Privacy in Wireless Network

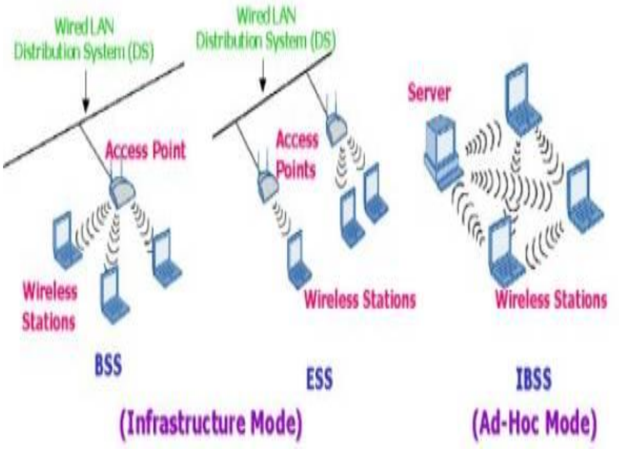
Sonali Rathod, Shiwangini Saurabh, Surbhi Sharma

Abstract— **The paper begins with the basic technologies of wireless networks and its security using the standard Institute of Electrical and Electronics Engineers (IEEE) 802.11.The purposes of this paper is to display awareness of security risks faced by wireless computer networks, This paper gives us information about network types and LAN standards, advantages of wireless network This paper concludes that guidelines for establishing secure wireless networks connection against unauthorized access. Wireless Network offer greater flexibility than cabled networks and significantly reduce the time to create new network.**

Index Terms— **Access Point, Service Set Identifier, Ad-Hoc Mode, Mobility Infrastructure Mode, productivity, Productivity, Shared Key Authentication, Wi-Fi Protected Access, Media Access Control, Wired Equivalent Privacy, Wireless Intrusion Prevention Systems.**

I. INTRODUCTION

In a wireless network, the computers are not connected by wires. Wireless networks include mobility and the absence of unsightly wires using radio signals that occurred at the physical level of network structure.



The basic technologies of wireless networks are mentioned below.

Wireless Local Area Network - It is a local area network which uses high frequency radio waves.

Service Set Identifier – It acts as a single shared password between access points and clients. It allows wireless clients to communicate with an appropriate access point through configurable identification.

Access Point – It is a hardware device which allows wireless connection in personal digital assistant and mobile computers.

Open System Authentication- It is the default authentication protocol for the 802.11 standards that can be used with Wired Equivalent Privacy protocol for secure communication.

Infrastructure Mode – This consists of a number of wireless stations and access points for large-scale networks.

Shared Key Authentication - Wired Equivalent Privacy and shared secret key to provide authentication. Encrypting text with shared secret key, this succeeds only when access point decrypts to the same challenge text.

1) *Ad-Hoc Mode- Ad-hoc mode consists of at least two wireless stations where no access point is needed in their communication. These are less expensive to run.*

Wi-Fi Protected Access- It is a wireless security protocol designed for data encryption.

II. TYPES OF WIRELESS NETWORKS

A) Wireless Personal Area Network (WPAN) - It operates within short range (1 m). Examples include print services or enabling a wireless keyboard or mouse to communicate with a computer.
B) Wireless Local Area Networks (WLANs) - It operates within a limited geographic area (100 m), Examples include office building or campus that are capable of radio communications
C) Wireless Metropolitan Area Networks (WMANs) - It operate within a few miles of each other(1 km). Examples include wireless broadband access to customers in metropolitan areas.
D) Wireless Wide Area Networks (WWANs) - It operates individuals and devices over large geographic areas (up to 10 km). Example include for mobile voice and data communications, satellite communications.

III. WIRELESS NETWORKS LAN STANDARDS

a) **802.11** –It provides 1 or 2 Mbps transmission in the 2.4 GHz band
b) **802.11a** – It provides up to 54 Mbps in the 5GHz band.
c) **802.11b** -It provides 11 Mbps transmission in the 2.4 GHz band.
d) **802.11g** - It provides 20+ Mbps in the 2.4 GHz band.

IV. WIRELESS NETWORK ADVANTAGES

Sonali Rathod, Shiwangini Saurabh, Surbhi Sharma, Department of Computer Science and Engineering Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

1. Convenience – wireless network can access within coverage area or from any Wi-Fi hotspot network resources from any location.

2. Mobility – Not possibility of longer physical connection, as you were with a wired connection. You can go online in conference room meetings.

3. Productivity - This access to the Internet resources helps our staff get the job done and encourages collaboration.

4. Easy setup- As no cable connection so installation can be quick and cost-effective.

5. Expandable - wireless networks can be easily expanded with existing equipment.

6. Security – The wireless networks have robust security protections.

7. Cost - wireless networks eliminate or reduce wiring costs.

V. WIRELESS NETWORK SECURITY

When unauthorized access or damage to computers is occurred using wireless networks the security is used to prevent. Two most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Today's many laptops, computers have wireless cards pre-installed. That card has ability to enter a network. Hackers can easily break wireless network. Hacking methods have become much more sophisticated and innovative with wireless. The organizations define effective wireless security policies that protect against unauthorized access for important resources like Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS).

VI. WIRELESS NETWORK SECURITY METHODS

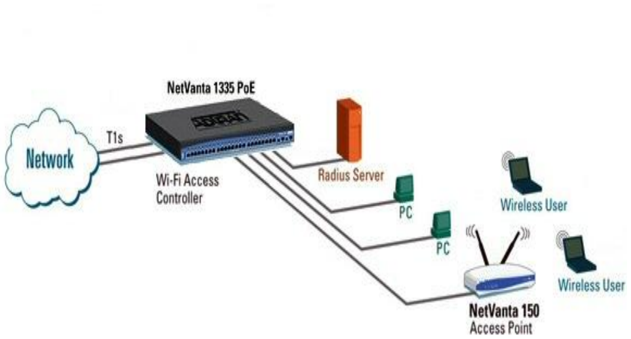
1. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access uses an encryption device which encrypts the network with a 256 bit key. It encrypts information and makes sure that the network security key has not been modified. Wi-Fi Protected Access also authenticates users to help ensure that only authorized people can access the network.

2. Wired Equivalent Privacy (WEP)

This is weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer, when you enable WEP; you set up a network security key.

VII. WIRELESS NETWORKING SECURITY



The following key helps us to secure a Wi-Fi network against unauthorized access

A) Turn Encryption On

Wireless routers often come out of the box with the encryption feature disabled, so be sure to check that encryption is turned on. To turn on encryption, you will need to pick a wireless network password. Stronger passwords that utilize a combination of letters, numbers and symbols are more secure.

B) Turn the Firewall On

A "firewall" is designed to protect computers from harmful intrusions and can be hardware-based or software-based. Wireless routers generally contain built-in firewalls.

C) Change Default Passwords

Most wireless routers come with preset passwords for administering the devices settings. It is different from the password used to access the wireless network itself.

D) Change the Default Name of the Network

When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID (network's name).

E) Turn Network Name Broadcasting Off

The routers broadcast the name of the network public. These features are often useful for businesses, libraries, hotels and restaurants that want to prefer wireless Internet access to customers.

D) Use the MAC Address Filter

Each and Every device which connects to a Wi-Fi network having unique ID called the "physical address" or "MAC" (Media Access Control) address. If we want to create other obstacle to unauthorized access, then change your router's settings.

VIII. CONCLUSION

In this paper, we have given a solution to privacy in wireless network. Wireless network having advantages as convenience and access, cost but it increases the risks of outside intrusion and misuse criminal offences in communication technologies. Todays world is developing fastly so wireless local area networks is growing rapidly. Human factors are as important as technical factors in providing wireless security. This paper contains few tips to secure a wireless network against unauthorized access.

REFERENCES

[1] 802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard., White Paper, 2002, www.proxim.com
Wireless Networking Choices for the Broadband Internet Home.

[2] Department of Education and Training (Government of Western Australia.

[3] Frankel, S et al. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. NIST Special Publication 800-97.

[4] Ossman, M. WEP: Dead again. Security Focus In focuses, 14 December 2004. Part 1.

[5] Aventail, Practical solutions for securing your wireless network, Aventail Technical White Paper, http://www.bitpipe.com