A Report on Wireless Local Area Networks And Technologies Used

Mr. A. NARENDER  
Asst. Professor, Dept. of CSE  
Teegala Krishna Reddy Engineering College  
Hyderabad.

K. RAJYALAXMI  
Asst. Professor, Dept. of CSE  
Teegala Krishna Reddy Engineering College  
Hyderabad.

Abstract: Day by day technology is growing and people are attracted to the new technologies. This thinking made to have the new technology in the communication era. Initially it is wired communication where people or the device does not have the mobility while communicating. In this paper, it is clearly discussed about the technology known as “Wireless Local Area Network”. The existing networks are of different types like Wired and Wireless. Now, I am going to present the History of the networks, Importance of the networks, Types of the networks and their advantages and disadvantages, security implementations etc. There are so many other concepts which may creep in discussing the WLAN. All these things are explained in the following sections one after the other.

Keywords— Networks; WLAN; Security;

I. INTRODUCTION

Now a days with the growth of the technology, Wireless LAN became more ubiquitous. This technology became the default network for all the mobility based devices. In the initial days of this mechanism, because of the security and the speed people are not interested in using this type of network. But slowly as the time passes and because of the comfort people are habituated in using the WLAN. Now a day, if any of the users wants to connect to the global network, then one should have a connection to the global network. This connection is made simple by the WLAN. With the help of WLAN one can establish their own private network and they can communicate globally by establishing the connection with the network of networks. As the use of WLAN increases, there may be a chance of miss-utilization of the network by the intruders or hackers. As the technology is increasing and the usage of technology is increasing with the same pace. To overcome all the risks which are associated with this environment, different security measures should be implemented [1].

Before entering into the WLAN in detail, let me present the basics about the types of the Networks. Network is divided into 3 types based on the speed, distance and accuracy. They are

a. Wide Area Network.

b. Metropolitan Area Network.

c. Local Area Network.

From all the above 3 types of networks, this paper is totally concentrating on Local Area Network. Again LAN is divided into two types[2]. They are

i. Wired LAN.

ii. Wireless LAN.

Generally, in the earlier days, the systems or nodes in the organization are connected through the wires and established the network. The radius of this type of network will be in limited range like 1-2 kilo meters. This network is established with fixed wire and there is no mobility with the devices. Now, the departments which are present in the organization will establish the communication along with this wired network. As days are passing and with the improvement of the technology WLAN came into picture. This network is easy to establish and provides different benefits like connecting the multiple users to share the information like files, data, devices and the other resources which are available in the network. Apart from this it establishes the connection between the users to interact each other when and where necessary. Another advantage of the WLAN is its mobility nature. Users and devices can move from one place to the other within the network. The features which are present with the wired technology with the usage of 10BASE-T communication media, the same speed and data rate is achieved here. Apart from this so many problems and risks are overcome like wiring, cabling, drilling the walls etc. WLAN became popular because of the features like mobility, flexibility, no physical cabling and any other extra infrastructure is needed.

To define what exactly a Wireless LAN is connecting the communicable devices which are present in the limited range i.e., either in the same organization or within the departments of the same organization. When compared to the other transmission media, this is very much in expensive and provides the same features like traditional wired network.

History of WLAN:

Initially, in the earlier days of WLAN people are not interested to adopt this technology because of its cost, very slow and consumes more electrical energy. Even though it has the feature like mobility still it is not
attracted by the people. In the late 1990 it is started implementing its working like connecting to the broadband networks from a local network and provides the features like mobility and concentrated on the drawbacks like speed and data rate. By implementing different specification and providing the features, slowly the use of WLAN is increased. So many services are offered with the WLAN like Voice over Internet Protocol, watching videos, playing games etc. [18].

**Need of WLAN:**

Now a days use of communicable devices are growing and all these devices are mobility based devices like laptop, mobiles, PDA’s, tablets etc. All the users of these devices needs the connectivity even when they are in moving and still they want to be connected to the network.

Another reason to have the WLAN is that we can have the easy installation. No physical wiring, drilling and configuring the systems again. If the organization which consists of wired networks, then because of any of the reason if it has to change the location then all the cabling should be removed and again they have to have the rewiring in the new place. We are not sure that again these cables may be used or may not be. Again physical stress is associated with it. But if at all we use the WLAN, no such kind of risks, just simply shifting the devices that’s it. This network is very much portable, we can shift it to wherever we want without any overhead.

**Access Point:** This is one of the device which establish the connection between the wireless LAN and Wired network. With the help of access point the range of wireless network will be increased. For less number of systems we won’t require any access point, but when there are more number of systems then we require access points.

**LAN Card and Adapters:** These are another peripherals which will be present in the system or laptop to connect to the wireless LAN. PC card used to establish the connection between the laptop and wireless LAN as well as PCI adapter is used to establish the connection between the desktop computers and the Wireless LAN.

**Router:** After establishing the connection, this device used to share the internet connection among the computers or the devices which are connected in the wireless networks. By using the one internet connection, multiple systems are connected.

### III. WLAN TECHNOLOGIES

WLAN Technology concept will be achieved by so many mechanisms. All these mechanisms main intention or goal is to provide Wireless networking. This concept is achieved by Bluetooth, Infrared, IEEE 802.11 and HomeRF. All these methods are used currently based on the requirement of the organization. All these mechanism supports public and private networks. We can even protect the network which were established by us. If needed only anyone can enter into the network by applying different authorization mechanisms. The following are the brief description about the different mechanisms.[19].

**Bluetooth:**

This is one of the Wireless network mechanism which is introduced in the year 1999. Its specifications are mainly covers the shorter distance and the connectivity is portable i.e., for any sort of device communication is possible. It establishes the communication on the frequency of 2.45 GhZ. This frequency is set by the international agreement which can be used for industrial, health and scientifically. Another important feature of the Bluetooth is, it is license free and any device which are in that range can have the communication. There exists some rules and regulations to be followed in communication will be taken care by the Bluetooth protocol. Apart from the Bluetooth protocol, there exists communication protocol which will be taking care of data to sent and receive reliably between the both parties.

---

In the above figure 1, the structure of WLAN has shown. It consists of some infrastructure like Router, Switch and the wired Ethernet. In the above figure there are different communicable devices like laptop, PC and if you require we can even use mobiles and other electronic gadgets. All these radius which are in the radius of the router will get the signals and they are identified in that network. This is a logical network and users can come and join and as well as they can leave. Here once identified device need not to be have any identification or reconfiguration to it. These are the different advantages which are offered by the WLAN.

![General Structure of WLAN](http://www.cisco.com/c/dam/en_us/about/ac123/ac147/images/ipj/ipj_9-3/93_wlan_fig1_lg.jpg)
Currently, in mobile devices Bluetooth is using to exchange the information in between the mobiles. The main drawback of the Bluetooth is its shorter distance i.e, nearly 10 meters.

**Figure 2: Symbol used to represent the Bluetooth.**


The above symbol present in the Figure 2 represents the Bluetooth technology. This technology can be used in the devices like mobiles, earphones, laptops, tablets, detachable Bluetooth devices etc.

**Wireless LAN with InfraRed:**

InfraRed is another kind of technology which is used to establish the Wireless LAN. Generally Wireless LAN uses the Radio frequencies, but here to transfer the signals infrared light is used and for this generally the devices are installed with the infrared ports.[20].

Generally, the devices which are present in the high speed networks will consume more power and it should be in less weight and size. All these limitations and requirement made to concentrate on the infrared technology.

This technology will communicated with the help of propagation of light wave by using the infrared bands as a communication media.

**Figure 3: Infrared communication technology.**

[Image: https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcS3LjfwFzC4GDYas6bnXt_bBCYiYq_nZeua2GCJxNIUKkJRmR]

The best example for the infrared technology is TV Remote. When we press any key on the remote, then the signal is emitted by the remote emitters and the signal will transmit with the propagation of the light waves in the line of transmission. Receiver will receive the signal and perform the functionality.

**IEEE 802.11 Technology:**

To implement the Wireless LAN technology, IEEE released a standard which contains some set of protocols, guidelines for establishing the communication in the available network. This is the initial standard of the IEEE for wireless LAN which operates in 2.4 GHZ. The speed of the data transfer is 1 mbps to 2 mbps. As this is very low transmission for the users, that’s why it did not reached upto the expectations of the users.

The following are different versions or specifications of 802.11 standard. As 802.11 is explained in the previous paragraph, now we will continue the remaining standards.

**802.11a:**

With the drawbacks present in the 802.11 standards, this standard mainly concentrated on the data rate which is in different ranges like 6, 12 or 24 mbps. This standard used FDM to have the higher data rate. The signals which has to transmit will be further divided into sub signals and these are sent parallel through different frequencies to achieve higher data rate. This 802.11a is not a global standard which is also called as WiFi5 technology.

**802.11b:**

Again this standard will also operates in 2.4 GHZ. But the transmission had by this standard will have higher data rate when compared to 802.11a. It uses the complementary code keying modulation which achieves higher data rate and less error prone. The coverage of using this standard greatly increases to the 70% of existing coverage. Apart from this the other features achieved with this standard is interoperability and security. This standard is compatible with other standard compatible devices and it uses the encryption and decryption mechanism for security along with MAC authentication mechanism.

**802.11g:**

This is the latest standard which is released by the IEEE and also operates in the same frequency of 2.4 GHZ. It is having the higher data rates nearly 54 mbps. But this operation will be had for the limited
distance. If the distance is getting more and coverage will be decreased. It is best compatible with the 802.11a and 802.11b and all the features of these two standards are established in this standard.

Every standard which is explained are using carrier sense multiple access and collision detection approach(CSMA/CD). All these standards are having the interoperability feature by which it can be working with any vendors manufactured device.

Apart from the above standards mentioned, the other standards are 802.11g, 802.11n, 802.11ac, 802.11ad, 802.11p and 802.11af. All these standards are having different specifications from each other like having higher data rate, uses in some environment like 802.11p uses in the vehicular environment, to achieve high throughput etc. Even the other standards are explained in the below sections[4].

802.11c:
This standard is used to establish a link between the wireless LAN and the MAC protocol. This can be used as a bridge. The functionalities of the bridge are similar to the Internet Protocol. Bridge is a simple mechanism which is better than IP protocol.

802.11d:
This standard will operate at 5 MHz and it is used as an additional support for 802.11 which is used for additional regulatory domains.[11].

802.11e:
This standard is implemented in the year 2005 and it is the supporting standard for 802.11. This is mainly developed for the quality service. This standard improves the polling efficiency and also the channel robustness. Generally more quality is responsible for video streaming and telephony conversations. There this standard will be used.

802.11f:
This standard is used to establish the communication in between the access point and multi-vendor systems. It can also be used as a bridge to connect the WLAN’s and also checks the continuity of the transmission. This standard allows the roaming of the device from one AP to another AP. This can also be used for Inter access point protocol.

802.11h:
This standard uses 5GHz frequency apart from the use of 802.11 standard. This standard introduced two mechanisms. They are

a. Dynamic Frequency selection: This scheme prevents the collision by detecting other networks operating frequency and changes the current network operating frequency.

b. Transmission Power control: This control is used to keep the signal level below the preset level. It also improves the link condition by switching from the current frequency to the new channel which reduces the power consumption also.

802.11i:
The main use of this standard is to address the security issues in the wireless network. These issues were defined in the MAC layer. This standard makes use of advanced encryption standards, stream cipher techniques and block cipher mechanisms.[13].

Robust security network: This can be achieved by the two protocols. These are

4 Way Handshake:
Group key handshake.

All these utilize the different authorization controls and port accessing controls.

IV. LAYERS USED BY 802.11 TECHNOLOGY
To achieve the functionality of 802.11 standard, it uses different layers of the networking.

Physical Layer:
In order to increase the throughput of the standards, layered approach should be used. This standard(802.11) uses different physical layers namely Frequency Hopping Spread Spectrum(FHSS), Direct Sequence Spread Spectrum(DSSS) and Infrared spectrum. 802.11a and 802.11g will be using the Orthogonal Frequency Division multiplexing for increasing the throughput of the standard.

Frequency Hopping Spread Spectrum: In this technique signal is carried by switching in between the networks. This frequency hopping spread spectrum is divided into types. Slow frequency hopping spread spectrum, which carries more number of symbols in a single hop, by this there is some transfer delay established due to the more number of symbols that to be transmitted in one hop. Another one is Fast FHSS, which transmits a single symbol in more number of hops so that it can have the fast transmission.[8]. This spectrum is mainly developed for military purpose. It is having the higher bandwidth where the frequency of the signals will be altered throughout the transmission. It also synchronizes both transmitter and receiver frequencies. It transmits the data for some time before changing the frequency.

Direct Sequence spread spectrum: It uses more bandwidth when compared to FHSS. But it is reliable when compared to FHSS. In this technology, the transmitted signal will be broken into small pieces of data to a frequency channel. It transmits through bits of data, for each bit of data transmitted a chipping code will be generated. This chipping code will be used for recovering of data when the data is lost in transmission.[9].
Narrow Band: This technology uses a particular radio frequency for the communication and data transmission.

b. Medium Access Layer:

Generally 802.11 uses CSMA/CA technology whenever there exists a collision. All these collisions are avoided by using this technology. But MAC layer introduces the new concept like point coordination function(PCF). This mechanism is divided into two phases. In the first phase access points will scan all the stations to know whether there exists any packet to send by any of the station in a round robin fashion. Round robin method is an approach which follows some time quanta to be allocated to each station and gets shifted one after the other during the time quanta and checks all the stations for the packets to send. By using this, it requires polling by the stations which reduces the throughput of the system.

Problems to address by 802.11:

Security: As 802.11 provides the Wireless LAN technology, any unauthorized user can enter into the network and capture the data. There are different protocols which provide security in WLAN like WEP, WPA and WPA2. Still these protocols are not providing enough security. It requires standard and complex encryption algorithms which provide the maximum security.

Data Rate: when compared wired LAN standard it provides very less data rate. Even 802.11g provides 54 mbps only. More concentration is needed on this area.

This 802.11 standard will operate in two different modes. These modes explain how the communication is established between the access points and the base stations. These modes are

d. Infrastructure mode: In the given network, there exists number of access points and the stations. If the station want to communicate with the other station, it has to establish the connection with the access points. The following figure explains that how the Infrastructure mode will operate.

Figure 5: Infrastructure mode of operation.


ii). Independent mode: To have the communication in between the station, no access point is required. Every station can establish the connection with the other station directly. Every station will establish an adhoc connection between the stations when they need communication. After communication these adhoc links will be disconnected automatically[10].

![Figure 6: Independent mode of operation](http://arxiv.org/abs/1307.2661)

When we are discussing about the advantages, importance and technology about the Wireless LAN, then we have to concentrate on other risks like providing security features. As this is the wireless communication, there is high possibility of stealing the data. At any point of time intruders may enter into the network and can had the theft of data. The following are some of the measures that should be taken care by the wireless network providers.

Preventing unauthorized access: Wireless LAN is a kind of open entry system which allows anyone to enter into the network. To prevent the loss of the data one has to detect the unauthorized users. This can be done by continuously monitoring the network.

Providing security to the devices: Every device which is used for communication in WLAN should be equipped with one of the software agent. This agent functionality is to prevent the unauthorized access and loss of data.

Security to the data: When the data is in transit, there is a chance of hacking it. To eliminate such kind of theft of data, it should present in the unknown language. Later on after receiving again it should be decrypted to the known language. This encoding and decoding is known as cryptography, which had both the terms encryption and decryption.

Implementing the security policies: Every organization should enforce some policies which can prevent the theft or loss of data. Maintaining passwords, not to use flash drives, no entry for unauthorized persons. If some of these policies are followed by the organizations then at least some sort of security is provided to the data.

V. NEW TECHNOLOGIES

Zi-Fi Technology: This technology is developed for discovering the Wi-Fi coverage availability for different mobile devices. ZiFi enables the Zigbee radios to identify the unique interference of signatures which are generated by the WiFi signals. The main advantage of ZiFi is it uses digital signal processing and also uses the stochastic signal
identification mechanisms are used to identify the periodic interferences which are caused because of the beacon frame of Wi-Fi technology.[6].

Figure: Implementation of ZiFi on two different platform.[6].

This technology device is having the USB interface which will be easily connected to the mobile devices like laptops, mobiles etc. This technology uses the digital signal processing algorithm known as common multiple folding. This algorithm recharges the unknown signals from different RSS samples. The main advantage of this algorithm is that it have the less computational overhead. A constant false alarm rate was developed to reduce the false negatives.

ZiFi Architecture:

Figure 5: ZiFi Architecture[6].

The following are the components of ZiFi enabled system. In this there exists a built in sampler which reads the signal strength indicator register at a known frequency. After reading these samples they are processed by the shaper which will be adjusting the values to mitigate the noise that is present in the signals. These signals are processed by the algorithm known as common multiple folding. This is one of the DSP algorithm which is used to recharge the signal strength. The main advantage of the CMF algorithm is reducing the cost of amplifying the unwanted signals. Another component is component false alarm which are fed by the sample signals and is used to classify the periodic signals that whether they are genuine Wi-Fi signals or not by checking the threshold of the signal. The architecture also contains AP profiler and radio controller, where AP profiler is used to check the quality of the detected signal. At the end the radio control will on the Wi-Fi NIC card when the quality of the detected signal. At the end the radio control will on the Wi-Fi NIC card when the quality of the detected signal. At the end the radio control will on the Wi-Fi NIC card when the quality of the detected signal. At the end the radio control will on the Wi-Fi NIC card when the quality of the detected signal. At the end the radio control will on the Wi-Fi NIC card when the quality of the detected signal. At the end the radio control will on the Wi-Fi NIC card when the quality of the detected signal.

ZiFi is basically designed for unlicensed bands which is operated at 2.4GHZ and uses the 802.11 standards. While designing, the following are the issues which are concentrated.[6].

Accuracy: In this technology accuracy is detected by the False positive and false negative rates. These will give the information of falsely triggering which leads to energy wasting and also missing the opportunity of Wi-Fi connectivity.

Low delay: Generally wireless networks are slow when compared to the wired networks. But this technology takes less time for short connectivity when compared to the other wireless network technologies.

Low overhead: As we are creating the mobile environment, and the availability of energy and power will be less. While designing one has to concentrate on less utilization of these resources.[6].

VI. CONCLUSION

This paper purely concentrated on wireless Technologies. Initially I have gone through with different papers in order to understand the concept, terminology and technology. After knowing the concept I came to know the history of Wireless LAN. In implementing the wireless LAN some set of standards are required to provide the quality, security, reliable services. All these features are incorporated in this paper. Even I have concentrated on the future research areas as well as the challenges which are facing by the wireless LAN. At the end I came to know that wireless LAN became default network for current generation. This generation is totally using the smart devices. Where there is a open network, there also exists the risks which has to be concentrated. I have analyzed some risks and associate loss and also how to overcome those risks. While writing the paper I came to know the new concepts regarding the wireless LAN. Even I have concentrated on the new technologies like ZiFi.

VII. REFERENCES


