SCIREA Journal of Computer Science and Technology

http://www.scirea.org/journal/Computer

December 21, 2016

Volume 1, Issue 2, December 2016

Analysis of Wireless Hotspots and their Challenges to Increase the Internet penetration in rural areas

[1]**Attada Venkataramana**

Associate Professor, Department of Computer Science & Engineering,

GMR Institute of Technology, Rajam, Andhra Pradesh, India-532127

venkataramana.a@gmrit.org

[2]**K.Jayasri**

Assistant Professor, Department of Computer Science & Engineering,

GMR Institute of Technology, Rajam, Andhra Pradesh, India-532127

jayasri.k@gmrit.org

ABSTRACT

Wireless Hotspots plays significant role in today's working environment. Business as usual no longer involves working in a traditional workplace at set hours. Today's workforce is more mobile and every day more people are working from virtual offices, client sites, home offices, coffee shops, airports, hotels, and any number of remote workplaces. In urban Areas, we can easily locate wireless Internet access with mobile device like notebook or handheld computer that supports the wireless LAN protocol known as Wi-Fi. Wi-Fi hotspots are becoming an increasingly common form of Internet access. Hotspots are considered a valuable productivity tool for business travellers and other frequent users of network services. Hotspots are convenient in providing internet access to the rural areas, but there are some usability and

security problems. This paper examines various issues of Wi-Fi hotspots and their challenges in today's wireless technology towards providing quality Internet service to rural communities.

Keywords: Wi-Fi, Hotspot, MANET, Internet

1. INTRODUCTION

Communication is one of the primary factors of science that has constantly been a focal point for exchanging information between communication parties at distant locations. Wireless and mobile communication networks are becoming more and more fashionable in today's mobile world. Wireless communication is an emerging technology since last two decades and it is showing rapid growth worldwide compared to its traditional wired counterpart. This growth is mainly due to trendy in mobile equipment like Apple iPhone, Research in Motion's Blackberry, and consequently Android-based phones such as smart phones, tablets, notebooks, laptops, etc., with an increase of connection speed. Wireless communication entails the transmission of information over a distance without help of wires or any other forms of electrical conductors.

In this mobile world with increasing mobility, there is a rising need for people to communicate with each other apart from the location of the individuals. A phone call placed from a traveller may close a big business deal, remote access to medical records may save a life, or a request for investigation updates by a warrior with a handheld device may affect the outcome of a battle.

All these instances of wireless communication pose an engineering challenge that can be met only with a well-organized, consistent, wireless communication network. The demand for wireless communication systems of increasing complexity and ubiquity has led to the need for a better understanding of fundamental issues in communication theory and their implications for the design of highly-capable wireless systems.

Wireless communications is a well-established and expanding technology that has been squeeze in most homes and work places, and is ubiquitous in our everyday lives. High speed Internet connections allow for real-time interaction through video and audio on a global level. Wireless communication takes this step further by moving the Internet out of the home and with you wherever you go.

Being incorporated into communication devices such as cell phones, laptops, and Global Positioning Systems (GPS), wireless communications has become an essential part of life. That is, consumers desire seamless, high quality connectivity at all times and from virtually all locations. There has also been significant interest lately for all businesses to set up mobile computing workplaces for their employees and also mobile computing for other functions of the business from distributors, suppliers, and service providers. Wireless is being adopted for many new applications such as to connect computers, to allow remote monitoring and data acquisition, to enable control and security, and to provide a solution for environments where wires may not be the best implementation.

The explosion of mobile and wireless technology initiates demanding requirements in terms of effectiveness and performance oriented issues in wireless communications. In the past few years, we have seen a rapid expansion in the field of mobile computing due to the propagation of inexpensive, widely available wireless devices. However, current devices, applications and protocols are solely focused on cellular or wireless local area networks, not taking into account the great potential offered by mobile ad hoc networking. Wireless communications networks are basically of two types. One is infrastructure based and other one is infrastructure less. Infrastructure based is cellular communications whereas infrastructure less is ad hoc networks. Mobile ad hoc networks are a type of ad hoc networks, consisting of collection independent of mobile nodes communicates one another without aid of any centralized administration. MANETS are self generated, self organized and self handled. Every node in the network will acts as both node as well as router. All the nodes are frequently moving around the network region. The following sections describe cellular and Mobile Ad hoc networks.

Globally, data usage continues to grow strongly in part to the driving force of Smartphone's and tablets into the mainstream market. The amount of mobile data generated globally is staggering and shows no sign of slowing down. This growth is largely driven by insatiable demand for innovative Smartphone's, tablets, and connected devices, as well as mobile applications and content. The growth of mobility—and the way it has changed our lives—is unprecedented. Close to 80 percent of the world's population now enjoys access to a mobile phone. In 97 countries around the world, there are now more mobile devices than people. Exciting new devices, including iPhones, Android-based Smartphone's, and tablets, are flooding the market and consuming large amounts of mobile network traffic.

Wi-Fi has existed from the last decade; most technologists and mobile industry executives viewed it as the “poor cousin” to licensed mobile communications, because it operated in unlicensed spectrum and suffered from security issues, interference, and poor quality of service. A hotspot is any location where Wi-Fi network access (usually Internet access) is made publicly available [3]. Wi-Fi allows laptops and smart phones to connect to the internet at high-speed without the use of wires. Thousands of public-access points called *"hot spots"* are springing up worldwide. Today, hotspots can be found in airports, public parks, college campuses, coffee shops, bookstores, airports, hotels—as well as in diverse locations such as truck stops, parks, and malls. With a wireless hotspots and an enabled device, we can easily connect to the internet at high-speed virtually anywhere. While some of these hotspots are free to use, others charge a fee. Hotspots are considered a valuable productivity tool for business travelers and other frequent users of network services. Technically speaking, hotspots consist of one or several wireless access points installed inside buildings and/or adjoining outdoor areas. These APs are typically networked to printers and/or a shared high-speed Internet connection. Because Wi-Fi lacked power and range, yet was the first available wireless Internet service, it had limited use and acceptance in rural areas. Most of the companies jumped at the chance to use this new wireless technology, and some even decided it was economical enough to use in rural areas. Wi-Fi was their first real opportunity to make quality Internet available to rural areas.

1.1 Requirements of Wi-Fi Hotspots

Computers (and other devices) connect to hotspots using a Wi-Fi network adapter. Newer laptop computers contain built-in adapters, but most other computers do not. Wi-Fi network adapters can be purchased and installed separately. Depending on the type of computer and personal preferences, USB, PC Card, Express Card, or even PCI card adapters can be used. Public Wi-Fi hotspots normally require a paid subscription.

The sign-up process involves providing credit card information online or by phone and choosing a service plan. Some service providers offer plans that work at thousands of hotspots throughout the country. A few pieces of technical information are also required to access Wi-Fi hotspots. The network name (SSID) distinguishes hotspot networks from each other. Encryption keys (a long series of letters and numbers) scramble the network traffic to and from a hotspot; most businesses require these as well. Service providers supply this *profile* information for their hotspots.

1.2 Finding Wi-Fi Hotspots

Computers can automatically scan for hotspots within range of their wireless signal. These scans identify the network name (SSID) of the hotspot allowing the computer to initiate a connection. Instead of using a computer to find hotspots, some people prefer to use a separate gadget called a *Wi-Fi finder*. These small devices scan for hotspot signals similarly to computers, and many provide some indication of signal strength to help pinpoint their exact location.

A wireless access point (AP or WAP) serves as the most basic hardware "glue" for connecting computers without wires [1] [2]. Comparable to hubs in a wired network, an access point allows wireless devices to join an existing Ethernet LAN. The products below follow the 802.11b standard that supports a maximum bandwidth of 11 Mbps. 802.11b is a cost-effective standard wireless technology for home networking.

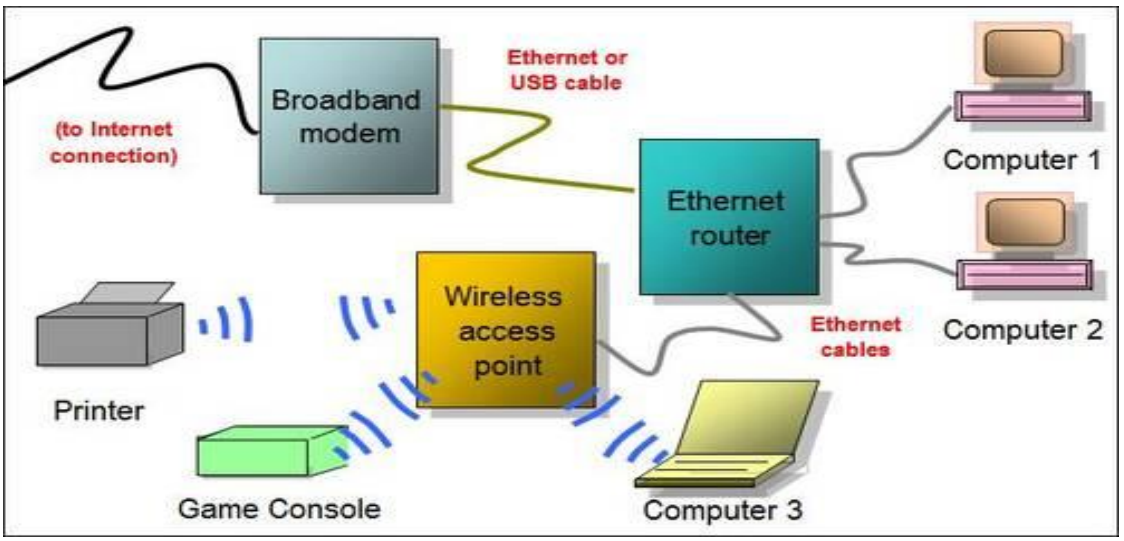

Fig 1. Scenario of Wi-Fi Access Point/Hotspot in Wireless Lan

1.3 Connect to Wi-Fi Hotspots

The process for connecting to a Wi-Fi hotspot works similarly on home, business and public wireless networks. With the profile (network name and encryption settings) applied on the wireless network adapter, you initiate the connection from your computer operating system (or software that was supplied with the network adapter). Paid or restricted hotspot services will require you to log in with a user name and password the first time you access the Internet.

Free Hotspots : Free hot spots are beneficial to Wi-Fi users, not only because they don't cost anything but also because users can go directly online without spending time buying vouchers or working out how much they want to spend. If you're hosting a hot spot, you can benefit from making it free to use. A free hot spot is a powerful marketing tool. If you tell customers they can use the Internet for free on your premises, you're likely to get more foot traffic. People will stay longer and buy more of your products in order to justify their stay or make it more enjoyable.

2. Growth in Wi-Fi Access Points

Wi-Fi access points have rapidly found their way into homes, businesses, and public spaces. In November 2010, International Data Corporation (IDC) predicted that there would be more than a quarter-billion Wi-Fi access points in homes throughout the world by 2017. Once shunned by corporate IT departments, Wi-Fi has increasingly made its way into most businesses.

In fact, one Research estimates that more than 95 percent of U.S. businesses have now adopted Wi-Fi. Once a luxury in select coffee shops or hotels, Wi-Fi hotspots can now be found in many public spaces, including trains, sports stadiums, and even parks [6] [7]. In-Stat estimates that there are currently 4 million public hotspots in the world, a number that will double in the next three to four years.

Most of the users spent their time in Mobile Internet and Mobile Video. The following is graph for Location of mobile data and time spent for Activity as per Cisco survey-2011.

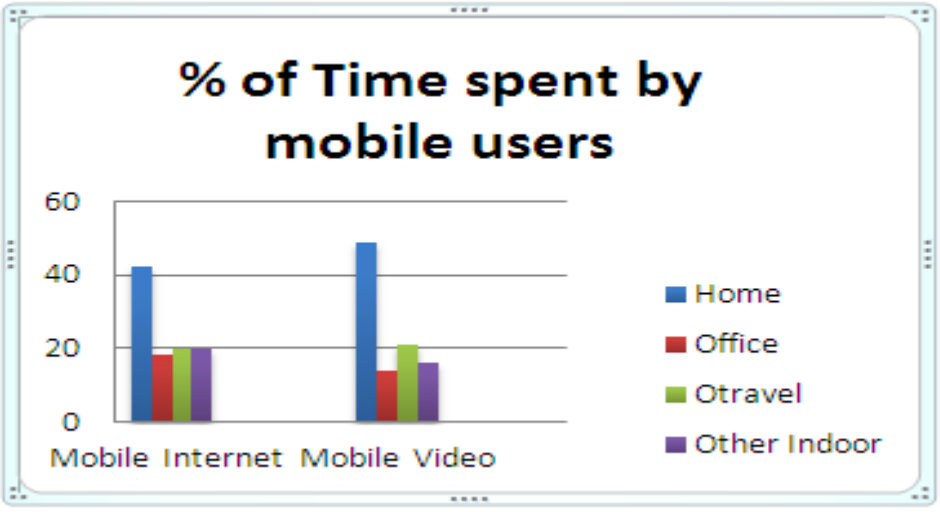

Fig 2. Location of mobile data usage and Percentage of time spent

2 .1 Hosting and Using Hotspots

If you host a Wi-Fi hotspot, you are giving your customers access to high-speed wireless Internet. This gives you an edge over competitors who don't offer a hot spot, as you're providing something extra. This could attract more customers to your business and increase revenue. You also have access to a private network that you and your employees can use for personal and professional purposes. If you own a cafe or a restaurant, people are likely to become regular patrons if they know they can access the Internet there. If you run a hotel, hosting a hot spot will encourage guests to stay longer as they don't have to rush back home to check their email. It's easy to advertise the fact that you host a hot spot, as you can just put a sign in your window or submit information to a hot spot directory.

We can use several portable devices to access the Internet in a hot spot, including laptops and Wi-Fi phones. Most of these devices are now Wi-Fi enabled. Using your own device in a hot spot is advantageous because you have easy access to all your online accounts and bookmarks. The broadband connection in most hot spots is much faster than that of most cell phones. A hot spot is a convenient place to check your email for important updates while you're on the go. Many coffeehouses, bars and restaurants offer hot spots, meaning you can get something to eat or drink while you go online. If you're staying at a hotel that has a hot spot, you can use the Internet as if you were at home without having to go to an Internet cafe.

M-Hotspots: Mobile Hotspot is an application which facilitates your Internet phone connection sharing either with your tablet or PC via a Wi-Fi connection (tethering). You can easily share your Internet mobile with only one click. Mobile Hotspot shows the number of devices connected to your hotspot. It is also possible to see in detail the list of all connected devices. We can define a timer to turn off your Hotspot automatically after a number of minutes.

Also we can automatically activate our Hotspot as you connect your phone on AC or USB power. In the same way, as you disconnect your phone from a power source you can automatically turn off the Hotspot application. Finally, in order to save your battery "Mobile Hotspot" turns itself off and instantly stops sharing when your battery is running at less than 20%. Most parameters can be changed via a configuration screen available via the menu: SSID, timer, battery level, notification. Mobile Hotspot is the most complete application on Google Play to manage tethering and share your Internet connection from your phone.

Hotspot's (vs.) Congestion

In recent years, wireless public networks have been widely deployed to provide high-speed Internet access to mobile users. Due to the dynamic and unexpected growth in internet users, in ad hoc networks some access points ("Hotpots") may be congested by many users. "Hotspots" represent transient but highly congested regions in wireless ad hoc networks that result in increased packet loss, end-to-end delay and out-of-order packets delivery. During hotspot conditions nodes typically consume more Resources. There are some methods and protocols like Hotspot Mitigation Protocol [3] to overcome the congestion from hotspots.

3. Advantages of Wireless Hotspots

Wi-Fi is a mature and widespread technology, today reaching over 700 million homes, schools, enterprises and hotspot locations worldwide. As mobile data usage continues to sky rocket and as Wi-Fi-enabled mobile devices become more abundant and diverse, mobile operators are beginning to see great potential for leveraging Wi-Fi hotspots services in order to reduce congestion on cellular networks and to capitalize on new revenue channels. The following are some of the key advantages of wireless hotspots [6]:

- Wi-Fi hotspots can provide a complementary method to delivering internet services to mobile subscribers at a relatively low cost per byte.

- In launching and managing Wi-Fi hotspots, mobile operators can gain control over their subscribers' Wi-Fi experience, in terms of security, accessibility and consistency across multiple hotspot locations.

- Mobile operators can offer Wi-Fi as a value added service (VAS) to boost customer loyalty and ARPU, as well as generate new revenue streams by extending monetized Wi-Fi hotspot services to a wide reach of customers.

- Mobile Data Offload: Mobile data offload can be a win-win situation for mobile operators and subscribers. By offloading data (Internet) traffic from a cellular network to a Wi-Fi hotspot network, mobile operators can optimize available cellular network resources, increase overall capacity and reduce bottlenecking of service. By alleviating congestion caused by heavy Smartphone data usage, mobile operators can better allocate their cellular network resources to other customers [11].

4. Safety Threats in Hotspots

Although few incidents of hotspot security issues are reported in the press, many people remain doubtful of their safety. Some caution is justified as a hacker with good technical skills can break into your computer through a hotspot and potentially access your personal data. Taking a few basic precautions will ensure reasonable safety when using Wi-Fi hotspots [4]. First, research the public hotspot service providers and choose only reputable ones who use strong security settings on their networks. Next, ensure you do not accidentally connect to non-preferred hotspots by checking your computer's settings. Finally, be aware of your surroundings and watch for suspicious individuals in the surroundings, who may be reading your screen or even plotting to steal your computer. The following are some of the security risks normally faced by hotspot users.

Lack of encryption: Many hotspots decline data encryption protocols such as WEP (wired equivalent privacy), 802.11i, or WPA (Wi-Fi Protected Access.) This makes it especially easy for others to eavesdrop on a session.

The evil twin: There are a variety of tools that can be used to eavesdrop on an unsecured network session. An evil twin is a wireless network signal that masquerades as a legitimate hotspot for the purpose of stealing information from the user, such as a network password or a credit card number. With a little software and some ingenuity, a thief can make a device with a wireless signal look just like an access point to the unsuspecting computer.

Session hi-jacking: In this, an attacker mimics the access point to which the user's mobile is associated and causes the user's mobile device to disassociate from the Wi-Fi network. The attacker then assumes the victim's session, resulting in theft of service.

Session side-jacking: In a side-jacking attack, the attacker snoops on unencrypted Wi-Fi communications and intercepts a victim's session cookie. The attacker can then access the victim's personal, private WebPages for example, Facebook pages.

Eavesdropping: Unencrypted Wi-Fi communications can be intercepted by an attacker. This subjects personal information such as passwords, credit card numbers, photographs, and email to exploitation.

5. Conclusion

Mobile has been highly successful in communications and changing the ways we work and

play. Wi-Fi is now a major element of next-generation wireless access networks. Wi-Fi hotspots are becoming an increasingly common form of Internet access. The business value of Wi-Fi will continue to expand by offering users consistent, portable connectivity. According to a latest research report by *Berg Insight* (Sweden-based market research Company) Telecom operators had deployed more than 7 million carrier-grade Wi-Fi access points worldwide at the end of 2012. By 2018, that number is going to more than double to about 15 million units.

As per the results given by Cisco survey, by 2016, annual global IP traffic is forecast to be 1.3 zettabytes. Therefore we say that Wi-Fi lunches a new era for this innovative industry. This paper discussed the key issues and challenges of wireless hotspots for the next Generation Wireless access networks.

References

[1] P. Bahl, A. Balachandran, and S. Venkatachary, June-2001, "Secure Wireless Internet Access in Public Places". In Proc. IEEE ICC'01, pages 3271–3275.

[2] A. Balachandran, P. Bahl, and G. M. Voelker, 2002, "Hotspot congestion relief in public-area wireless networks," in Proc. IEEE Workshop on Mobile Computing Systems and Applications, pp. 70–80.

[3] Seoung-Bum Lee and Andrew T. Campbell -2003. "HMP: Hotspot Mitigation Protocol for Mobile Ad hoc Networks".

[4] A white paper on "The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular"

[5] William Gerhardt, Richard Medcalf, Stuart Taylor and Andrew Toouli -2006, "Profiting from the Rise of Wi-Fi for Innovative Business Models for Service Providers".

[6] A white paper "A manager's guide to Wireless Hotspots" from Motorola.

[7] Stuart Taylor, 2011, "A New Chapter for Mobile? How Wi-Fi Will Change the Mobile Industry as We Know It.

[8] Jiancong Cheny Jingyi Hez S.-H. Gary Chany-2010, "A Framework to Relieve Wireless Hotspot Congestion by Means of Ad Hoc Connections"

[9] Analytics, Sue Rudd, Phil Kendall -2009, "Wi-Fi Offload - Roadmap to Seamless Mobile Interoperability – Strategy".

[10] Cisco Visual Networking Index: Forecast and Methodology, 2010–2015

[11] Hetting-2013, "Seamless Wi-Fi offloads from vision to reality".

[12] Sinha Naveen Kumar, University Shilong -2013 “Indian Wireless Data Business - Challenges and Future Prospects “International Journal of Management and Science.