ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Wireless Hotspots: Current Challenges and Future Directions For Next Generation Hotspot

Divya Aggarwal[*1], Pankaj Mehendiratta[2], Monika Vasisth[3]
[*1,2,3]Department of Electronics and Communication , Dronacharya College of Engg (MDU,Rohtak), Gurgaon-123506, India
divyaaggarwal1992@yahoo.in

Abstract

In this work, we study the effects of hotspots in wireless cellular networks. In recent years, wireless Internet service providers (WISPs) have established Wi-Fi hotspots in increasing numbers at public venues, providing local coverage to users and empowering them with the ability to access email ,Web , and other Internet applications on the move. Wi-Fi hotspots are one of the most promising scenarios for mobile computing .In this paper, we observe that while the mobile computing landscape has changed both in terms of number and type of hotspot venues, there are several technological and deployment challenges remaining before hotspots can become an ubiquitous infrastructure. These challenges include authentication, security and coverage .Thereby introducing a new concept of NGH ,that would enable mobile subscriber or user to connect automatically and securely to hotspots ,hence providing a complete solution for Wi-Fi so as to enhance the performance and meet the upcoming demands of the market .

Keywords: NGH - Next Generation Hotspot , SIM - Subscriber Identity Module , Wi-Fi - Wireless Fidelity ,VPN- Virtual Private Network.

Introduction

Wi-Fi networks are an essential component and will continue to expand by offering users consistent, portable connectivity providing seamless authentication, security and roaming. The past few years have seen unprecedented and unexpected growth in the number of wireless users, various applications and network access applications. Wireless local area networks (WLANs) have emerged as a networking platform to extend network connectivity to these public places, or hotspots, as they are commonly known. Recently, wireless Internet service providers (WISPs) have established Wi-Fi hotspots in increasing numbers at public venues, providing local coverage to traveling users and empowering them with the ability to access email Web, and other Internet applications on the move. [6,7,8].Internationally, the cost to the home operator of delivering a MB of data over a foreign 3G mobile network to a roaming subscriber can be far more expensive than Wi-Fi. Accordingly, Wi-Fi is even more attractive internationally than in-country, where the home usually has the option to deliver data traffic “on-net” or via an inexpensive, in-market roaming partner . Nevertheless, there are several technological and deployment challenges remaining before hotspots can become an ubiquitous infrastructure. Is there a common way for users to authenticate to each hotspot service provider?

The goal of this paper is to highlight the challenges posed by the vision of a global hotspot infrastructure, we argue that the performance benefits of wireless LANs make them ideally suited as a platform for networking in public places and discuss the research problems that remain to realize this vision . It is clear that the wireless LAN connection is of tremendous value.
Nevertheless, Can a user completely trust the hotspot provider network? We observe that, although there is a desire for high speed wireless connectivity in public areas, several technical problems need to be addressed before such connectivity can be provided ubiquitously through Wi-Fi hotspots. These problems include authentication, security, coverage, management, location services, billing, and interoperability. Thus, NGH will act as a solution that would enable mobile subscriber or user to connect automatically and securely to hotspots.

Authenticating to the Hotspot Provider

Hotspot providers in public areas typically provide access to unknown users, who might not have visited the network before. In this aspect, hotspots are significantly different from private networks in homes, university campuses, and enterprises. This necessitates

ISSN: 2277-9655
Impact Factor: 1.852

the use of a formal authentication mechanism that enables users to identify themselves to the network. In many commercially deployed Wi-Fi networks today, authentication is coupled with wireless-hop security where only authorized users receive network access. Authentication helps the network to establish the users' identity, while wireless-hop security ensures data privacy for authenticated users and protection for the network .Today since each hotspot is likely administered by a different provider, users will have to repeatedly authenticate themselves at each hotspot location. The goal of providing fast and seamless service, involves a tradeoff between ease of use and robustness. This tradeoff raises several research questions:

Ease of Access: What form of authentication is ideal in a public environment that would give a traveling user the easiest and fastest way to get access to the network?

Mechanism: Is it adequate for the network to authenticate the users through software mechanisms such as one-time passwords [39] . Howcan users verify the identity of the hotspot provider?

Wireless-hop security: Security mechanisms provide data privacy to network users and also protect the network against malicious use. Users who do not trust the hotspot infrastructure can use higher-layer security mechanisms such as SSH,SSL, or VPNs to connect to a private network. However, the provisioning of wireless-hop security is still important for a number of reasons. First, the average user is not very familiar with these higher-layer security mechanisms. Finally , wireless-hop security gives the hotspot provider a way to protect its network against unknown, potentially malicious users, as well as a means to manage the use of network resources. Current approaches achieve network security through per-user authentication.

Radio Frequency range: Inherent limitations of range and multipath interference from indoor RF propagation restricts user mobility to limited areas within a hotspot. If RF coverage is not adequate, roaming users can easily lose connectivity. Therefore, to provide uninterrupted connectivity to roaming mobile users, hotspot operators need to find ways to increase the density of hotspot coverage to span larger geographic regions.

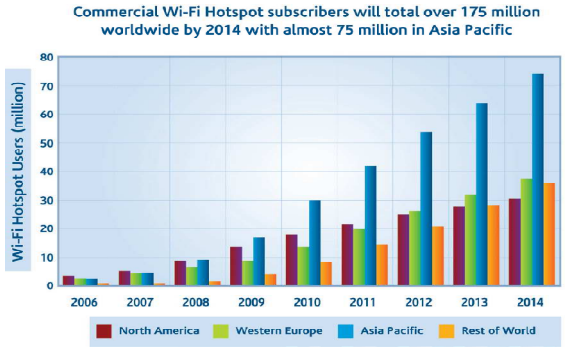

FIG : **Subscriptions to Commercial Wi-Fi *Hotspots Growing [Strategy Analytics]***

In 2011, the number of WiFi hotspots reached 1.3 million worldwide. By 2015, WiFi users will be able to connect to 5.8 million hotspots,according to a report commissioned by the Wireless Broadband Alliance.

Use of VPN's while Connecting to Wireless Hotspot's

The best way to protect all your information from hotspot hackers, every time you connect, is to use a Virtual Private Network. VPNs encrypt all the data travelling to and from your laptop and other mobile devices by sending it through a secure tunnel that's invisible to hackers. That's why the Federal Trade Commission recommends using a VPN when you connect to public WiFi networks in their article Tips for Using Public Wi-Fi Networks. Unfortunately, survey after survey shows that most WiFi users aren't protecting their information at public hotspots. A 2012 survey conducted by the Identity Theft Resource Center with Private Wi-Fi found only 27% respondants said they used a VPN to protect their data. And 44% said they weren't even aware that there was a way to protect their sensitive information when using a public hotspot. Wi -Fi hotspots are public wireless networks. Whether they're free or paid hotspots , that means there's no privacy .The 2013 Javelin Identity Fraud Report found that tablet users were 80% more likely than other consumers to be victims of ID fraud. Every three seconds, someone in the U.S. becomes a victim of identity fraud.

ISSN: 2277-9655
Impact Factor: 1.852

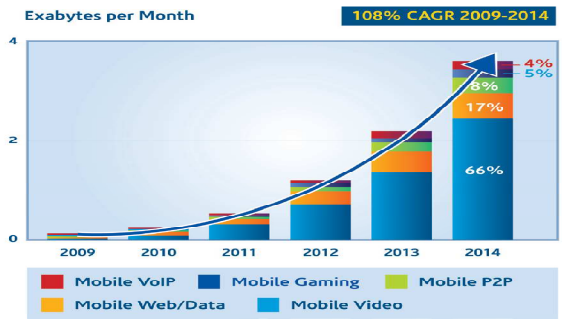

FIG: Data traffic continues to grow exponentially [Cisco VNI]

Security Challenges to Wireless Hotspots

The current hotspots do not protect customers from fraud that can steal valuable data and undermine customers' confidence in their use. This leaves user's open to the following attacks:

Evil twin attack: An evil twin is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider.Once an Evil Twin gains access to your computer, it can launch a **Man-in-the-Middle Attack** which allows it to eavesdrop on Internet traffic and capture passwords and other important information and can even control which websites appear.

Ad hoc or peer-to-peer network : Another sign you could be in for trouble: Two little computer symbols that appear when you're trying to connect to a wireless network. That means you're connecting to someone else's laptop – an *ad hoc or peer-to-peer network*, not a Wi-Fi hotspot. Once you connect to a viral network like that, your shared files can be accessed by every other laptop connected to the network.This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Session Hijacking: Side jacking typically happens when users type in their user names and passwords when connecting to a website not properly protected by *https*

Eavesdropping. Unencrypted Wi-Fi communications can be intercepted by an attacker. This subjects personal information such as passwords , email details and so on to exploitation

Next Generation Hotspot (NGH)

- A new program called Next Generation Hotspot (NGH) using the latest Hot Spot 2.0 specification1 - allows a mobile subscriber to connect automatically and securely to Hotspots using his service provider credentials while maintaining roaming visibility for the operator. NGH enables operators to continuously monitor and manage "cellular-like" service over Wi-Fi domestically and internationally so as to enhance performance and meet the demand for mobile data services over Wi-Fi. In many parts of the world both consumer and business subscribers are demanding mobile access from a smart phone or tablet with a data plan.[1,2]
- In today's scenario, when an end-user who enters a hotspot with a non-SIM device and does not have a relationship with service provider, there is no mechanism to validate that the network that he is accessing is a legitimate network and he could be providing his credit card credentials to a rogue hotspot.The second phase of Next Generation Hotspot will therefore deal with non-SIM devices allowing a customer to buy a tablet, bring it to an NGH Hotspot (whether public or residential), and relatively easily and securely sign up for NGH roaming service.
- **Operator-Friendly Hotspots :** NGH is the program in theWireless Broadband Alliance that uses Hotspot 2.0 and other technologies to enable operators to make their Wi-Fi networks interoperable and create a global Wi-Fi roaming system complementing GSM. Operators are just starting to use Wi-Fi as an additional radio network, to add coverage and capacity to their own 3G networks. Next Generation Hotspots (NGH) using the "Hot Spot 2.0" specification will accelerate the utility of Wi-Fi for mobile operators by allowing more subscribers automatic access, and minimizing network changes for the operator to connect to a different technology. Hotspot 2.0 is the technical specification being developed in the Wi-Fi Alliance for seamless and secure access.
- **Automated Network Selection**
  Unlike 3G, Wi-Fi users are burdened with the need to manually select which hotspot to use, from a list of potential hotspots in the end-user's device. These roaming lists can get complicated. Some operators claim to have more than 1,000 SSIDs32 in their devices and expect the list to grow to 200,000 SSIDs. This is an unwelcome, awkward, and manual process that does not scale to meet the capacity needs of the industry. Hot-Spot 2.0 33 enables the device to automatically discover and select the Wi-Fi network preferred by the home mobile service provider.
- **Use of Mobile Credentials**
  To ensure the mobile subscriber is not inconvenienced by having to acquire and maintain a separate subscription for Wi-Fi , HotSpot 2.0 reuses the subscriber's existing credentials stored in her SIM card. Further, with HotSpot 2.0,34 that SIM card can

ISSN: 2277-9655
Impact Factor: 1.852

be removed and used in a different device. This ensures the subscriber gets Internet access anywhere in the world simply by turning on their device, just like 3G service. The reuse of existing credentials in the handset is a major step that simplifies both the subscriber use and gain operator support of Wi-Fi Roaming.

- **A Complete Solution for Wi-Fi ROAMING :- Roaming is a Broader Solution than Network Construction**

As mobile operators have learned over the last 25 years of operating mobile networks, roaming is an excellent solution to obtaining coverage, since it is not feasible to construct your own network everywhere that your subscribers may wish to obtain service. Although it may be feasible in some areas for the operator to build their own network (with traditional RAN or Wi-Fi), this option is not available in all locations. Roaming, in contrast, multiplies the home operator's coverage outside of their home market, without requiring capital investment in the build-out.Operators will want to (a) employ Wi-Fi to reduce their costs and (b) use roaming to increase their coverage. In combination, Wi-Fi will become a roaming network to complement the operator's own 3G or 4G network. Operators can use Wi-Fi networks as roaming partner.In fact, in the NGH, operators can use the same technology and processes to roam using Wi-Fi, without requiring the operator to change the way it operates. Just like the GSM standardized roaming across cellular operators, we envision NGH to provide a Wi-Fi Roaming system that is similarly integrated and available across GSM operators.

- **For Operators: Simple and Secure Use of Wi-Fi**

To accomplish the goal of minimizing the impact on the operator,Wi-Fi Roaming fits to the existing network interfaces and business procedures used for 3G Roaming. This solution can be provided today, enabled by NGH. Currently, mobile operators efficiently achieve 3G Roaming across hundreds of other mobile networks ("roaming partners" that serve their subscribers in another market or coverage area where the Home Operator does not have their own network to provide service). By connecting once to a "Hub" the operator is instantly connected to all of their roaming partners via this shared network, which allows the home operator to avoid the cost and complexity of individually establishing and maintaining direct connections to a hundred or more roaming partners. Wi-Fi Roaming reuses this business process, allowing mobile operators to reach a global footprint of Wi-Fi Roaming partners they can select and use to complement their coverage and capacity, at terms both parties agree upon.

Conclusion

In this paper, we have highlighted several technical and deployment-related challenges that need to be addressed before such connectivity can be provided ubiquitously through Wi-Fi hotspots. In particular, for the end user to benefit, the system has to provide a mechanism that is easy to use, economically attractive, and provides fast access in a transparent, device independent, and access-technology independent manner. Also, introduced a new concept of NGH ,that would enable mobile subscriber or user to connect automatically and securely to hotspots using his service provider credentials while maintaining roaming visibility for the operator and thereby providing a complete solution for Wi-Fi roaming so as to enhance the performance and meet the upcoming demands of the market.

References

[1] *Eric Geier* . Wi-Fi Hotspot Security: The Issues.(July 28, 2006)
[2] Sue Rudd (Strategy Analytics), Esteban Torres (Cisco) , Robert Duncan (Transaction Network Services). **Next Generation Hotspot: Maintaining the Profitability of Mobile Data Services**.(June 2011)
[3] ANAND BALACHANDRAN ,GEOFFREY M. VOELKER, PARAMVIR BAHL .Wireless Hotspots: Current Challenges and Future Directions**.** Mobile Networks and Applications 10, 265–274, 2005.(2005)
[4] G. Anastasi, M. Conti, E. Gregori, A. Passarella.A performance study of power-saving polices for Wi-Fi hotspots.(Mar 10th2013**)**
[5] Private Wifi - Kent Lawson,Why Public WiFi Hotspots Are Trouble Spots for Users
[6] Cometa Networks. www.cometanetworks.com.
[7] T-Mobile. www.tmobile.com.
[8] Wayport . www.wayport.net.