PROVING THE LOCATION OF A MOBILE DEVICE USER

Jack Brassil, Pratyusa K. Manadhata
HP Laboratories
5 Vaughn Dr., Princeton, NJ 08540
[jack.brassil,pratyusa.k.manadhata]@hp.com

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 computing device associated with a femtocell while remotely monitoring its traffic activity, a sender can verify the cooperating receiver's location. We describe a prototype femtocell-based location authentication system we constructed, and explain how to use rate-control to construct data transmissions with distinct traffic signatures that can be 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.**

1. Introduction

Mobile devices such as smart phones and netbooks have seen an exponential growth in their usage and play an increasingly important role in their users' lives. The users accomplish many day to day tasks such as banking and shopping on their devices by utilizing third party services. The service providers, especially location based service providers, can offer better services to the users based on the users' locations. For example, a bank may be able to authenticate a customer's Automated Teller Machine (ATM) transactions from the customer's location. If the bank can authenticate the customer's location and conclude that the customer is near the ATM, then the bank may infer that the transactions are legitimate. If, however, the customer is not near the ATM, then the transaction is suspicious, e.g., a thief might be using a stolen ATM card to withdraw cash from the customer's account.

Many Web 2.0 Location-based Application Providers (LAPs), ranging from discount distributors such as *LivingSocial* and *GroupOn* to geo-social services including *Foursquare*, will also benefit from user location authentication. 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 (e.g., AT&T's FamilyMap). Authorized access to operator location services would benefit LAPs who might wish to partner with operators; their location service works adequately well indoors, and the positioning information can be reasonably trusted. Mobile operators, however, currently have no straightforward means of authorizing and sharing subscriber location information with third parties while ensuring subscriber privacy.

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). As users benefit from location authentication, e.g., location based discount coupons in Foursquare, the economic incentives to provide false location information are growing. We unsurprisingly find many location spoofing applications on the Android market. Hence we anticipate that authenticating client location will become increasingly important as emerging location-driven ecosystems evolve, and that some LAPs will demand to authenticate clients to both enhance and measure service delivery quality.

Other potential applications of mobile user location authentication are both diverse and expanding. Location authentication is a fundamental building block of Location-Based Access Control (LBAC) systems. Mobile user authentication can be used to grant limited access permissions to off-site workers and customers. Location authentication applications also arise in military settings; prior to transmission it is desirable to verify the destination of location-specific content such as maps of areas for immediate reconnaissance.

To address these challenges we have proposed to authenticate a mobile device's location by placing 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. We have a showed [2] that by impressing a *voice* traffic signature while remotely monitoring femtocell ingress link activity, a remote calling party can verify *any* called party's location.

In this paper we show how rate-controlled *data* traffic can be used to impress a traffic signature at a femtocell to authenticate user location, and argue that this approach leads to a far more robust solution than one using voice traffic. 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 WiFi APs and requiring no trust on them beyond their normal operation; 3) a reliable means of authenticating a smartphone user's location that can use the same authentication infrastructure as a voice-only phone authentication approach; 4) the ability to authenticate locations while keeping the located party's and the verifier's location unknown to the location service provider; and 5) an evaluation of our approach by developing an operating prototype system.

The remainder of the paper is organized as follows. Section 2 describes our challenging design goals. The next section provides a brief refresher on femtocell technology, then outlines our proposed authentication system architecture and operation. The prototype we constructed to empirically evaluate our proposal is described in Section 4. Section 5 examines 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 parties sharing the femtocell. We compare our work with related with in Section 6. In the final section 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 mobile device, but the LAP has no knowledge of – or relationship with – either the client's mobile operator or device capabilities. The LAP requires a *spontaneous, one-time* authentication. Indeed, 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*, as determined by a LAP's *investment*s in the transaction, e.g., a discount retail coupon's values 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 might be unaware that a location verification even took place, and no records need be kept. Indeed, authorized authentications should be able to proceed 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 desirable system properties seems potentially unachievable, in the next section we will show how femtocell-equipped access points can be strategically deployed to achieve just these goals. Intriguingly, despite the use of femtocells our solution does not entail mobile operators providing the location service at all.

3. System Operation

A. System Architecture

To realize the operational objectives described in the previous section 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 [3] 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 initially introduced to improve cellular coverage inside buildings and areas with relatively poor cell tower coverage. More recently, carriers including Vodafone are deploying ruggedized ”metro” femtocells in outside settings to capitalize on spatial frequency re-use and the low-cost of third party owned backhaul, or alternately to provide limited public service to rural areas.

Residential femtocells typically support only 2-8 active mobile device associations (i.e., users), though such limits can be dictated by an assumption about the necessary available uplink bandwidth to ensure adequate quality-of-service for multiple active voice calls. Each call consumes roughly a continuous 50 kbs duplex rate, depending on the coding mechanism employed. Enterprise femtocells supporting 8-32 active users are rapidly emerging, with interconnection technologies and interference management in dense deployments being topics of considerable current research interest [4].

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 and control traffic between the mobile operator's core network and femtocell is tunneled and encrypted with protocols such as the Encapsulated Security Payload (ESP) protocol [5], and transported over UDP. Hence, confidentiality is assured against exactly the passive monitoring that we will describe in the next section.

B. Participants in Location Authentication

Participating in a location authentication are:

1) *Bob* is a mobile device user whose location is to be authenticated. He is willing to cooperate with the authentication to realize some benefit but we can not trust his assertion of his location. To be located Bob requires a data-capable mobile device (e.g., smartphone) capable of associating with a femtocell at his current location.
2) *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. In some applications, however, Alice and Bob may have a relationship, e.g., family member or employer, that compels his cooperation. In general, Alice will extend some benefit to Bob only after verifying his location. 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.
3) 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 LSP is incented to provide location service to realize some either direct benefit (e.g., a payment from Alice for participating in a verification), or an indirect benefit (e.g., to be known as a discount coupon distributor). 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.

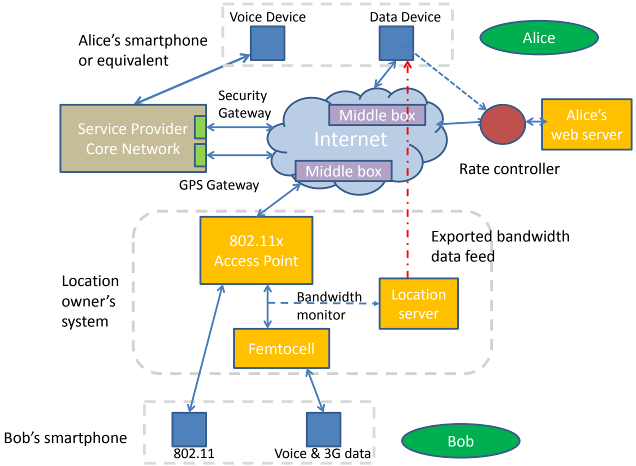


Fig. 1: Architecture of a single-carrier location authentication system using data transfers to authenticate smartphones. A multi-carrier system would employ one femtocell for each mobile operator.

C. System Architecture and Operation

Figure 1 depicts the basic authentication system architecture. 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 the average bandwidth 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 geolocation 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.

Alice controls a data source (e.g., a web server) that can be used to exchange data with Bob. Alice can rate-control her data transmissions to Bob from that source. We assume that Bob carries a smartphone and is in erange 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 to impress a data 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 data 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 transmissions, she can not conclude that Bob is on-site. Alice can elect to retry her transmission at a later time to confirm Bob's presence.

Alice's transmission to Bob impresses a distinct traffic envelope on the AP-femtocell downlink. Within a few seconds of initiating a transfer, Alice expects to observe the measured average bandwidth values increase by the bandwidth she privately sets for her rate-controlled transmission. She expects a similar decrease within a few seconds of hanging up. Though Alice can choose to visually display and examine the returned bandwidth stream, in the next section we will describe an automatic detection algorithm she can run to reliably detect the presence or absence of her call, even when competing with significant cross-traffic from other users of the AP-femto link.

Before we describe our prototype system and analyze system performance, we pause to highlight a few key elements of system operation and participant trust; A related paper [6] provides a much more detailed discussion of system security, privacy, and collusive and/or malicious third party attacks.

First, suppose Bob seeks to defeat the authentication by sending Alice a fake URL reporting false location information. Alice can query the location URL again at any future time, or have other parties query for her. If Alice, or a proxy, does not receive the same location information for each inquiry, she can invalidate any previous confirmation of Bob's presence at the false location. Bob is committed to maintaining a false location URL indefinitely. Bob might also choose to deceive Alice by creating a false exported data stream (e.g., by communicating to Alice via a private femtocell). This too Bob would be forced to operating indefinitely. Indeed, during an authentication a suspicious Alice can even observe the exported bandwidth streams of all Bob's previously provided URLs to detect the unexpected presence of her impressed traffic.

Second, note that an LSP supports – but does not actively participate in – an authentication transaction, and since observed femtocell communications are encrypted, would not ordinarily know the parties involved. The LSP simply offers a service which operates persistently and consistently; Alice trusts the LSP until she proves otherwise, in part because the LSP stands to economically benefit from providing a service. Suppose an LSP seeks to transmit a phony bandwidth stream to trick Alice that Bob is present. Recall that the communications between femtocell and mobile operator is encrypted. Only Alice knows when and how she impresses a signal on the channel. The location owner is unable to reliably guess when and how Alice (or her proxy) is performing a verification.

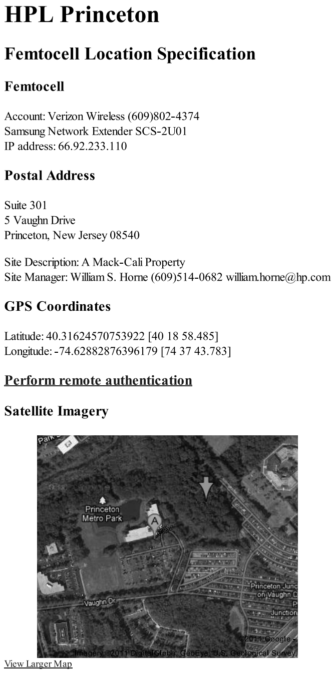
4. Prototype System

To explore the practicality of our proposed location authentication system we have constructed a complete single-carrier system prototype. When not performing controlled tests, we also observe typical system behavior by allowing the femtocell to serve occupants of our small office. Our prototype uses the Verizon 3G Network Extender (Samsung 2CS-2U01) femtocell; the bandwidth measurements we report here are representative of voice codecs and transport protocols deployed by Verizon Wireless. An x86-based commodity PC with multiple ethernet NICs running a standard Linux 2.6.34 kernel serves as the location server. In contrast to Fig. 1, the server is located inline between the AP and femtocell, and traffic is forwarded between NICs via a standard network bridge. Bandwidth measurements are taken by reading a bridged interface directly with one of various, widely available tools such as *bwm-ng v.0.6* and *ifstat v.1.1*. The upstream link from the wireless AP is a shared DSL connection with rates of 3 Mbs downstream and 768 Mbs upstream, which we would expect to be representative of the modest bandwidth available for many broadband public internet access channels.

An Apache web server offers users a static page with detailed site location information, including GPS coordinates, and a URL to access online bandwidth measurements; Figure 2 shows the page for the prototype in the authors' office. Real-time measurements are initiated on-demand, and exported via *netcat* on a separate interface to not impact bandwidth measurements. Verifiers are also able to request graphical views of bandwidth measurements for an epoch; compact *sparklines* are generated with Javascript for remote parties who are display-limited (e.g., smartphones). Our offline detection algorithms – to be introduced in the next section – are compactly implemented in Python.

5. Authentication Signal Design and Detection

We next consider the problems of 1) the design of the traffic signal 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 3) evaluating the probability that Alice herself is using the link, and consequently authenticating Bob's location. Note that we limit our attention to traffic signals Alice can send and Bob can receive with no change to existing mobile handsets or infrastructure; we will revisit this assumption in Section 7 to discuss how mobile operators can facilitate authentication. In the remainder of this section, we explore how Alice can authenticate Bob's location using a traffic signal using rate-controlled data transfers.



HPL Princeton

Femtocell Location Specification

Femtocell

Account: Verizon Wireless (609)802-4374
Samsung Network Extender SCS-2U01
IP address: 66.92.233.110

Postal Address

Suite 301
5 Vaughn Drive
Princeton, New Jersey 08540

Site Description: A Mack-Cali Property
Site Manager: William S. Horne (609)514-0682 william.horne@hp.com

GPS Coordinates

Latitude: 40.31624570753922 [40 18 58.485]
Longitude: -74.62882876396179 [74 37 43.783]

Perform remote authentication

Satellite Imagery

View Larger Map

Fig. 2: Location web page for the prototype system.

The high bandwidths achievable by data transfers (e.g., up to 2 Mbs) suggests that they may be ideally suited for use as an easily identifiable authentication signal. Using data requires certain modifications to our system architecture, as Fig 1 depicts. Bob must have a data-capable device such as a smartphone or mobile computer, and Alice must be capable of controlling a data transfer. 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.

In the next sections we discuss an approach that might be used for data signaling. In this scheme, Alice controls the rate at which data is transmitted. Alice examines the exported data streams to determine if her data transfer is present at the femtocell ingress; if the transfer is deemed present, she has authenticated Bob's location. If she can not identify her signal, she can make no determination about Bob's presence or absence.

1) **Rate Encoder Implementation:** Figure 1 shows how we enhanced our basic prototype system to permit Alice to send rate-controlled data to authenticate Bob's

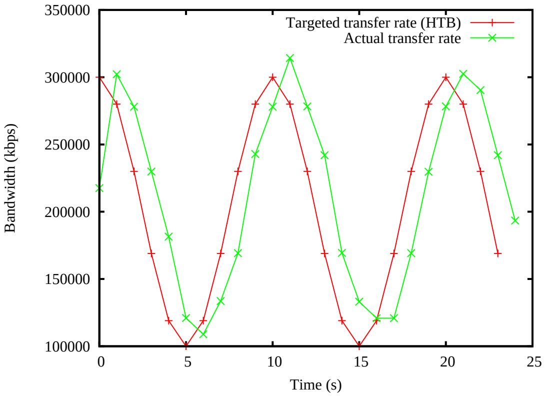


Fig. 3: The targeted transfer rate of backlogged data leaving Alice's rate-controlled server (red) is a raised sinusoid with 200 Kbs average rate and a 10 second period. The actual measured transfer rate (green) closely follows the rate target.

location. For the data source we introduced an *httpd* server on a second x86-based commodity PC running a standard Linux 2.6.34 kernel. Immediately prior to a location authentication we create a randomly named file with dummy data using the *dd* utility; the file must be sufficiently large in size to continuously transmit for the duration of the epoch at the rate specified by Alice; we typically used $200 - 800$ KB file sizes.

Rate control is implemented using native Linux traffic control on the egress interface; we chose to use a *Hierarchical Token Bucket* (HTB). Note that the rate determined by Alice should be lower than the available bandwidth on the end-to-end transmission path between the server and Bob, otherwise the transmitted packets will be delayed in the network and the average bandwidth rates observed at the femtocell ingress would be less than the rates transmitted at the source. We typically operated conservatively by using rates in the range of 50-300 kbs for authentication.

Figure 3 reveals that our prototype can perform this rate control accurately. A file transfer from Alice's server to Bob is rate-limited at all times, ensuring the rate envelope is achieved due to a continuous backlog of data to transfer. The rate of our HTB is modified each second by a sinusoid with amplitude 100 kbs and period $T = 10$ seconds (i.e., fundamental frequency $f_0 = 0.1$ Hz), i.e.,

$$s(n) = 200 + 100\,cos(0.2\pi n), \quad n = 0, 1, 2, \ldots . \qquad (1)$$

The figure shows the target rate imposed by our limiter, and the actual transfer rate at the egress of Alice's server. Both rate and timing are controlled sufficiently accurately for our purposes.

2) **Using Rate Controlled Transfers:** Network queuing and congestion will modify the envelope of a transmitted flow before its arrival to the femtocell, even if that envelope is slowly changing. The flow's path through the network is long; from web server through the public internet through Bob's operator's network and back out across the internet to the femtocell.

Given this imprecise control of the arrival stream, how should Alice rate-control an authentication data transfer to ease her detection of her signal's presence in the returned bandwidth feed? One simple approach is to alternate the transmission rate between two fixed values (e.g., 150 and 250 kbs) chosen randomly by Alice on a per-transaction basis. Alice can then observe the channel for rate changes of approximately ± 100 kbs occurring at the times she adjusts rates. Of course, as was the case with voice signals, cross-traffic sharing the femtocell downlink can still interfere with detecting this signal.

Figure 4 shows the average arrival rate at the femtocell for a transmission oscillating between target rates of 50 and 150 kbs every 5 seconds. Such a slowly time-varying envelope can be readily detected by Alice, though it requires an observation period of 10 seconds or longer. To shorten the necessary observation period, we rely on our intuition about the behavior of rate-controlled TCP sources. These sources tend to rapidly enforce a rate limit lower than the current transmission rate, but are less speedy in achieving a higher rate upon a rate limit increase above the current transmission rate. Hence we propose to modify rate asymmetrically in time, effectively varying the duty cycle of the modulating square wave. Figure 5 shows the average arrival rate at the femtocell if we set the rate at 50kbs for 1 second, and 150 kbs for 2 seconds, shortening the necessary observation period for reliable detection to perhaps 3-6 seconds in the absence of cross-traffic. Of course, the longer Alice chooses to transmit an authentication signal and observe femtocell arrivals, the more reliable her detection promises to be.

A more sophisticated authentication signal modulates Alice's transmission envelope with a raised sinusoid of fixed but randomly-chosen amplitude and frequency. This approach offers several compelling advantages. First, rate-limiting at the sender is no more difficult than for a simpler signal. More important is that signal detection signal is simpler, as we will explain in the next section. Detecting such a signal should be robust; we intuitively expect relatively little energy observed at the sinusoid's fundamental frequency due to interfering cross traffic. Finally, the presence of this signal is less easily perceived by any observers of the channel. Figure 6 shows the average arrival rate at the femtocell for

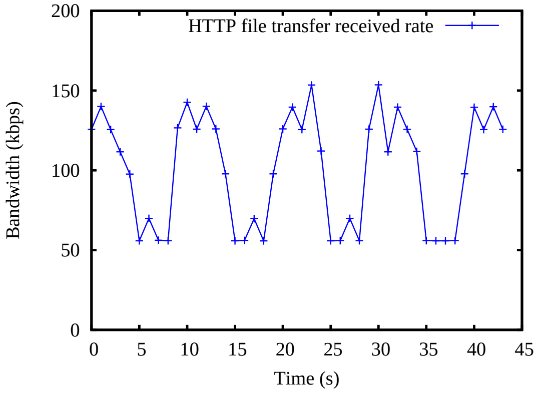


Fig. 4: The arrival rate to the femtocell for a source alternating between 100 kbs and 150 kbs with a 10 second period.

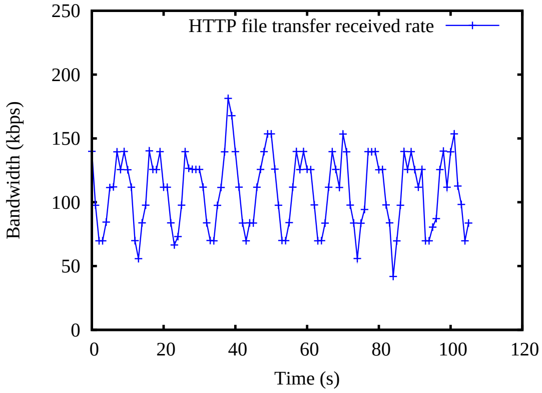


Fig. 6: The arrival rates for a rate-controlled source modulated by a raised sinusoid.

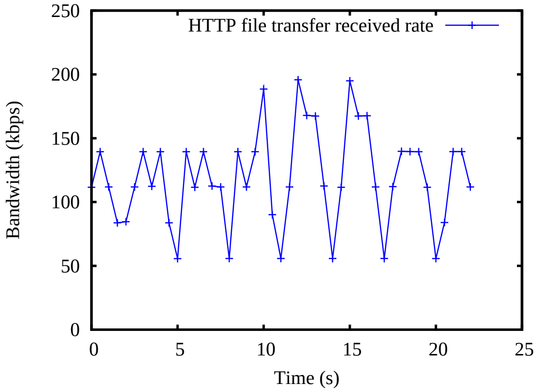


Fig. 5: The femtocell arrivals for an oscillating rate source transmitting at 50 kbs for 1 second, and then 150 kbs for 2 seconds. Altering the time in each states shortens the observation period necessary for reliable detection.

an authentication signal modulated with rate given by $s(n) = 100 + 50\,cos(0.2\pi n),\ n = 0, 1, 2, \ldots$.

In the next section we discuss how a detector is constructed to identify these rate-controlled signals in the bandwidth feed returned to Alice.

3) **Detector Implementation:** In the presence of limited cross-traffic – such as a collection of text messages to other femtocell users – Alice can trivially identify the presence of an oscillating-rate authentication signal using a combination of edge and threshold detection, as we explored for voice call detection in [2]. However, we instead seek to develop a single detector for a large class of periodic authentication signals, and one that is reliable in the presence of a moderate amount of cross-traffic.

By modulating rates with a raised sinusoid, Alice is effectively sending a *hidden tone* as her authentication signal. Hence, our detector should resemble a frequency-selective bandpass filter tuned to the the selected tone. The implementation is simple; Alice receives the set of returned bandwidth samples for each epoch, i.e., $\{r[i],\ i = 0, 1, \ldots, T-1\}$, and calculates its Discrete Fourier Transform (DFT). Alice evaluates the amplitude of the DFT coefficient corresponding to the frequency of the hidden tone, and determines if that value is larger than the coefficient evaluated in other epochs when she is not transmitting.

The effectiveness of this detector is demonstrated in the following synthetic example. For 30 seconds we embedded the captured sinusoidal authentication signal in Figure 3 in 300 time-offset instances of a captured text message, with offsets either randomly chosen or correlated (in separate experiments). In each case the nominal bandwidth of the aggregated interfering messages is roughly 120 kbs, while that of the signal is only 100 kbs. As expected, the random interfering traffic has little energy at the signal's fundamental frequency. The magnitude of the amplitude of the corresponding DFT coefficient always exceeded that of the noise alone by a factor of 5 to 10, permitting easy detection of the presence of the authentication signal.

To further improve the reliability of detection Alice can sustain a rate-controlled authentication signal for as long as necessary. But as before, if her authentication signal shares the femtocell ingress with high-rate data transfers to other users, she will be unable to detect her signal reliably to confirm Bob's location.

6. Related Work

Despite nearly 2 decades of research [7], [8], [9], [10], authenticating mobile client location remains difficult. Classical authentication system proposals often relied on distance bounding [11], [12]. Location proof architectures almost invariably rely on deploying trusted infrastructure, often distributing trust across multiple system elements in a complex authentication overlay. Such systems typically strive to achieve a high degree of confidence in verification, frequently using cryptographic protocols to bind devices and identities. In contrast, our system places no trust in infrastructure beyond their normal operation, and aims for a simple architecture that avoids the complexities of trusted infrastructure management, but provides authentication strength consistent with the commercial needs of existing LAPs .

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 [13], [14], [15]. Second, in implementation, we extend existing infrastructure by adding femtocells and location servers. In comparison, prior work requires certification authorities [16], APs capable of issuing cryptographic location proofs [13], [15], and trusted platform modules (TPM) [17], [18], [19], [20]. Hence, the proposed approaches' success depends on the widespread deployment of either femtocells, cryptographically enhanced APs, and/or TPMs in smartphones. Our approach, however, differs in one key aspect: we don't use any cryptographic primitives and rely on lightweight traffic signals for authentication; hence we avoid managing complex infrastructure such as public key infrastructure and TPMs. Zeng et al. also use non-cryptographic techniques for authentication in a different context; they use physical layer characteristics for user authentication and device identification in wireless networks [21].

Lenders et al. use localization/certification authorities to securely tag location information to content generated on mobile devices [16]. Their approach, however, depends on an external mechanism to identify device location. Authentication systems that assume trusted user devices have also been proposed. Dua et al. [17] and Saroiu & Wolman [18] use TPMs to protect the integrity of raw sensor data. Similarly, Gilbert et al. use TPMs to guarantee the integrity of data derived from raw sensor data [19], [20]. TPMs, however, are not universally found in mobile devices, e.g., to the best of our knowledge, no commodity smartphone has a TPM chip. Moreover, even if devices had TPMs, the location sensing device inputs remain vulnerable to manipulation, e.g., using GPS signal simulators [22].

Due to the vast deployment of 802.11x wireless APs, the research community has focused almost entirely on location proof systems based on APs. Several proposals extend an AP's basic functionality to support location authentication; Luo & Hengartner [13] and Saroiu & Wolman [15] propose solutions that involve APs capable of issuing location proofs. Faria and Cheriton [23] introduce an authentication architecture where a centralized wireless appliance controls a group of APs, and broadcasts a set of random nonces through its controlled APs.

Some research on location authentication cleverly exploits channel observations in broadcast wireless networks (e.g., broadcast packets [24], [25], modulated power [26]) to form shared secrets to establish user proximity to an AP. Such proposals rely heavily on details of the underlying physical and link layer communications protocols. A weakness of these approaches is that they closely associate location architectures to protocols that can change over time as communication standards evolve. An alternate approach to reduce trusted infrastructure and resist collusion relies on the presence of on-site corroborators to verify user presence; some systems strengthen trust in unknown third parties by turning to reputation systems [27]. In contrast, our approach doesn't rely on any other system user's presence or actions.

Community interest has recently shifted to authentication systems using other communications technologies. Bertino and Kirkpatrick explore Near-Field Communications (NFC) and dedicated location devices to create an access control scheme [28]. Relatively little research has focused on the role femtocell technology can play in providing location services. Borgaonkar et al. describe how the lack of physical security makes femtocell location reporting an appealing target for hackers [29]. Indeed, it is precisely this lack of physical security – femtocells are located on customer premises – that permits us to construct an authentication service.

Taking a markedly different approach to *who* should provide location services, Gorlatovar et al. argue that femtocell locations should be actively hidden through the use of dynamic base station identifiers [30]. Their motivation is to preserve the exclusive ability of mobile operators to deliver femtocell-based location services. In contrast, our approach requires opening femtocell locations to any third party, and we have argued that mobile operators may be poorly suited to deliver the type of spontaneous, transaction-based service demanded by LAPs.

Despite the proposed location proof systems' broad diversity, most systems – including ours – remain vulnerable to certain attacks. Collusive 'wormhole' attacks – where a remote party colludes with an on-site associate to fake one's presence – are the most challenging shared threats. Though distance bounding techniques may be a practical solution to these threats [31], it too suffers from weaknesses [32].

Despite these vulnerabilities, LBS systems have enjoyed tremendous success in practice. WiFi Positioning Systems (WPS) and hybrid WPS/GPS systems (e.g., Skyhook Wireless [33]) are the most popular location determination systems in use today for indoor/outdoor applications. Despite locating only smartphones and other 802.11 equipped devices, these systems have enjoyed tremendous growth and provide a valuable service. Researchers have shown, however, that these systems are vulnerable to location-spoofing and denial-of-service attacks, often realized by attacking APs or manipulating their signals [34].

More recently, *location-as-a-service* or *Where 2.0* companies (e.g., LOC-AID [35], Veriplace [36]) have begun to serve as intermediaries between mobile operators and third parties seeking client location. These aggregators not only locate clients with any mobile phone device, but serve the crucial role of locating clients served by different operators. While promising, bootstrapping these services is challenging; each client and third party must proactively establish a relationship with each aggregator.

7. Conclusion

We have proposed and demonstrated a novel approach to infrastructure-based location authentication that operates in a spontaneous, transaction-oriented fashion. 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 on-the-spot. We studied a diverse set of traffic signals that can be used to authenticate parties associated with a femtocell in a rapid and robust way.

Many possible embellishments of our basic system proposal are fairly 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. 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.

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] R. Netravali, J. Brassil, "Femtocell-assisted Location Authentication (poster/extended abstract) ," *IEEE LANMAN 2011*, Oct. 2011.

[2] J. Brassil, R. Netravali, S. Haber, P.K. Manadhata, P. Rao, "Authenticating Location with Femtocells," *submitted for publication*, Oct. 2011.

[3] V. Chandrasekhar, J. Andrews, A. Gatherer, "Femtocell Networks: A Survey", *IEEE Communications Magazine*, Vol. 46, No. 9, September 2008, pps. 59-67.

[4] Qualcomm, http://www.qualcomm.com/product-services/wireless-networks/femtocells

[5] S. Kent, "IP Encapsulating Security Payload (ESP)," *IETF RFC 4303*, December 2005.

[6] J. Brassil, P.K. Manadhata, "Security Vulnerabilites of a Location Location with Femtocells," *submitted for publication*, Jan. 2012.

[7] R. Want, A. Hopper, V. Falco, J. Gibbons, "The Active Badge Location System", *ACM Trans. on Information Systems*, Vol. 10, No. 1, 1992, pp. 91-102.

[8] N. Priyanatha, A. Chakraborty, H. Balakrishnan, "The Cricket Location Support System," *Proc. of MobiCom'00*, Aug. 2000, pp. 32-43.

[9] D. E. Denning, P. F. MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security," *Computer Fraud & Security*, Feb. 1996.

[10] T. Kindberg, K. Zhang, N. Shankar, "Context Authentication Using Constrained Channels", *Proc. of Fourth IEEE WMCSA*, 2002, pp. 14-21.

[11] S. Brands, D. Chaum, "Distance-Bounding Protocols," *Advances in Cryptology - EuroCrypt*, Lecture Notes in Computer Science, 1994, vol. 765/1994, pp. 344-359.

[12] N. Sastry, U. Shankar, D. Wagner, "Secure Verification of Location Claims," *Proc. of WiSe '03*, 2003.

[13] W. Luo, U. Hengartner, "VeriPlace: A Privacy-Aware Location Proof Architecture," *Proc. of 18th ACM SIGSPATIAL GIS 2010*, 2010, pp. 23-32.

[14] W. Luo, U. Hengartner, "Proving your Location without giving up your Privacy," *Proc. of HotMobile 2010*, Annapolis, MD, 2010.

[15] S. Saroiu, A. Wolman, "Enabling New Mobile Applications with Location Proofs," *Proc. of HotMobile 2009*, pp. 1-6.

[16] V. Lenders, E. Koukoumidis, P. Zhang, M. Martonosi, "Location-based Trust for Mobile User-Generated Contents: Applications, Challenges and Implementations," *Proc. of Hotmobile 2008*, 2008.

[17] A. Dua, N. Bulusu, W. Hu, W. Feng, "Towards Trustworthy Participatory Sensing," *Proc. of USENIX HotSec*, August 2009.

[18] S. Saroiu, A. Wolman, "I Am a Sensor, and I Approve This Message," *Proc. of HotMobile 2010*, pages 37-42.

[19] P. Gilbert, L. Cox, J. Jung, D. Wetherall, "Toward Trustworthy Mobile Sensing," *Proc. of HotMobile 2010*, pps. 31-36, 2010.

[20] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A. Sheth, L. Cox, "YouProve: Authenticity and Fidelity in Mobile Sensing," *ACM SenSys*, 2011.

[21] K. Zeng, K. Govindan, P. Mohapatra, "Non-cryptographic Authentication and Identification in Wireless Networks," *Wireless Communications 2010*, vol. 17, no. 5, pp. 56-62, Oct. 2010.

[22] N. Tippenhauer, C. Ppper, K. Rasmussen, S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," *Proc. of ACM CCS*, 2011.

[23] D. Faria, D. Cheriton, "No Long-term Secrets: Location Based Security in Overprovisioned Wireless LANs," *Proc. HotNets-III*, 2004.

[24] Y. Wei, K. Zeng, P. Mohapatra, "Adaptive Wireless Channel Probing for Shared Key Generation," *Proc. of IEEE Infocom 2011*, 2011.

[25] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, D. Boneh, "Location Privacy via Private Proximity Testing," *Proc. of NDSS 2011*, 2011.

[26] Y. Zhang, Z. Li, W. Trappe, "Power-Modulated Challenge-Response Schemes for Verifying Location Claims," *IEEE Globecom 2007*, 2007.

[27] M. Talasila, R. Curtmola, C. Borcea, "Location Verification through Immediate Neighbors Knowledge," *Proc. of Mobiquitous'10*, 2010.

[28] M. Kirkpatrick, E. Bertino, "Enforcing Spatial Constraints for Mobile RBAC Systems," *Proc. SACMAT'10*, 2010, pp. 99-108.

[29] R. Borgaonkar, K. Redon, J.-P. Seifert, "Experimental Analysis of the Femtocell Location Verification Techniques," *Proc. of 15th NordSec*, 2010.

[30] M. Gorlatova, R. Aiello, S. Mangold, "Managing location privacy in cellular networks with femtocell deployments," *Proc. of WiOpt'11*, 2011, pp. 418-422.

[31] K.B. Rasmussen, S. Capkun "Realization of RF distance bounding," *Proc. of 19th USENIX Security Symposium*, 2010.

[32] C. Cremers, K. B. Rasmussen, S. Capkun. "Distance Hijacking Attacks on Distance Bounding Protocols," *Cryptology ePrint Archive: Report 2011/129*, 2011.

[33] Skyhook Wireless, http://www.skyhookwireless.com/

[34] N. Tippenhauer, K. Rasmussen, C. Ppper, S. Capkun, "Attacks on Public WLAN-based Positioning," *Proc. of MobiSys'09*, 2009.

[35] LOC-AID, Inc., http://www.loc-aid.com.

[36] Veriplace, Inc., http://veriplace.com.