Area Networks . Proceedings of the IEEE, Vol. 66, 11, November 1978.
[2] IEEE Working Group for WLAN Standards (http://grouper.ieee.org/groups/802/11/index.html)
[3] IEEE 802.11Working Group. http://grouper.ieee.org/groups/802/11/index.html
[4] Holt, Keith, (2005). Wireless LAN: Past, Present, and Future. Intel Corporation. [5]John Cox, "LAN Services Set to Go Wireless," Network World, August 20, 2001
[5] http://www.nwfusion.com/news/2001/0820wireless.html)
[6] Joseph Williams, "Providing for Wireless LAN Security, Part 2". IEEE IT Pro, November | December 2002.
[7] Matthew S. Gast, 802.11 Wireless Networks, O'REILLY, 2002.
[8] Negus, Kevin J., & Petrick, Al,(2009). History of Wireless Local Area Networks (WLANs) in the Unlicensed Bands. info, Vol. 11 Iss: 5, pp.36 - 56.
[9] Prem, Edward C., (2000). Wireless Local Area Networks. www.cis.ohio-state.edu/~jain/cis788-97/wireless_lans/index.html.
[10] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless network security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.
[11] Rancourt, .J. D., (1993). Safety of Laser Products. Int. Electrotech. Commission, EI/IEC825-1: Optical Thin Films. New York: Macmillan
[12] The Wireless LAN Standard.Cisco Systems, 2000.
[13] "802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard", White Paper, 2002, www.proxim.com.

