# A Peer-to-Peer Model for Ubiquitous Broadband Connectivity Sharing

Santashil PalChaudhuri
Computer Science
Rice University
Email: santa@cs.rice.edu

Somshubhro Pal Choudhury
The Wharton School
University of Pennsylvania
email: somshubh@wharton.upenn.edu

***Abstract*— Over the last few years, there has been an unprecedented growth in residential broadband access, and number of public hotspots. But, the average broadband bandwidth utilization at each home remains low for majority of the subscribers compared to the bandwidth provided to each. The price of the broadband connection is high, but residents feel the need for it for the infrequent surges in bandwidth demand by some common applications. The public hotspot business model has also not taken off primarily due to additional cost of access for the user outside home, and having to take service from separate hotspot entities.**

**Peer-to-peer systems have created a storm in recent years, by facilitating robust decentralized systems for file sharing. We envision a peer-to-peer broadband bandwidth sharing system, to address the limitations pointed out in the previous paragraph. In our model, peers with already established broadband connection will share their connection with their neighboring peers either for recovering their cost or for profit. The neighboring peers without broadband access will have on-demand shared broadband access for a low usage-based fee. The system will enable a ubiquitous wireless broadband connectivity for the peers, by providing access on demand at competitive rates. We back up our technology with details of the business model that will make this competitive bandwidth sharing possible.**

***Index terms*—p2p, hotspot, broadband**

## A. INTRODUCTION

Over the last few years, there has been an unprecedented growth in residential and hotspot broadband Internet access all over the world. Even though, thousands of hotspots are mushrooming everywhere, there is still ongoing debate on a viable business model to provide hotspot access to paying users. Boingo and other aggregators have approached the problem by consolidating all hotspot access points under a monthly payment scheme. Few others have approached the business model by directly partnering with the venue providers - T-Mobile is partnering with Starbucks, Wayport with McDonald and Cometa Networks closed down after loosing the contract with McDonald.

Shifting to wired broadband, we find that a typical Cable/DSL user pays a high monthly flat fee for access at home. But, the average bandwidth utilization at each home remains low for majority of the subscribers compared to the bandwidth provided to each. Moreover, the broadband users at home face the same issue of broadband access outside their home territory and have to rely again on a paid hotspot scheme on top of the broadband access fee at home.

Peer to peer (p2p) systems have opened up new avenues for setting up of decentralized robust systems for file sharing. We propose to facilitate sharing of residential and public hotspot broadband connections in the same vein as p2p systems provide for file sharing. The *Provider peer group* with already established broadband connection will either recover a percentage of the cost or make a profit by sharing or reselling unused bandwidth amongst their neighbors. And the peers without broadband access, which we will call the *Consumer Peer group*, will have shared high-speed access for a low usage based single monthly fee at home and elsewhere. The innovative sharing scheme is a competitive multi- provider and multi-consumer p2p environment, which would ensure a healthy balance of demand and supply. Our proposal is analogous to Customer-to-Customer (C2C) model in the business domain that eBay has so successfully implemented.

We strongly believe that the current payment schemes and differences between wireless and wired broadband access have to be resolved as the consumer's ultimate desire is to have ubiquitous broadband access while paying a single fee on a usage basis in a competitive provider environment. In the paper, we elaborate on the technology along with details on the business model that will make the competitive bandwidth sharing possible supported by a comprehensive payment and logistics infrastructure.

## B. BACKGROUND SCENARIO

In this section, we will highlight some of the key data, statistics and thoughts that motivated us towards the Peer-to-Peer Bandwidth sharing concept. The background we provide pertains to the current environment in USA, though we believe that many of our theories and assumptions on the business side will be valid all over the world.

**B.1 A look at the Hotspot industry**

The number of hotspot access points has grown tremendously in US to over 10,000 by the end of Year 2003 [1]. The reduced cost of wireless routers, emergence of low cost Wi-Fi ready handheld devices and pre-wired laptops with Wi-Fi access are the main reasons behind Wi-Fi popularity. An analysis of the Hotspot industry shows four key segments in the entire value chain – Brand name providers, Aggregators, Hotspot Operators and venues (Figure 1).

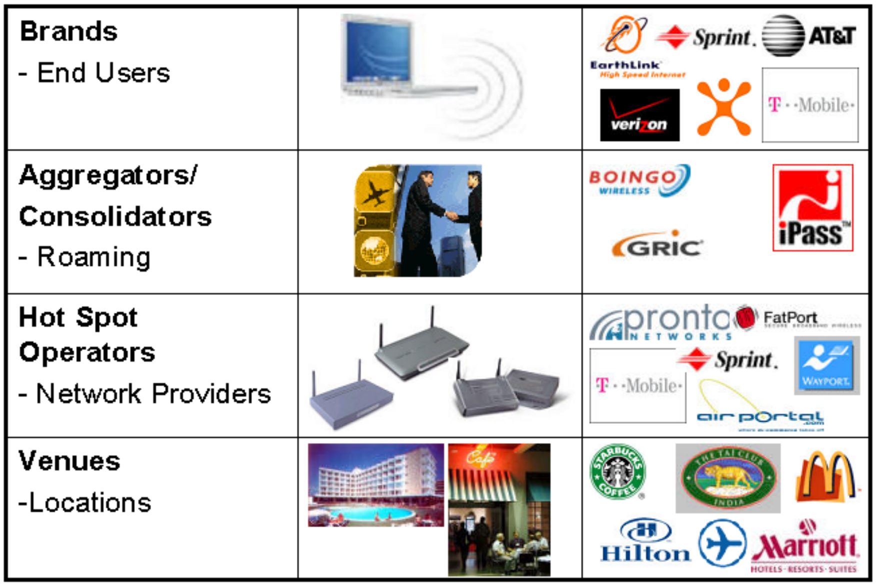



**Figure 1: Hotspot Industry Segmentation**

Venue owners are most interested in providing hotspots as an amenity and convenience to their customers more than generating direct revenue. The HotSpot Providers (HSOs) are proliferating fast as the barrier to entry is low with relatively small setup cost, which leads to massive fragmentation at the HSO layer. Ultimately, we believe that there will be literally thousands of HSOs, with probably dozens of large ones. Multiple brand name providers in the HSO layer are already in operation - T-Mobile operates their own hotspots in many venue chains.

The economics of the Hotspot industry clearly demonstrates that there will always be a lot many HSOs than the actual service providers who ultimately connect with the end customer. This is where aggregators like Boingo come in striking wholesale agreements with HSOs for a monthly fee paid by the customer. The customer would then have access to all the HSOs covered by Boingo, essentially giving him a seamless network. There are serious limitations to this approach as its success will depend on the consolidation of hotspots by the aggregator and as well as the customer's willingness to pay a flat additional monthly fee compared to a usage based fee.

Companies like Linspot [1] helps hotspot providers set up operations in their community for a monthly access fees by their neighbors. Though innovative and probably closest to our proposed model, Linspot fails to achieve the ubiquitous broadband connectivity, competitive and dynamic access pricing and a single payment scheme for access to home and elsewhere. We achieve all of the above, thereby providing a competitive advantage over current hotspot providers and enablers.

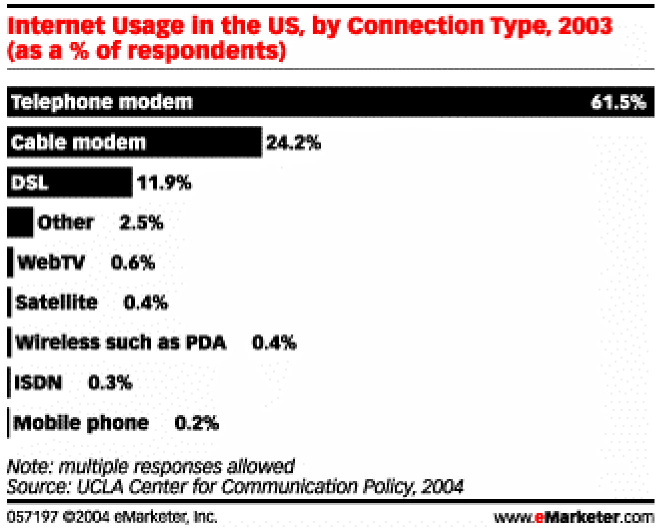
**B.2 Broadband access at home**

A similar overview of Broadband access at home shows that currently 33.5 million [3] US users have broadband access, a 36.5% penetration among Internet users with average monthly fees in excess of $35.

Table 1 shows the end of Year 2003 statistics on technologies used for Home access.

We believe that the early adopters of broadband technology are many of the professionals who needed high-speed access for work reasons and are more acceptable to the high monthly broadband access fees. The recent and would-be movers to residential broadband are in the more price sensitive category and the price differential between broadband and dialup affects them the most. We may as well see a sharp saturation in the next few years for users switching over from dial-up to broadband.

**Table 1**: **Technologies used for Home access [4]**



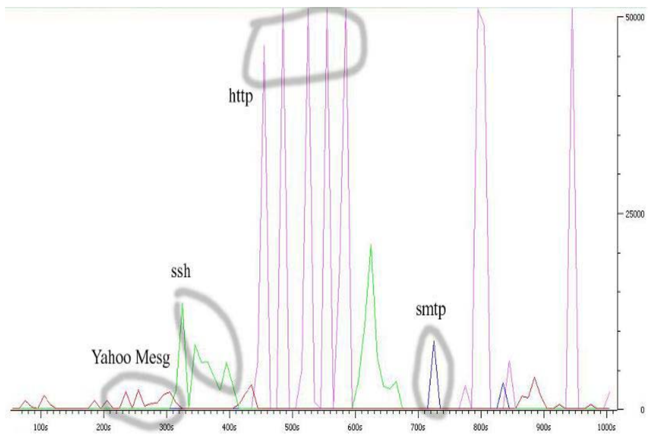

A recent interesting study by Forrester [5] shows that **Cost matters most** for both for switchers and leavers of broadband access**.** The high price of broadband is the top reason that 57% consumers want to switch from one broadband provider to another and the top reason for consumers wanting to give up broadband altogether. We believe that even though broadband is a necessity for most of the users at home, the high cost of access is the most limiting factor to the proliferation of residential broadband. An additional flat fee for Wi-Fi access outside home adds to the pain.

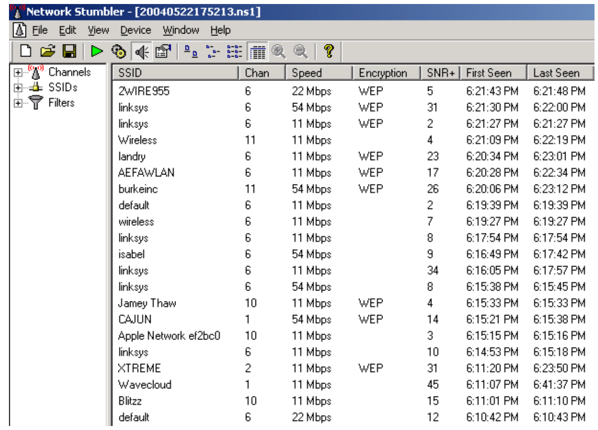
DSL and Cable providers typically allow between 30-50 Gigabytes of downstream data transfer per month. Though no specific statistics on bandwidth usage for each residential household is available, the estimated current average usage is 2 GB per month assuming that a large percentage of the broadband users are standard and premium users (Table 2).

**Table 2**: **Analysis by Forrester for typical bandwidth utilization by the target consumers**

| | Starter | Standard | Premium |
|---|---|---|---|
| Bandwidth | 128-256 K | 500-1.5 MB | 2 GB or more |
| Target Audience | Low income novices | Moderate/high income older consumers | Moderate/high income younger customers |
| % Of target audience with broadband today | 21% | 52% | 55% |
| Motivation for getting broadband | Free dialup service expired | Faster surfing and communication, drop/free-up phone line | Download music & video; online gaming; working from home |
| Broadband activities | Classifieds, emails, personal ads | Sending & managing photos, checking stock quotes, medical info, email | Publishing WebPages, video, download video |

To analyze the typical bandwidth requirement of a residential user, we did the following experiment. We used Ethereal Network Protocol Analyzer [6] to see the bandwidth being consumed by some standard applications run by an average home user. We ran these standard applications – browsing, mailing, chatting – from a home environment with standard usage patterns, to capture their bandwidth requirement. This reflects a majority of the home user's access pattern, but few may have unique requirements, which is not captured by the figure below.




| SSID | Chan | Speed | Encryption | SNR+ | First Seen | Last Seen |
|---|---|---|---|---|---|---|
| 2WIRE955 | 6 | 22 Mbps | WEP | 5 | 6:21:43 PM | 6:21:48 PM |
| linksys | 6 | 54 Mbps | WEP | 31 | 6:21:30 PM | 6:22:00 PM |
| linksys | 6 | 11 Mbps | WEP | 2 | 6:21:27 PM | 6:21:27 PM |
| Wireless | 11 | 11 Mbps | | 4 | 6:21:09 PM | 6:22:19 PM |
| landry | 6 | 11 Mbps | WEP | 23 | 6:20:34 PM | 6:23:01 PM |
| AEFAWLAN | 6 | 11 Mbps | WEP | 17 | 6:20:28 PM | 6:22:34 PM |
| burkeinc | 11 | 54 Mbps | WEP | 26 | 6:20:06 PM | 6:23:12 PM |
| default | 6 | 11 Mbps | | 2 | 6:19:39 PM | 6:19:39 PM |
| wireless | 6 | 11 Mbps | | 7 | 6:19:27 PM | 6:19:27 PM |
| linksys | 6 | 11 Mbps | | 8 | 6:17:54 PM | 6:17:54 PM |
| isabel | 6 | 54 Mbps | | 9 | 6:16:49 PM | 6:17:42 PM |
| linksys | 6 | 11 Mbps | | 34 | 6:16:05 PM | 6:17:57 PM |
| linksys | 6 | 54 Mbps | | 8 | 6:15:38 PM | 6:15:45 PM |
| Jamey Thaw | 10 | 11 Mbps | WEP | 4 | 6:15:33 PM | 6:15:33 PM |
| CAJUN | 1 | 54 Mbps | WEP | 14 | 6:15:21 PM | 6:15:38 PM |
| Apple Network ef2bc0 | 10 | 11 Mbps | | 3 | 6:15:15 PM | 6:15:16 PM |
| linksys | 6 | 11 Mbps | | 10 | 6:14:53 PM | 6:15:18 PM |
| XTREME | 2 | 11 Mbps | WEP | 31 | 6:11:20 PM | 6:23:50 PM |
| Wavecloud | 1 | 11 Mbps | | 45 | 6:11:07 PM | 6:41:37 PM |
| Blitzz | 10 | 11 Mbps | | 15 | 6:11:01 PM | 6:11:10 PM |
| default | 6 | 22 Mbps | | 12 | 6:10:42 PM | 6:10:43 PM |

**Figure 2: Bandwidth usage of typical home user** **Figure 3: Ubiquity of residential access points**

The typical used applications are browsing (http), mail (smtp), interactive shell (ssh) and chatting (yahoo messenger), and their bandwidth consumed is shown in Figure 2. For about 1000 seconds, the bandwidth usage is plotted as bits/second in Figure 2. Browsing consumes about 50 Kbps, with the other applications being less than 20 Kbps. This shows the extremely low utilization of a typical residential user of his broadband connection. We did not plot MPEG, MP3 and large file downloads, which will typically take up as much bandwidth that is available. But the premise is that those big downloads are comparatively infrequent and rarely done by bandwidth sharing multiple users all at the same time.

The motivation of our proposal is based on a 30 minutes walk around an apartment complex and neighborhood in Houston, Texas, which showed the availability of 40 access points in the community. Figure 3 shows a 10 minute snapshot showing more than 20 access points. This high density of access points inspired us to design our proposed solution, particularly in the residential complexes. We felt the lack of a suitable architecture, which will enable a peer-to-peer sharing of the residential broadband connectivity.

### C. THE PROPOSED MODEL

A number of technological challenges need to be solved before this idea of p2p bandwidth sharing becomes a reality. The concept of bandwidth sharing is essentially a much simpler (routing-wise) form of ad hoc networking. In theory, the consumer peers might be multi-hop through other consumer peers, to reach the nearest wireless access points providing service. But, the economics of multi-hop routing in ad hoc networks is still an issue of research. Also, the density of wireless routers in residential complexes portends to single-hop connectivity to access points, available at majority of locations.


**Figure 4: Connectivity Model**

Figure 4 shows the high-level connectivity model we envision. A provider peer with a broadband connection has a wireless router connected to the broadband. The provider computer executes the server side of our connectivity software and controls the wireless router configuration. The consumer peers, which are within the range of any wireless router, use the client side of the connectivity software to choose and connect through a wireless router.

A number of key technological challenges for deploying public hotspots have been identified recently [10]. Our approach for sharing residential bandwidth shares some of these challenges. We have an additional challenge of choosing an access point, especially as multiple such access points can potentially be used. The key technological challenges that needs to be solved for providing this bandwidth sharing are the following:

- Auto-negotiation of contract matching according to preferences
- Secure authentication and access in a transparent manner to the user
- Adaptation of authentication for roaming users

Each of the above issues will be addressed in our framework, to provide a practical deployable business model.

### C.1 Basic mechanism

The provider infrastructure consists of a wireless router, a computer running the provider software and a broadband connection. The consumer infrastructure consists of a wireless enabled laptop, desktop or PDA, running the consumer software. The consumer software can be downloaded on-demand through the wireless router from the provider peer, if not already present. This is done using standard http-redirection mechanism though the web-browser in the consumer computer. The web browser will be redirected to a nearby provider computer location from where it can download the consumer software.

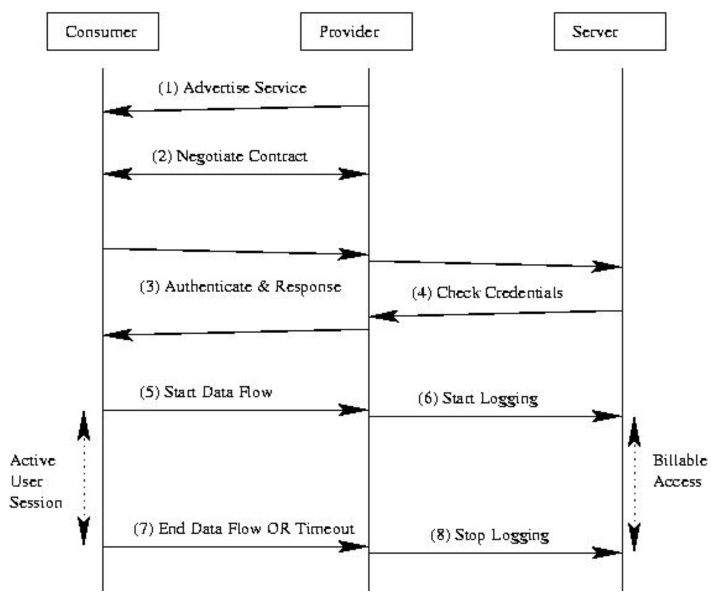



**Figure 5**: **Basic Mechanism**

Figure 5 explains the bandwidth sharing mechanism in detail. All the wireless routers willing to act as providers of broadband access, advertise their intent by periodic broadcasts of the SSID of the access point. However, the DHCP server is not run in the router, thus preventing it from assigning arbitrary IP addresses to any DHCP request. In our model, the provider computer does the assignment of the IP address after contract negotiation and authentication has taken place. The provider configures its router to do MAC layer filtering allowing only specified MAC addresses to go through, by dynamically adding the consumer MAC address to the wireless router. This periodic broadcast stops when the capacity of the wireless router is close to saturation. We enable admission control schemes using dynamic bandwidth usage analysis. The advertisement contains details of the connection speed, bandwidth availability and access pricing for the consumer peer group. The consumer might receive multiple such advertisements. The software running on the consumer computer chooses one of the connections based on signal SNR, advertised rate and user preference. The consumer-defined policy determines the choice of the provider, and the degree of process automation is flexible – from complete transparency to prompting the user. We assume the existence of a certificate authority trusted by all the peers. This Public Key Infrastructure can be coupled with the server that maintains all the logging information, or can be a implemented as separate entity. We also assume that all the peers can verify any given certificate. Authentication takes place through the server for verification, and after that a private key/cookie is exchanged between the consumer and provider for all further communication. Following this, data flow can be initiated. The wireless hop is secured by a mechanism detailed later, which enables data privacy. Logging of the exact access times is done through a central server for billing purposes. This logging through a central server also prevents a malicious provider to dishonestly log the access time of clients using it's service.

Wireless routers can be configured to use WEP encryption. But, WEP is not a strong encryption and is vulnerable to attack [13][14]. They work by collecting traffic statistics, from which the encryption key can be extracted. Instead of this, we provide access security by other means that are much more secure. This mechanism will be detailed in the following sections. In addition to this security, consumers can use higher layer SSL/TLS end-to-end security after authentication is done, based on the level of encryption the consumer desires.

### C.2 Auto-negotiation of Contract

As potentially more than one provider peer can be reachable simultaneously by the consumer peer, the consumer can choose the connection. This process is completely automated by the client software based on preferences, and provides the user with the "best" possible access at any time. The provider will broadcast a periodic advertisement with the bandwidth being provided along with the access rate for the consumer. It also learns of the other providers in the neighborhood and their bandwidth-rates. A provider uses this information to adaptively provide a rate competitive to the other providers in the neighborhood.

An average user's bandwidth requirement has been analyzed recently [11] in a comprehensive survey. It demonstrates that browsing, chatting and e-mailing are the most common applications run by an average user and has low bandwidth requirement. We verified the low bandwidth usage by an average residential user by logging the usage as shown in Figure 2. Hence, a statistical multiplexing of many such consumers can be done on a single broadband link, without saturating the network. Based on an initial survey of operations on Internet in terms of email, chat, browsing, MP3, video streaming by each user and based on daily usage henceforth, the software would give a good statistical estimate on the projected bandwidth usage for the peer groups on a dynamic basis. The daily usage statistics on a per user basis is stored on the peer computers. We plan to query the data on a regular basis to update the usage statistics on a zonal basis to portray the best possible bandwidth utilization for our p2p bandwidth sharing model. This statistical model enables the provider to determine the admission control through its wireless router.

Our model also allows for maintaining a "free access" list. This list allows the consumers listed to have free access, after authentication of the user. The "free access" list enables the provider peer to give hotspot service for free to selected consumers, and to the different wireless devices the owner of the broadband uses to access the Internet.

The software at the consumer end selects all advertising providers above a minimum SNR threshold as potential connection points. Based on the offered data rates and bandwidth requirement, the consumer software then chooses a specific provider to connect to and starts the authentication mechanism described next. This auto-negotiation of connection is unique amongst the solutions for hotspots proposed and commercialized. All previous approaches relied on an URL redirection to the login or registration page of the provider when a network access is requested. Our novel approach allows for overlapping hotspots to be active at the same time, which is the essence of a competitive p2p bandwidth sharing model.

### C.3 Secure Adaptive Authentication

Our secure adaptive authentication method is based on the single sign-on (SSO) technology [9]. It reduces the burden of multiple authentications while maintaining separate credentials, without sacrificing on the security aspect. It requires a valid credential, which every peer has in the form of a valid certificate. The provider peer checks the credentials of the consumer peer through the central authentication server. If the authentication is successful, then a cookie is returned to the consumer. When the roaming consumer needs to verify itself with another provider, it can use this cookie which remains valid for a limited duration. The consumer can also verify that the certificate of the provider is valid. Either the RADIUS [7] or the Liberty Architecture [8] can be used as the authentication models.

This authentication mechanism can be adapted based on the trust relationship between the provider and consumer. This adaptation is based on a policy engine that determines the trust relationship and applies the specific policy. If the provider and consumer belong to a trusted domain, then the authentication will be in the form of a validation, pre-shared between them. For authentication in public spaces, any of the previously mentioned authentication architectures that are supported by both parties is be used. The policy engine prompts the user for his approval before authentication is done in a non-trusted domain, if so desired by the user.

Once the consumer is authenticated, the provider adds the MAC address of the consumer in valid access list maintained in the wireless router. Standard wireless routers come with a configurable MAC address filtering list. The provider dynamically updates this list by adding the authenticated user, and removing the this entry when the consumer has disconnected.

### C.4 Wireless Access Security

After authentication and during wireless access, security is important for providing data privacy as well as protecting the network from malicious access. Theft of IP or MAC addresses or message alteration can be done, which entails some cryptographic security mechanism in the wireless hop. Higher-level data security like SSL/TLS or VLN can be used, but the initial keys have to be exchanged insecurely, initially. Also, the average residential user will typically not use this higher-level security.

IEEE 802.1X security mechanism can be used, but it requires a shared secret between the provider and the consumer. This is not feasible in a public wireless LAN. A secure mechanism has been developed in [9] as a compound of layer 2 and web authentication approach. This method is used to provide secure access to the consumer.

Our proposed model will enable a consumer to automatically do the following – detect available access routers, connect to the router providing the "best" service, use the connection with strong security, and be charged based on usage. A provider will automatically do the following – provide access to consumers, provide strong security to enable only valid users, configure a pricing which is adaptive depending on competition, and use dynamic admission control based on consumer usage. We have designed our complete architecture, and are currently implementing it. We plan to deploy it in a residential community frequented by students of Rice University for real-life usage and experience.

## D. THE BUSINESS MODEL

In here, we describe a complete infrastructure for the provider peers with broadband access to share or resell the bandwidth among their neighbors based on a p2p ad hoc networks technology. The provider peer group will include both the hotspot providers who want to operate a business in the community and as well as residential broadband subscribers who want to recover some of their cost. The consumer peer group without any form of broadband access, that includes visitors within the community will be able to select the best lowest rate connectivity available in the neighborhood and pay on a usage basis without any of the monthly flat rate home or hotspot access fee that typical providers charge.

On a monthly basis, our projection on the financial benefits for both the peers is given in Table 3 and Table 4. Our conservative projection for the residential broadband provider peer group shows an immediate breakeven of the wireless router cost within 3 months with a 60% access fee recovery on a month to month basis. Likewise, the consumer peer group is likely to have a zero installation cost as most of the laptops sold in the market today come pre-wired with Wi-Fi. A projection of 80-85% cost reduction for broadband access cost for consumer peer group is achievable which brings it to the same level as dial-up Internet access today. It is difficult to predict the immediate benefit to the Hotspot provider peer group, as his returns will be based on a rising population of consumer peers in the community.

**Table 3**: **Residential Owner Peer group cost savings**

| | |
|---|---|
| Broadband access cost | Avg: $35/month |
| Wireless Router Cost | Avg: $60 |
| Typical bandwidth provided | 30 GB/month |
| Avg. Personal Broadband usage rate | 2 GB/month |
| P2P Bandwidth shared (3 more users) | 6 GB/month |
| Price of Bandwidth sharing | 0.33 ¢ per MB |
| Cost recovered | $20 per month |
| New cost of ownership | $15 per month |

**Table 4**: **Sharer peer group cost savings**

| | With @Home broadband | With p2p Broadband share |
|---|---|---|
| Monthly fees | $35/month | $7 for 2 GB/month |
| Installation | $35 | $20 (if not pre-wired for Wi-Fi) |
| Hotspot access | $35 per month | Rate will depend on HSO competition |

Even though there could be higher bandwidth sharing among the providers and consumers, there is a limit to the availability of strong Wi-Fi connections based on the current distance limitation of Wi-Fi. Public venue based HSO's revenue potential will not have any such issues and the limit to their bandwidth distribution will solely depend on the number of consumers, total bandwidth available and neighborhood access rates. Through our current research in different apartment complexes in Houston and Philadelphia, we project the broadband access to be shared on an average by 4 users including the owner. The owner could limit the number of IP ports available for sharing through an easy interface in the installed software.

The ad hoc network based p2p bandwidth sharing/selling approach will detect and negotiate the best possible connection on the behalf of the consumer peer group based on three relevant criteria – *Speed of connection, broadband access rate and signal strength.* The three criterion negotiation and connection access will be seamless to the user. The early movers to p2p bandwidth sharing would be the tech savvy and price sensitive broadband users at home who would want to recover some of their access cost. The low cost broadband access opportunity through a pre-wired laptop or an add-on Wi-Fi card of $20 value will encourage the proliferation of Wi-Fi in the community. Next would follow the local HSOs, possibly affiliated with brand name providers or aggregators, who would want to benefit from the growing Wi-Fi users in the community through the p2p model. The competitive rates will create a healthy demand-supply curve and keep the prices in check, as statistics on a daily basis will recommend both the owner and the sharer peers on current and recommended rates in the neighborhood.

Payment processing and logistical access to bandwidth sharing/selling will involve both the peer groups registering on a website http://www.p2pbandwidth.org to download access and sharing software that would be installed on both the broadband provider and consumer laptop, desktop and mobile devices. From a consumer's perspective, the installed software will search for available connections in the neighborhood, negotiate access fee, make connection and update access timeslots on a central server. On the provider's side, the software would enable him to set bandwidth share rates based on current competition, negotiate access connections with temporary encryption and log access and termination times for bandwidth access by the consumers. All transaction will remain peer-to-peer during the entire phase of searching, negotiating and terminating, with usage statistics, access times and confirmation by both the parties to accept a connection at a given rate.

It is probably impractical to initiate fee transaction from consumer to provider after each and every access session. The installed software will enable logging in of the exact connection times and amount of resulting fee transfer between both the peer groups on the central webserver. In the initial stages, we propose to have a link with *Paypal* () to initiate bank transfers on a monthly basis for both the peer groups. Both of them need to have a Paypal account that they will access through a link from the main registration website at http://www.p2pbandwidth.org. The complete business model is shown in Figure 6.

We believe, that creation of this intermediate community for broadband sharing in the community along with proliferating hotspots will have far reaching consequences by accelerating the deployment of broadband and Wi-Fi among US households.

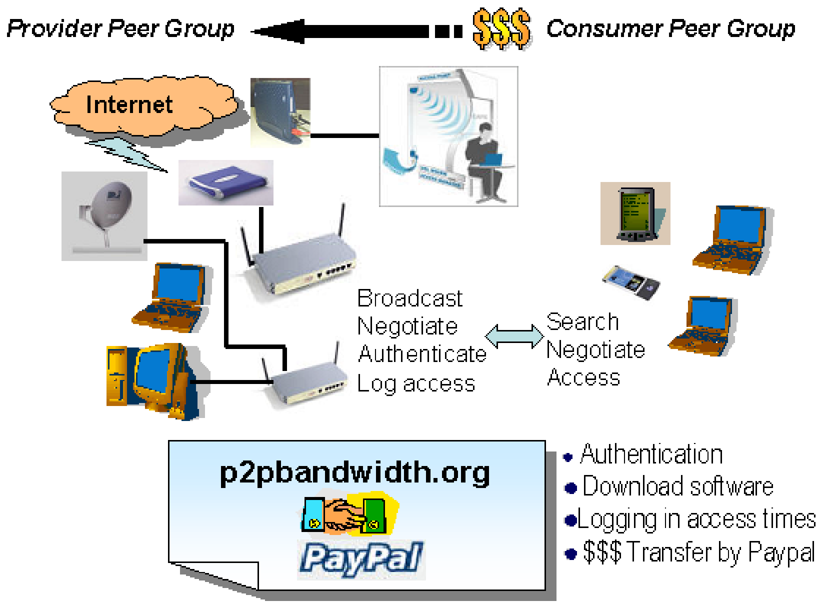



**Figure 6: Business Model**

## E. DISCUSSION

We believe that the p2p bandwidth sharing/selling proposal with "Pay As You Go" scheme for ubiquitous wireless broadband connectivity will find widespread acceptance in the community on similar lines that of Open Source today. A typical flat fee for broadband access and signing up for a multiple monthly fees for at and outside home access will never be appealing to average consumers. Even though logistics is a challenge, the ability for users to have access in a competitive service provider environment, having access anywhere and everywhere through their mobile devices and ultimately getting a single bill at the end of the month on actual bandwidth used, will be the Internet access model in the future.

We design the architecture to show that it is feasible to build such a system. Our proposed architecture has secure mechanisms to prevent malicious use or threats, while providing enough flexibility to configure the architecture to suit specific requirements. Free-for-all community hotspots can be configured as a specific instance of the architecture, by making the price for bandwidth access to be zero. The authentication and secure access will still remain to prevent abuse of the access, and for data security. The auto-negotiation aspect of our architecture is unique amongst the proposed and deployed solutions, providing an additional dimension for competitive hotspot coverage.

Our proposal would initially alienate the current brand name residential broadband providers, branded hotspot operators and aggregators, as they will view the growth of the peer-to-peer community as a serious threat to their revenue earning potential. A typical response from the providers will be to severely limit the bandwidth allowed per subscriber and add legal contract to prohibit bandwidth reselling. Taking a realistic look at the benefits of our model, we find that most of the DSL/Cable operators charge a high fees and installation cost to recover their installation, equipment and wiring costs to each home. A saturation level would surely be encountered in near future where further drop in price would be necessary to get more consumers, most likely at a loss. The above p2p business model can easily be embraced by the branded broadband service providers in the community. Even if residential broadband sharing by reselling is not agreeable to them, installing Wi-Fi hotspots in big apartment complexes and charging a usage based fee would be a viable option to get the price sensitive subscribers. This would enable them to utilize their bandwidth to the fullest without the associated infrastructure cost of reaching each and every home. With the success of Wi-Fi almost a certainty and a new infrastructure requirement for WiMAX in near future, the DSL/Cable providers will probably profit more by restricting new wired infrastructure to every home and being the facilitators of the p2p framework, generating a fractional revenue from the consumer to provider peer group access payment.

There have been recent efforts in providing free community-wide wireless access, like the Austin Wireless City Project [15]. While we believe that communities such as these will continue to grow, it will be difficult for them to cover entire cities. Further, our model will enable free Wi-Fi access networks to be used benefiting both the user and the provider. Hence, the free Wi-Fi communities and our model will be complementary to each other.

We believe, that the consumer driven p2p community will evolve at a fast pace into a critical mass of broadband and Wi-Fi users on the same likes as eBay of today, where the end consumer has the ultimate flexibility and the control. We believe that the p2p model will bring about a fast transition to the world of anywhere and everywhere Wireless broadband connectivity by creating a critical mass of well informed Wi-Fi users in the community.

## F. References


[1] Market Overview: US WLAN hotspots – Forrester Research: http://www.forrester.com
[2] Linspot: http://www.linspot.com
[3] Yankee Group: http://www.Yankeegroup.com
[4] Internet usage in the US, by Connection Types, 2003 - EMarketer Inc: http://www.eMarketer.com
[5] How to stop Broadband churn before it starts - Forrester Research: http://www.Forrester.com
[6] Ethereal Network Protocol Analyzer – http://www.ethereal.com
[7] IETF, RFC 2865 "Remote Authentication Dial In User Service (RADIUS)", June 2000
[8] Liberty Alliance Project, "Liberty Architecture Overview", version 1.1, Jnuary 2003
[9] Yasuhiko Matsunaga, Ana Sanz Merino, Takashi Suzuki and Randy H. Katz. Secure authentication system for public WLAN roaming. 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH workshop, Sep 2003
[10] Anand Balachandran, Geoffrey M. Voelker and Paramvir Bahl. Wireless Hotspots: Current Challenges and Future Directions. 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH workshop, Sep 2003.
[11] David Kotz and Kobby Essien. Analysis of a Campus-wide Wireless Network. MobiCom Sep, 2002.
[12] Paypal – http://www.paypal.com
[13] J. Walker. Unsafe at any key size: An analysis of the WEP encryption. Technical Report 036288E, IEEE 802.11 Committee, March 2000.
[14] W. A. Arbaugh, N. Shankar, and J. Wang. Your 802.11 Network has No Clothes. In *Proc. IEEE International Conference on Wireless LANs and Home Networks,* pages 131-144, December 2001.
[15] Austin Wireless City Project: http://www.austinwirelesscity.org