Wireless Hotspots: Current Challenges and Future Directions

Anand Balachandran, Geoffrey M. Voelker
University of California, San Diego
9500 Gilman Dr., Mail Code 0114
La Jolla, CA 92093
(anandb,voelker)@cs.ucsd.edu

Paramvir Bahl
Microsoft Research
One Microsoft Way
Redmond, WA 98052
bahl@microsoft.com

ABSTRACT

In recent years, 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. 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, coverage, management, location services, billing, and interoperability. We discuss existing research, the work of standards bodies, and the experience of commercial hotspot providers in these areas, and then describe compelling open research questions that remain.

Categories and Subject Descriptors

C.2.5 [**Computer-Communication Networks**]: Local and Wide-Area Networks

General Terms

Performance, Economics

1. INTRODUCTION

The past few years have seen unprecedented growth in the number of wireless users, applications, and network access technologies. Today, widely traveling laptop users access the Internet at a variety of places and environments including their homes, corporate offices, and even at public places of congregation such as conference venues, airports, shopping malls, hotels, libraries, arenas, and so on – places where they spend a considerable amount of time outside private networks. Wireless local area networks (WLANs) have emerged as a promising networking platform to extend network connectivity to these public places, or *hotspots*, as they are commonly known. Contemporary "Wi-Fi" wireless LANs, based on IEEE 802.11b technology [25], provide relatively high data connectivity at 11 Mb/s at these places, and this data rate is expected to grow tenfold in the next few years [7, 39].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
WMASH'03, September 19, 2003, San Diego, California, USA.
Copyright 2003 ACM 1-58113-768-0/03/0009 ...$5.00.

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 [17, 49, 57]. For example, Cometa Networks announced that it would like to build a nationwide Wi-Fi network spanning over 20,000 hotspot nodes by the year 2007. Furthermore, recent work addressing the challenges of wireless-hop security and authentication, coupled with a software-based approach to connectivity, have led to the acceptance of Wi-Fi as a convenient and cost-effective means of network access for mobile users. Nevertheless, 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.

Can a mobile user open her notebook computer or take out her PDA anywhere she roams and find hotspot coverage? How easy is it to configure her connection parameters (channel, SSID, security keys, etc.) at these locations? Is there a common way for her to authenticate herself to each hotspot service provider? What is the payment model for her connection? Are all her connections charged by a single billing entity using a common charging model? What does she do when she goes out of range of a hotspot while roaming? Are there alternative network access technologies that she can use to always remain connected?

In this paper, we argue that the substantial throughput and performance benefits of wireless LANs make them ideally suited as a platform for networking in public places. Although next-generation cellular data services will undoubtedly play a role in providing long-range, wide-area coverage, these networks require expensive licenses and have a high installation cost [28]. Furthermore, wide-area cellular networks, which primarily carry voice traffic, would not meet the connectivity needs in places where users congregate in large numbers and use data and performance-intensive multimedia applications. Wi-Fi networks, on the other hand, are not best suited for scenarios that are characterized by frequent roaming. The seamless coexistence of these different access networks, possibly through a unified service and billing infrastructure, could deliver the promise of ubiquitous and convenient connectivity.

The goal of this paper is to highlight the challenges posed by the vision of a global hotspot infrastructure, and discuss the research problems that remain to realize this vision. We observe that, although there is a demonstrated desire for high-speed wireless connectivity in public areas, several technical and deployment-related 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. We discuss existing research,

the work of standards bodies, and the experience of commercial hotspot providers in these areas, and then describe compelling open research questions that remain. We discuss these problems in the context of the needs of a typical business traveler, although the overall vision is applicable to general consumers as well.

The rest of this paper is organized as follows. In Section 2, we sketch a scenario of a traveling business user's computing needs. Using this scenario as a basis, we discuss the research challenges in the areas of security, authentication, coverage, network performance, network management and pricing of hotspot networks in Section 3. We discuss alternate approaches to connectivity in Section 4 and finally conclude the paper in Section 5.

2. AN EXAMPLE SCENARIO

To provide a context for a vision of what hotspots can provide, we sketch the following scenario of a typical business traveler, Kate, who uses her laptop and PDA and requires Internet connectivity while on the move. We use this scenario to motivate our vision of widespread Wi-Fi availability and to explore the various barriers to realizing this vision.

Kate needs to travel from San Francisco to New York to attend a business meeting. Her day starts off at the San Francisco airport waiting for her flight. She has been working on her presentation which she would like to email (using her Wi-Fi connection) to her colleagues before her flight departs. On arriving in New York, Kate goes to the meeting venue and registers with the Wi-Fi network there. The wireless LAN in the building determines her geographic location within the building and guides her through an interactive building map to the meeting room. While at the business meeting, Kate discovers that she needs to retrieve some important data from her corporate network back in San Francisco, which she connects to through a virtual private network (VPN) using the wireless LAN in the meeting room. She retrieves her data and shares it with her colleagues, perhaps over an in-room ad hoc wireless network rather than sending it to them over email. At the end of the meeting, Kate and her colleagues decide to go out to dinner. They want to find a good restaurant and then get driving directions to go there as they are on the road. Kate is a Verizon subscriber for cellular voice and data services. She plugs in her CDMA2000 1xRTT card into her laptop and is now connected to the Internet even while driving. She gets her directions through a well-known locator service (e.g., yp.yahoo.com) and is easily able to navigate to her destination. Later that evening, Kate is back in her hotel room and can again access her corporate email using the hotel Wi-Fi network. She works on her meeting minutes and emails it to her team back in San Francisco.

It is clear that the wireless LAN connection is of tremendous value to Kate. Nevertheless, how easy is it for her to get connected when traveling from one hotspot to another? How much time does she have to spend in configuring her notebook for the appropriate connection? Is there one single authentication entity at all places? Can she completely trust the hotspot provider network? Is she able to get access from any location within the hotspot, or are there areas where there is not adequate coverage? How is the network able to grant her the bandwidth that she needs and simultaneously serve many other users? And above all, how much does she pay for connectivity during the trip? We discuss these questions as key design and implementation challenges that need to be overcome before a traveling user can get seamless, convenient, widespread connectivity through hotspot networks.

3. TECHNOLOGICAL CHALLENGES

At first, it seems that the scenario just described is easily realizable using the existing component technologies – wireless LANs, wide-area data services, secure authentication, data encryption, dual-mode WLAN operation, and WLAN-based location determination. However, a closer look at the requirements for the whole system to work in a seamless, convenient, and reliable manner reveal challenges that arise from the fact that the system as a whole is greater than the sum of its parts. In this section, we focus on the technological challenges of authentication, security, radio frequency range, network performance, network management, and support for context-aware services.

3.1 Authenticating to the Hotspot Provider

Hotspot providers in public areas typically provide access to unknown users, like Kate, 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 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 (e.g, those who have paid for the service) receive network access. However, authentication and network security are inherently different. Authentication is a precursor to wireless-hop security. Authentication helps the network to establish the users' identity, while wireless-hop security ensures data privacy for authenticated users and protection for the network. For the business user like Kate, it is important that the network identify her and give her access to the resources in as quick and seamless a manner as possible. Today, since each hotspot is likely administered by a different provider, users will have to repeatedly authenticate themselves at each hotspot location. And since each hotspot is configured differently for access, either through a Web-based user interface or through proprietary client software requiring installation and configuration, hotspot users need to get used to the various provider-specific modes of authentication. Systems like CHOICE [8] and SPINACH [4] were the first to demonstrated the use of well-known, third-party authentication mechanisms. On the other hand, hotspot providers like Wayport and T-Mobile [49, 57] offer access to users through a pre-established account (username and password), while others like Cometa [17] hand out *scratch-off cards* containing a one-time login and password to users. These schemes have the inconvenience of the users having to cope with multiple modes of authentication as they roam from one hotspot provider to another.

The goal of providing fast and seamless service, while simultaneously ensuring user accountability, involves a trade-off 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: What authentication mechanisms are best suited in such an environment? Is it adequate for the network to authenticate the users through software mechanisms such as one-time passwords [37], Kerberos [48] or are more sophisticated hardware mechanisms needed? And lastly, how can user verify the identity of the hotspot provider. We discuss this in more detail in Section 3.2.
- Startup Latency: How feasible is it to use SIM-card based authentication in wireless LANs [2, 3]? Currently, GSM net-

works provide each subscriber with SIM cards that enable easy, real-time authentication. However, SIM-card based systems have two inherent security weaknesses: (i) if users lose their SIM cards, anyone who finds (or steals) it can gain access to the network, and (ii) a malicious user can potentially clone a SIM card and use it illegally.

- User Identity: The easiest and most convenient way for users to identify themselves is with existing identities, such as those users already have through other services (e.g., email addresses, cell phone numbers). Can existing mechanisms for identity be conveniently used for hotspot networks? Can users continue to use hotspots at various locations they travel to without having to remember multiple login names and passwords?

- Third-Party Authenticators: How can global databases be used to establish user identity? How can multiple authentication domains be integrated into the infrastructure? One approach is to use trusted third-party authentication databases that allow hotspot providers to offer users with end-to-end security [8]. Authenticating users to well-known third party domains (e.g., *aol.com, msn.com*) does not require users to implicitly trust the provider network. The user simply launches her web browser, which takes her to a home screen branded by the hotspot provider serving that location. Upon entering her identity, the network automatically redirects her connection to the appropriate authenticator, and is not privy to any information exchanged during the authentication phase.

3.2 Wireless-hop Security

A second, related challenge to the authentication problem is 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. For these users, the availability of wireless-hop security would not be a major concern. 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. Second, since user authentication is done before procuring a secure tunnel or a VPN connection, sensitive information such as username, password, keys, etc., need to be exchanged securely with the authenticating entity. 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, authorization of authenticated users through access keys, and access control of all user traffic through per-packet verification [8, 27]. User data security is achieved through data encryption, where authorized users can choose from several encryption mechanisms providing varying levels of security.

A number of schemes that provide authentication and security at the medium access control (MAC) and network layers are being deployed in contemporary wireless LANs. We describe them briefly below, and then discuss open problems that remain.

3.2.1 MAC Layer Approaches

Wireless LAN standards such as IEEE 802.11 [25] and Home RF [32] include an optional provision for authentication and privacy based on shared keys, known as the *Wired Equivalent Privacy* (WEP) function. In this scheme, a shared key is configured into the access points and its wireless clients ahead of time. Only those devices with a valid shared key are allowed to access the network. WEP keys are simple to manage in environments with known users. However, they are not immediately suitable for use in public network environments for two reasons. First, it is not scalable to configure keys to a large numbers of users, many of whom are unknown ahead of time. Second, recent research has shown that the encryption algorithms in WEP are vulnerable to attack [5, 15, 52].

Another security mechanism implemented at the MAC layer is port-based network access control. Under this scheme, network ports are configured to block all traffic except authentication messages until the user identity is established. Port-based access can be implemented either in hardware [38, 56], or in software as is being done in the IEEE 802.1X standards community [27, 35]. Under 802.1X, authentication information is first encapsulated in a wireless Ethernet frame and sent to a specific multicast Ethernet address. The access point forwards this packet to a backend authentication server over a centralized authentication protocol such as RADIUS [43]. Upon successful authentication, a client-specific key is generated for future network access and the access point ports are signaled to forward packets into the access network. 802.1X is a more secure system than approaches like WEP, but is more cumbersome to implement. First, keys lose validity after a short amount of time, after which they need to be renewed. Further, since keys are provided by individual access points, users changing association need to re-authenticate themselves to the network.

3.2.2 Network Layer Approaches

The CHOICE network architecture [8] uses a software approach at the network layer to per-packet verification, where access keys are issued and verified using a centralized Authorizer-Verifier entity. The Authorizer handles authentication and access key provisioning and renewal, while the Verifier performs access verification of individual packets. As opposed to 802.1X, which performs access control at the access points, CHOICE performs verification at the access router in the access subnet. Although this scheme allows unauthenticated traffic to traverse one extra hop in the network, it requires less state maintenance in the access points and is hence more scalable.

3.2.3 Security Challenges

Despite the aforementioned research and standards efforts in wireless hop security, commercial hotspot operators have not yet included any form of security support in their networks due to various practical limitations. We discuss them as open research questions below:

- Mutual Trust: How can wireless-hop security be provided in a way to ensure mutual trust between the user and the hotspot provider? For instance, approaches like WEP assume an implicit trust in the key distributor. However, this opens up the potential for malicious users to spoof the keys and launch masquerading attacks.

- Simplicity-Robustness Tradeoffs: Can hotspot networks employ WEP-based security by choosing from a set of *guest-access* WEP keys as opposed to a single access key, thereby providing stronger security? Can these networks trade-off implementation ease for the slight overhead in key management? How can WEP keys be distributed transparently and scalably under such circumstances?

- Dynamic Key Management: How can key exchange and renewal be simplified and transparent? Approaches like 802.1X require firmware support on the access points, system support on the mobile clients, and explicit reauthentication with

roaming. Software architectures like the CHOICE, on the other hand, involve third-party software installation and configuration.

- Hardware Approaches: Are there ways to provide the robustness of 802.1X through alternative hardware-based approaches? Do smartcards provide the appropriate tradeoff between security and convenience [16, 18]?

- Denial-of-Service: Current 802.11 Wi-Fi networks are highly susceptible to denial-of-service (DoS) attacks targeting the management and media access aspects of the 802.11 MAC protocol [14]. What countermeasures can hotspot providers take to protect their networks against such attacks? Even standards bodies like the 802.11 TGi [1] have deferred discussion about protection against such attacks, yet the public nature of wireless hotspots make them highly vulnerable.

- Malicious Attacks: Hotspots are a comparatively open environment for malicious users to eavesdrop on communication traffic and threaten network security. What measures must these vendors take to prevent masquerading attacks by rogue APs?

3.3 Radio Frequency Range

A third challenge posed by wireless LANs is radio frequency range. Inherent limitations of range and multipath interference from indoor RF propagation restricts user mobility to within the 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. Today's wireless LANs are severely range-limited and the RF signals are subject to limitations posed by the structural properties of hotspot location. This problem will be exacerbated as hotspots migrate to higher frequency standards like 802.11a [39].

There are numerous research solutions that have addressed the problem of range extension through dynamic power management, bridging, specialized antenna technology, and interoperation with cellular networks. The use of these solutions in hotspot networks raise several research questions:

- Power Management: How can wireless LAN range be effectively increased through varying the power levels of the access points? Since the power of the transmitted signal directly affects the cell size, can increasing the access point transmit power help mitigate the effects of indoor RF propagation?

- Wireless LAN Bridging: What are the tradeoffs in using wireless bridges between access points to increase wireless network range? Recently, some hotspot vendors have used wireless LAN-to-LAN bridging to cover a larger geographic area, thereby making the network accessible from a parked car or inside a cafe. For example, hotspot vendor WiFi Metro has created *hotzones* that provide tens of miles of blanket Wi-Fi coverage in downtown San Jose and San Francisco [24].

- Hardware Approaches: How effective are directional antennas using phased arrays in increasing the range of contemporary wireless LANs [21]? Can such sophisticated hardware be deployed in hotspots and be economically viable? If so, will it be backward-compatible with existing wireless LAN hardware?

- Wireless MANs: Metropolitan-area networks (MANs) like Seattlewireless [47] and NYC Wireless [41] claim to offer uninterrupted connectivity over a few miles of outdoor city areas. While this solution seems to address the problem of range, it poses several management and performance bottlenecks including lack of a single management entity, heterogeneous vendor hardware, and lack of infrastructure support. What are the ramifications of connecting through such metropolitan networks? What infrastructure support do these networks provide? And what inter-AP roaming support is offered in such networks?

- Multihop Hotspots: Can mobile nodes that are out of range of an access point access the network through other nodes that have better connectivity? With the use of higher-bandwidth, but range-limited access technologies, future hotspot architectures could be *multihop*, i.e., a network where mobile nodes reach the access point over one or more hops of an ad hoc network. Multihop hotspots pose several challenges to the network designer, which we cover in greater detail in Section 4.

- Interoperability with Cellular Data Networks: It might be more efficient for roaming users to use wide-area wireless data services when they go out of range of hotspot networks. Interoperation between cellular and hotspot networks is beneficial to both wireless carriers (indoor wireless LAN users can help take the load off the cellular data network) and hotspots (users that are out of range of hotspot networks get better connectivity outdoors through cellular data services). However, cellular-to-Wi-Fi roaming service handoff is an open problem and raises many interesting questions. When a user on a cellular network enters into a Wi-Fi coverage area, how can connectivity be seamlessly handed off from the cellular network to the Wi-Fi network, and vice-versa? Do all mobile devices have the hardware capability to use both networks on the same host? Again, we discuss these issues in greater detail in Section 4.

3.4 Network Performance and QoS

A fourth challenge facing hotspot administrators is the ability to adequately provide capacity and coverage to handle dynamically-varying, location-dependent user load. Further, as users pay for connectivity, it is reasonable that they expect a certain minimum level of quality of service (QoS) from the network in the form of sustained wireless bandwidth, end-to-end delay bound, etc. For instance, in the usage scenario described earlier, Kate might be performing a large file transfer that requires a certain minimum bandwidth for her to complete her task before her flight departs. Also, if other users have similar network usage patterns like Kate does, it is crucial for the network to manage the wireless bandwidth scalably and efficiently. Dynamic load management and bandwidth provisioning in the wireless network require that the network: (i) has an understanding of the users' arrival behavior, data-rate demands, and duration in the network; (ii) adapt to the changing resource availability or the changing traffic characteristic either statically (through overprovisioning) or dynamically by readjusting load; and (iii) suggest some form of corrective action to the user [45] if adaptation is not possible in the time-scale that the resource change happens. We discuss each of these requirements below.

Traffic characterization studies of campus [30], conference-room [12], and enterprise [13] have given initial insights into the usage patterns of these networks. Although these environments likely share characteristics with other similar wireless settings, it is not

clear whether these usage models and network throughput characteristics directly translate to hotspots in public areas. To handle network load dynamically, hotspot providers need to better understand mobile user behavior and network resource demand in hotspot settings such as airports, hotels, parks, and so on.

As mentioned before, one of the ways to manage resource usage is to install enough access points to handle the estimated load as given by a traffic measurement. Unfortunately, there are limitations to this approach. First, installation and operation of more access points translates to a larger infrastructure and maintenance cost. Second, an increased number of APs in the network would limit the number of APs that can be operated on non-interfering channels due to the inherent limits of channel reuse in 802.11 networks. Dynamic resource adaptation, on the other hand, requires: (i) a robust and accurate way of measuring load at each access point; and (ii) a way to allocate available resources assuring at least a minimum guarantee.

Suggesting corrective actions to users broadens the range of possibilities for adaptation, and may be very useful when users cannot accept the resources allocated through dynamic adaptation [11]. In our example scenario, for instance, Kate could be guided by the airport hotspot network to the best access point location that has enough bandwidth to send her file. If the network instead had tried to accommodate Kate's request in her original location, she may not have received adequate bandwidth to complete her file transfer before her flight.

To effectively manage scarce wireless resources and plan network capacity, the following research questions still need to be addressed:

- Measurement and Modeling: To what extent do measurements and models of user behavior and network performance in previously measured wireless networks apply to current and future hotspot network deployments?
- Monitoring: To what extent should hotspots be introspective, using measurements of throughput, channel contention, packet errors, etc., to improve service and network utilization?
- How can the hotspot network effectively measure and monitor load on its access points? Is the average throughput at the access points a good measure of load? Does media access delay to acquire the channel need to be taken into account? Under fluctuating channel conditions, Wi-Fi clients to hop between data rates depending upon the bit-error-rate (BER) in the channel. Therefore, a client that operates at a lower data rate (e.g. 1 Mb/sec) occupies the channel for a longer duration, even though its contribution to the instantaneous throughput at the access point might be small. How does this affect the accuracy of the estimated load at the access point?
- QoS Enforcement: How can MAC protocols be designed to guarantee users a fair share of the wireless bandwidth and better channel utilization [33, 40]? If users are allocated a certain share of the bandwidth (through admission control and reservation), how is this bandwidth provisioned and monitored for accounting purposes and trend studies? For example, is it possible to determine the percentage of users that account for over 80% of the consumed bandwidth? And how should the network curtail users who consume a disproportionately large share of the bandwidth?
- End-to-End QoS: How important is last-hop quality of service provisioning as opposed to end-to-end QoS? What is the effect of wired network congestion on the effectiveness of resource reservation in hotspots [31]?

3.5 Network Management

A related challenge to load balancing is network capacity planning. As hotspot coverage grows, access points need to be installed at various parts of the network, which in turn brings the additional challenge of network management. Furthermore, access points can only be effectively installed after a *site survey* to estimate the ability of RF signals to propagate under the geographic constraints of the space (walls, metallic objects, etc.). And, besides additional network management, it incurs extra capital cost (cabling, VLAN routing, site survey, etc.). The need for network management raises a number of research questions:

- Heterogeneity: Organizations providing hotspots (e.g., airport authorities, mall owners, etc.) might handle network installation through third-party contracts. Therefore, the network may have access points from multiple vendors. How can such a network be best managed? Is there a common management interface (e.g., SNMP) that all access points support?
- AP State Management: Dynamic capacity planning requires sharing state information between various access points. How is this best done in large networks? There is no standardized Inter-Access-Point-Protocol [26] that all vendors support. How do large networks share state information between access points under these circumstances? In the CHOICE network architecture [8], state management is performed by a centralized hotspot controller. What are the trade-offs of centralized vs. decentralized management?
- Switched Wireless LANs: Can wireless LAN switching serve as an alternative to managing large numbers of access points? Recently, companies such as Vivato and Aruba Networks have introduced wireless LAN switches to target coverage over an entire building or a large campus environment, eliminating the need for multiple access points [6, 51]. How can such switched networks interoperate with contemporary wireless LANs in hotspots?

3.6 Location and Context-Awareness

The ubiquitous availability of hotspots has the potential to make location and context-aware services more valuable and readily accessible to users. Hotspots providing location-based information and services thus have the opportunity to offer specific applications to attract more users and extend the use of these networks beyond simple connectivity [45, 46]. Despite the many efforts in estimating mobile user location [9, 42, 54, 55], it is still not clear how this location is best represented and used. Implementing a rich location and context-aware system still requires a number of issues to be addressed:

- Application Scenarios: What are the most useful and compelling scenarios in which location can be used? What incentives does location-awareness give to mobile users?
- Location Privacy and Anonymity: What are the best ways to balance the privacy of location information with its utility for user applications and the network [19]? What are the implications of the network knowing precise user location information (i.e., user privacy) or the user having full information about the layout of the network premises (e.g., private areas in an enterprise)?

- Sensor Fusion: How can we integrate multiple location sensing technologies to provide applications better *location fidelity* [23]?

- Absolute vs. Relative Location: How important is it for applications to have absolute location information vs. relative location information? For instance, several pervasive computing scenarios benefit from knowledge of relative and proximate location information (e.g., near the cafeteria, a few feet from Bob's PDA, etc.) without requiring absolute location.

- Interpreting Location: Every location-aware system needs the capability to translate geographic location information into a more usable form (e.g. *Gate 23 in the United Airlines terminal*)? How can we bootstrap the creation of a universal location database that applications can leverage [46]?

3.7 Pricing Model

Despite the many islands of data connectivity provided by hotspots currently throughout the world, hotspot operators have yet to demonstrate a viable model that is lucrative for them and that encourages widespread user acceptance. While hotspot operators are currently implementing pricing schemes to get the maximum return on their investment, their poor revenues show that Wi-Fi users are still not compelled to buy prepaid monthly subscriptions for Wi-Fi connectivity as they do for wide-area cellular services. As we mentioned in Section 3.3, Wi-Fi networks are at a disadvantage compared to their cellular counterpart due to the lack of widespread coverage. However, the higher throughput of these networks, has the potential to offer users a higher *dollar/(bits/sec)* value. What can hotspot providers learn from the success of cellular service penetration? Do the same pricing models hold in both networks? We discuss these and other related challenges below:

- Payment Model: Currently, hotspots offer *pay-per-use* pricing as opposed to subscription-based (prepaid) pricing. Would users that regularly visit hotspots prefer a prepaid subscription as opposed to a pay-per-use model?

- Central Billing Entity: Most users pay monthly subscription charges to network providers for Internet service to their homes (e.g., dial-up, cable modem, DSL, etc.). Can the same provider charge users for their monthly hotspot usage with just another entry in their monthly bill? What does it take to implement such a unified pricing mechanism?

- Third-Party Billing Contracts: In Section 3.1, we discussed the challenge of integrating multiple authentication domains into the hotspot infrastructure. Similarly, can hotspot operators establish billing contracts with multiple ISPs that have already invested in a billing infrastructure [22]? What trust relationships do hotspot vendors need with these domains for authentication, authorization, and accounting?

- Usability: Akin to handling billing through a trusted third party, hotspot area owners (e.g., mall owners, airport authorities, etc.) are contracting the task of infrastructure deployment, management, and support to third party vendors. This model is currently being used, for instance, by Starbucks coffee shops with T-Mobile, and by McDonald's restaurants with Cometa's Wi-Fi venture [17, 49]. What implications does this model have for customer support? How equipped are these places with personnel who can answer questions for people who use hotspot networks for the first time? Wayport [57], in addition to having a in-house technical support, supplies hotel guests with a toll free number to call for configuration, access, and billing related questions?

4. ALTERNATIVE APPROACHES TO CONNECTIVITY

Having discussed the various challenges that need to be overcome to provide widespread Wi-Fi connectivity, we now discuss a few alternative research and industry efforts that have looked beyond the pure Wi-Fi model to a solution that encompasses multiple access modes and technologies.

4.1 Multihop Hotspots

As mentioned in Section 3.3, range limitations of next-generation technologies such as 802.11a may push hotspots beyond single-hop access to multihop, i.e., a network where mobile nodes reach the access point over one or more hops (through intermediate network nodes, or users). Multihop access increases the network diameter and allows clients out of range of access points to receive connectivity. However, multihop hotspots introduce many challenges to the network and protocol designer because of their inherent dynamic nature:

- Node Mobility: In hotspots, users may constantly enter or leave the network or may be mobile while communicating. Consequently, the number of active nodes in the ad hoc network, the network topology, and the volume of network traffic is constantly changing [53]. How does node mobility affect the end-to-end throughput and delay characteristics of TCP connections? How are routing algorithms that send user data using available topology information tolerant to short-term and long-term route loss?

- Channel Interference: Since all nodes in the ad-hoc network are not within RF range of the access points, they may not hear the access point transmission. However, their transmissions can cause interference (due to the particular topology, hidden terminals, etc.) at the access points, degrading effective throughput and the channel capacity. How can co-channel interference be mitigated when nodes are in an ad-hoc network are operating within transmission range of the access point?

- Power Management: Since each node in a multihop network may be transmitting information on behalf of other nodes, nodes may be more severely power constrained. Therefore, more *power-aware* channel access protocols and more effective power saving algorithms need to be implemented [29].

- Multiple Network Access: Finally, nodes in the multihop hotspot that are just one hop away from the access point act as the access routers, or gateways, between the two networks (i.e., the ad hoc network of user nodes and the infrastructure-mode network w.r.t. the access point). How can such devices communicate with multiple physical networks simultaneously? To do so, such nodes need: (i) a wireless network adapter with more than one radio [36]; or (ii) a wireless network adapter with the capability to multiplex connections from more than one network [10, 34]; or (iii) more than one wireless adapter.

4.2 Interoperation with WAN Data Services

Today's network wireless user has several different options of network access, through both wired and wireless means. In this section, we discuss alternate wide-area cellular access technologies that complement Wi-Fi connectivity for a typical mobile user such as GPRS over GSM, CDMA data services, etc., and discuss potential challenges in integrating Wi-Fi services seamlessly with these technologies [44].

As mentioned in Section 3.3, interoperation between cellular and hotspot networks is beneficial to both wireless carriers and hotspot operators. Since cellular networks have better coverage, they can support the connectivity needs of users that are out of range of hotspots. On the other hand, when cellular users enter a building, they can avail of high-bandwidth Wi-Fi connectivity indoors, and reduce the load on the cellular network.

There are different ways in which interoperability can be provided to the user. An obvious way to achieve it is to include hardware support for both cellular data services (e.g., GPRS, CDMA, etc.) and Wi-Fi on mobile devices to migrate the connection across access technologies. In addition to the hardware, these devices need the software ability, through sensing, to switch to the most resource-efficient mode of access [20], where the resource could be network bandwidth, power, device form factor, price, etc. A second way to achieve interoperability is to migrate connections across devices and across access technologies. In addition to the former method, this migration also requires context-sensing to pick the appropriate device and access network.

A second infrastructure related challenge to achieving interoperability is the establishment of roaming relationships and agreements between network operators of these various access networks. There are industry efforts underway to achieve this goal. For instance, TOGEWAnet AG [50], a Swiss infrastructure company, offers a seamless integration of WLAN and GSM GPRS services and an integrated authentication, security, and billing over a common infrastructure. From a research standpoint, however, some other questions need to be explored:

- Handoff Mechanism: When a user on a cellular network enters into a Wi-Fi coverage area, how can connectivity be seamlessly handed off from the cellular network to the Wi-Fi network, and vice-versa? Can user location be used to determine when the handoff might occur? For instance, cellular networks that already support location capabilities through GPS, TDOA, etc., are capable of tracking device locations. By combining this cellular location with a Wi-Fi coverage zone map, the network would have the capability to trigger a cellular-to-Wi-Fi services hand-off based on location when a user enters into a Wi-Fi zone.
- System Support for Handoff: Is handoff initiated at the user device or by the network? For user device initiated handoff, what support does it need from the network for handoff to occur smoothly and quickly? Can handoff latency be reduced so as to not affect the performance of real-time applications? And for network initiated handoff, what support does it need at the user device?
- Billing: Which access network receives the revenue for the user's access? How can potential conflicts be resolved? If both networks get a share of the revenue and billing information is transferred between them, how can this be done securely?

5. CONCLUSIONS

The continuing rollout of hotspot deployment is being fueled by the growing requirement for high-speed connectivity in public areas such as airports, shopping malls, conference venues, hotels, and so on. However, a successful and viable hotspot business model will depend on the extent that it can provide value for all its stakeholders – the end user, the network service provider, and the building and premise owners. 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. These challenges include authentication, security, coverage, network management, billing, and interoperability. 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. For the hotspot network providers to benefit, they must have a reliable and robust third-party authenticating entity, establish peering agreements with other providers for seamless billing, and accommodate the various resource and performance demands of the users. For the premise and building owners to benefit, they must establish business agreements with hotspot network providers for installation, maintenance, monitoring, and support and make network access an everyday utility for the end user.

Acknowledgments

We would like to thank Bill Schilit from Intel Research and Kittur Nagesh from Cisco Systems for their advice and feedback on the ideas expressed in this paper. We would also like to thank the program committee chairs, Sung-Ju Lee and Guiseppe Bianchi, for giving us the opportunity for sharing our work and vision in the area of Wi-Fi hotspots at this workshop. This work was supported by Ericsson and by U.C. Discovery CoRe Grant 01-10099 as a Cal-$(IT)^2$ sponsored research project.

6. REFERENCES

[1] B. Aboba. IEEE 802.1X Pre-Authentication. *Presentation to 802.11 WGi*, July 2002.

[2] A. Ahmad, R. Chandler, A. A. Dharmadhikari, and U. Sengupta. SIM-Based WLAN Authentication for Open Platforms. Technology at Intel *Magazine*, August 2003.

[3] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa. Wireless LAN Access Network Architecture for Mobile Operators. *IEEE Communications Magazine*, 39(11), Novemeber 2001.

[4] G. Appenzeller, M. Roussopoulos, and M. Baker. User-Friendly Access Control for Public Network Ports. In *Proc. IEEE INFOCOM'99*, March 1999.

[5] 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.

[6] Aruba Networks. www.arubanetworks.com.

[7] P. Bahl, A. Balachandran, A. Miu, W. Russell, G. M. Voelker, and Y.-M. Wang. PAWNs: Satisfying the Need for Secure Ubiquitous Connectivty and Location Services. *IEEE Wireless Communications Magazine, Special Issue on Future Wireless Applications*, pages 40–48, February 2002.

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

[9] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building

RF-based User Location and Tracking System. In *Proc. IEEE INFOCOM'00*, April 2000.

[10] V. Bahl, P. Bahl, and R. Chandra. MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card. Technical Report MSR-TR-2003-46, Microsoft Research, July 2003.

[11] A. Balachandran, G. M. Voelker, and P. Bahl. Hot-Spot Congestion Relief in Public-Area Wireless Networks. In *Proc. Workshop on Mobile Computing Systems and Aplications, WMCSA'02*, pages 70–80, June 2002.

[12] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan. Characterizing User Behavior and Network Performance in a Public Wireless LAN. In *Proc. ACM SIGMETRICS'02*, pages 195–205, June 2002.

[13] M. Balazinska and P. Castro. Characterizing Mobility and Network Usage in a Corporate Wireless Local-Area Network. In *Proc. MobiSys'03*, pages 303–316, May 2003.

[14] J. Bellardo and S. Savage. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *Proc. USENIX Security Symposium*, August 2003.

[15] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. *www.isaac.cs.berkeley.edu/isaac/wep-faq.html*, January 2001.

[16] S.-C. Chan. An overview of smart card security. *White Paper*, August 1997.

[17] Cometa Networks. www.cometanetworks.com.

[18] D. Deville, A. Galland, G. Grimaud, and S. Jean. Smart Card Operating Systems: Past, Present, and Future. In *Fifth USENIX/NordU Conference*, February 2003.

[19] M. Gruteser and D. Grunwald. Anonymous Usage of Location-based Services Through Spatial and Temporal Cloaking. In *Proc. First International Conference on Mobile Systems, Applications, and Services (MobiSys'03)*, pages 31–42, May 2003.

[20] E. Gustafsson and A. Jonsson. Always Best Connected. *IEEE Wireless Communications Magazine*, February 2003.

[21] H. L. Van Trees. *Optimum Array Processing*. John Wiley & Sons, March 2002.

[22] H. Haverinen, J. Mikkonen, and T. Takamki. Cellular Access Control and Charging for Mobile Operator Wireless Local Area Networks. *IEEE Wireless Communications*, 9(6), December 2002.

[23] J. Hightower and G. Boriello. The Location Stack: A Layered Model for Location in Ubiquitous COmputing. In *Proc. Workshop on Mobile Computing Systems and Aplications, WMCSA'02*, June 2002.

[24] G. Hyman. Wi-Fi, Wherefore Art Thou? *Wireless Online*, April 2002.

[25] IEEE. 802.11b/d3.0 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, August 1999.

[26] IEEE. P802.11. *http://grouper.ieee.org/groups/802/11*, May 2000.

[27] IEEE 802.1X-2001. IEEE Standards for Local Area Networks: Port-Based Network Access Control, 1999.

[28] ITU-R Rec. M. 1225. Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000.

[29] E.-S. Jung and N. Vaidya. A Power Control MAC Protocol for Ad Hoc Networks. In *Proc. ACM MobiCom'02*, September 2002.

[30] D. Kotz and K. Essien. Characterizing Usage of a Campus-wide Wireless Network. In *Proc. ACM MobiCom'02*, pages 107–118, March 2002.

[31] L. Qiu and P. Bahl and A. Adya. The Effect of First-Hop Wireless Bandwidth Allocation on End-to-End Network Performance. In *Proc. NOSSDAV'02*, May 2002.

[32] J. Lansford and P. Bahl. The Design and Implementation of HomeRF: A Radio-Frequency Wireless Networking Standard for the Connected Home. *Proceedings of the IEEE*, November 2000.

[33] S. Lu, V. Bhargavan, and R. Srikant. Fair Scheduling in Wireless Packet Networks. In *Proc. ACM Sigcomm'97*, pages 63–74, August 1997.

[34] H. Luo, R. Ramjee, P. Sinha, L. Li, and S. Lu. UCAN: A Unified Cellular and Ad-Hoc Network Architecture. In *Proc. ACM MobiCom'03*, September 2003.

[35] A. Mishra and W. A. Arbaugh. An initial security analysis of the ieee 802.1x standard. Technical Report CS-TR-4328, University of Maryland, February 2002.

[36] Mobilian. http://www.mobilian.com.

[37] N. Haller and C. Metz. A One-Time Password System. *IETF RFC 1938*, May 1996.

[38] E. A. Napjus. Netbar – carnegie mellon's solution to authenticated access for mobile machines. *White Paper*, August 1989.

[39] R. V. Nee. New High-rate Wireless LAN Standards. *IEEE Communications Magazine*, pages 82–88, December 1999.

[40] E. Ng, I. Stoica, and H. Zhang. Packet Fair Queuing Algorithms for Wireless Networks with Location-Dependent Errors. In *Proc. IEEE Infocom'98*, March 1998.

[41] NYC Wireless. www.nycwireless.net.

[42] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location support system. In *Proc. ACM MobiCom'00*, July 2000.

[43] C. Rigney, A. C. Rubens, W. A. Simpson, and S. Willens. Remote Authentication Dial-In User Service (RADIUS). *IETF RFC 2138*, April 1997.

[44] A. K. Salkintzis, C. Fors, and R. Pazhyannur. WLAN-GPRS Integration for Next-Generation Mobile Data Networks. *IEEE Wireless Communications*, 9(5), October 2002.

[45] M. Satyanarayanan. Pervasive Computing: Vision and Challenges. *IEEE Personal Communications*, August 2001.

[46] B. Schilit, G. Boriello, W. G. Griswold, D. McDonald, E. Lazowska, A. Balachandran, and V. Iverson. Ubiquitous Location-Aware Computing – The Place Lab Initiative. In *Proc. First ACM Workshop on Wireless Mobile Applicaitons and Services on WLAN Hotspots*, September 2003.

[47] Seattle Wireless. www.seattlewireless.com.

[48] J. G. Steiner, G. Neuman, and J. I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In *Proc. Winter 1998 USENIX Technical Conference*, February 1988.

[49] T-Mobile. www.tmobile.com.

[50] TOGEWAnet AG. http://www.togewanet.com, July 2002.

[51] Vivato Systems. www.vivato.net.

[52] J. Walker. Unsafe at Any Key Size: An Analysis of the WEP Encapsulation. Technical Report 036288E, IEEE 802.11 Committee, March 2000.

[53] K.-C. Wang and P. Ramanathan. End-to-End Throughput and Delay Assurances in Multihop Wireless Hotspots. In *Proc. First ACM Workshop on Wireless Mobiel Applicaitons and Services on WLAN Hotspots (WMASH'03)*, September 2003.

[54] R. Want, A. Hopper, and J. GIbbons. The Active Badge Location System. *ACM Transactions on Information Systems*, 10(1), January 1992.

[55] A. Ward, A. Jones, and A. Hopper. A New Location Technique for the Active Office. *IEEE Personal Communications*, 4(5), October 1997.

[56] D. L. Wasley. Authenticating Aperiodic Connections to the Campus Network. Technical Report WPR005, U. C. Berkeley, June 1996.

[57] Wayport. www.wayport.net.