CallForge: Call Anonymity in Cellular Networks

Sebastian Kay Belle
University of Konstanz
Konstanz, Germany
sebastian.belle@uni-konstanz.de

Oliver Haase
Konstanz University of Applied Sciences
Konstanz, Germany
haase@htwg-konstanz.de

Marcel Waldvogel
University of Konstanz
Konstanz, Germany
marcel.waldvogel@uni-konstanz.de

ABSTRACT

In cellular networks, the locations of all subscribers are continously tracked even when they only passively carry their mobile devices with them. This privacy sensitive data can be an invaluable source of information, not only for benevolent parties. We therefore present CallForge, the concept of a location management scheme that preserves the subscribers' anonymity – in many cases even while they participate in a phone call – as well as a theoretical analysis of the approach. CallForge improves on PathForge, a previously presented location management scheme, and as such is based on ID switching that we have combined with the emulation of a media break within a single call set-up procedure. We have analyzed and compared the anonymity of PathForge and CallForges, and shown that CallForge consistently provides superior anonymity. Callforge can be implemented entirely in the end device and run on existing network infrastructure without any modifications.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*; C.2.4 [**Computer-Communication Networks**]: Distributed Systems; K.4.1 [**Computer and Society**]: Public Policy Issues—*Privacy*

General Terms

Location Anonymity, Cellular Networks

1. INTRODUCTION

Thanks to the enormous advancement of network and handheld technologies, we are nowadays in the convenient position to access the Internet from nearly anywhere as long as our mobile phone is connected to the provider's cell phone network. We can browse the Web, write emails and other types of text message, or simply place and receive phone calls. Moreover, *location-based services* (LBS)[13] disclose a multitude of possibilities to facilitate powerful applications that make life easier or safer.

Though, this ubiquitous connectivity comes at a price: Users are continuously tracked by their service providers. The scientific community presented several approaches to preserve the anonymity of users in LBS using either techniques based on *centralized spatial cloaking* [5, 8, 9], or on *decentralized spatial cloaking*, [4, 6], respectively. Nevertheless, these techniques are specialized in that their targeted area of application is limited to LBS and is not transferable to cellular networks in general. The reason for this is that a cellular provider must be able to connect calls to their mobile subscribers, and therefore – to prevent paging the complete network –, the network tracks and stores everyone's location information, even when they only passively carry their mobile devices with them. It is clear that access to this privacy sensitive data by a third party could be of great value, e.g. for personal preferences profiling and marketing, to give an example from the comparably harmless end of the spectrum. What makes things even worse – from the privacy perspective – is that Krumm and Horvitz [10] have shown that destinations of people can be extrapolated with a high probability given only a part of their path, even if the person has never visited the destination before. Their results show a median prediction error of a destination estimation that comes close to three kilometers after a trip fraction of 0.5 for the *open-world model*. Simplified, tracking a person for about half of their trip is enough to get a good estimation about their potentially sensitive destination.

Cellular network providers are generally well established, trust-worthy entities. What we are concerned about is that possessing large amounts of highly valuable, private data about their suscribers makes them worthwhile targets for burglary and theft, blackmailing, and similar criminal activities from both inside and outside. Rather than protecting the data, which is expensive and never absolutely secure, we advocate to "break-up" the link between a user and the information collected about her. Of course, this requires a novel location management scheme that works on anonymous location data, and that provides the same service with the same degree of scalability. It is often argued that location information can also be of great value for law enforcement agencies, in particular to fight organized crime and terrorism. Finding the right balance between security and privacy is far from being easy; undoubtedly, within the last decade there has been a clear shift towards less privacy, i.e. more and more access to private information by the law enforcement authorities, for the sake of supposedly higher security [12, 17].

However, a pending lawsuit filed with the German Constitutional Court[1] against telecommunication data retention[18] presents evidence that the impact of data retention does not result a significant increase in the prevention or solution rate

[1]The German Constitutional Court lately acceded this lawsuit and enacted that the act on telecommunication data retention is unconstitutional.

Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
May 17, 2010, Helsinki, Finland

of criminal activity in that governments want us to believe when giving up more and more of our privacy.

Li et al. [11] observed the relevance of location anonymity – specifically in the context of the ubiquitous connectivity we have nowadays – and proposed an interesting approach to disguise the location of users in a wireless local area network (WLAN). The idea of Li et al. is based on cooperating nodes that exchange their IDs based on a public/private keys and an authentication authority. They assume that every user that participates in the ID exchange protocol enters a contractual agreement with a trusted third party that maintains a authentication server to validate the IDs of the exchanging users. However, Li et al. state that their ID exchange protocol is less suited to mobile networks due to the requirements of the ID validation process with the authentication server.

Similar to Li et al. [2, 3] propose an approach to design a location management scheme, called PathForge, that keeps the whereabouts of the mobile subscribers anonymous as long as they remain passive[2]. Though, in contrast to Li et al., [2, 3] aim to provide location anonymity in cellular networks[3] instead of a WLAN. PathForge can provide this increased level of location anonymity without compromising the signaling performance of the cellular network. With PathForge, however, the anonymity of a subscriber gets temporarily lost when the service provider has to route a call (or more general, any kind of data) to their location. Another drawback of PathForge is that it requires (minor) modifications of the network infrastructure and signaling protocols.

In this paper we present CallForge, a novel location management approach based on PathForge that is superior to the later in two regards: (1) CallForge can keep the subscribers' location information anonymous not only when they are passive, *but, in many cases even when they are actively communicating*. The basic idea behind CallForge is to emulate a media break in the call set-up procedure that makes a single call set-up look like two independent calls to the service provider, each of which by itself does not reveal the true location of the callee, or the callee's identity, respectively. (2) CallForge can be implemented entirely on the mobile devices without requiring any modifications of network equipment or protocols. This is a huge advantage from a practical standpoint, because mobile devices are cheap and programmable, and they follow a very fast innovation cycle. Furthermore, the later also eliminates the necessity of a trusted third party as ID exchange takes place on a user-to-user level instead.

Additionally, for a theoretical evaluation and comparison of CallForge with PathForge, we define the anonymity that a cellular network – or a location management scheme for that matter – provides in a quantitative manner. Our comparative analysis illustrates how an increasing call volume in a cellular network also increases the location anonymity of its subscribers. It also shows that even in the worst case, that is with very little call volume in the network, CallForge still consistently provides a better anonymity than

[2]In this context, passive denotes users that do not actively initiate (or accept) a data exchange.

[3]Cellular networks are mobile networks that constitute the most ubiquitous devices we use today, namely mobile-/smart-phones.

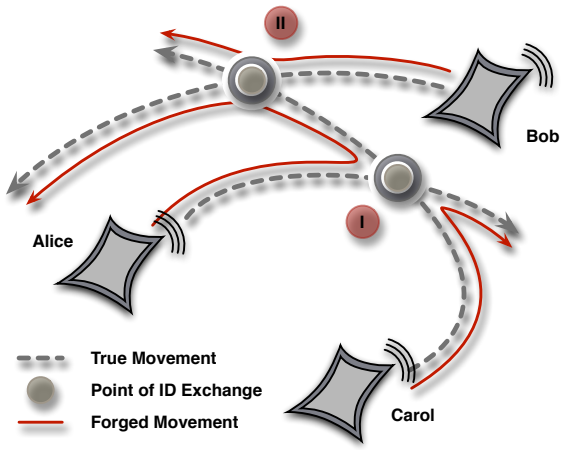


Figure 1: Identity switching in PathForge. ID switching takes place at I and II, respectively.

PathForge, not to mention the location management used in today's cellular networks. CallForge, albeit having very interesting properties, is a concept at this point, and further research, prototypical implementations, and simulations will be needed. However, this paper aims at soliciting feedback from the community at this conceptual stage because of the relevance of the topic on a social and political level. The resonance on PathForge in the non-scientific public, see, e.g., [15, 14], indicates that there exists a good deal of public interest in privacy issues related to location tracking. This interest has encouraged us not only to further improve the privacy level, but to also invent a scheme that can be implemented entirely in the mobile devices, atop existing network infrastructure.

The rest of this paper is organized as follows: In Sec. 2, we introduce the threat and the trust models that underlay our approaches. In Sec. 3, we revisit the PathForge location management scheme that is the basis for our new CallForge approach, that in turn, is introduced in Sec. 4. Sec. 5 contains the comparative analysis of the anonymity of PathForge and CallForge, and Sec. 6 finally concludes the paper with an outlook on future work.

2. THREAT & TRUST MODELS

Threat Model. The anonymity considerations in the following sections are based on three different threat models that differ in the extent to which the service provider is considered a potential information leak, or – through manipulation, sabotage, or burglary – even an entity that actively undermines the subscribers' location anonymity:

- *Misuse of existing information*: This threat model is meant for theft and misuse of information that has been collected during normal operation. The assumption is that a malicious party gets access to the service provider's information base – e.g. the Home Location Register (HLR) or the Customer Relationship Management (CRM) system – but cannot manipulate

the information collecting process itself. Note, this threat model is similar to the *Global Passive Adversary* (GPA) as described in [11].

- *Information inference*: The service provider – or a malicious party acting on its behalf – uses the regularly collected information to infer additional, privacy sensitive information that is not needed to provide the service, and this information gets stolen. The difference between this threat model and the previous one is that the additional information cannot be reconstructed in retrospective, but only during normal operation.
- *Active probing*: The service provider – or a malicious party acting on its behalf – actively collects privacy sensitive data, .e.g by acting as a subscriber who uses the regular call set-up process to determine the location of the callee. This threat model is meant for scenarios when the service provider is manipulated — most likely from the inside – and does not follow the normal protocol. Note, this threat model is similar to the *Local Active Adversary* (LAA) as described in [11]. We agree with Li et al. that active probing is the most severe threat model as it is equivalent to physical pursuit of the targeted user.

Trust Model. Both PathForge and CallForge are based on the idea that subscribers swap their identities when the come into close proximity. For close proximity ID exchange we consider to utilize Bluetooth, or, if available, a wireless network access point. This ID swapping requires each party to trust the other one to run the correct protocols and procedures on their end device, and not to misuse the borrowed ID.

At first, this is an obvious vulnerability – at least from a social point of view – as entities that utilize this exchange protocol rather need to trust each other instead of the service provider. It is arguable which party, the service provider, or the users are the more trustworthy entities in the network. We follow the argumentation of Bruce Schneier [16] that the probability that a "stranger" – in our case any other user in the network that runs the proposed exchange protocol – is a malicious node is by magnitudes less than the probability to exchange IDs with a trustworthy "stranger". On a technical level, this trust relationship can be established through a bilateral authentication process that ensures that the other handset runs the required, pre-certified software, and that this software has not been tampered with.

3. PATHFORGE REVISITED

In [2, 3] the authors proposed PathForge, an anonymization technique to disguise the movement data that can be obtained by mobile service providers or malicious partys in a cellular network. As CallForge extends this idea, it is necessary to understand the basic idea of PathForge.

The key idea behind PathForge is best explained as follows: Each subscriber u registers with two IDs, in two separate registration processes that the service provider cannot associate with each other. The first ID – the so-called proxy ID I_u^P – is fix and denotes the subscriber u. This ID is switched

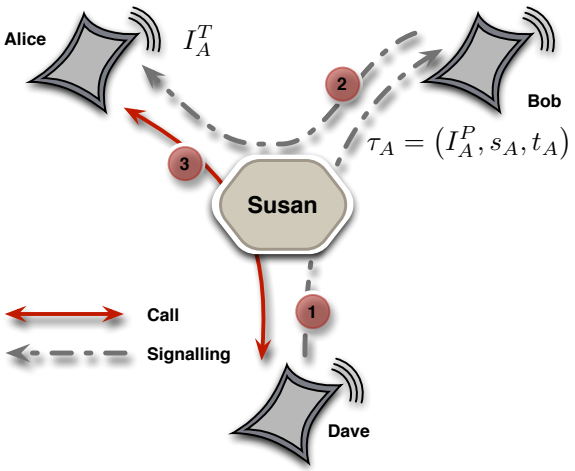


Figure 2: Call setup in PathForge. The depicted call setup procedure takes places after ID switching at point II in Fig. 1.

between subscribers when they come into each other's vicinity[4]. We emphasize that ID switching can happen multiple times along the path of a user. The second ID is a temporary ID I_u^T that keeps changing according to a predefined scheme. For all registrations, the own temporary ID and the acquired proxy ID will be used. Therefore, as long as the subscriber remains passive, the service provider, Susan, cannot associate neither the proxy ID nor the temporary ID with the subscriber.

The computation of the temporary ID involves a *pseudo-random number generator* (PRNG) and an individual seed s_u. The PRNG, initialized with s_u, is used to generate I_u^T, as well as the time intervals this temporary ID is valid for as

$$I_u^T = h(I_u^P || r_i), \text{ with } t_u + \sum_{j=0}^{i-1} r_j < t_{sys}, \quad (1)$$

where $h()$ denotes a one-way hash function[5], r_i is a number obtained from the PRNG, t_u is the time at which the user exchanged his proxy ID for the first time, and t_{sys} is the current system time. By exchanging not only I_u^P between users, but, a triple $\tau_u = (I_u^P, s_u, t_u)$ every user that carries τ_u is able to compute the actual temporary ID I_u^T of the user. Note, $t_u = \emptyset$ before the initial exchange of τ_u.

Fig.1 depicts three users in the system, Alice (with $\tau_A = (I_A^P, s_A, t_A)$), Bob (with $\tau_B = (I_B^P, s_B, t_B)$), and Carol (with $\tau_C = (I_C^P, s_C, t_C)$) that switch their triples along their movement path at the locations highlighted by the roman literals I and II. After I Alice and Carol will carry the triple $\tau_C = (I_C^P, s_C, t_C)$ and $\tau_A = (I_A^P, s_A, t_A)$, respectively, with $t_C, t_A =$ I. Subsequently, Alice and Carol will use their

[4]E.g. they come within Bluetooth range
[5]E.g. a hash function from the *Secure Hash Algorithm* (SHA) family

newly acquired proxy IDs to register with Susan. As identity switching in PathForge can happen multiple times along the movement path, a user may consecutively identify herself with new IDs over time. Consider the state in Fig.1 at **II**. Carol switches her (actual) triple τ_A again, this time with Bob's triple τ_B who initializes $t_B = \mathsf{II}$ before the exchange takes place. Due to this (multiple) ID switching the location of a user in the network can no longer be correlated with the ID of the user as long as the user stays passive, that is, as long as neither the user nor another person initiates a call from/to the user's phone.

To complete the running example, consider a call from Dave to Alice that takes place after **II**, as shown in Fig.2. Dave signals a call set-up request for I_A^P to Susan at step **1**. Because at this point, Bob has registered with I_A^P, the call request reaches Bob rather than Alice. Bob therefore replies Alice's temporary ID I_A^T – that he can compute according to Equ.(1) – to Susan (step **2**, first part). Susan redirects the call set-up signalling, contacting Alice at her temporary ID I_A^T that she got from Bob (step **2**, second part) and finally establish a media connection between Dave and Alice (step **3**). Please note that it is only now that Susan can associate Alice's temporary ID with the person Alice.

Obviously, the true identities of Bob and Alice will be revealed in this process. Assuming the *Misuse of existing information* threat model, this happens each time a call is set up. In the case of the *Active probing* threat model, however, the service provide, Susan, could at any point in time play the role of a caller and continously reveal each subscriber's location. She would not even have to complete the call but would only need Bob's reply to her attempt to reach Alice. The *Information inference* threat model, finally, is not applicable for PathForge, because there is no additional location information that Susan could infer from what she automatically learns through the call set-up processes.

4. CALLFORGE

With PathForge, the movement and the location of a subscriber can be kept anonymous, as long as they remain passive, i.e. neither initiate or receive a call. In CallForge we extend this idea to stay anonymous even when placing and receiving a call. The idea is based on using two distinct SIM cards in a mobile device[6]. Basically, this dual SIM card approach enables us to (1) simulate a media break in the same communication technology, and (2) solves the reasonable question of accountability when introducing ID switching. Again, we emphasize that due to multiple ID switching an eavesdropping party never knows if the ID it received from an exchange is the "real" ID of the exchanging user or if it is actually the ID of a third user in the network. Combining multiple ID switching with the ability to stay anonymous during a call setup, the probability of an eavesdropping entity in the network decreases according to the time a user participates in the ID switching process and the average number of other entities in the vicinity of the user.

Building upon PathForge, we assign the two distinct IDs introduced with PathForge to either of the SIM cards. Thus, a user u now has I_u^P assigned to his first SIM card u', and I_u^T assigned to his second SIM card u'', respectively. To preserve a callers anonymity we assume that the second SIM is charged with prepaid minutes to initiate outgoing calls as this basically eliminates the necessity of the service provider to correlate the caller with a registered subscriber in the network. Though, prepaid accounts imply restrictions on the flexibility in terms of the user's calling behaviour, we believe that a gain in privacy countervails this lag in flexibility.

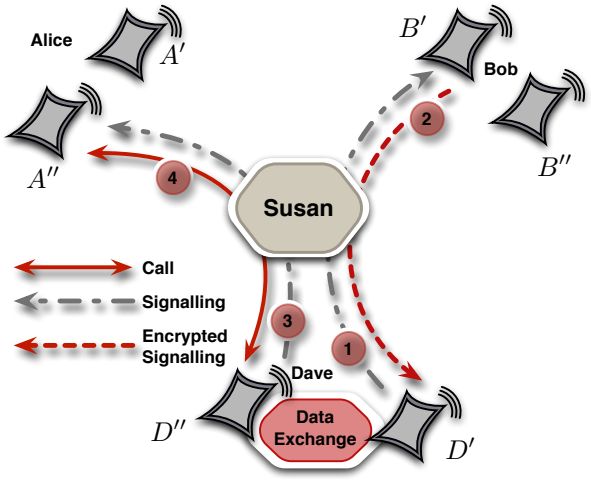


Figure 3: The Y-Routing concept in CallForge. The two distinct phones per user (i.e. D' and D'' for Dave) correspond to the two SIM cards used.

Not having to reveal the identity of the callee and the forwarding user while still enabling Susan, the service provider, to locate them is more challenging. The first intuitive idea could be the following modification of PathForge: When Dave wants to call Alice but reaches Bob instead, due to Alice and Bob having swapped their identities, Bob requests Dave, rather than Susan, to place the call to Alice's temporary ID. This way, Susan is kept out of the loop and does not learn Alice's location. The problem with this naive approach is, however, that Susan sees Dave's second call request shortly after the failed request to Alice and thus can infer with high probability that the second request is placed to Alice's temporary ID. The correlation between the first and the second call request would get lost for Susan, if Dave could use another technology or another carrier for the second request. In certain, limited scenarios this might even be a feasible approach, it is not, however, generally applicable.

Instead of a communication media break, we thus propose a technique that simulates a break within the same technology and the same service provider. Fig. 3 depicts this concept. As an analogy to the illustrated call setup protocol we coined the term *Y-Routing* for this concept and refer to the *right call-leg* (the edges labeled with **1** and **2**) and *left call-leg* (the edges labeled with **3** and **4**), respectively. To discuss the call setup in CallForge in detail we continue with our running example from Sec. 3 where Dave wants to initiate a call to Alice. The first step (**1** in Fig.3) is similar to

[6]Either by utilizing a dual SIM card adapter with a software switch, or a device that supports two SIM cards.

PathForge as Dave signals Susan that he likes to call Alice. In the attempt to setup the call Susan mistakenly contacts Bob that currently holds the triple τ_A, thus, identifies himself as Alice (assuming the ID changes according to Fig.1). However, in contrast to signal Susan the temporary ID of Alice I_A^T – that Bob can compute according to Equ.(1) – he uses an encrypted signalling channel to pass over I_A^T *directly* to Dave (cf. **2** in Fig.3). This prevents Susan from learning Alice's temporary ID I_A^T and, as shown subsequently, from learning Alice's true location. After decrypting the information obtained from Bob, Dave initiates the call to I_A^T using his second SIM D'' (cf. **3** in Fig.3) instead of D' that was used to setup the call in the first place. As soon as Alice can identify herself with I_A^T during the call setup in step **3**, Susan finalizes the call setup and connects Alice and Dave (cf. step **4**).

The exchange of the two IDs between the first and second call-leg in Fig. 3 emulates the intended media break, disabling Susan to correlate the two call-legs. With the *misuse of existing information* threat model, Susan is not even expected to try and correlate the two call legs, because that is not necessary to provide the service. Hence with this threat model, there are no location revelations at all, and thus the level of anonymity is perfect. Assuming the *Information inference* threat model, Susan tries to correlate the two call legs of a Y-routed call. Under this assumption, the privacy level of this approach strongly depends on the statistics of the originating cell; as long as there is enough outgoing traffic in Dave's cell, Susan cannot correlate the two subsequent call requests, because they originate from different IDs. In section 5.3 we will analyze the probability that Susan can infer Bob's location depending on various statistical metrics. Again, in the case of the *Active probing* threat model, Susan could behave like a caller to probe any subscriber's location. The only protection against this severe threat model would be to use *closed user groups* and only allow a pre-specified set of friends to call one another. This approach might be feasible for some dedicated application scenarios, it is not generally, however, a good scheme for telephony.

Again, we emphasize that the later threat model is similar to the one described in [11] as *Local Active Adversary* (LAA) that colludes with a *Global Passive Adversary* (GPA) and probes the network by injecting messages. In our definition, the GPA and LAA are basically combined and represent the service provider Susan. We agree with Li et al. that this threat model is equivalent to physical pursuit and is out of the scope of this paper.

5. COMPARATIVE ANALYSIS

We believe that (location) anonymity should be treated as one additional network quality measure, similar to other quality of service criteria, such as cell coverage, call setup time, or voice quality. We therefore compare the two approaches presented above, PathForge and CallForge, with regard to the anonymity they provide to their subscribers. We start by defining anonymity in a quantitative manner.

5.1 Quantifying Anonymity

We express the anonymity of a network by how often a subscriber's location is revealed within a certain time period on average. Anonymity on one hand and number of revelations on the other hand are reciprocal terms, i.e. the more location revelations, the lower the anonymity, and vice versa. Also, we aim at a definition that normalizes anonymity in the sense that its value is in the interval $(0, 1]$, with the highest anonymity of 1 if there are no location revelations, and converging towards 0 for an increasing number of location revelations. These considerations result in the following definition:

$$\alpha \stackrel{\text{def}}{=} \frac{1}{1+\rho} \tag{2}$$

where ρ denotes the average number of location revelations of a subscriber per time unit Δt. In today's cellular networks, e.g., the locations of all subscribers are continously tracked and revealed, resulting in an anonymity close to 0.

5.2 Anonymity in PathForge

As shown in section 3, with PathForge each call reveals the identity of two subscribers, namely those of the forwarding node and of the callee. Please note that we do not consider the caller, because their anynomity can be preserved rather easily as we have argued in section 4. Because of the double location revelation per call, the average number of location revelations, ρ_{PF}, of a subscriber in the time interval Δt is twice the average call rate γ, i.e. the average number of originating calls per subscriber per Δt:

$$\rho_{\text{PF}} = 2\gamma \tag{3}$$

Evidently, the higher the average call rate per subscriber, the lower the average anonymity in the system. Inserting Equ. (3) into Equ. (2) yields the anonymity of the PathForge approach as a function of the average call rate:

$$\alpha_{\text{PF}} = \frac{1}{1+2\gamma} \tag{4}$$

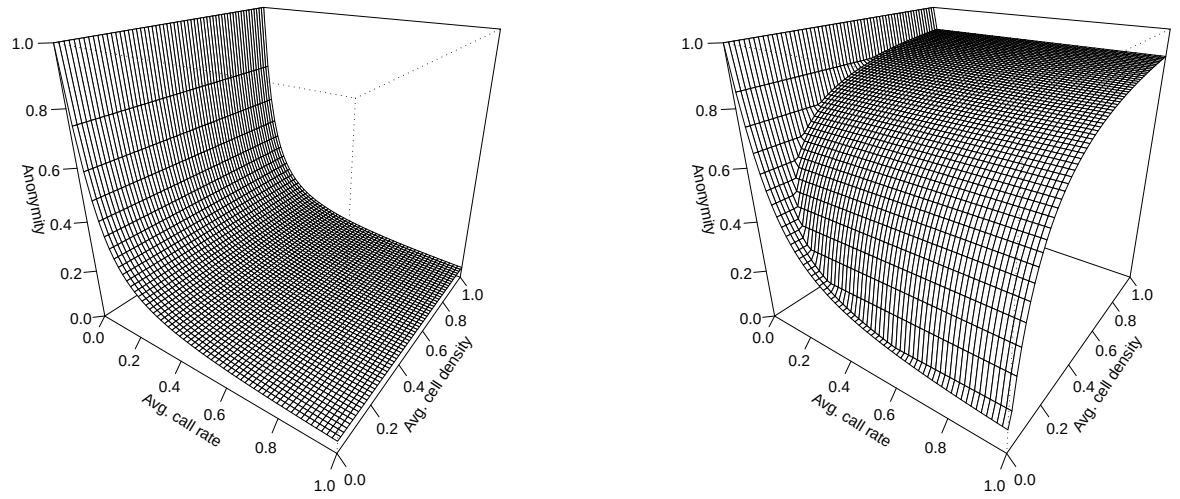
Fig. 4(a) left side, depicts α_{PF} graphically. Please note that the graph shows α_{PF} as a two-dimensional function of the call rate γ and the cell density δ, even though δ has no impact on α_{PF}. This representation was chosen for easier comparison with the anonymity of the CallForge approach which will be discussed in section 5.3, where also a definition of the cell density δ will be given.

5.3 Anonymity in CallForge

For the computation of the anonymity of the CallForge approach, not only the average call rate γ, but also the average cell density δ, i.e. the average number of subscribers per cell, needs to be taken into account. The reason is that the cell density, δ, together with the average call rate, γ, determine the average call volume of all originating calls from the same cell within a time period Δt.

Now we choose Δt to be the maximum time period between the first and the second call leg that make up a Y-routed call. The probability, P_R, that Susan, the service provider, can correlate the two call legs of a single call and thus reveal the callee's location, is then reciprocal to the call volume $\gamma\delta$ that originates from the same cell within Δt, but at most 1:

$$P_R \begin{cases} \frac{1}{\gamma\delta} & \text{, if } \gamma\delta > 1 \\ 1 & \text{, otherwise} \end{cases} \tag{5}$$



(a) (b)

Figure 4: Anonymity quantification for PathForge[2] (a) and CallForge (b). The generated plots are rotated along the vertical z-axis (anonymity) by 35° and along the horizontal x-axis (cell density) by 25°.

We compute the average number of revelations in CallForge, ρ_{CF}, of a single subscriber in Δt as the product of the number of originating calls per subscriber, i.e. the call rate γ, and the probability for each call to be correlated:

$$\begin{aligned}\rho_{\text{CF}} &= \gamma \cdot P_R \\ &= \begin{cases} \gamma \cdot \frac{1}{\gamma\delta} & \text{, if } \gamma\delta > 1 \\ \gamma & \text{, otherwise} \end{cases} \\ &= \begin{cases} \frac{1}{\delta} & \text{, if } \gamma\delta > 1 \\ \gamma & \text{, otherwise} \end{cases} \end{aligned} \tag{6}$$

Finally, Equ. (6) can be inserted into Equ. (2) to get the average anonymity of the CallForge approach as a two-dimensional function of the call rate and the cell density:

$$\begin{aligned}\alpha_{\text{CF}} &= \begin{cases} \frac{1}{1+\frac{1}{\delta}} & \text{, if } \gamma\delta < 1 \\ \frac{1}{1+\gamma} & \text{otherwise} \end{cases} \\ &= \begin{cases} \frac{\delta}{\delta+1} & \text{, if } \gamma\delta < 1 \\ \frac{1}{1+\gamma} & \text{, otherwise} \end{cases} \end{aligned} \tag{7}$$

Fig. 4(b), depicts α_{CF} graphically. As can be seen, the graph consists of two subgraphs that meet in an intersection line whose points all satisfy the condition $\gamma\delta = 1$. This is because for small call volumes, each individual call leads to a location revelation, whereas for greater call volumes the revelation probability decreases, as we have seen in Equ. (5).

In the area with $\gamma\delta < 1$, the graph looks pretty much the same as the anonymity plot for PathForge, except that the CallForge subgraph consistently lies above the PathForge graph. The reason is that with PathForge, each call leads to two location revelations, whereas with CallForge, only one location is revealed (please also compare Equ. (4) and the 'otherwise' case of Equ. (7)). The true superiority of CallForge, however, appears in the subgraph that covers the area with $\gamma\delta > 1$; in that area, the average anonymity of a user is independent of the call rate, because two effects negate each other: with increasing call rate, Susan has more opportunities to reveal the callee's location; the revelation probability for each call, however, decreases with increasing call rate and thus call volume. For increasing cell density, the average anonymity of a subscriber converges towards 1, i.e. perfect anonymity. This is because increasing cell density leads to increasing call volume, which is good in terms of hiding a single subscriber's call activities.

In summary, the anonymity plot for CallForge consists of a part that is similar to, though consistently better by the constant factor of 2, PathForge, and a part that is far superior to CallForge because a call does not automatically lead to any location revelation.

6. CONCLUSION AND FUTURE WORK

In this paper we have presented CallForge, a location management scheme for cellular networks that keeps the subscribers' location anonymous, in many cases even when they are actively involved in phone calls. CallForge extends on PathForge (cf. Sec. 3), a previously presented scheme in which the location of the callee has to be revealed for call set-up purposes. Both approaches are based on the idea that subscribers dynamically switch IDs when they get near each other. In CallForge, we additionally emulate a media break in the call set-up process to make a single call look like two

unrelated call legs to the service provider. In contrast to the approach of Li et al. [11] CallForge is specifically designed to be used in mobile/cellular networks and does not require a trusted third party but introduces a simple ID exchange protocol that works on a bi-lateral basis.

A topic for further conceptual research is how to establish the trust relationship between two ID switching parties. We intend to study two directions: An authentication process that guarantees that the expected certified software runs on the other party's handset, and the application of friend-to-friend-network principles.

We have defined a quantitive anonymity measure that is based on the number of location revelations that a subscriber is subject to within a certain time period. Our comparative analysis shows the superior anonymity that CallForge provides compared to PathForge. For reasonable high call volumes, CallForge's average anonymity converges to the maximum value of 1. What remains to be investigated in this context is the validation of our theoretical analysis against concrete statistics in a cellular network.

Additionally, CallForge is designed to be implemented completely in the mobile handset, without any modification of existing cellular network infrastructure. This is a tremendous advantage when it comes to the real world applicability of the approach. CallForge, at this point, is a very promising concept. We plan to implement a prototype and conduct tests in cellular networks. However, it is unrealistic to build a prototype of CallForge and deploy it in a real world cellular network. Therefore, we investigate the possibility to build our own cellular network at the University of Konstanz. A potential candidate to build a test setup of a cellular network is the OpenBTS project [7] [1] that is part of the GNU Radio SDK.

What remains arguable, though, will be observed in the future, is the utilization of prepaid contingents to setup calls. In the current state we argue that the constraint to us prepaid minutes for the call setup is favorable over the loss of anonymity in the common setup.

7. REFERENCES

[1] The OpenBTS project, 2010. http://openbts.sourceforge.net/.

[2] S. K. Belle, M. Waldvogel, and O. Haase. Pathforge: Faithful anonymization of movement data. In *MobiHeld '09: Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pages 63–64, New York, NY, USA, 2009. ACM.

[3] S. K. Belle, M. Waldvogel, and O. Haase. Pathforge:: Faithful anonymization of movement data. Technical report, Bibliothek der Universität Konstanz, Universitätsstr. 10, 78457 Konstanz, 2009.

[4] C.-Y. Chow, M. F. Mokbel, and X. Liu. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In *GIS '06: Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems*, pages 171–178, New York, NY, USA, 2006. ACM.

[5] B. Gedik and L. Liu. Location privacy in mobile systems: A personalized anonymization model. In *ICDCS '05: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pages 620–629, Washington, DC, USA, 2005. IEEE Computer Society.

[6] G. Ghinita, P. Kalnis, and S. Skiadopoulos. PRIVE: Anonymous location-based queries in distributed mobile systems. In *WWW '07: Proceedings of the 16th international conference on World Wide Web*, pages 371–380, New York, NY, USA, 2007. ACM.

[7] GNU Radio. OpenBTS, 2010. http://gnuradio.org/redmine/wiki/gnuradio/OpenBTS.

[8] B. Hoh and M. Gruteser. Protecting location privacy through path confusion. In *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 194–205, Washington, DC, USA, 2005. IEEE Computer Society.

[9] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz. AnonySense: Opportunistic and privacy-preserving context collection. In T. R. Jadwiga Indulska, Donald J. Patterson and M. Ott, editors, *Pervasive Computing*. LNCS, Springer-Verlag, 2008.

[10] J. Krumm and E. Horvitz. Predestination: Inferring destinations from partial trajectories. In *Ubicomp*, pages 243–260, 2006.

[11] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran. Swing & swap: user-centric approaches towards maximizing location privacy. In *WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 19–28, New York, NY, USA, 2006. ACM.

[12] J. Markoff. F.B.I. seeks access to mobile phone locations. New York Times, July 1998.

[13] M. F. Mokbel, W. G. Aref, S. E. Hambrusch, and S. Prabhakar. Towards scalable location-aware services: requirements and research issues. In *GIS '03: Proceedings of the 11th ACM international symposium on Advances in geographic information systems*, pages 110–117, New York, NY, USA, 2003. ACM.

[14] Network World. How to keep Big Brother from tracking cell phone, 2009. http://www.networkworld.com/news/2009/082709-cell-phones-anonymous.html.

[15] Pc World. Is This the Future of the Cell Phone?, 2009. http://www.pcworld.com/article/180135/pathforge.html.

[16] B. Schneier. The Kindness of Strangers, 2009. http://www.networkworld.com/news/2009/082709-cell-phones-anonymous.html.

[17] C. Soghoian. Exclusive: Widespread cell phone location snooping by NSA? CNET News, September 2008.

[18] M. Starostik. Verfassungsbeschwerde: Vorratsdatenspeicherung. Lawsuit filed at the German Constitutional Court, September 2008. In German.