QoS–Continuous Lane Streaming in Road Network Security Measures in Wireless LAN Communication Network

[1]V.Thrinath Subramanyam, [1]K.Prasanth Kumar, [1]BasavPrasad.S and
[2]K. John Singh,
[1]PG Student, School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India.
[2]Assistant Professor (Selection Grade), School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India.

***Abstract*: Wireless technology has become an important module for communication and for the data transmission. This technology has replaced the present LAN in terms of security and as well as with the data transfer. Wireless Local Area Network (WLAN) effectively satisfies needs within buildings and campus environments. Developing security measures for the WLAN is a major issue when compared to the security features of LAN. The aim of this paper is to make the communication in the campus more secure, reliable and a standard one. This paper discusses about the important security features that are intended for the wireless network to be more stable. Contains the construction of the important modules used for the security of WLAN, secure data transfer, data encryption, wireless security types and the other issues on this network for making it a more stable one to provide and construct a secure digital network.**

Keywords: ***Wireless Modules, Local Area Network (LAN), Wireless Markup Language (WML), Denial of Service (DoS), Service Set Identifier, Virtual Private Network***

I. INTRODUCTION

The present generation of accessing the data totally depends on the type of the networks they use. Comparing with the previous years, the mode of accessing the data from the Internet have changed dramatically with the introduction of the LAN. LAN commonly known as the Local Area Network is a connection between the host server and the client mainly used for the purpose of the data access from the host server to the client. Proven to be more reliable, the LAN technology has made a huge impact in the field of networking but it lacks the concept of mobility. So for the implementation of the mobility the WLAN have been introduced. The WLAN is the successor of the LAN technology. The WLAN uses the Radio waves instead of the Ethernet cables used in the LAN. The WLAN technology has been introduced by the (IEEE) organization on 802.11 standards. This WLAN can be any type of device like the switch or a router. This generates Radio waves that are produced under some certain frequency rates. In the present state of networking technology the WLAN has became a revolution for its flexibility and the feature of mobility. This technology has gradually over taken the LAN Network. Now a day, we can find the WLAN network in many of the places like restaurants, corporate offices, Malls etc used for the data access on the move. The WLAN network is easy to access and this can be done by just connecting to the respected network's access point. This access point contains all the necessary security modules for a secure connection between the host and the client. But still there are still vulnerabilities present in the network connection. As the use of WLAN has tremendously increased, it is very much important to maintain the security for the wireless networks also. Basically there are many
network vulnerabilities present in the wireless networks. These are to be reduced for the better functioning of the network. In order to overcome this fact in this paper we bring out the security issues present in the network and also the modules that can be used to reduce the vulnerabilities present in the network.

II. MATERIALS AND METHODS

*Modes of accessing WLAN***:**

The data from the WLAN devices can be received through the access point that is present in the WLAN device (Jim 2005). The access point lets the client devices to transmit and receive the data securely using some of the modules present in the device. This Device allows the sharing of the data through the access points and through the LAN that present in it. Most of the devices that are compatible with it are connected for data transmission and receiving. The transmission of the data takes place securely through different security modules present like WEP, WPA, WPA2 security standards that are implemented for the access points (Yang 2006).

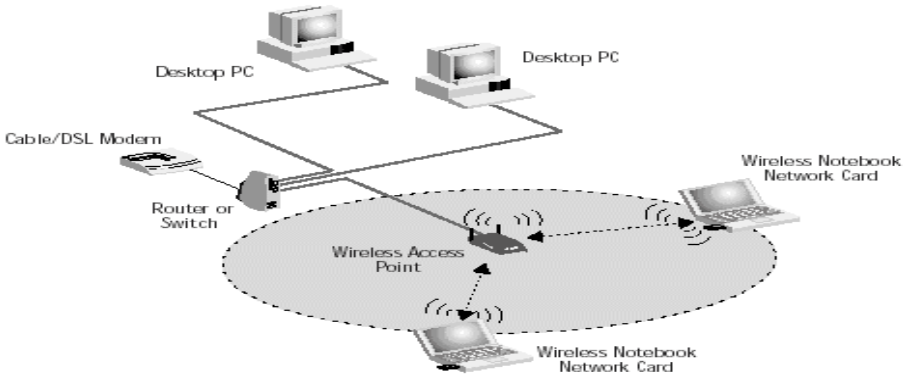

Fig. 1: Connection Modes of WLAN Network

PROTOCOLS USED IN WLAN

There are several WLAN protocols that are used for the transmission of the data to the compatible device. Out of them only few of them are used for the data transmission (Yong 2012). The below are some of the protocols that are followed for the data transmission.

*802.11a***:** This protocol runs in the standard 5 GHz band and is capable of having a data transmission rate of about 54Mbps and uses the OFDM (orthogonal frequency deviation Modulation).

*802.11b***:** The IEEE 802.11b was approved in 1999.This standard uses the DSSS (Direct Sequence Spread Spectrum) and uses the 2.4 GHz band that Provides a maximum data rate of 11Mbps and with minimum rate of 5.5Mbps

*802.11g***:** This standard has a data transmission rate up to 54Mbps and uses the 2.4 GHz band same as the 802.11b. This protocol was approved by the Wi-Fi Alliance in October 2003 and this protocol is now widely used as access point for the data transmission.

*802.11n***:** This is the newest standard that uses both the 2.4 GHz band and the 5 GHz band having a data rate of 150mbps on draft and up to 300Mbps on full band. It is the new multi streaming modulation technique. It uses MIMO (Multiple input and multiple output) standard. Of the above protocols 802.11b, 802.11g are the commonly used standards

SECURITY ISSUES IN WLAN

Security is the most important and essential part for the data that is to be transmitted over the internet through the WLAN devices. There are four standard security protocols that are used for safe access to the access points. WEP, WPA, WPA2 are the most commonly used Security modules in most of the wireless devices.

*WAP***:** Wireless application protocol is used as a wireless access mostly in the mobile phone. This implements the WML (Wireless mark up language) which is similar to the HTML (Yang 2006). The WAP gateway interprets between WML and HTML and facilitates the use of security protocols and encryption. Accessing through this mode without any encryption is highly vulnerable. This module can also use the TCP\IP protocols.

*WEP***:** This the older security module that provides minimal security and is preferably known as Wired Equivalency Privacy.WEP uses the 40 bit or 60 bit key for the encryption process. WEP2 is the advanced module which uses the 128 bit encryption. Minimal security and key management made this module least preferable and has many disadvantages.

*WPA***:** This module is commonly used in all the WLAN devices and implements more security features. Known as Wi-Fi protected access it uses the TKIP (Temporary Key Integration protocol) encryption Standard mode which allows dynamic changing of the encryption keys. This security protocol over comes the WEP as the WEP has to rearrange the Keys manually. This module requires a password length of 6 to 80 characters for the user to gain access to the network.

*WPA2***:** Wi-Fi protected access implements all the encryption standards present in the above modules and implements one more standard called as AES (Advanced encryption standard). This module has overcome all the issues present in the above modules and it is highly secured for the data transmission.

RESULTS AND DISCUSSION

Security Issues in the WLAN

As most of the wireless access points contains the security modules but still there are issues present in it (Min 2008). Not all the modules are neither highly sophisticated nor secured. These modules can also be hacked using its own encryption standards. The client devices can identify the wireless networks using the

service set identifier (SSID) along with some of the security parameters. This SSID is broadcasted along with its security modules used so that the hacker can identify the module used and can break the encryption modes of it and compromise the network. The real security comes from a proven security technique. The most important technique is the 802.11i which is also known as the WPA2.This standard provides two modes of operation mainly known as the PSK (Pre Shared Key) and Enterprise (Yang 2006).

Some of the securities issues present in the protocols are like the DOS (Denial of Service attack), Rouge access points and passive capturing. Among the above mentioned issues the denial of service is the most frequently present issue in the modules. The issue is about sending large amount of data to particular target and making it temporarily unavailable or limiting the network access. The flooding of the data to a particular target is not only the main reason but the interference can also be considered for this issue. As to attack the particular target hacker just needs to bypass the interference. Mac filtering is also the possible threat that can be occurred in the network communication. As far as the rouge access point is considered it's just like creating a certain ad-hoc private network making the user to access the network without knowing the possible threats of the network and its vulnerabilities .The hacker can have ample of time to just hack the information present in it. But network provides the internet access and leaves the user unaware of the vulnerability present in the network. The middle in the man attack can also be considered as one of the possible vulnerabilities in the network. This middle in the man attack can change the communication from the AP and the host station making the data to travel from its position manipulating itself as the originator of the data access.

PRACTICAL SOLUTIONS FOR SECURING WLAN

Despite the risks and vulnerabilities associated with wireless networking, there are certainly circumstances that demand their usage. Even with the WEP flaws, it is still possible for users to secure their WLAN to an acceptable level. This could be done by implementing the following actions to minimize attacks into the main networks:

Changing Default SSID:

Service Set Identifier (SSID) is a unique identifier that is broadcasted with the access points of WLAN. When a mobile device tries to connect to a particular access point the SSID differentiates one access point from another, so all devices attempting to connect the access point of the WLAN must use the same SSID. In fact, it is the only security mechanism that the access point requires to enable association in the absence of activating optional security features. Hiding the SSID from broadcasting its name makes the network only available for the users who are previously using it.

Encryption:

Encryption is the possible way of securing the data from being compromised over the network. Many of the encryption Techniques and software's are available to make the connection to access point more secure one. Encryption modules are also present in the WLAN devices, each having its own encryption technique and security measures (Yong 2012).

Utilize VPN:

Virtual Private Network (VPN) can be used to secure the WLAN networks (Bourdoucen 2009). The virtual private network is generally used to connect to an isolated remote access computer from a point of location. This provides the security for the data that is to be accessed. The VPN follows protocols like the tunneling and the IPSec (Internet Protocol Security) for the secure communication in the private network. So by integrating the WLAN network in to the VPN the privacy of the data can be improved and the access can only be available to the required content so that it becomes difficult to the hacker for compromising over the network. This VPN has become the most secured and trusted network for the communication between remote computers.

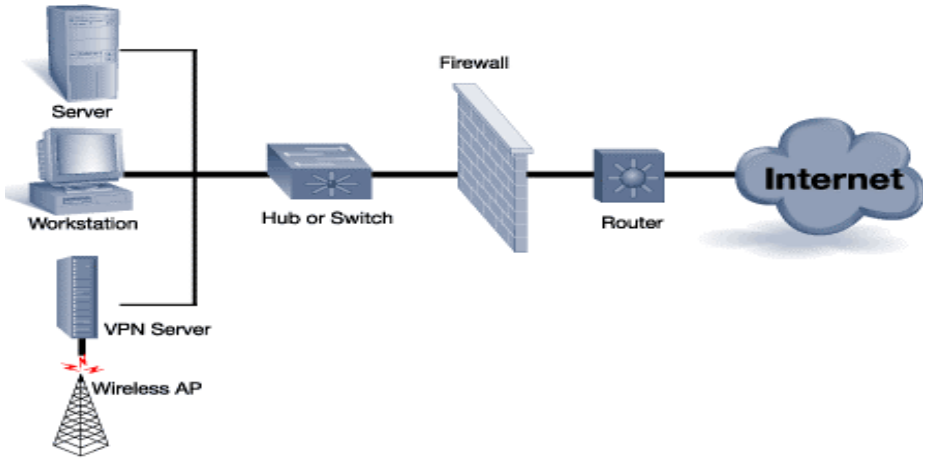

Fig. 2: Securing a wireless Access Point Using VPN

Antivirus and Firewalls

Using genuine Antivirus software some the security issues can be reduced. The firewalls place an important role of denying of the packets received through the network which are considered suspicious. The Dos attack can be reduced by using the firewall as this checks the inflow and out flow of the packets sent over the network and also monitors the ports of the network.

CONCLUSION

In this we have proposed a defensive technique for some of the attacks in WLAN and we have also reviewed wireless network security issues in Network Communications have identified a number of open problems in this area. This approach is based on the authentication technique which includes an Authentication Server (AS), VPN etc. However, there will be no complete fix for the existing vulnerabilities. All in all, the very best way to secure WLAN is to have the security knowledge, proper implementation, and continued maintenance.

REFERENCES

[1] Jim Gefer, 2005. Wireless Networks first step, Pearson Education, pp. 105-110.

[2] Haishen Peng, 2012. WIFI network Information security analysis research, IEEE 2012.

[3] Bourdoucen. H, Al Naamany. A and Al Kalbani. A, 2009. Impact of Implementing VPN to Secure wireless LAN, International Journal of Computer and Information Engineering, Vol. 3, No. 1, pp. 17-22.

[4] Yang Xiao, Chaitanya Bandela, Xiao Jiang(James) DU, Yi Pan and Edilbert Kamal Dass, 2006. Security mechanisms, Attacks and security Enhancements for the IEEE 802.11 WlAN'S, International Journal of Wireless and Mobile Computing, Vol. 1, No. 3/4, pp 276-288.

[5] Yong You, Qun Wang, Yan Jiang,"Research on the security of the WLAN Campus Network", 2012 International Conference on E-Health Networking, Digital Eco Systems and Technologies.

[6] Min Kyu Choi, Rosslin John Robels, Chang-hwa Hong and Tai-hoon Kim, 2008. Wireless network Security: Vulnerabilities, threats and Counter measures", International Journal of Multimedia and Ubiquitous Engineering, Vol 3, No 3, pp.77-86.