Ad Hoc Networks 37 (2016) 110–121

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Establishing location-privacy in decentralized long-distance geocast services

Martin Florian*, Felix Pieper, Ingmar Baumgart

Institute of Telematics, Karlsruhe Institute of Technology (KIT), Karlsruhe 76131, Germany

ARTICLE INFO

Article history:
Received 23 February 2015
Accepted 25 July 2015
Available online 4 August 2015

Keywords:
Location privacy
Geocast
Overlay networks

ABSTRACT

The ability to communicate over long distances is of central importance for smart traffic applications like cooperative route planning or the discovery and reservation of charging stations for electric vehicles. Established approaches are based on centralized architectures with singular service providers. This setup leads to strong privacy concerns, as great amounts of sensitive location data need to be stored at a non-local, centralized entity. Decentralized approaches like the overlay-based geocast service *OverDrive* propose to solve this issue by eliminating the central data sink and sharing location information with a small subset of other participants. In this paper, we propose techniques for further improving the location privacy offered by decentralized long-distance geocast services. Through obfuscation of location data and mechanisms for detecting location spoofing attempts, we can ensure that precise location data is only shared with participants in the physical vicinity. Simulation results show that our extensions render both the large scale surveillance and the targeted tracking of OverDrive users unfeasible even for strong adversaries controlling hundreds of overlay nodes. In addition, we discuss practical considerations when deploying decentralized and privacy-sensitive systems that rely on cellular networks and present results from an empirical evaluation of connectivity properties.

1. Introduction

The availability of Internet access in vehicles offers a variety of new opportunities to assist road users that are not easily realized with short range vehicular networking approaches. Examples include smart-traffic applications like cooperative route planning, where vehicles exchange traffic information for improving route planning decisions, or the localization and reservation of charging stations for electric vehicles. Long-distance communication is also important for vehicular cloud applications like [1], where vehicles act as service providers to which location-based service requests need to be propagated.

Current solutions mainly follow a centralized, server-based architecture, which, among scalability concerns and the tendency of creating dependencies on individual providers, raises strong privacy concerns. As all communication and service provision is handled by the service provider, he also needs to collect all sensitive user information required for realizing the service. In the context of smart traffic, this specifically includes location data, which was found to enable far-reaching insights into the private life of users [2].

As an alternative to the centralized setup, we propose the exploration of *decentralized* solutions where users exchange information and provide services directly among each other. Decentralized overlay networks providing *geocast* services [3,4] are a recent development in this direction with significant potential for resolving the inherent drawbacks of

* Corresponding author. Tel.: +4972160846408.
E-mail addresses: florian@kit.edu (M. Florian), felix.pieper@web.de (F. Pieper), baumgart@kit.edu (I. Baumgart).
URL: http://tm.uka.de/~florian (M. Florian)

http://dx.doi.org/10.1016/j.adhoc.2015.07.015
1570-8705/

centralized smart-traffic systems. Roughly, the idea is the creation of a logical *overlay network* on top of a cellular communication network based on the *Internet Protocol (IP)*. In the overlay network, nodes propagate their location to other participating nodes and use this information for choosing overlay neighbors and forwarding messages. Thus, neither a central entity nor additional infrastructure support is necessary. With *OverDrive* [3], this approach was specifically adapted to smart traffic scenarios. The evaluation of OverDrive showed [3] the capability to address the scalability and innovation issues of traditional centralized systems. Follow up works [5] demonstrated a series of possible attacks on the OverDrive approach that could allow a strong adversary to break individual pseudonyms with context knowledge and track identified targets.

In this paper, we introduce two techniques for negating such attacks. Our contributions aim at establishing *data locality*, i.e., ensuring that precise location data is only shared with entities that are physically located in the close vicinity. Specifically, we make the following contributions:

1. An *obfuscation* mechanism for OverDrive that reduces the precision of location data in relationship to the distance at which it is shared. Our approach is resistant to intersection attacks resulting from the combination of data points from multiple observers.
2. Data locality cannot be established if participants can fake their location. Thus, we propose a *location spoofing detection* mechanism based on private proximity testing [6,7]. Our solution is based on high-entropy data collected from a GSM network and allows proximity checks over multiple kilometers of obstructed terrain.
3. A thorough evaluation of our solutions as extensions to the overlay-based geocast service OverDrive. Through simulation, we evaluate their impact on possible privacy attacks as well as their impact on performance.

While developed with an application in OverDrive in mind, the proposed techniques are widely applicable to other decentralized systems in which location data needs to be shared with possibly non-local entities. We significantly extend our work presented in [8] by including additional details about the design of our enhancements and our evaluation setup. In addition, we include a discussion of connectivity and privacy properties of current cellular networks that are relevant to decentralized systems. In this context, we present novel results from a measurement study involving the cellular networks available in Germany.

2. Related work

Privacy issues in vehicular networking have been studied thoroughly, focusing mostly on short-range communication and vehicular ad-hoc networking (VANET) scenarios [9,10]. However, local one- and few-hop communication is insufficient for realizing applications depending on long-distance communication, like wide area vehicular navigation and parking space search. For realizing these types of services, the existence of dedicated infrastructure support or a trusted centralized service provider is usually assumed. Decentralized approaches have been proposed, e.g., for traffic information systems [11], but without a serious consideration of location privacy issues.

Location privacy has been a major topic in the context of location based systems (LBS) in general. [12] gives an excellent overview over different techniques, including multiple obfuscation approaches. However, existing approaches are focused on centralized setups and not directly applicable to decentralized systems. Also, location privacy techniques from the LBS domain often lose their efficiency when confronted with continuous updates as required by smart-traffic applications. If location updates can be linked into routes, a subsequent linking to user identities is possible [2].

In [13], the authors describe an approach for the privacy preserving collection of continuous location updates in a vehicular traffic scenario. Location updates are communicated only when a vehicle passes a previously determined virtual trip line. Thus, a spatial sampling of the passed routes is achieved. However, the approach is only suitable for the privacy-preserving collection of location-specific data, e.g., floating car data, and not for the realization of geocast.

In [5], the privacy characteristics of overlay-based geocast services are analyzed and evaluated, leading to the discovery of possible attacks. No detailed countermeasures were proposed or evaluated. The reduction of the precision of shared location information as well as the protection against location cheating remained open questions. Solutions for the latter exist that require additional infrastructure support or spot checks [14]. If the problem can be reduced to proximity checks, short range radio beacons can be used, as well as private proximity testing mechanisms as proposed in [6] and [7]. However, no approach for integrating any of these solutions into a long-distance geocast system has previously been proposed.

3. OverDrive

3.1. Functionality

Originally proposed in [3], the main service provided by *OverDrive* is the delivery of messages to nodes in a given geographic region. Technically, OverDrive is based around two concepts:

- An overlay neighborhood structure based on a partitioning of geographic space into concentric *rings*, as well as mechanisms for maintaining this structure.
- A routing mechanism for forwarding messages to nodes in a desired geographic area. Messages are forwarded using connections from the overlay neighborhood structure.

An overview of the functioning of OverDrive is given in Fig. 1. The figure depicts a possible application for the geocast service, namely the sending of a geographic query to a point in geographic space (e.g., a road segment) lying ahead of the requester. From all of its neighbors, which are chosen based on a partitioning of geographic space into concentric rings, the requester greedily chooses the one neighbor that is closest to the destination region in terms of geographic distance. The request is sent via the cellular network and standard IP to this neighbor, who then forwards it according to the same rule, sending it to the one of its overlay neighbors that is closest to the destination region. Once the message