Secure and Flexible Support for Visitors in Enterprise Wi-Fi Networks

Haidong Xia and José Carlos Brustoloni
Dept. Computer Science, University of Pittsburgh
210 S. Bouquet St. #6135, Pittsburgh, PA 15260, USA
Email: {hdxia, jcb}@cs.pitt.edu

***Abstract*— Secure Opportunistic Hotspots (SOHs) are Wi-Fi networks that provide secure access not only to members of the organization (e.g., company or home) that owns a network, but also members' invitees and any paying visitors that may be within range. Support for invitees can enhance their visit and promote collaboration, while paying visitors can help the organization recover its fixed networking costs. SOHs allow visitors to access only the Internet, and limit the bandwidth they may use. Because paying visitors use trusted third-party online payment servers, such as PayPal, they can use without long-term commitment any SOH they may come across. Unlike commercial hotspots, SOHs tolerate low utilization and availability. Experiments demonstrate the limited effect of visitors on the performance experienced by members and acceptable delay for visitors' online payment.**

I. Introduction

Convenient and inexpensive Wi-Fi networks are rapidly being deployed in homes and businesses worldwide. To take advantage of these networks, many notebook computers and personal digital assistants (PDAs) come with built-in Wi-Fi interface.

Clearly, Wi-Fi has the potential to enable ubiquitous Internet access. It is not clear, however, what business models could bring such a vision to full fruition. Commercial Wi-Fi hotspots are deployed specifically to support nomadic users, but hotspot installation and operating costs make them viable only in high-utilization areas. An overwhelming majority of Wi-Fi networks are noncommercial, each intended for use only by members of the organization that owns it, and therefore do not support ubiquitous Internet access by other people. Because the number of nonoverlapping Wi-Fi channels can be quite limited, interference may prevent installation of commercial hotspots where noncommercial Wi-Fi networks are also needed. Although noncommercial Wi-Fi networks often are *open* and technically allow anybody to connect to them [1], in many jurisdictions such connections can be considered trespass and be illegal.

This paper contributes *secure opportunistic hotspots* (SOHs), a novel architecture that enables noncommercial Wi-Fi networks to provide secure connectivity to organization members as well as Internet access to invited or paying visitors. SOHs may enhance invited visitors' experience during their stay in an organization and increase collaboration and productivity. Moreover, revenues from paying visitors may help an organization amortize the fixed costs of providing connectivity to the organization's members and invited visitors. From the point of view of paying visitors, SOHs are opportunistic because visitors can find, pay, and use any SOH that happens to be within range, without consulting (possibly obsolete) directories and without assuming any long-term commitment.

The SOH architecture is depicted in Fig. 1. SOHs combine several mechanisms to preserve the security and performance of organization members' connections. First, SOHs use 802.1x-based Wi-Fi security protocols [2], such as WPA [3] or 802.11i [4], to guarantee the authenticity and confidentiality of members' packets. Second, SOHs implement firewall-like packet filtering, such that visitors can communicate only with the Internet, and only organization members can communicate with the organization's intranet. Third, SOHs limit the network bandwidth that visitors may use.

A major challenge for enabling visitors in SOHs is that although 802.1x-based Wi-Fi security protocols can provide very high security, they are also new and difficult to configure and interoperate with existing equipment. An organization's technical support can overcome these hurdles for members, but probably not for visitors. We describe in Section II a novel scheme that enables a Wi-Fi access point to support at the same time member authentication based on 802.1x and visitor authentication based on a *captive portal*. Captive portals interoperate well and are easy to use because they do not use Wi-Fi security mechanisms and require only that user computers have an SSL-capable Web browser. However, certain attacks enable theft of service in networks protected by captive portals. We describe in Section III defenses against such attacks.

Billing is another major potential difficulty for supporting paying visitors. Billing mechanisms used in commercial hotspots are unsuitable for noncommercial Wi-Fi networks. The latter networks offer access only in a single area, may not be up all the time, and typically will not have staff for marketing, selling, or supporting Internet access. Therefore, few people would consider establishing a subscription or pay-per-use account with such a network. The other billing method commonly used in commercial hotspots, physical prepaid tokens, may also not be feasible if there is no outlet or staff for selling them. We describe in Section IV a novel method that enables the use of third-party online payment servers, such as PayPal, for billing in such networks.

We implemented a prototype SOH and report on its performance in Section V. We discuss related work in Section VI, and conclude in Section VII.

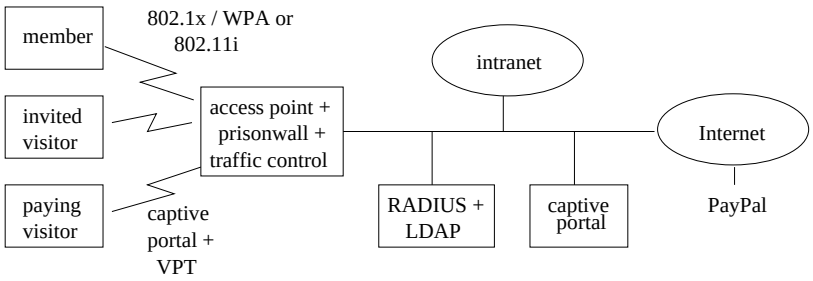

Fig. 1. SOHs use 802.1x-based native Wi-Fi security protocols, such as WPA or 802.11i, for authenticating and encrypting member traffic. Visitors are authenticated by a captive portal, which is easier to use. The prisonwall automatically redirects to the captive portal Web requests from unregistered visitors. The captive portal authorizes Internet access by registering the visitor's addresses in the prisonwall. Visitors who do not have a password have the option of purchasing a virtual prepaid token using an online payment server, such as PayPal. The prisonwall prevents visitors from communicating with the intranet. Traffic control limits the amount of bandwidth that visitors may take away from members. MAC sequence number tracking at the access point and session id checking at the captive portal block theft of service.

II. Supporting both 802.1x and captive portal clients

802.1x enables many authentication schemes. Several of them provide mutual authentication between the client and the network's authentication server. For example, PEAPv2 [5] with MS-CHAPv2 [6] uses a certificate to authenticate the server to the client, and a password to authenticate the client to the server. At its final phase, 802.1x allows access point and client to share secret keys for the client's session and for broadcast traffic. New Wi-Fi security protocols, such as WPA or 802.11i, use such keys to authenticate and encrypt all traffic between access point and clients. The security thereby achieved can be comparable to that of virtual private networks (VPNs) and vastly better than that of Wi-Fi's original security scheme, WEP. WPA or 802.11i are therefore well-suited for members' traffic.

The operation of captive portals is completely different and potentially incompatible with that of 802.1x. Captive portals do not use Wi-Fi authentication or encryption, and require instead a *prisonwall* (implemented, e.g., at the access point or a router) between the visitor and the network. The prisonwall forwards to the Internet only visitor packets with *registered* MAC and IP source addresses. In addition, the prisonwall redirects to the captive portal any Web requests from an unregistered visitor. The captive portal is SSL-secured and requests the visitor's user id and password. If the captive portal successfully verifies these, it registers the visitor's addresses in the prisonwall. The visitor can then communicate freely. The captive portal usually also sends the visitor a *session management page* on a small pop-up widow. This page contains a button that the visitor can click to terminate the session. Finally, the captive portal redirects the visitor to the Web site the visitor originally requested. Unlike WPA or 802.11i, captive portals do not encrypt or authenticate client packets after authorizing a client's access. Clients who desire such protection need to use end-to-end security protocols, such as SSL/TLS, IPsec, or SSH. Because captive portals interoperate readily with most user equipment and are easy to use, they continue to be used in commercial hotspots and are well-suited for visitors.

If there are both 802.1x and captive portal clients on the same network, the problem is how to broadcast packets. The access point needs to encrypt packets destined to 802.1x clients, using the client's session key in case of unicast or the broadcast key otherwise. On the other hand, the access point must not encrypt unicast or broadcast packets destined to captive portal clients.

SOHs solve this problem by having access points monitor the number of associated 802.1x and captive portal clients. If an access point has associated clients of both types, the access point transmits broadcast packets twice, first encrypted with the broadcast key, and then unencrypted. Because commonly only DHCP and ARP packets need to be broadcast, the overhead of doing so is low.

III. Blocking theft of service

It has long been known that *session hijacking* enables unauthorized clients to gain access to networks secured by captive portals. The hijacker first eavesdrops to obtain the MAC and IP addresses of an authorized client. The hijacker then periodically sends to that client a disassociation or deauthentication notification purported to come from the access point. According to the 802.11 standard, these notifications are not authenticated and must be obeyed. The hijacker can then use the client's addresses to gain Internet access. Session hijacking requires special attack tools and is fairly easy to detect, since it causes denial of service.

We have discovered, however, that the increasing use of personal firewalls (e.g., in Windows XP SP2's default configuration), enables a much simpler attack, *freeloading*. Freeloading does not require special tools and can easily go undetected. The freeloader simply eavesdrops and obtains the MAC and IP addresses of an authorized client, and then starts using them. This attack does not work well if the client does not have a personal firewall, because the client may then respond to packets destined to the freeloader in ways that disrupt the freeloader's communication. For example, when the client receives a TCP packet that belongs to a connection that the client ignores (e.g., because it actually belongs to the freeloader), the standard response is to reply RST to the sender (i.e., freeloader's peer). The RST aborts the freeloader's connection. However, if both client and freeloader have personal firewalls, each firewall

stops the respective node from transmitting any packets that the firewall does not identify as belonging to a connection or session initiated by the node. (Personal firewalls interpret such packets as responses to possible attempts to port-scan or fingerprint the respective node.) Therefore, both freeloader and client can share the same addresses, in potential collusion against the access provider.

SOHs use *session ID checking* to thwart session hijacking. SOHs associate with each captive portal client a cryptographically random session id. The captive portal sends the client a nonpersistent cookie containing this session id, along with the client's SSL-secured session management page. This page also gets a http-equiv="refresh" directive with a certain period. The directive causes the client's browser to send periodic requests to the captive portal for refreshing the session management page. Each such request is automatically accompanied by the cookie and SSL-secured. Because the session id cannot be guessed, hijackers cannot spoof these requests. The captive portal can therefore detect hijacking of a client's session by noticing that the client has not sent a refresh request in the previous period. The captive portal can then unregister from the prisonwall the client's MAC and IP addresses, blocking the hijacker's communication.

Because freeloading allows the client to continue sending refresh requests, session ID checking does not detect freeloading. SOHs use another technique, *MAC sequence number tracking*, to thwart freeloading. The 802.11 packet header includes a 12-bit sequence number that increments for each new packet sent and remains the same for MAC-layer fragmentation or retransmissions. Because of tight timing constraints, the sequence number is typically set by network adapter firmware, and cannot be modified by host software. Consequently, in case of freeloading, the access point can observe that consecutive packets using the same source MAC address form more than one trend line. When the access point observes that a MAC address's sequence number drops from one trend line to its previous trend line, the access point notifies the captive portal for unregistering the respective client's addresses. The captive portal then contacts the prisonwall, which blocks the freeloader's communication.

Note that MAC sequence number tracking does not detect session hijacking, which causes a simple jump in sequence number. Simple jumps can occur also for legitimate reasons, e.g. when a client goes out and back in range of the access point. Therefore, for robust detection of freeloading, MAC sequence number tracking requires that the sequence number return to a previous trend line. Note also that session id checking and MAC sequence number tracking are needed only for combating the impersonation of visitors. SOHs use stronger methods, such as WPA or 802.11i, to prevent impersonation of members. The SOH prisonwall allows only members to communicate with the respective organization's intranet.

IV. Billing

Commercial hotspots typically require users to maintain an account with the access provider. The account may be debited a flat fee per month, or debited for each use. Alternatively, users may maintain an account with another access provider or with a billing aggregator, such as Boingo [7], with which a hotspot has previously established a revenue-sharing agreement. Billing methods such as these are cumbersome for access providers and users to set up and maintain.

More informal billing methods are needed in SOHs. *Physical prepaid tokens* (PPTs) are an existing method that has some of the required characteristics. Such a token typically contains a user id and password, perhaps revealed by scratching the token's surface, and corresponds to a temporary account that expires some time after first being used. These tokens can be informally bought over the counter, and therefore could be considered for SOHs. However, many organizations that could be interested in setting up a SOH do not have sales outlets or staff for selling tokens where and when users might need them. Additionally, we anticipate that many users will find SOHs serendipitously, by scanning Wi-Fi channels, and will not necessarily know where to go to get a physical token.

We propose the use of *virtual prepaid tokens* (VPTs) for billing in SOHs. Users can buy VPTs online, instead of over the counter. Therefore, SOHs do not need sales outlets or staff for selling VPTs. Users pay for VPTs using general-purpose third-party online payment servers (OPSs), such as PayPal [8], without any long-term commitment with the access provider. Therefore, users do not need to know where to go to get VPTs: the SOH's captive portal itself tells visitors what OPSs they may use. OPS accounts are easy to set up and maintain both for hotspots and users. Unlike access provider or aggregator accounts, users can employ OPS accounts also for giving or receiving payment in many other types of transaction, including auctions and e-commerce. For hotspots, OPSs may offer the advantage of much lower transaction costs than those typically charged by aggregators. For example, currently the largest OPS, PayPal, charges $0.30 plus 2.9% of the value of a transaction, whereas the largest Wi-Fi aggregator, Boingo, may, depending on the plan, charge as much as 25% of a hotspot's revenue or any revenue in excess of $1 per connect day.

SOHs support VPTs as follows. First, the SOH captive portal allows unregistered visitors to pick a user id and password and select a desired account expiration and OPS. The captive portal reserves the user id in the account database and forwards the visitor to the selected OPS. SOH prisonwalls allow unregistered clients to communicate not only with the captive portal, but also with the SOH-accepted OPSs. The communication between visitor and OPS is secured end-to-end by SSL. The hotspot cannot eavesdrop or tamper with such communication. After the OPS authenticates the user (typically based on the user's email address and password), the user confirms the payment. The OPS then notifies the captive portal of the payment. In the case of PayPal, instant payment notification (IPN) can be used for this purpose. IPN is faster than email-based notification, but is also unauthenticated. Therefore, the captive portal has to confirm the payment by accessing the OPS using SSL. After confirmation, the captive portal establishes

the visitor's temporary account in the database and registers the visitor's addresses in the prisonwall, so that the visitor can communicate with other nodes on the Internet.

V. Experimental results

We implemented an SOH access point that simultaneously supports 802.1x and captive portal clients, using the method described in Section II. The SOH access point has a built-in prisonwall that allows unregistered visitors to communicate only with the SOH's DHCP and DNS servers and captive portal, and with the SOH-accepted OPSs. The prisonwall redirects Web requests from unregistered visitors to the SOH's captive portal. After the captive portal registers a visitor's addresses in the prisonwall, the prisonwall forwards visitor packets to the Internet without restriction. The prisonwall also prevents visitors from communicating with the SOH's intranet. The SOH access point limits the bandwidth that visitors may use, and also implements MAC sequence number tracking for blocking freeloading, as discussed in Section III. Our prototype SOH access point is based on an IBM ThinkPad T30 notebook computer with 1.8 GHz Pentium 4 CPU, 256 MB RAM, and built-in 802.11b interface using the Intersil Prism 2.5 chipset. The access point's software is based on Linux 2.4.20 with modified HostAP Wi-Fi driver. We modified Linux's iptables to implement the prisonwall, and used the Hierarchical Token Bucket algorithm in Linux's Traffic Control module to limit visitors' bandwidth. Our modifications required only about 32 KB of code, plus 1 KB for status of up to 50 simultaneous sessions.

We also implemented an SOH captive portal that authorizes access by invited and paying visitors. The SOH captive portal supports session id checking for blocking session hijacking, as described in Section III, and VPTs for billing, as discussed in Section IV. Our prototype SOH captive portal is based on a Dell Dimension 4550 computer with 2.4 GHz Pentium 4 CPU and 256 MB RAM, running Linux 2.4.20 and the Apache Web server. For the 802.1x authentication server used by members, and the account database used both for members and visitors, we used an almost identical Dell computer, running Windows 2000 Server SP3 with 802.1x patch, IAS RADIUS server, and Active Directory.

As clients, we used a variety of notebook computers by IBM, Dell, and Sony, as well as Sharp Zaurus PDAs, employing Wi-Fi interface cards by Intel, Cisco, Proxim (Orinoco), Netgear, Linksys, and D-Link. We verified that all computers could connect as members or visitors with the various interface cards, and that members and visitors could connect at the same time. We also verified that only members can access the intranet, and that session ID checking and MAC sequence number tracking thwart session hijacking and freeloading attacks against visitors. We found that session hijacking imposes acceptable overhead, on the order of 4% of the network throughput and 5% of the captive portal CPU for 15 visitors with refresh each second (longer refresh periods decrease this overhead). We found that MAC sequence number tracking's overhead is negligible.

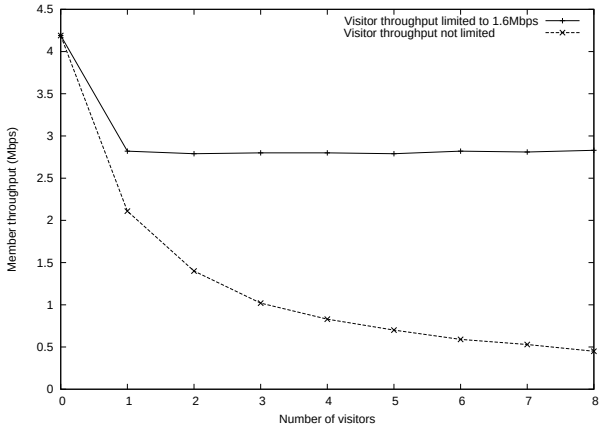

Fig. 2. Packet scheduling at the gateway limits the impact of visitor traffic on member throughput.

From the point of view of members, the main potential difference between a SOH and a regular noncommercial Wi-Fi network is the throughput that may be taken away by visitors in SOH's case (security is similar in both cases). Fig. 2 illustrates the effectiveness of our techniques for limiting this problem. Without traffic control, members' throughput can plummet as the number of active visitors increases. With traffic control, however, SOHs can limit this impact to an acceptable amount.

From the point of view of paying visitors, the main difference between a SOH and a commercial hotspot is the delay that may be involved in traveling to a place within reach of the access provider's network and being authenticated and authorized. (The visitors' security is similar in both cases.) We measured the time our prototype SOH takes for authenticating and authorizing a user using PayPal at different hours of the day. The average was 14.3 s. Although commercial hotspots may take only a couple of seconds to authenticate and authorize a subscriber, the total delay is in general likely to be dominated by travel time. If a user is already within reach of a SOH, it may be much faster and more convenient for the user to use the SOH.

VI. Related work

IPsec-based [9] VPNs have commonly been used to secure connections of members of organizations that own Wi-Fi networks. However, new native Wi-Fi security protocols, particularly 802.11i, can provide equivalent security at lower cost, and therefore are used in SOHs.

Captive portals were first proposed by Stanford's SPINACH project [10]. They are now widely used in access Wi-Fi networks, e.g. in commercial hotspots and university campuses. IPsec could give such networks much greater protection, with strong user and network authentication and per-packet authentication and encryption [11]. However, IPsec is difficult for users to configure. PANS [12] can provide security similar to that of IPsec, and if the user has a supported operating system, can be easy to install. However, as PANS uses proprietary link-layer protocols and user authentication methods, it has not been widely adopted.

Session id checking, MAC sequence number tracking, and VPTs can be advantageous also in commercial Wi-Fi hotspots. We proposed and evaluated such use in earlier papers [13], [14]. This paper extends that work by integrating these techniques into SOHs, so as to leverage enterprise Wi-Fi networks for ubiquitous Internet access.

Aboba proposes access point virtualization techniques in [15]. Our scheme described in Section II can be considered an instantiation of Aboba's Single SSID/Beacon, Single Beacon, Single BSSID class, specialized for the needs of SOHs. In our scheme, the access point's beacon advertises the organization's SSID's visitor capabilities (e.g., open/captive portal authentication without WEP), enabling discovery by any stations within range. Organization members do not need the advertisement of member capabilities (e.g., WPA or 802.11i) because the latter are preconfigured in members' computers. Members' probing and roaming between access points occurs normally, based on this preconfiguration. This specialization interoperates and performs well, and can result in smaller access point memory footprint and less network overhead than Aboba's preferred scheme, Single SSID/Beacon, Multiple Beacon, Multiple BSSIDs. The latter scheme duplicates the entire MAC layer, as well as parts of the IP and application layers, so as to support multiple BSSIDs, SSIDs, capabilities, default keys, periodic beacons, SNMP MIBs, RADIUS configurations, and Web or telnet servers on the same physical access point. Such a complete virtualization could also be used in SOHs. However, the higher costs of such an implementation may be more justifiable in commercial hotspots, where it enables a single infrastructure to support multiple access providers.

Visits of a network's members to another network are traditionally handled according to roaming agreements between the networks. Patel and Crowcroft critique roaming agreements and propose instead direct payment by users to visited networks [16]. Peirce and O'Mahony survey existing payment methods for mobile communications, and propose micropayment schemes for prepaid roaming [17]. Blaze et al. enable credit-based roaming with another micropayment scheme, TAPI [18]. TAPI uses *OTP Coins*, i.e. electronic coins based on one-time passwords. These coins enable fine payment granularity that limits the risk of session hijacking attacks. A Wi-Fi access network using TAPI over the 802.1x protocol can, e.g., disconnect a client if the client does not pay an OTP Coin every few seconds. TAPI does not address the risk of freeloading, however. Additionally, as Lesk points out [19], although micropayment schemes can have desirable properties, many reasons conspire against their adoption in the marketplace. SOH's VPTs may be more practical because they can use OPSs that already exist and have an established clientele (e.g., PayPal alone currently has more than 78 million users). VPTs provide only coarse payment granularity, however, and therefore need other mechanisms to block theft of service (e.g., session id checking and MAC sequence number tracking). Because TAPI requires 802.1x configuration, it may also be more difficult to use than are SOH's VPTs, which require only a Web browser in the visitor's computer.

Mann analyzes how existing U.S. federal regulations apply to OPSs, such as PayPal [20]. A client who uses only credit cards to fund her OPS payments has the same protections as any credit card user. In particular, she can withhold payment if a seller (e.g., hotspot) fails to perform as agreed, and has a maximum liability of $50 in case her credentials are somehow captured and used for purchases she has not authorized. Oddly enough, however, the client may not have the same protections if, instead of a credit card, she uses existing balances or transfers from bank accounts to fund OPS payments.

P2PWNC is a peer-to-peer architecture for ubiquitous Wi-Fi-based Internet access [21]. P2PWNC allows members of an organization that owns a Wi-Fi network (e.g., home, business, or Internet service provider) to visit the Wi-Fi networks of other organizations in the same confederation. Domain agents in the visitor's and in the visited networks negotiate the terms of service and payment. Payment is in the form of unforgeable tokens that the receiving network can later use for funding visits by its members to other networks. It is unclear how P2PWNC would deal with trade imbalances. For example, it appears that an organization's member cannot visit other networks if the organization runs out of tokens. Thus, if an individual's network never gets visitors, that individual may not be able to visit other networks while traveling. SOHs do not have this problem because individuals can use money to pay for visits to other networks.

Currently, the largest commercial hotspot operators in the U.S. are T-Mobile, Boingo, and Wayport, each with several thousand directly owned or affiliated locations. Finding a viable business model for commercial hotspots is surprisingly difficult, and several companies in this space have failed, including MobileStar, AirZone, HereUAre, Joltage, and Cometa [22]. Commercial hotspots need to offer broad coverage and availability in order to attract account holders, but they are profitable only in areas that bring high enough utilization, such as certain cafés and hotel and airport lounges. In contrast, SOH visitors pay for and expect service only at a particular place and time of access. Additionally, SOHs leverage Wi-Fi networks that organizations would need to maintain anyway for their members or invited visitors. Therefore, unlike commercial hotspots, SOHs can tolerate low availability and utilization.

Another Wi-Fi business model that is being tested is that of *promotional* hotspots, which offer free Internet access to attract customers to a particular business (e.g., café, fast-food restaurant, or hotel) or venue (e.g., airport, convention center, mall, or business district). SOHs offer a superset of the functionality of promotional hotspots: in addition to invited visitors (promotional users), SOHs can securely support members and paying visitors.

Surveys consistently show that more than half of all Wi-Fi networks are *open*, i.e. do not use any mechanisms to prevent strangers from using them [1]. Presumably, open networks do not suffer security or performance problems severe enough to make their owners bother with closing them. In many cities, there are organizations promoting *community* networks, where individuals knowingly offer their Wi-Fi networks for

Internet access by others in the community [23]. There are also many volunteer efforts to map such locations [24]. These observations suggest that SOHs are viable: even without SOH's security and performance protection techniques, Wi-Fi network owners are often willing to offer Internet access to others, and many users are keen on finding and using such networks.

Other technologies could complement or compete with Wi-Fi for ubiquitous Internet access. In particular, after years of delay, telephone companies are now offering data services on third-generation (3G) wireless networks in many markets. 3G offers lower bandwidth but potentially more ubiquity than does Wi-Fi. WiMax is an emerging alternative that could match Wi-Fi's bandwidth while offering greater ubiquity.

VII. Conclusions

Although Wi-Fi holds great promise for ubiquitous Internet access, this promise is not being fully realized by existing architectures. Wi-Fi networks are abundant, but most of them are meant to serve only members of the organizations that own them. Nomadic users can use commercial hotspots. However, commercial hotspots are viable only in high-utilization areas, such as cafés and airports. Moreover, interference may prevent installation of commercial hotspots where noncommercial Wi-Fi networks are also needed. We proposed secure opportunistic hotspots (SOHs), a new architecture that enables a Wi-Fi network to provide secure connectivity to members of the organization that owns the network, as well as Internet access to invited or paying visitors. We discussed the need to provide strong security to member traffic, while employing easier-to-use techniques for authenticating visitors. We proposed and verified experimentally a solution for this problem, supporting 802.1x-based security and captive portals on the same access point. We described session id checking and MAC sequence number tracking, new techniques that block theft of service by impersonating visitors. Our experiments showed that these defenses are effective and have acceptable overhead. We also proposed the use of virtual prepaid tokens (VPTs) for billing paying visitors. VPTs are well-suited for SOHs because they do not require outlets or staff for selling them, are easy to set up and use, and have lower transaction costs than those of existing alternatives. They also allow visitors to opportunistically pay and use any SOH they may come across, without long-term commitment. Our experiments show that a visitor can buy a VPT and gain access to the Internet in less than 15 s, and that the impact of visitors on the network performance experienced by members can be acceptably limited. SOHs tolerate low utilization and availability and can reach areas that are unlikely to be ever served by commercial hotspots. We therefore believe that SOHs could significantly benefit the availability of legal, low-cost, high-bandwidth, ubiquitous Internet access.

Acknowledgments

This research was funded in part by The Technology Collaborative (formerly known as Pittsburgh Digital Greenhouse) through a grant from the Commonwealth of Pennsylvania, Department of Community and Economic Development, and in part by NSF ITR medium ANI-0325353.

References

[1] Lemos, R.: Security: Open Networks Pose Dilemma. In: news.com, Feb. 5 (2003) [Online] http://news.com.com/2009-1033-982324.html?tag=rn

[2] IEEE: Port-Based Network Access Control. 802.1x Std. (2001) [Online] http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[3] Wi-Fi Alliance: [Online] http://www.weca.net

[4] IEEE: Medium Access Control (MAC) Security Enhancements. 802.11i Std. (2004) [Online] http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[5] Palekar, A., Simon, D., Salowey, J., Zhou, H., Zorn, G., Josefsson, S.: Protected EAP Protocol (PEAP) Version 2. IETF. Internet Draft, Oct. 2004. [Online] http://www.watersprings.org/pub/id/draft-josefsson-pppext-eap-tls-eap-10.txt

[6] Zorn, G.: Microsoft PPP CHAP Extensions, Version 2. IETF, RFC 2759, Jan. 2000. [Online] ftp://ftp.rfc-editor.org/in-notes/rfc2759.txt

[7] Boingo. [Online] http://www.boingo.com/

[8] PayPal. [Online] http://www.paypal.com/

[9] Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol. IETF, RFC 2401 (1998) [Online] ftp://ftp.rfc-editor.org/in-notes/rfc2401.txt

[10] Appenzeller, G., Roussopoulos, M., Baker, M.: User-Friendly Access Control for Public Network Ports. In: Proc. INFOCOM, IEEE, Mar. (1999) 699–707 [Online] http://mosquitonet.stanford.edu/publications/WebSpinach.ps

[11] Brustoloni, J. and Garay, J.: MicroISPs: Providing Convenient and Low-Cost High-Bandwidth Internet Access. In: Computer Networks **33** (2000) 789–802 [Online] http://www9.org/w9cdrom/249/249.html

[12] Bahl, P., Venkatachary, S., Balachandran, A.: Secure Wireless Internet Access in Public Places. In: Proc. ICC, IEEE, June (2001) [Online] http://www.cs.ucsd.edu/users/abalacha/research/papers/ICC01.pdf

[13] Xia, H. and Brustoloni, J.: Detecting and Blocking Unauthorized Access in Wi-Fi Networks. In: Proc. IFIP Networking'2004, LNCS 3042:795-806, Springer-Verlag, May 2004. [Online] http://www.cs.pitt.edu/~jcb/papers/net2004.pdf

[14] Xia, H. and Brustoloni, J.: Virtual Prepaid Tokens for Wi-Fi Hotspot Access. In: Proc. LCN'2004, IEEE, Nov. 2004, pp. 232-239. [Online] http://www.cs.pitt.edu/~jcb/papers/lcn2004.pdf

[15] Aboba, B.: Virtual Access Points. Proposal to 802.11 Technical Group, IEEE, May 2003. [Online] http://www.drizzle.com/~aboba/IEEE/11-03-154r1-I-Virtual-Access-Points.doc

[16] Patel, B. and Crowcroft, J.: Ticket Based Service Access for the Mobile User. In: Proc. MOBICOM'97, ACM, 1997, pp. 223-233.

[17] Peirce, M. and O'Mahony, D.: Flexible Real-Time Payments for Mobile Communications. In: Personal Communications, IEEE, Dec. 1999, pp. 44-55.

[18] Blaze, M., Ioannidis, J., Ioannidis, S., Keromytis, A., Nikander, P. and Prevelakis, V.: TAPI: Transactions for Accessing Public Infrastructure. In: Proc. 8th Personal Wireless Communications Conf., IFIP, Sept. 2003. [Online] http://www.prevelakis.net/Papers/otpchecks.pdf

[19] Lesk, M.: Micropayments: An Idea Whose Time Has Passed Twice? In: Security & Privacy, IEEE, Jan. 2004, pp. 61-63.

[20] Mann, R.: Regulating Internet Payment Intermediaries. In: Proc. 5th Intl. Conf. Electronic Commerce, ACM, 2003, pp. 376-386.

[21] Efstathiou, E. and Polyzos, G.: A Peer-to-Peer Approach to Wireless LAN Roaming. In: Proc. 1st Workshop Wireless Mobile Applications and Services on WLAN Hotspots (WMASH), ACM, Sept. 2003. [Online] http://mm.aueb.gr/publications/2003-P2Proaming-WMASH.pdf

[22] Boutin, P.: Waiting for Wi-Fi. In: Salon, May 3, 2002. [Online] http://archive.salon.com/tech/feature/2002/03/05/wi_fi_nation/

[23] Schmidt, T. and Towsend, A.: Why Wi-Fi Wants to Be Free. In: Communications of the ACM, 46(5):47-52, May 2003.

[24] Boutin, P.: Warchalking: The Underground Culture of Wi-Fi. [Online] http://www.jiwire.com/warchalking-1.htm