Managing Location Privacy in Cellular Networks with Femtocell Deployments

Maria Gorlatova*, Roberto Aiello†, Stefan Mangold*
Disney Research
*Zurich, Switzerland, †Glendale, CA, U.S.A.
mag2206@columbia.edu, [aiello,stefan]@disneyresearch.com

***Abstract*—Femtocell deployments allow for high precision in localizing mobile devices. Many of today's location based services have long been mapping the placements of wireless base stations and using the obtained maps to localize mobile devices. Allowing unauthorized third parties to obtain the locations of femtocell base stations may not be desired by network operators. Localizing mobile devices using the information about femtocell base stations' locations is a service that an investor in a femtocell deployment may want to exploit exclusively. In this work we present a station identity management system that enables preserving femtocell base stations *location privacy*. Through the use of dynamic base station identifiers, the system ensures that unauthorized third parties are not able to map the locations of the base stations for use in their localization services. We analyze the design tradeoffs of the presented approach for different femtocell technologies. Results indicate that complexity will be limited, and that the presented system creates network dynamics smaller than the existing dynamics due to mobility. Additionally, we present an approach for providing location information to authorized systems at different resolution levels.**

I. Introduction

In addition to offering technological advantages (cellular network capacity, coverage extensions and relaying in challenged environments), femtocell deployments allow for *precise fine-grained localization of mobile devices*. With femtocell-aided localization, as each femtocell base station's coverage area is small, it becomes possible to determine whether a device is inside a house, at a particular restaurant, near a specific park attraction, in a particular section of a store, or in a particular part of an office building. Femtocell-aided localization may become the preferred method of localizing devices in indoor environments, given the challenge of using GPS receivers indoors. Additionally, femtocell-based localization may be preferable over localization based on IEEE 802.11 Wi-Fi hotspots since cellular devices typically remain connected with the network at all times to be able to receive voice calls, while Wi-Fi is often turned off when not in use. Precise localization of mobile devices offers many exciting opportunities for entertainment theme parks, where users will not only be able to determine their location on a map, but will also be able to interact with entertainment attractions (e.g., play scavenger hunt games, unlock treasures) [1].

Third-party localization systems (TLSs) that map wireless base station locations and use the information later to provide devices with estimates of their positions are becoming more and more common [2]–[5]. However, severe security and privacy risks exist when unauthorized third parties are allowed to localize devices at a level of precision made possible by femtocell deployments [6]. For example, allowing third-party systems to precisely determine where devices are in an office may lead to leakage of important business information [7].

TLSs are able to localize mobile devices due to wireless base stations broadcasting their unique persistent station identifiers. In this paper we present the *Intelligent Station Identity Manager (ISIM)* system that *preserves location privacy of wireless base stations* by making their identities (W-IDs) *dynamic*. In ISIM, globally unique station identities are never shared with mobile devices or third-party systems. Instead, the wirelessly broadcasted station identifiers in ISIM are dynamic, and are changed periodically based on some policy determined by the femtocell network operator.

In conjunction with ISIM, we propose to use the *Multiple Resolution Location Generator (MRL)* module that provides authorized systems with *location information of different resolution levels*. The level of location resolution provided to a system depends on permission levels granted by the network operator. For example, the permission level could depend on the level of service a system purchased, or the type of user device (i.e., different levels of localization information are provided to users with dedicated devices and users with general-purpose smart phones or laptops).

In this paper we focus on *3GPP Long Term Evolution (LTE)* [8] and *WiMAX IEEE 802.16* [9] femtocells. However, the developed approach could be applied to other femtocell technologies (i.e., CDMA2000 or TD-SCDMA femtocells), as well as to *Wi-Fi IEEE 802.11* hotspots [10]. In Section II we review today's third-party location services and discuss the related work. Section III discusses the Intelligent Station Identity Manager (ISIM), and Section IV briefly presents the Multiple Resolution Location Generator (MRL). Section V summarizes and concludes the paper.

II. Today's Location Services and Related Work

Providing localization services for mobile devices is a well-developed research area [11]. Current third-party location services (i.e., [2]–[5]) localize mobile devices based on pre-mapped positions of cellular towers and Wi-Fi base stations. The TLS operation can be described as the following process. First, a device capable of localizing itself (i.e., a GPS-enabled device) surveys an area, recording base station identifiers it

978-1-61284-824-2/11/$26.00 ©2011 IEEE

TABLE I
NOMENCLATURE.

f_j^*	Permanent station ID of femtocell base station j
W-ID(f_j^*, t_i)	Dynamic station ID of base station j at time t_i
K	Total number of distinct W-IDs possible
λ_{ch}	Rate of W-ID changes $[1/h]$
t_{ch}	Time a W-ID change takes $[s]$
N_{nbr}	Number of base stations in a neighborhood
L	Number of stations synchronously changing their W-IDs
f_{em}^L	Fraction of time L base stations do not have calls in progress
$\lambda_{\text{hoff,c}}$	Handoff rate induced by ISIM $[1/h]$
$\lambda_{\text{hoff,m}}$	Handoff rate induced by device mobility $[1/h]$
P_T	Probability of a W-ID collision in interval T
λ_{call}	Femtocell base station call arrival rate $[1/h]$
h_{call}	Average call duration $[h]$
A	Femtocell coverage area $[m^2]$
d_{dev}	Distance a mobile device travels inside a femtocell $[m]$
v_{dev}	Average speed of a mobile device $[m/s]$
c_{dev}	Concentration of mobile devices $[1/m^2]$
f_{loc}	Fraction of mobile devices that report base station locations to a TLS
T_{loc}	Time until arrival of a mobile device that reports base station locations to a TLS
F	Total number of base stations running ISIM

overhears (wireless base station ID, W-ID), and its estimates of the base stations' locations [12], [13]. The location information captured by the device is recorded in a centralized TLS database (similar to, for example, [14], [15]). Later on, mobile devices that want to localize themselves submit the W-IDs they overhear to the database, get back the locations of the corresponding base stations, and localize themselves based on this data [16], [17]. Security measures that prevent unauthorized users from accessing the network, such as Closed Subscriber Groups [8], do not prevent such localization, as they do not prevent devices from receiving base stations' broadcasts containing their identity information. This approach to localization works as long as unique and persistent W-IDs are transmitted by base stations (femtocell base stations, cell towers, Wi-Fi hotspots, etc).

Current research in preserving location privacy focuses on location privacy of *mobile devices* rather than *base stations' location privacy* examined in this work. For *mobile devices*, dynamic identifiers (pseudonyms) in Wi-Fi [18], [19], and in vehicular networks [20], [21] have previously been examined. Additional related research includes examinations of TLS compromises [16] and security considerations for device-to-TLS-database communications [22].

Finally, we note that unlike traditional cellular towers that are configured by cellular operators, femtocell base stations require more flexibility and are more dynamic. For example, for LTE femtocells several adaptive physical cell identity (PCI) assignment schemes have been proposed [23], [24]. Enabling automatic and adaptive femtocell base station configuration can be seen as a first step towards enabling the dynamic station W-ID assignment scheme proposed in this paper.

III. INTELLIGENT STATION IDENTITY MANAGER (ISIM)

The *Intelligent Station Identity Manager* (*ISIM*) module protects femtocell base stations' location privacy by *making wirelessly transmitted base station identifiers (W-IDs) dynamic*. In this section we discuss the ISIM design and associated tradeoffs. The key notation used throughout this paper is summarized in Table I.

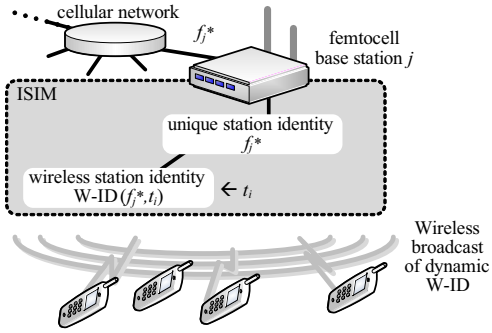


Fig. 1. A schematic diagram of the Intelligent Station Identity Manager (ISIM). A femtocell base station j has a unique ID f_j^* that it uses in communication with the rest of the cellular network. Base station j's *wirelessly broadcasted* identifier is a dynamic, time-dependent entity W-ID(f_j^*, t_i).

ISIM structure is shown schematically in Fig. 1. Each femtocell base station j has a unique ID, f_j^*. The f_j^* is used in base station j communications with the rest of the cellular network (macrocell, gateways, etc.). However, f_j^* is *never revealed to mobile devices*. Instead, each femtocell base station's wirelessly broadcasted identifier (*femtocell W-ID*) is a *dynamic*, time-dependent entity W-ID(f_j^*, t_i), where t_i denotes the time instance.[1] The dynamically generated W-IDs follow the femtocell technology (*LTE*, *WiMAX*, etc.) specifications. In the technologies we consider, the wirelessly broadcasted information that identifies a station is as follows:

- *W-CDMA/LTE*: a base station has a globally unique *Cell Global Identity (CGI)*. A CGI consists of a set of codes identifying the network area, and also includes a 16 bit Cell Identity code that we can modify. In addition, in *LTE* the cell can be identified by a locally unique *Physical Cell Identity* (*PCI*). LTE allows for only 504 PCIs [8].
- *IEEE 802.16 (WiMAX)*: a base station has a 48 bit *base station ID (BSID)* where 24 bits indicate the station operator and the remaining 24 bits can be modified [9].

We denote by K the number of different W-IDs possible for a particular technology (*W-ID selection space*). Thus in cellular systems K is upper-bounded by 2^{16}, and in WiMAX maximal K is 2^{24}.

W-ID changes are performed with a target nominal changeover rate λ_{ch}. When a femtocell base station changes its W-ID, it disconnects its mobile clients and becomes temporarily unavailable. We denote the time it takes a femtocell base station to complete a W-ID change by t_{ch}. We denote the number of base stations in a neighborhood by N_{nbr}. We use L to denote the number of base stations simultaneously changing their W-IDs, and f_{em}^L to denote the fraction of time the L base stations do not have calls in progress. We denote the rate of

[1]Note that the base station ID visible to the rest of the network, f_j^*, does not change with time. Thus, ISIM does not require modifications to the overall network architecture. For example, *cellular operator-side* positioning services, such as E911 services, are not affected by ISIM.

handoffs due to W-ID changes and due to mobility by $\lambda_{\text{hoff,c}}$ and $\lambda_{\text{hoff,m}}$, respectively. In Section III-A we comment on the effect of ISIM on femtocell base stations' performance.

A W-ID change can be initiated by a base station itself, or by a controller with a more global knowledge. We use P_T to denote the probability of a *W-ID collision* in a time interval T. In Section III-B we comment on distributed versus centralized W-ID selection schemes.

We denote the average femtocell call arrival rate by λ_{call}, and the average call duration by h_{call}. The area covered by a femtocell base station is denoted by A. The average distance a mobile device moves inside a femtocell base station coverage area is denoted by d_{dev}. We use v_{dev} and c_{dev} to denote, respectively, the speed and the concentration of mobile devices. In numerical results, we use $d_{\text{dev}} = 10m$ (a small femtocell), $v_{\text{dev}} = 1.5km/h$ (very slow walking), and $A = 100m^2$. We expect *femtocell base stations to be associated with many mobile devices, but to be relatively lightly loaded with traffic*. This is a reasonable assumption for many public environments, such as stadiums or entertainment parks [1].

We use f_{loc} to denote the fraction of mobile devices that update the TLS database with W-ID-to-location mappings, and let T_{loc} denote the time until the first arrival of such mobile device to a femtocell. We use F to denote the overall number of femtocell base stations whose identifiers are reported to the TLS database. In Section III-C we discuss ISIM's effect on the operation of TLSs. Additional considerations are discussed in Section III-D.

A. ISIM effect on Femtocell System Performance

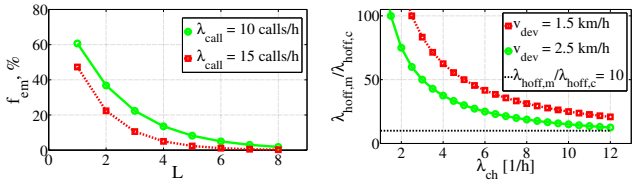
In general, femtocell base stations performing W-ID changes affects system performance.[2] It should be noted, however, that W-ID changes *only affect femtocell base stations' wireless interfaces*. During W-ID changes, mobile clients can connect to a macrocell whose functionality is not affected. The femtocell base station connection with the rest of the cellular operator network is also not affected.

1) Calls not serviced: The number of calls not serviced due to a base station changing its W-ID is simply $\lambda_{\text{call}} \cdot t_{\text{ch}} \cdot \lambda_{\text{ch}}$. This indicates that t_{ch} should be kept short if relatively frequent W-ID changes are desired. For a lightly loaded system (small λ_{call}), the femtocell base station inaccessibility associated with W-ID changes should not be significant, particularly since mobile devices are serviced by a macrocell while a femtocell is temporarily unaccessible.

2) Disruptions to calls in progress: W-ID changes should be conducted without disrupting calls in progress, if possible. We refer to λ_{ch} as the target W-ID change rate since the W-ID change is not necessarily performed at the exact $1/\lambda_{\text{ch}}$ intervals; rather, the base stations may wait until they have no calls in progress to change their W-IDs. Assume each base station can simultaneously maintain k calls. The expected fraction of time that L base stations do not have calls in progress, f_{em}^L, can be approximated, using standard M/M/k queue calculations, as

$$f_{\text{em}}^L = \left(\sum_{n=0}^{k} \frac{1}{n!} \left(\frac{\lambda_{\text{call}}}{1/h_{\text{call}}} \right)^n \right)^{-L}.$$

The f_{em}^L value is demonstrated in Fig. 2(a) as a function of the number of base stations L. It can be observed that when L is relatively small, the expected fraction of time the base stations do not have calls in progress is relatively high, and thus it should be generally possible to not disrupt the mobile devices' calls to change the base stations' W-IDs.



(a) (b)

Fig. 2. ISIM and femtocell system performance: (a) the percentage of time femtocell base stations do not have calls in progress, as a function of the number of stations, and (b) the ratio of handoffs introduced due to mobility, $\lambda_{\text{hoff,m}}$, to the handoffs introduced by W-ID changes, $\lambda_{\text{hoff,c}}$.

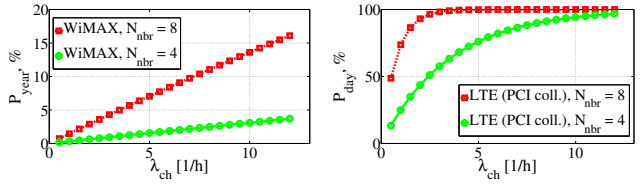
3) Handoffs introduced by W-ID changes: When a femtocell base station performs a W-ID change, the devices within its coverage area that have calls in progress have to handoff. In many practical environments, however, the *number of handoffs due to mobility is substantially higher than the number of handoffs introduced by ISIM*. We can demonstrate that the ratio of handoffs due to mobility and handoffs due to W-ID changes, $\lambda_{\text{hoff,m}}/\lambda_{\text{hoff,c}}$, is equal to $(v_{\text{dev}}/d_{\text{dev}})/\lambda_{\text{ch}}$. Fig. 2(b) shows the $\lambda_{\text{hoff,m}}/\lambda_{\text{hoff,c}}$ ratio as a function of λ_{ch} for two different values of average mobile device speed v_{dev}. It can be observed that handoffs due to mobility greatly exceed handoffs due to W-ID changes. Even for relatively frequent W-ID changes (10-12 times per hour), $\lambda_{\text{hoff,m}}$ is over 10 times greater than $\lambda_{\text{hoff,c}}$.

B. W-ID Selection Schemes: Centralized and Distributed

For each time interval t_i, W-ID(f_j^*, t_i) can be set by the femtocell base station j itself, or by a control station (*distributed* or *centralized* W-ID selection). A *W-ID collision* happens when more than one base station j in a neighborhood uses the same W-ID(f_j^*, t_i) for the same t_i. Some of base station identifiers we modify, such as GCIs and MAC addresses, are considered by the protocols to be fixed and unique, and collisions between them are highly undesirable [18]. For others, such as LTE PCIs, collision alleviation mechanisms exist, but nonetheless it is preferable to avoid collisions [24]. Collisions are easily avoided with a centralized mechanism, but are possible with distributed assignments.

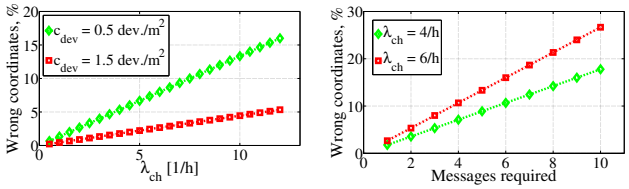
The W-ID collision probability can be upper-bounded as follows. Suppose each station chooses its W-ID in a purely random fashion. The probability of a W-ID collision during a time interval T, P_T, can be obtained using *birthday paradox*

[2]In certain scenarios W-ID changes can be performed without any disruptions to mobile devices. In an entertainment park, for example, once-daily W-ID changes can be conducted during off-business hours.



(a) (b)

Fig. 3. Probability of a W-ID collision P_T for W-IDs randomly chosen by stations: (a) for *a year* for IEEE 802.16 BSIDs, and (b) for *a day* for LTE PCIs.



(a) (b)

Fig. 4. Percentage of devices receiving wrong location information from a TLS: (a) for a TLS database updated based on a single W-ID-to-coordinates report, and (b) as a function of the number of W-ID-to-coordinates reports required by the TLS.

calculations [18]:

$$P_T = 1-(1-p_c)^{T\cdot\lambda_{\text{ch}}}, \text{where } p_c = 1-\left(\frac{K-1}{K}\right)^{\frac{N_{\text{nbr}}\cdot(N_{\text{nbr}}-1)}{2}}.$$

As previously noted, K, the W-ID selection space, depends on the femtocell technology. For different technologies, P_T differs drastically. For example, Fig. 3(a) demonstrates P_T values for IEEE 802.16 BSIDs ($K = 2^{24}$) for $T = year$, while Fig. 3(b) demonstrates P_T for LTE PCI ($K = 504$) for $T = day$. It can be observed that the probabilities of W-ID collisions are high for LTE PCIs and low for IEEE 802.16 BSIDs. Thus for IEEE 802.16 simple decentralized BSID assignment schemes can be used, while for LTE coordinated PCI assignments are preferable.

Where decentralized assignments are suitable, stations can, for example, use cryptographic hash functions [18] to independently generate their W-IDs. Simple algorithmic improvements (i.e., considering W-IDs of neighboring stations) may reduce the number of W-ID collisions relative to the above-stated upper bounds. More involved distributed assignment algorithms, such as those based on graph coloring [24], could also be considered.

C. ISIM Effects on the Performance of Third-Party Localization Systems (TLSs)

Third-party localization systems record in a centralized database W-ID-to-locations mappings obtained and provided by mobile devices, and look up the mappings when localizing a mobile device based on W-IDs it overhears. Below we provide some insights into ISIM's disruption of TLS operations.

1) TLS database integrity: When *dynamic W-IDs* are reported to a TLS's centralized database, database integrity becomes difficult to preserve. When ISIM is in use, *in-database W-ID collisions* are a major issue for a centralized TLS database. For the femtocell system, W-ID collisions are 'local', and their probabilities are relatively small due to a relatively small number of neighboring stations N_{nbr}. When locations and W-IDs of F different femtocell stations (where $F \gg N_{\text{nbr}}$) are aggregated, the probability of a W-ID collision in an interval T is

$$P_T = 1-\left(\frac{K-1}{K}\right)^{\frac{T\cdot\lambda_{\text{ch}}\cdot F(T\cdot\lambda_{\text{ch}}\cdot F-1)}{2}},$$

which is generally high since the number of possibly colliding entries, $T\cdot\lambda_{\text{ch}}\cdot F$, is large. For example, for $F = 100$ and $\lambda_{\text{ch}} = 4$, $P_T > 99\%$ when T is just an hour.

2) TLSs providing correct location information: Typically, a TLS needs to obtain several W-ID-to-location reports from mobile devices before it updates its database with a W-ID-to-location mapping [16]. Assume that a TLS database is updated after *a single mobile device* reports an updated W-ID-to-location mapping. It can be demonstrated that the expected time until the TLS entry is updated is $\mathbb{E}(T_{\text{loc}}) = [d_{\text{dev}}/v_{\text{dev}}]/[f_{\text{loc}}\cdot c_{\text{dev}}\cdot A]$. Prior to T_{loc}, all mobile devices that request location information from a TLS receive grossly incorrect information. The number of the devices that receive incorrect location information after a W-ID change is $1/f_{\text{loc}}$, and their percentage is demonstrated in Fig. 4(a) for $f_{\text{loc}} = 1\%$ for two different values of device concentration c_{dev}. It can be observed that a substantial percentage of devices relying on a TLS obtain incorrect location information (which is desired in our case) when W-ID change is performed as unfrequently as four to six times per hour. The percentage of devices receiving incorrect information, for a more practical case of a TLS requiring more than one report prior to updating its database, is demonstrated in Fig. 4(b). It can be observed that the percentage of devices receiving wrong information grows with the number of measurements required by the TLS.

D. Additional Considerations

A stationary device positioned next to a femtocell base station is able to observe, at all times, the W-IDs the base station uses. In the environments we consider, mobile devices are *transient*, and each is able to observe only a few W-IDs.

Parameters other than W-IDs, such as radio-frequency (RF) signatures, may allow identifying femtocell signal's base station of origin. RF signature-based base station identifications are resource-intensive and may require specialized hardware [16]. Additionally, their relatively low reliability (rates of false-positive and false-negative identifications) makes them poorly fitted for a centralized database-based look-ups.

IV. Multi-Resolution Location Generator (MRL)

ISIM prevents unauthorized parties from obtaining base station location information. With the *Multi-Resolution Location Generator* (*MRL*), the location information is provided to authorized parties. In MRL, femtocell base station location is broadcasted wirelessly throughout the femtocell at multiple resolution levels, all at the same time, as shown schematically in Fig. 5. Each femtocell base station specifies its location

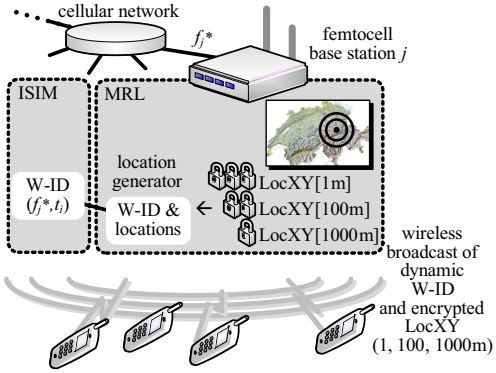


Fig. 5. A schematic diagram of *Multi-Resolution Location Generator* (*MRL*). Femtocell base station broadcasts its location information, at different resolution levels simultaneously, with the information at different resolution levels separately encrypted.

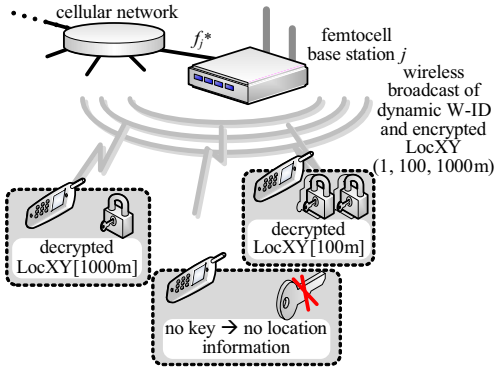


Fig. 6. Encryption use in MRL. Each mobile device decrypts the location information its permission levels allow it to access.

with several levels of precision, and separately encrypts each of the specified resolution levels. Fig. 6 demonstrates how mobile devices use the broadcasted information to localize themselves. Each device decrypts the location information corresponding to its permission level.

The design parameters in MRL are the number of supported resolutions and area specifications, which depend on technical parameters (for example, system complexity and base station locations), as well as business needs. Using MRL to provide location information is only reasonable when the previously described ISIM module is used to preserve the location privacy of the femtocell base stations. The combination of MRL and ISIM gives operators the full control to manage location privacy in cellular networks with femtocell deployments.

V. Summary and Conclusions

In this paper we introduced a novel system that allows network operators to fully control the usage of their base station's locations by location based services. We highlighted the security and privacy risks associated with the current open provision of base station identifiers. We proposed an *Intelligent Station Identity Manager (ISIM)* system that preserves the location privacy of femtocell base stations by making the broadcasted station identifiers *dynamic*. We highlighted and analyzed the design tradeoffs associated with ISIM, and argued that for relatively lightly loaded public femtocells the implementation of dynamic station identifiers does not severely degrade network performance. In addition, we presented a *Multi-Resolution Location Generator (MRL)* module that communicates the femtocell base station locations to authorized systems at resolution levels corresponding to systems' permission levels. The combination of the presented ISIM and MRL modules enable network and venue operators to control the use of their assets by systems providing location based services. We expect that infrastructure owners and network and hotspot operators can benefit from the approach presented in this paper.

References

[1] K. Collins, S. Mangold, and G.-M. Muntean, "Supporting mobile devices with wireless LAN/MAN in large controlled environments," *IEEE Commun. Mag.*, vol. 48, no. 12, pp. 36–43, Dec. 2010.

[2] "Skyhook Wireless," www.skyhookwireless.com.

[3] "Google My Location," googlemobile.blogspot.com/2007/11/new-magical-blue-circle-on-your-map.html.

[4] "Apple location services," support.apple.com/kb/HT1975.

[5] "Navizon," www.navizon.com.

[6] I. Bilogrevic, M. Jadliwala, and J. Hubaux, "Security issues in next generation mobile networks: LTE and femtocells," in *Proc. 2nd International Workshop on Femtocells*, June 2010.

[7] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," *IEEE Computer*, vol. 36, no. 12, pp. 135–137, Dec. 2003.

[8] "3GPP TS 22.220 V11.0.0 (2010-01) Technical Specification: Service requirements for Home Node B (HNB) and Home eNode B (HeNB)," www.3gpp.org/ftp/specs/html-info/22220.htm, 2010.

[9] "IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005," standards.ieee.org/getieee802/download/802.16e-2005.pdf, 2006.

[10] "IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)," standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[11] A. Smith, H. Balakrishnan, M. Goraczko, and N. Priyantha, "Tracking moving devices with the cricket location system," in *Proc. ACM MobiSys'04*, June 2004.

[12] J. Yang, A. Varshavsky, H. Liu, Y. Chen, and M. Gruteser, "Accuracy characterization of cell tower localization," in *Proc. ACM Ubicomp'10*, Sept. 2010.

[13] A. Subramanian, P. Deshpande, J. Gaojgao, and S. Das, "Drive-by localization of roadside WiFi networks," in *Proc. IEEE INFOCOM'08*, Apr. 2008.

[14] "Wireless geographic logging engine (WiGLE)," wigle.net.

[15] "Opencellid," www.opencellid.org.

[16] N. Tippenhauer, K. Rasmussen, C. Popper, and S. Čapkun, "Attacks on public WLAN-based positioning systems," in *Proc. ACM MobiSys'09*, June 2009.

[17] M. Kim, J. Fielding, and D. Kotz, "Risks of using AP locations discovered through war driving," *Pervasive Computing*, vol. 3968, pp. 67–82, 2006.

[18] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," *Kluwer J. Mob. Netw. and Appl.*, vol. 10, pp. 315–325, June 2005.

[19] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proc. ACM MobiSys'07*, June 2007.

[20] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of anonymity in VANETs - putting pseudonymity into practice," in *Proc. IEEE WCNC'07*, Mar. 2007.

[21] J. Freudiger, M. Manshaei, J. Le Boudec, and J. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in *Proc. IEEE INFOCOM'10*, Mar. 2010.

[22] K. P. N. Puttaswamy and B. Y. Zhao, "Preserving privacy in location-based mobile social applications," in *Proc. HotMobile'10*, Feb. 2010.

[23] G. De La Roche, A. Valcarce, D. Lopez-Perez, and J. Zhang, "Access control mechanisms for femtocells," *IEEE Commun. Mag.*, vol. 48, no. 1, pp. 33–39, Jan. 2010.

[24] T. Bandh, G. Carle, and H. Sanneck, "Graph coloring based physical-cell-ID assignment for LTE networks," in *Proc. IEEE IWCMC'09*, June 2009.