Preserving Privacy in Social City Networks via Small Cells

Geert Vanderhulst
Alcatel-Lucent Bell Labs
Copernicuslaan 50
2018 Antwerp, Belgium
geert.vanderhulst@alcatel-lucent.com

Fahim Kawsar
Alcatel-Lucent Bell Labs
Copernicuslaan 50
2018 Antwerp, Belgium
fahim.kawsar@alcatel-lucent.com

ABSTRACT

An increasingly large amount of small cells – e.g. WiFi hotspots – is being deployed in residential areas to connect a plethora of smart devices to the Internet. In this paper, we present a social city network leveraging small cells for sharing content geographically and temporarily whilst preserving the privacy of its users. Unlike a social network built around friends, we propose a social city network addressing geographically co-located people and smart objects, e.g. residing in a street, on a square, around a building, etc. Our goal is to facilitate interaction with smart cities by easily sharing short-lived data fragments with others in a given area and for a limited time span. To this end, we designed an architecture in which small cells deliver location proofs that grant access to location-restricted content.

INTRODUCTION

Social networks have radically changed the way content is shared on the Web. By following someone on Twitter or becoming one's friend on Facebook, relationships between people – family, friends, colleagues – are explicitly composed. Also location data retrieved by social networking applications is often used to associate shared information with a point on the map, e.g. checking in at a place on Foursquare or Google Places. The impact of such networks has grown beyond sharing one's social status to marketing a business (e.g. collecting 'likes') and engaging in a dialogue with customers (e.g. after sale service). Yet, within the scope of a city, present social networks still lack intuitive means to disseminate content that is constrained in place and time. Rather than addressing known individuals, we envision a location-based social network [8] in which content is shared with a street, a square, a part of a city, ... and only for a limited period. Such a social network also fits the vision of the Internet of Things where smart objects autonomously exchange social facts derived from sensor data with other objects in the direct vicinity or across city boundaries [1]. The notion of friendly objects and associated configuration work for setting up proper sharing policies could vanish if users can be assured that shared data is short-lived and constrained within geographical boundaries rather than being publicly available on the Internet.

To preserve a user's privacy when using a city's social network, shared content thus must be contained within the indicated spatial and temporal boundaries. However, present location-based services typically rely on an implicit trust relationship between content provider and consumer: it is assumed that a user indeed resides at the location he claims to be at. As location coordinates can easily be falsified, a more robust solution is needed to prevent users from lying about their whereabouts and hence obtain unauthorized access to shared content. In this paper, we leverage small cells as witnesses that can testify a user's presence in a given area at a given time. We contribute to the state of art with an adapted algorithm for generating secure location proofs that preserve the privacy of the prover. With a location proof, a user can authenticate herself to the social city network and access location-restricted content.

RELATED WORK

GeoLife [12] is a location-based social network which enables users to share life experiences and build connections among each other using human location history. Similarity matching of location trajectories is applied to generate friend and travel recommendations. In our system no explicit relationships between people or objects are established. Everyone visiting an area within a period that content is shared, can interact with it.

Previous works have studied the use of WiFi hotspots to offload traffic from cellular networks [2, 9] and propose social participation to propagate data through opportunistic networks [5]. In these cases, local delivery nodes are exploited to increase network efficiency and overcome overloaded cellular networks. Likewise, access to shared content can be regulated via services running in a hotspot's local network [11] which requires a user to be connected with a specific wireless node to download a piece of data. As opposed to this approach, we exploit small cells as witnesses that can testify the presence of a user at a certain place and time.

Several systems have also been proposed to give users the ability to prove that they were in a particular place

at a particular time [10, 6, 13]. Some systems rely on computing an upper bound of the user's distance, e.g. by measuring the round-trip time of a wireless signal [4]. Other approaches which do not depend on dedicated hardware, obtain proofs from wireless access points (e.g. VeriPlace [6]) and Bluetooth devices (e.g. APPLAUS [13]). Our privacy system is based on a simplified version of the APPLAUS architecture, yet adapted to hotspots as trusted witnesses instead of Bluetooth devices. In many usage scenarios, location proofs are used as evidence for later, e.g. to proof to a teacher that all classes were attended or to detect loyal customers. Instead, we leverage them as on-site as authentication tokens to gain access to location-restricted content. IP-to-Geo schemes [7] are often too inaccurate for this matter and can easily be tricked using proxies. On the one hand, we want to protect the privacy of the content provider by restricting the place and time where and when content can be accessed, but on the other hand we also need to preserve the privacy of the content consumer by ensuring that the latter's identity and current location are obfuscated in a proof. As pointed out in [13] and [6], this can be achieved by distributing trust among multiple parties involved in the provisioning and verification of location proofs.

SOCIAL CITY NETWORK

In this section we elaborate on a design of a social city network service in which messages and media can be posted, similar to Twitter. The social city network sets itself apart from other social networks as (i) content is shared within specific geographic areas rather than with a predefined set of people and can only be accessed by users physically residing within this area; and (ii) content is only made available for a limited duration and then disappears again – hence it does not circulate in the network until it is explicitly deleted. Consider the following motivational use cases:

1. The water company announces construction works in Arlington Road and indicates an expected cut of the water supply tomorrow between 8 am and 12 am. Live updates on the works are propagated via the social city network to the residents of the street.

2. A restaurant owner interacts with the city's social network to advertise daily lunch specials to people in the neighborhood. This information is shared between 11 am and 1 pm within a 10 km radius of the restaurant.

3. During a summer festival in Regent's Park, camera feeds capturing the stage from different angles are made available to the local audience. Hence people at the festival who have no clear view on the podium can still watch the performance on their mobile devices.

4. A smart car automatically broadcasts a flat tire to approaching vehicles, i.e. shares a situation with a particular road segment.

Figure 1 shows a user interface prototype for a mobile application by which users can engage with the social city network and is further elaborated on in the remainder of this section.

(a) Posting content.

(b) News feed

Figure 1. User interface mock-up of an application for interacting with the social city network.

Posting Content

When posting new content to the social city network using the dialog depicted in figure 1, users need to specify *where* and *when* a fragment is shared. For the *where* part, addresses or place descriptions can be specified or an area can be indicated on the map using selection tools. We use OpenStreetMap[1] data to translate place names into geometric shapes composed of location coordinates, e.g. the geographic boundaries of a park in the figure. This spatial data is stored along with the content in the social network as it determines the location from where the content can be accessed. For the *when* part, users can specify a start time and a duration after which the content is deleted. By focusing on short-lived data, we anticipate privacy concerns and promote the news value of published content. Moreover, a desired privacy and security policy can be enforced in our system: trust a user's provided location or require a location proof – the latter being selected as default.

News Feed

The news feed mimics the layout of Google Mail where social and promotional messages are separated from a primary feed as illustrated in figure 1. These feeds are

[1] `http://www.openstreetmap.org`

populated with content that is revealed based on the user's location. Hence, when moving through the city, the news feed will continuously update. Note however that our approach is different from e.g. Foursquare where information about a place (e.g. restaurant reviews) is made available on-site. Displayed content is not necessarily linked with the user's current location, but it has rather been shared within the area the user currently happens to be in. To retrieve protected content, users need to authenticate via a location proof which is retrieved from small cells in the vicinity as discussed in the next section.

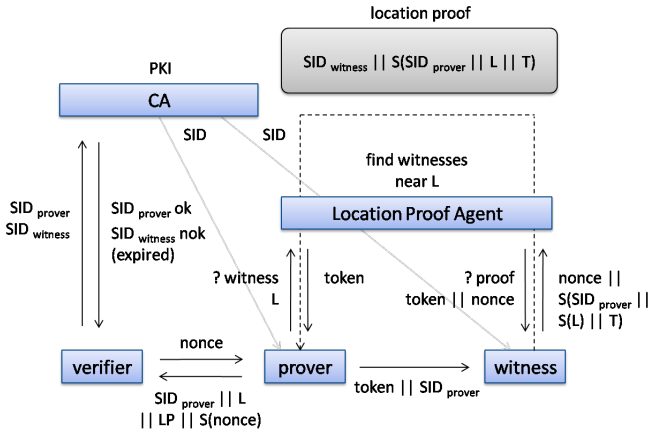
LOCATION PROOFS

Since location coordinates can be spoofed easily, we need a mechanism to verify that a user indeed resides at a claimed position. Even if access to shared content is restricted to a number of small cells, there is no guarantee that an individual is within the range of e.g. a WiFi hotspot as a local proxy can route network traffic from anywhere in the world to the hotspot (e.g. wormhole attack). To protect against this, we modified an algorithm presented in [13] for handing out personalized location proofs and leverage it for instant location-based authentication. The location proof authorizes a user to access content that resides on the Internet (i.e. in the cloud) but that was only shared within a particular city. These proofs are handed out by small cells which act as unique trusted witnesses (i.e. when managed by a trusted provider) that confirm the presence of a user.

In the next sections, we discuss our location proof architecture supported by figure 2, and identify the role of the different entities in the context of a social city network.

Algorithm and Architecture

As illustrated in figure 2(a), several entities are involved in the provisioning and verification of location proofs to preserve the privacy of its users. No single entity is aware of both the identity and the location of a user at any moment. Provers and witnesses communicate with each other and a Location Proof Agent (LPA) using secret identities which also serve as public encryption keys. To this end, provers and witnesses first identify themselves to a Certified Authority (CA) that provides them with secret identifiers (public keys). To obtain a Location Proof (LP), a prover queries the LPA for nearby witnesses that can confirm its location. The LPA responds with a list of witnesses (e.g. WiFi hotspot identifiers) and notifies nearby witnesses that a prover wants to acquire a location proof using the shared token as a reference. The prover then contacts a witness within range using the shared token and its secret identifier – i.e. connects to a hotspot with a given SSID and interacts with a service in the hotspot's network. The witness generates an intermediate LP that consists of the location of the witness (L), the current time (T) and the prover's secret identifier (SID_{prover}). This data is signed with the witness' private key ($S(...)$) and forwarded to the LPA. The



(a) Different parties involved in the provisioning and verification of proofs.

CA	LPA	Prover	Witness	Verifier
ID prover	L prover	SID witness	SID prover	SID prover
ID witness	L witness	L witness		SID witness
SID prover	SID prover			L prover
SID witness	SID witness			L witness

(b) Preserving privacy: who knows what? (ID = identity, SID = secret reference to identity, L = location)

Figure 2. Location proof architecture.

LPA verifies the identity of the witness using its public key ($SID_{witness}$) and composes a final LP which is passed on to the prover. This location proof is then sent by the prover to the verifier which checks with the CA whether the secret identifiers of prover and witness are not expired and if the LP is valid, i.e. signed by the witness. Note from figure 2(b) that the LPA is only aware of the location of a user and the CA only knows the identity of a user. By distributing this information amongst different parties run by different organizations, the user's privacy is protected. To discourage cheating, we let location proofs expire (similar to session cookies) and limit the number of proofs per IP address. To increase trust, a content provider may also demand for multiple location proofs handed out by different witnesses.

Applied to the Social City Network

At the heart of the social city network, a verifier process regulates access to shared content. When a valid location proof is received, location-restricted content is unlocked for the corresponding user for a predefined time span. After that, the user's session expires and a new location proof must be provided as the user might have moved to a different place from where the content can no longer be accessed. To guarantee uninterrupted access to location-restricted content, a mobile application – running a prover process – can pro-actively collect location proofs and (re)authenticate to the social city network. Given the continuously growing network of WiFi hotspots, we believe that WiFi hotspots in particular are suitable candidates for generating these proofs. WiFi nodes are readily being used as location beacons due to

their stationary nature and the limited range of their radio signals. Many residential and public hotspots are also managed by telecom providers which can fulfill the role of Location Proof Agent. Note that the underlying authentication mechanism is completely transparent for the end-user of our service: a mobile application (prover) retrieves a location proof from a WiFi hotspot (witness) and passes it to the social city network (verifier) – no manual interaction is required.

CONCLUSIONS AND FUTURE WORK

A social city network built around *where* and *when* content is shared enables several new use cases that are hard to realize with present social networks. In our approach, content is shared within the boundaries of a street, a park or a custom geographic area and automatically expires. Instead of composing static relationships between people or objects, we enable users to reach out to crowds of people that are connected by the places they visit. Even so in an emerging world of connected objects that generate massive amounts of data, spatio-temporal sharing can assist in delivering the right facts to the right place at the right time. In this work, we have explored the technical requirements for safeguarding the privacy of the users of a social city network and propose location as an unobtrusive authentication mechanism. Although we have mainly focused on public WiFi hotspots as delivery vehicles of location proofs, the presented techniques are also applicable to other wireless nodes with limited coverage like Femtocells [3].

Further effort needs to be spent in combining our application prototypes and conceptual architecture into a real-world proof of concept implementation. Other directions for future work include quality control and ownership management of shared content. Possible pitfalls of a location-based social network service are inappropriate content postings and users pretending to be someone else. The former can be addressed via a crowd-sourced voting system (down-voting inappropriate content) or a cost model that attributes a fee to advertising messages based on the target area and the lifetime of the content. While content might be retrieved anonymously via location proofs, further research is needed to prevent identity abuse when posting content.

REFERENCES

1. Atzori, L., Iera, A., Morabito, G., and Nitti, M. The Social Internet of Things (SIoT) - When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization. *Computer Networks 56*, 16 (Nov. 2012), 3594–3608.
2. Balasubramanian, A., Mahajan, R., and Venkataramani, A. Augmenting Mobile 3G using WiFi. In *International Conference on Mobile Systems, Applications, and Services (MobiSys'10)*, ACM (2010), 209–222.
3. Chandrasekhar, V., Andrews, J. G., and Gatherer, A. Femtocell Networks: A Survey. *IEEE Communications Magazine 46*, 9 (2008), 59–67.
4. Ferreres, A. I. G. T., Alvarez, B. R., and Garnacho, A. R. Guaranteeing the Authenticity of Location Information. *IEEE Pervasive Computing 7*, 3 (2008), 72–80.
5. Han, B., Hui, P., Kumar, V. S. A., Marathe, M. V., Shao, J., and Srinivasan, A. Mobile Data Offloading through Opportunistic Communications and Social Participation. *IEEE Transactions on Mobile Computing 11*, 5 (2012), 821–834.
6. Luo, W., and Hengartner, U. VeriPlace: a Privacy-Aware Location Proof Architecture. In *International Conference on Advances in Geographic Information Systems (GIS'10)*, ACM (2010), 23–32.
7. MaxMind. GeoIP Database. http://www.maxmind.com/en/ip-location/.
8. Microsoft Research. Location-based Social Networks. `http://research.microsoft.com/en-us/projects/lbsn/`.
9. Pitkänen, M. J., Kärkkäinen, T., and Ott, J. Opportunistic Web Access via WLAN Hotspots. In *International Conference on Pervasive Computing and Communications (PerCom'10)*, IEEE (2010), 20–30.
10. Saroiu, S., and Wolman, A. Enabling New Mobile Applications with Location Proofs. In *Workshop on Mobile Computing Systems and Applications (HotMobile'09)*, ACM (2009), 3:1–3:6.
11. Vanderhulst, G., and Trappeniers, L. Public WiFi Hotspots at Your Service. In *International Conference on Pervasive Computing and Communications (PerCom'12 Workshops)*, IEEE (2012), 411–414.
12. Zheng, Y., Xie, X., and Ma, W.-Y. GeoLife: A Collaborative Social Networking Service among User, Location and Trajectory. *IEEE Data Eng. Bull. 33*, 2 (2010), 32–39.
13. Zhu, Z., and Cao, G. APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services. In *International Conference on Computer Communications (INFOCOM'11)*, IEEE (2011), 1889–1897.