Verifying the Location of a Mobile Device User

Jack Brassil and Pratyusa K. Manadhata

HP Laboratories

Abstract. Certain location-based services seek to spontaneously authenticate user location without the need to have a pre-existing relationship with each user, or with each location provider. We introduce an intelligent infrastructure-based solution that provides spontaneous, rapid, and robust mobile device location authentication by supplementing existing 802.11x APs with femtocells. We show that by transferring data to a mobile device associated with a femtocell while remotely monitoring its traffic activity, a sender can verify the cooperating receiver's location. We explain how to design data transmissions with distinct traffic signatures that can be rapidly and reliably detected even in the presence of heavy cross-traffic introduced by other femtocell users. Neither mobile operators nor location providers need be aware that an authentication is taking place.

Keywords: Distance bounding, GPS, indoor positioning, location privacy.

1 Introduction

The combination of handset-based and mobile operator network-based location services have stimulated the emergence of a growing number of compelling location services. Yet neither type of location service is ideally suited to address the needs of many internet-based Location-based Application Providers (LAPs), ranging from discount distributors such as *LivingSocial* and *GroupOn* to geosocial services including *foursquare*. Many LAPs not only seek to locate clients, but also authenticate those client locations. In many cases, those clients are new users of the LAP's service with whom they have no pre-existing relationship, such as a consumer entering a shopping mall.

Few options are available to LAPs to spontaneously authenticate a new client; mobile operators provide ubiquitously available network-based location services, though these services are targeted at their subscribers, and operators are unable, unauthorized or simply reluctant to provide subscriber location information to third parties who are not partners (e.g., E-911).

As a result inexpensive and widely deployed GPS receivers have made handset-based location service the preferred choice of LAPs. Existing services generally rely on a user's assertion of location (e.g., via an application uploading GPS coordinates). But the economic incentives for users to provide false location information are growing, as evidenced by the growing number of location spoofing

A.U. Schmidt et al. (Eds.): MOBISEC 2012, LNICST 107, pp. 57–68, 2012.

apps available on the Android market. As a result, a discounter such as *Cheap Sally* is unable to report to its advertisers that all coupons that were distributed went to mobile consumers whose locations were authenticated.

Other potential applications of mobile user location authentication are both diverse and expanding. Conventional Location-Based Access Control (LBAC) systems limit access to sensitive information systems from only known, authorized sites (e.g., fixed banking institution locations). But the rise of mobile computing and telecommuting has increased demand for limited access permissions to be granted to off-site workers and customers.

To address the desire to create a public location authentication infrastructure we have proposed to place femtocells at existing public WiFi sites [1]. The short wireless range of these basestations permits us to locate associated User Equipment (UE) to within tens of meters, and indoor operation is supported. In this paper we show how *data* traffic can be used to impress a traffic signature at a femtocell to authenticate user location. Our key contributions include 1) a lightweight non-cryptographic method of verifying an untrusted party's location; 2) an authentication architecture requiring no modifications to existing mobile handsets, operator infrastructure, or public APs, and not requiring trusted infrastructure; and 3) the ability to authenticate locations while keeping the located party's and the verifier's identities unknown to the location service provider.

The remainder of the paper is organized as follows. Section 2 describes our design goals. The next section provides a brief refresher on femtocell technology, then outlines our proposed authentication system architecture and operation. We also examine the problem of designing and detecting traffic signatures in the presence of interfering cross-traffic including voice calls, text messages and data transfers introduced by other femtocell users. We present a security analysis in Section 4, where we describe plausible attacks and attempts to defeat our system, with and without collusion. In the final sections we summarize our contributions, and identify several envisioned enhancements of our authentication approach.

2 Design Goals

Consider a LAP that seeks to authenticate a previously unknown client's current location. Suppose that the client carries a 'smart' mobile device, but the LAP has no knowledge of the client's mobile operator or device capabilities. The LAP requires a *spontaneous, one-time* authentication. A new client might be moving, and a verification transaction must be fast and involve minimal client engagement. Few restrictions should be placed on potential clients, so authentication must be 1) *device-independent* – including basic phones, smartphones, and tablets, and 2) *carrier-independent* – including devices spanning different data transmission technologies including 3G and LTE.

The location service itself should offer fine-grain location information – perhaps equivalent to GPS, while supporting both indoor and outdoor operation. The service must be trusted by the LAP. The system should be sufficiently *hard* for the client *to defeat* but need not be *unbreakable*, as determined by a LAP's *investments* in the transaction, e.g., a discount retail coupon's value and an unauthorized system access's cost.

Security and privacy requirements are also paramount. Clients must *opt-in* to each location verification. In some cases the client might seek to mutually-authenticate the LAP. Finally, the transaction itself should take place with a high-degree of client location *privacy.* Where possible, the location service provider should be unaware that a location verification even took place, and no records need be kept. Indeed, authorized authentications should occur while the located party and the verifier remain entirely anonymous to the LAP.

Of course, these design goals are not rigid requirements, and serve only as a starting point to characterize the needs of a wide variety of LAPs. Though our set of system goals seems potentially unachievable, in the next section we will show how they can be realized. Intriguingly, despite the use of femtocells our solution does not entail mobile operators providing the location service at all.

3 A Public Location Authentication System

To perform a location authentication we supplement existing public Wifi hotspots with off-the-shelf femtocells. We rely on various femtocell properties (e.g., limited transmission range, exposed uplink, private ownership, integrated GPS) to authenticate the location of a femtocell-associated mobile device, without requiring mobile operator involvement or any modifications to operator infrastructure or services.

Femtocells [2] are low-power, limited range (e.g., tens of meters) wireless access points that operate in licensed spectrum to connect subscriber's mobile devices to their mobile operator's network. Femtocells typically use wired public internet access as backhaul. They satisfy the various regulatory, compliance and spectrum use requirements of macrocells, including supporting location service. Femtocells were introduced to improve cellular coverage inside buildings and areas with relatively poor cell tower coverage. Residential femtocells typically support only 2-8 active mobile device associations (i.e., users), while emerging enterprise femtocells can support 8-32 active users.

Voice calls can originate on residential femtocells, and subsequently be handed over to cell towers as callers move, however active calls originating elsewhere may not be handed to a femtocell. Inter-femtocell handoffs are supported in enterprise equipment where dense access point coverage is desired. Femtocell owners may specify access control lists (e.g., family members only, any subscriber). GPS signal availability is typically required, and can be achieved in indoor devices through cabled remote antennas. In most ways a femtocell is best viewed as remotely managed and largely closed infrastructure that happens to reside on customer premises.

Voice and data traffic to and from the femtocell are directed to a Security Gateway (SG) at the edge of the operator's core network. Some control traffic may also be directed to other service points, such as a GPS Gateway. Voice, data

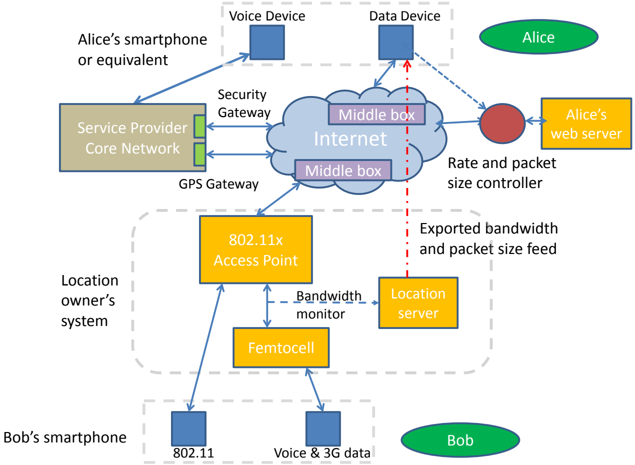


Fig. 1. Architecture of a single-carrier system capable of authenticating smartphone location. A multi-carrier system would employ one femtocell for each mobile operator.

and control traffic between the mobile operator's core network and femtocell is tunneled and encrypted with the Encapsulated Security Payload (ESP) protocol [3], and transported over UDP. Hence, confidentiality is assured against exactly the passive monitoring that we will describe in the next section.

3.1 System Architecture and Operation

We now introduce the participants in a location authentication. *Bob* is a smart mobile device user whose location is to be authenticated. He is willing to cooperate with the authentication to realize some benefit but *Alice* can not trust his assertion of his location. Alice seeks to verify Bob's present location (with his explicit approval). Alice and Bob do not need to have any pre-existing relationship; Alice could be a LAP unknown to Bob. Alice must have the equivalent capability of a smart phone, or more precisely a (mobile or landline) voice-only phone plus minimal compute and display capability; a web browser suffices. The *Location Service Provider* (LSP) seeks to provide a public-access location authentication service. The location itself – say a coffee shop – might already offer a public WiFi service. The site location is assumed to be fixed over time. The LSP – the coffee shop owner – has no prior relationship with either Alice or Bob, each of who can remain permanently anonymous to the LSP.

Figure 1 depicts the basic authentication system architecture; the specific implementation details of the prototype system we constructed are found in [4]. To an existing 802.11x access point with an internet connection, an LSP minimally adds 1) a femtocell, and 2) a computer operating as a *location server*. The location server hosts a web server, and offers a public page with detailed site location information (e.g., GPS, postal address, contact information, etc.) The location server also continuously monitors 1) the average bandwidth, and

2) the packet lengths on the (encrypted) downlink between the AP and femtocell; an average bandwidth for each 1 second interval is measured, and these values form a data stream that is publicly exported. Note that the computational burden of the location server is sufficiently small that in practice it can be run directly on either the AP or the femtocell. Internet middleboxes might exist between Alice and Bob, limiting her ability to use network geo-location techniques to locate him.

The figure also depicts Bob's mobile Service Provider's core network. Alice need not share a common operator network with Bob, nor even know Bob's operator. Regardless of source, any voice or data communication from Alice to Bob will ultimately traverse Bob's operator's network on route to Bob. Bob must have a data-capable device such as a smartphone or mobile computer, and Alice must be capable of controlling her data transfer's network traffic characteristics (e.g., transmission rate, packet lengths). The data can be pushed or pulled, and the underlying transfer protocol is unrestricted. One simple approach that is consistent with our design objectives – namely mobile device independence and mobile user opt-in – is for Alice to provide Bob the URL of a data file on a web server she controls, and allow Bob to initiate the data transfer. Note that *http* transfers potentially avoid the need for Bob to have a special-purpose application to receive the transfer.

Assume that Bob is in range of the LSP's femtocell. Note, of course, that other subscribers of Bob's mobile operator might be present at the location, be associated with the femtocell, and also might be receiving voice and data traffic through the femtocell. But many of those present will likely select the available higher-bandwidth Wifi data service, and opt less for data service through the femtocell channel. Consider the following basic authentication process:

1. Bob successfully binds to the femtocell.
2. Bob messages Alice, and provides her with the LSP's location URL.
3. The location server continuously monitors the (encrypted) AP-femto downstream link and exports two (logical) streams: 1) the average bandwidth over each one second interval, and 2) the number of packets received in the previous second of each observed packet length.
4. Alice transfers data to Bob and controls either the transfer rate or packet lengths (or both) to impress a unique traffic signature on the AP-femto link.
5. Alice monitors the exported bandwidth feed for characteristics of her data transfer.

Of course, these operations can be automated and need not be performed manually. When Alice communicates with Bob, she expects the bandwidth measured on the femtocell ingress to increase and expects the bandwidth to fall when she terminates communication.

- If the behavior of the bandwidth feed convinces Alice that she is observing her own traffic traverse the AP-femtocell link, Alice confirms Bob's phone's association with the femtocell, and concludes that Bob is present at the specified location.

– If the observed bandwidth feed does not reflect Alice's communications, she can not conclude that Bob is on-site. Alice can elect to retry her authentication transfer at a later time to confirm Bob's presence.

Of course, other coffee shop occupants might also be transferring data, or receiving voice calls using the femtocell. In the following sections we will describe how Alice can design a data transfer such that she can reliably detect the presence or absence of her call, even when competing with significant cross-traffic from other users of the AP-femto link.

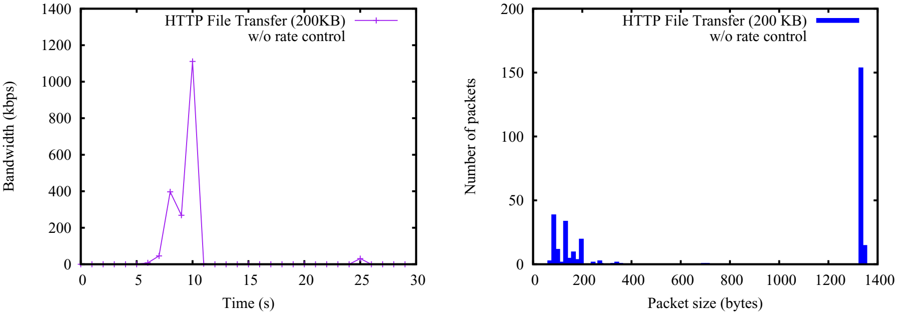
3.2 Authenticating with Data Transfers

We next consider the problems of 1) the design of the network traffic Alice chooses to use to serve as her *fingerprint* that she is indeed using the AP-femto link, and 2) extracting that signal from other cross-traffic generated by femtocell users on site (e.g., voice calls, text messages, data transfers), and consequently verifying Bob's presence at that site.

To begin, consider the cross-traffic characteristics. An active voice call has a well-defined traffic characteristic, and it appears as a relatively long duration, continuous data stream of small packets at a rate of approximately 50 kbs, depending on the voice codecs used. Data traffic (e.g., file transfers, web pages, MMS) are typically high bandwidth (e.g., $100-2000$ kbs) bursts of several to tens of seconds duration. Text traffic (i.e., SMS) are typically low bandwidth (e.g., $1-5$ kbs) bursts of similar duration. Even dozens of simultaneously arriving text messages represent insignificant 'noise' in Alice's signal detection. But even a single contemporaneous cross-traffic data transfer can potentially interfere with an authentication transfer.

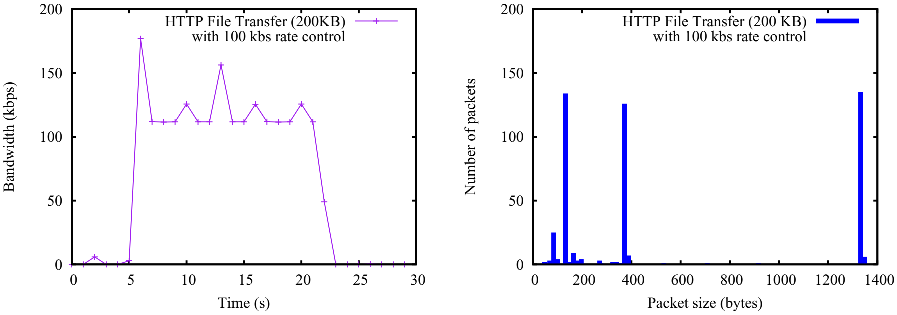
Alice seeks to create an easily discernible traffic signature that looks entirely unlike this cross-traffic. She performs two actions to modify the characteristics of her transfer. First, she controls the transmission rate such that her traffic stream does not have an bandwidth rate *envelope* similar to cross-traffic. For example, choosing a constant-rate transmission of higher bandwidth than a voice call is unlikely to be mistaken as either a voice call (low rate) or a data transfer (bursty). Such a rate-limited transfer is trivial for Alice to implement. Second, Alice should control the size of her individual packet transmissions. Modifying packet lengths arbitrarily is also easy to control. Her objective is to set each packet size to a randomly-selected, infrequently observed value; this size could be fixed, or could vary over the transfer lifetime. To determine such a value(s), we observe that the typical length distribution for packets arriving to femtocell ingress is bi-modal. Voice traffic comprises almost entirely small packets (e.g., 40-200 bytes), and data transfers are a mix of small (e.g., TCP acknowledgments for outbound data) and large (e.g., 1300 bytes) packets transporting data. Hence Alices chooses a value (or values) in the range of 400-1000 bytes, avoiding a few commonly occurring sizes (e.g., 512 bytes).

Suppose a file transfer normally includes N packets of size greater than 1200 bytes with a path MTU of 1500 bytes. If instead Alice chooses to reduce her



(a) Measured bandwidth **(b)** Received packet lengths

Fig. 2. Received bandwidth and packet lengths with no server rate control

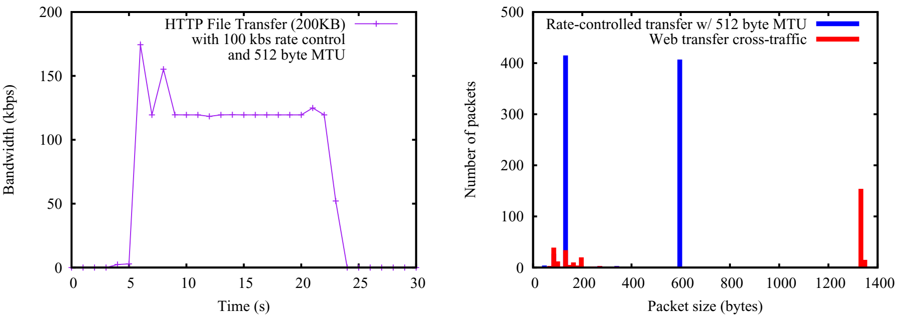


(a) Measured bandwidth **(b)** Received packet lengths

Fig. 3. Received bandwidth and packet lengths with 100 kbs server rate control and 1500 byte MTU

packet sizes to a maximum of 550 bytes (e.g., by temporarily setting her server's NIC's MTU to 550), we expect a data transfer to contain approximately $2N$ packets of length approximately 550 bytes. Recall that transfers to the femtocell are encapsulated by the mobile operator, representing a packet length increase of roughly 10% at the ingress link.

Consider the following example. Figure 2a depicts the measured average bandwidths of a high rate web transfer that might represent cross-traffic while Alice is transmitting her authentication signal. Figure 2b shows the numbers of packets at each length for that interfering transfer. As expected, we see a bi-modal distribution of entirely either small or large packets. Figure 3a depicts a rate-controlled transfer from Alice where she does not control packet length. Packets lengths associated with this transfer appear in Figure 3b; here we see approximately equal numbers of packets of two, tightly clustered lengths: large (i.e., 1390 B) and medium-sized (i.e., 390 B). Figure 4a illustrates the same data transmission with Alice electing to both rate-control and set packet size to 512 B for the duration of the transfer. As expected, Figure 4b shows (blue) that we



(a) Measured bandwidth

(b) Received packet lengths

Fig. 4. Received bandwidth and packet lengths with 100 kbs server rate control and 512 byte MTU

no longer see large packets during the transfer, but instead see more than double their number arriving with length of 590 B, the size of the largest possible transmitted packet with encapsulation overhead. The packet counts shown in red correspond to what Alice would also observe if the web transfer of Figure 2a occurred in the same interval as her authentication transfer. Clearly, a detector looking for the expected largest packet size of Alice's transmissions – in this case the unusual size 590 B suddenly arriving at a rate of 20 packets/sec – would rapidly determine that Alice is using the channel, and confirm Bob's location.

Our observations of femtocell ingress voice and data traffic indicate that each packet length on 16 B boundaries in the range of 600-1300 B occurs for ($\leq 0.1\%$) of arriving packets; most lengths are not observed at all. If desirable, of course, Alice could further improve the reliability of detection by sending a sequence of very short transfers each of which has a distinct, unusual packet length from that range. Such an approach would also strengthen the system from attacks, a topic we discuss in the next section.

4 Security Analysis

We next conduct a security analysis of our system and identify plausible attacks; additional discussion of attacks can be found in [5]. Informally, our system's *attack surface* consists of three actors – Alice, Bob, and the LSP (i.e., store owner) – and six devices – Alice's smartphone, her web server, the LSP's 802.11x access point, the femtocell, the location server, and Bob's smartphone. Hence our system can be attacked if the actors behave maliciously and/or if the devices are compromised. Also, an attacker can disrupt the system's operation via denial-of-service attacks.

Location authentication systems proposed in the literature almost invariably rely on trusted infrastructure, e.g., public key infrastructure (PKI) and trusted platform modules (TPM) (Section 5). Such systems use cryptographic protocols to achieve high confidence in authentication. In contrast, our system places no trust in infrastructure beyond their normal operation and avoids complex trusted infrastructure management, but provides authentication strength consistent with the commercial needs of existing LAPs. Most systems – including ours – however, remain vulnerable to certain attacks, e.g., collusive 'wormhole' attacks, where a remote party colludes with an on-site associate to fake one's presence.

4.1 Deceiving the System

Bob may *fool* our system, i.e., he may prove to Alice that he is near a Location Server (LS) even though he is not; we outline three plausible approaches to deceive our system.

First, Bob may be able to *modify* the length or bandwidth data feed observed by Alice and may impress a fingerprint on the feed so as to indicate his presence near the LS. For example, Bob may compromise the LS and modify the exported data feed, or may modify the bandwidth feed during its transmission from the LS to Alice. Bob, however, has to guess Alice's traffic signature in real time to carry out the attacks. In another difficult real-time attack, Bob may replace both the traffic signal exported by the web server to Alice and the bandwidth feed exported by the LS each with a signal of his choosing. Alice would then observe that the exported data stream has the expected characteristics of her data transfer, and hence believe that Bob is near the LS.

Second, either Bob or the LSP, acting independently or in collusion, may send a phony bandwidth feed to Alice (e.g., by using a fake location URL). We, however, assume that the LSP is unlikely to perform these malicious activities due to economic disincentives; all future economic benefit to the LSP is placed at risk if his malicious activities are detected.

Third, Bob may forward Alice's data file's URL to an on-site colluder (or a colluding LSP) and the colluder may download the file using the LSP's femtocell. The bandwidth feed Alice monitors will now have a fingerprint similar to what she expects, albeit not identical and slightly delayed. The delay, however, may not be decisive for Alice to detect foul play as there will be a legitimate time lag between when Bob receives Alice's URL and when Bob starts downloading the file. Alice may make the delay more easily detectable by *pushing* the data file to Bob instead of him pulling the data file from the URL.

4.2 Disrupting System Operation

Our system is susceptible to *denial-of-service* attacks, i.e., Bob may not be able to prove his location to Alice even if he wanted to. We outline four plausible approaches to disrupt our system's operation.

First, an attacker may modify the bandwidth feed observed by Alice to a feed that is different from Alice's expected bandwidth feed; hence Alice would believe that Bob is not near the LS. For example, as discussed in the previous section, the attacker may compromise the LS, Alice's device, and Alice's web server, or tamper with data transmission to achieve his goal.

Second, an attacker may perform a network DDoS attack on either Alice's network and/or the LS's network, and hence may prevent Alice from accessing the exported data feed and also may prevent Bob from downloading Alice's data file. Both Bob and Alice, however, can easily detect these attacks.

Third, an attacker may simultaneously use many phones at the location to exceed the femtocell's association capacity. Then Bob will be blocked from using the femtocell to receive calls and Alice won't be able to reach Bob.

Fourth, an attacker may compromise our system's components and prevent the components from performing their role. For example, the attacker may prevent the location server from measuring the bandwidth and/or exporting the bandwidth and may prevent Alice's web server from sending the file to Bob.

In the first attack, Alice concludes that Bob is not near the LS even though Bob is. Alice cannot conclude anything about Bob's location in the other attacks; Bob may or may not be near the LS. Hence the first attack is more severe than the rest, but is more difficult to mount.

Lastly, we briefly mention key privacy concerns. An attacker may be able to learn Bob's location by attacking our system. For example, if the attacker compromises Alice's device and gets access to her phone records and web access logs, then the attacker can learn Bob's location. Also, we assume that the LSP's exported data feed is available to any remote party; hence the feed's (in)activity might provide some general indication about the presence/absence of people on site, a potential security risk.

5 Related Work

Despite considerable research time and effort [6,7], authenticating mobile client location remains difficult. Classical authentication system proposals often relied on distance bounding [8], whereas recent proposals use PKIs and TPMs. Our approach is similar to related work in two aspects. First, in principle, we assume that we trust an entity's location and then prove that a mobile device is near the entity; the entity could be a femtocell or an 802.11x AP [9,10]. Second, in implementation, we extend existing infrastructure by adding femtocells and location servers. In comparison, prior work requires certification authorities [11], APs capable of issuing cryptographic location proofs [9,10], and trusted platform modules (TPM) [12,13,14]. Our approach, however, differs in one key aspect: we don't use any cryptographic primitives and rely on lightweight traffic signals for authentication.

Dua et al. [12], Saroiu & Wolman [13], and Gilbert et al. [14] use TPMs to protect the integrity of sensor data. TPMs, however, are not generally found in existing mobile devices. Moreover, the location sensing device inputs remain vulnerable to manipulation, e.g., using GPS signal simulators. Several proposals extend an AP's basic functionality to support location authentication; Luo & Hengartner [9] and Saroiu & Wolman [10] propose solutions that involve APs capable of issuing location proofs. Faria and Cheriton [15] introduce an authentication architecture using a group of APs controlled by a centralized wireless appliance.

Some research on location authentication cleverly exploits channel observations in broadcast wireless networks (e.g., broadcast packets [16], [17], modulated power [18]) to form shared secrets to establish user proximity to an AP. Also, reputation systems [19] and Near-Field Communications [20] have been explored for location based access control.

WiFi Positioning Systems (WPS) and hybrid WPS/GPS systems (e.g., Skyhook Wireless [21]), though popular for indoor/outdoor location determination, are vulnerable to location-spoofing and denial-of-service attacks [22]. More recently, *location-as-a-service* startups (e.g., LOC-AID [23]) have begun to serve as intermediaries between mobile operators and third parties seeking client location. While promising, bootstrapping these services is challenging; each client and third party must proactively establish a relationship with each aggregator.

6 Conclusion

We have proposed and demonstrated a novel approach to infrastructure-based location authentication that operates in a spontaneous, transaction-oriented fashion in public settings. Our approach strives to be well aligned with the evolving needs of internet location-based application providers, and particularly their desire to authenticate new users rapidly and robustly.

Many possible embellishments of our basic system proposal are straightforward, e.g., a multi-femtocell configuration to support more users in a small physical space. Multi-carrier operation can be achieved by simply arraying femtocells from each service provider. Digital signatures should be employed in transfers to authenticate Bob's presence, not just the presence of his smartphone. Femtocells are, of course, not widely deployed today, as would be required to scale our system. But, apart from enabling new services, the basic advantages of wider deployment of femtocell technology – both to operators and consumers – remain plentiful. Our system requires no changes to operator infrastructure or mobile user equipment. Hence, the technology required to deploy a large-scale location authentication system exists, is inexpensive, operates off-the-shelf, and can be deployed incrementally. While future large-scale deployment of femtocells is uncertain, we do envision the integration of femtocell and 802.11x radios in a single multi-access unit as being a potential catalyst for wider-scale deployment. Though our authentication scheme is not foolproof, it appears to be sufficiently difficult-to-defeat to support the modest authentication requirements of emerging internet LAPs.

Our system exploits mobile-operator technology without actually involving the operator directly in a transaction. Yet we believe that more robust authentications can be achieved with the mobile operator's active involvement. In particular, operators control the infrastructure, have preferential network vantage points, and can create easily discernible authentication fingerprints.

Acknowledgment. The authors would like to acknowledge contributions from R. Netravali, S. Haber, and P. Rao.

References

1. Netravali, R., Brassil, J.: Femtocell-assisted Location Authentication (poster/extended abstract). In: IEEE LANMAN 2011 (October 2011)
2. Chandrasekhar, V., Andrews, J., Gatherer, A.: Femtocell Networks: A Survey. IEEE Communications Magazine 46(9), 59–67 (2008)
3. Kent, S.: IP Encapsulating Security Payload (ESP). IETF RFC 4303 (2005)
4. Brassil, J., Manadhata, P.K.: Proving the Location of a Mobile Device User. In: 2012 Virgina Tech Wireless Symposium (May 2012)
5. Brassil, J., Manadhata, P.K.: Securing a Femtocell-based Location Service. In: Intl. Conf. on Sel. Areas in Mobile and Wireless Networking (iCOST 2012) (June 2012)
6. Denning, D.E., MacDoran, P.F.: Location-Based Authentication: Grounding Cyberspace for Better Security. In: Computer Fraud & Security (February 1996)
7. Kindberg, T., Zhang, K., Shankar, N.: Context Authentication Using Constrained Channels. In: Proc. of Fourth IEEE WMCSA, pp. 14–21 (2002)
8. Brands, S., Chaum, D.: Distance Bounding Protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
9. Luo, W., Hengartner, U.: VeriPlace: A Privacy-Aware Location Proof Architecture. In: Proc. of 18th ACM SIGSPATIAL GIS 2010, pp. 23–32 (2010)
10. Saroiu, S., Wolman, A.: Enabling New Mobile Applications with Location Proofs. In: Proc. of HotMobile 2009, pp. 1–6 (2009)
11. Lenders, V., Koukoumidis, E., Zhang, P., Martonosi, M.: Location-based Trust for Mobile User-Generated Contents: Applications, Challenges and Implementations. In: Proc. of Hotmobile 2008 (2008)
12. Dua, A., Bulusu, N., Hu, W., Feng, W.: Towards Trustworthy Participatory Sensing. In: Proc. of USENIX HotSec (August 2009)
13. Saroiu, S., Wolman, A.: I Am a Sensor, and I Approve This Message. In: Proc. of HotMobile 2010, pp. 37–42 (2010)
14. Gilbert, P., Jung, J., Lee, K., Qin, H., Sharkey, D., Sheth, A., Cox, L.: YouProve: Authenticity and Fidelity in Mobile Sensing. ACM SenSys (2011)
15. Faria, D., Cheriton, D.: No Long-term Secrets: Location Based Security in Overprovisioned Wireless LANs. In: Proc. HotNets-III (2004)
16. Wei, Y., Zeng, K., Mohapatra, P.: Adaptive Wireless Channel Probing for Shared Key Generation. In: Proc. of IEEE Infocom 2011 (2011)
17. Narayanan, A., Thiagarajan, N., Lakhani, M., Hamburg, M., Boneh, D.: Location Privacy via Private Proximity Testing. In: Proc. of NDSS 2011 (2011)
18. Zhang, Y., Li, Z., Trappe, W.: Power-Modulated Challenge-Response Schemes for Verifying Location Claims. In: IEEE Globecom 2007 (2007)
19. Talasila, M., Curtmola, R., Borcea, C.: Location Verification through Immediate Neighbors Knowledge. In: Proc. of Mobiquitous 2010 (2010)
20. Kirkpatrick, M., Bertino, E.: Enforcing Spatial Constraints for Mobile RBAC Systems. In: Proc. SACMAT 2010, pp. 99–108 (2010)
21. Skyhook Wireless, `http://www.skyhookwireless.com/`
22. Tippenhauer, N., Rasmussen, K., Popper, C., Capkun, S.: Attacks on Public WLAN-based Positioning. In: Proc. of MobiSys 2009 (2009)
23. LOC-AID, Inc., `http://www.loc-aid.com`