International Journal of Electrical, Electronics and Computer Engineering **2**(1): 123-126(2013)

ISSN No. (Online): 2277-2626

The Study of Wi-Fi Communication and Network Security Technique and Issues in Real Time

Jitender Singh*, Prof. Vijay Singh Rathod** and Prof. Abhijit Kulshrestha***

**Department of CSA, Jodhpur National University, Jodhpur (RJ), India*
***Department of CSE, Shri Karni College Jaipur, (RJ), India*
****Department of CSE, Jodhpur National University, Jodhpur (RJ), India*

(Received 17 April, 2013, Accepted 18 June, 2013)

ABSTRACT: The Wi-Fi radio standard, great leaps in the technology have been made. In the area of range Wi-Fi has been pushed to an extreme, and both commercial and residential applications of this Long Range Wi-Fi have cropped up around the world. It has also been used in experimental trials in the developing world to link communities separated by difficult geography with few or no other connectivity options. Provide coverage to a large office or business complex or campus. Establish point-to-point link between large skyscrapers or other office buildings. Bring Internet to remote construction sites or research labs. Bring Internet to a home if regular cable/DSL cannot be hooked up at the location. Bring Internet to a vacation home or cottage on a remote mountain or on a lake. Bring Internet to a Share a Neighborhood Wi-Fi network. Wi-Fi connects you to your favorite content and communications over your mobile phone, computer, media players and other devices - all without cumbersome cables. To protect Wi-Fi network you can install security safeguards like internet protocol security (IPSec), wired Equipment privacy (WEP) encryption standard, and the most used Wi-Fi protected access (WEP2).

Keywords**:** DSL; Wi-Fi; WEP; WEP2.

I. INTRODUCTION

A Wi-Fi enabled device such as a personal computer video game console mobile phone MP3 player or personal digital assistant to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more (interconnected) access point called a hotspot can comprise an area as small as a few rooms or as large as many square miles. Coverage in the larger area may depend on a group of access points with overlapping coverage. Wi-Fi technology has been used in wireless mesh networks.

In addition to private use in homes and offices, Wi-Fi can provide public access at Wi-Fi hotspots provided either free-of-charge or to subscribers to various commercial services. Organizations and businesses such as those running airports, hotels and restaurants - often provide free-use hotspots to attract or assist clients. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. As of 2008 more than 300 metropolitan-wide Wi-Fi projects had started. As of May 2008 the 879.Wi-Fi based Wireless Internet service providers (ISP). Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other premises, can provide Internet access and internetworking to all devices connected (wirelessly or by cable) to them. One can also connect Wi-Fi devices in ad-hoc mode for client-to-client connections without a router. Wi-Fi also enables places that would traditionally not have network access to connect, for example bathrooms, kitchens and garden sheds.

A. Wi-Fi Technology Work

Wi-Fi networks use radio technologies called 802.11 to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect electronic devices to each other, to the Internet, and to wire networks which use Ethernet technology. Wi-Fi networks operate in the 2.4 and 5 GHz radio bands, with some products that contain both bands (dual band). They can provide real-world performance similar to basic wired networks.

B. Frequency Band

Wi-Fi products operate over radio waves, in the same way as your cell phone, garage door opener, TV, radio, GPS navigation system or microwave. Each of these types of products operates in a specific slice, or frequency band, of the radio spectrum. Radio Band Examples:-

Table 1. Frequency Band.

Broadband band	(530-1610 kHz
Shortwave band	(5.9-26.1 MHz)
Citizens’ band	(26.965-27.405 MHz)
Television channels	(54-88 MHz)
FM_broadcast band	(88-108 MHz)
Wi-Fi	(2.4GHz or 5GHz)

Wi-Fi products operate in the 2.4GHz or 5GHz bands. These bands are designated as "license-free", which indicates that individuals may use products designed for these bands without a government license, such as those that are granted to TV or radio transmissions within licensed bands. Because the Wi-Fi bands are license free, it becomes more important for manufacturers to ensure that their products pass the standards of interoperability set by the Wi-Fi certifications. And because they also share these bands with non-Wi-Fi products, such as remote control toys, certification testing ensures that Wi-Fi products are good neighbors and will not interfere with signals from these devices.

C. Advantages

Operational advantages Wi-Fi allows the deployment of local area network (LANs) without wires for client devices, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LAN. As of 2010 manufacturers build wireless network adapters into most laptops. The price of chipset for Wi-Fi continues to drop, making it an economical networking option included in even more devices. Wi-Fi has become widespread in corporate infrastructures. Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Products designated as Wi-Fi Certified by the Wi-Fi Alliance are backwards compatible. Wi-Fi designates a globally operative set of standards-unlike mobile phones, any standard Wi-Fi device will work anywhere in the world. Wi-Fi operates in more than 220,000 public hotspots and in tens of millions of homes and corporate and university campuses worldwide. The current version of Wi-Fi Protected Access encryption (WPA2) as of 2010 is considered secure, provided users employ a strong perhaps. New protocols for quality of service (QoS) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video); and power saving mechanisms (WMM Power Save) improve battery operation.

D. Disadvantages

Wi-Fi uses the unlicensed 2.4GHz spectrum, which is often crowded with other devices such as Bluetooth, microwave ovens, cordless phones, or video sender devices, among many others. This may cause degradation in performance. Wi-Fi networks have limited range. A typical Wi-Fi home router might have a range of 45m (150ft) indoors and 90m (300ft) outdoors. The most common wireless encryption standard, wired equivalent privacy or WEP has been shown to be breakable even when it has been correctly configured. Access points could be used to steal personal and confidential information transmitted from Wi-Fi consumers.

E. Network security

Security is not just keeping people out of your network. Security also provides access into your network in the way you want to provide it, allowing people to work together. Strong network security opens up pathways to let people into your business, regardless of where they are located physically or what kind of connection they have. The tighter your security controls are, the greater the level of access that you can safely provided to trusted external parties, and likewise that they can provide to you. The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. With wired networking one must either gain access to a building (physically connecting into the internal network) or break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Thus gaining wireless connectivity provides an attack vector, particularly if the network lacks encryption or if the intruder can defeat any encryption.

F. Data security risks

The most common wireless encryption-standard, Wired Equivalent Privacy or WEP, has been shown to be easily breakable even when correctly configured.

Wi-Fi Protected Access (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi access points typically default to an encryption-free (*open*) mode. Novice users benefit from a zero-configuration device that works out-of-the-box, but this default does not enable any wireless security, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). On unencrypted Wi-Fi networks connecting devices can monitor and record data (including personal information), but such networks may use other means of protection, such as a virtual private network or secure Hypertext Transfer Protocol (HTTPS) and Transport Layer Security.

G. Securing methods

A common but unproductive measure to deter unauthorized users involves suppressing the access point's SSID broadcast, "hiding" it. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known MAC addresses to join the network. But intruders can defeat this method because they can often (though not always) set MAC addresses with minimal efforts. If eavesdroppers have the ability to change their MAC address, then they may join the network by spoofing an authorized address.

H. Testing programs technology

There are four generations of Wi-Fi technology currently available - 802.11n is the newest. All devices that undergo Wi-Fi CERTIFIED testing are tested according to their capabilities. An overview of these generations is below in table 2. Additionally, all Wi-Fi certified devices are tested to ensure that they support robust security capabilities. WPA2 (Wi-Fi Protected Access 2) certification indicates that a device can operate with both strong security and privacy.

I. Testing programs capabilities

Beyond core certifications, there are Wi-Fi certified designations for devices that have undergone testing for additional capabilities (Table 3).

Table 2. Testing Technology.

Wi-Fi Technology	**Frequency Band**	**Bandwidth or maximum data rate**
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz, 5 GHz, 2.4 or 5 GHz (selectable), or 2.4 and 5 GHz (concurrent)	450 Mbps

Table 3. Testing Capabilities.

Program	**Benefits**
Wi-Fi Protected Setup (WPS	Easy setup of network security using a Personal Identification Number (PIN), button, or by touching two devices together.
WMM(Wi-Fi Multimedia)	Support for multimedia content over Wi-Fi networks by prioritizing the traffic generated by multimedia applications.
WMM Power Save	Conserves battery life while using voice and multimedia applications by managing the time the device spends in sleep mode.

CONCLUSION

Authentication in wireless networks has improved considerably since the original open authentication mechanism used in early versions of 802.11. The release of 802.11i and, in the future 802.11w, and common security standards like 802.11 WEP, 802.11 WEP1, 802.11 WEP2 (802.11i), address many of the security and authentication issues. We can build on existing implementations to provide secure and reliable authentication in the wireless environment. Wireless authentication it is real and it can be implemented.

ACKNOWLEDGMENTS

I am immensely grateful to Prof. Dr. Vijay Singh Rathod and Prof. Dr. Abhijit Kulshrestha and Dr. Neeraj Bijalini for his valuable guidelines and suggestion without which it would not been possible to write up this paper.

REFERENCES

[1]. Wolter Lemstra A1 Vic Hayes and John Groenewegen. *The innovation journey of Wi-Fi: the road to global success*. Cambridge University Press. p. 121. ISBN 978-0521199711. Retrieved October 6, 2011.
[2]. Deb Smit; How Wi-Fi got its start on the campus of cmu, Pop city Media. Retrieved October 6, 2011.
[3]. "Wi-Fi gets personal: Groundbreaking Wi-Fi Direct launches today". Wi-Fi Alliance. 2010-10-25. Retrieved 2011-01-15.
[4]. www.muniwireless.com Retrieved 2008-03.
[5]. Roberta Bragg A1, Mark Rhodes-Ousley and Keith Strasberg. The complete reference Network Security. P.1-26.ISBN-9780070586710