Tobias Meuser, Daniel Bischoff, Ralf Steinmetz. *Poster: Location Privacy in Heterogeneous Vehicular Networks.* In Proceedings of The 13th ACM International Conference on Distributed and Event-based Systems (DEBS '19), June 2019, ISBN: 978-1-4503-6794-3/19/06

Poster: Location Privacy in Heterogeneous Vehicular Networks

Tobias Meuser, Daniel Bischoff, Ralf Steinmetz
{tobias.meuser,daniel.bischoff,ralf.steinmetz}@kom.tu-darmstadt.de
Multimedia Communications Lab, TU Darmstadt
Darmstadt, Germany

ABSTRACT

Vehicle exchange Floating Car Data (FCD) to increase their awareness beyond their local perception. For this purpose, the context-sensitive FCD is commonly distributed using the cellular network. To receive FCD via the cellular network, the vehicles share their current context (often location) with a backend.

This permanent and accurate observation of the vehicle's context interferes with the privacy of the occupants. In this work, we use obfuscation to protect the location privacy of the occupants. For this purpose, we adopt the precision of the context monitoring of the vehicle to the privacy needs of the occupants. As unnecessary FCD is transmitted to the vehicle, this imprecision reduces the share of useful FCD, which might lead to additional bandwidth consumption. We compensate for this additional consumption by filtering FCD with low impact for the vehicle and simultaneously relying on less-privacy-aware vehicles to provide FCD via local communication channels like Wifi.

CCS CONCEPTS

• **Security and privacy** → **Privacy protections**; • **Networks** → *Hybrid networks*; • **Theory of computation** → Network games.

KEYWORDS

privacy, cooperative, offloading

ACM Reference Format:
Tobias Meuser, Daniel Bischoff, Ralf Steinmetz. 2019. Poster: Location Privacy in Heterogeneous Vehicular Networks. In *DEBS '19: The 13th ACM International Conference on Distributed and Event-based Systems (DEBS '19), June 24–28, 2019, Darmstadt, Germany*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3328905.3332515

1 INTRODUCTION

In future vehicular networks, vehicles will exchange enormous amounts of Floating Car Data (FCD) to improve traffic safety and driving comfort. As FCD is context-sensitive often required at other locations than they are measured, the cellular network and a centralized backend are used for the transmission of FCD. To receive the context-sensitive FCD, the vehicles generally share their context with the backend, which is considered to be a trusted entity.

This context-sharing with a centralized backend is an intrusion into the privacy of users. With current solutions, the users can either accept this intrusion or disable context-updates. Disabling this communication leads to vehicles without knowledge of their environment and cancels the advantages of vehicular networks.

In this work, we propose the idea of a communication mechanism with adjustable privacy, in which the user can set the privacy level of the communication while still receiving crucial information. For this purpose, we hide the real location of the vehicle by increasing the occupancy area of the vehicle like in [1, 4]. This leads to less accurate filtering at the backend and, thus, less relevant FCD. We assume that a vehicle only has limited assigned bandwidth for the exchange of FCD. The imprecision of context leads to fewer FCD, that match the vehicle's context. In the following, we describe the extension of our previous work [3] in Section 2. After that, we describe the implications of privacy-sensitivity in heterogeneous vehicular networks in Section 3. In Section 4, we provide preliminary results to showcase the validity of our developed idea and conclude the paper with Section 5.

2 SYSTEM OVERVIEW

In our previous work [3], we developed a game-theoretic approach to improve the communication quality in heterogeneous vehicular network. Our approach offloads messages from the cellular network using Wifi. That is, every message is assigned an impact. The impact depends on the message type and, for context-aware messages, on the vehicle's context. Each vehicle aims to maximize the sum of the impact values of received messages while sticking to predefined bandwidth requirements. Through the sharing of bandwidth between vehicles, this approach increased the communication quality.

3 PRIVACY-SENSITIVITY FOR HETEROGENEOUS NETWORKS

In our previous work [3], we assumed that there always is an accurate description of the vehicle's context available. Generally, this context referred to the location of the vehicle. In this work, we focus on the possibilities to protect the vehicle's privacy while still providing context-sensitive information.

In the literature, there exist different types of privacy for location-based services, (i) anonymity-based privacy, and (ii) obfuscation-based privacy. Obfuscation-based privacy provides different possibilities again to protect the user's location privacy by a combination of the methods inaccuracy, imprecision, and vagueness [2]. According to Dockham et al. [2], inaccuracy refers to the vehicle sharing wrong context-information, such that the backend cannot decide on the correct context-information, while imprecision is the sharing of context-information of low precision, i. e., an area of location is shared instead of an exact location. Vagueness refers to the description of the context in linguistic terms, which increases the complexity of interpreting the context.

DEBS '19, June 24–28, 2019, Darmstadt, Germany

ACM ISBN 978-1-4503-6794-3/19/06.
https://doi.org/10.1145/3328905.3332515

3.1 Location Privacy Protection Mechanism

In this work, we use imprecision to protect the privacy of the users, as imprecision ensures that the user still will receive all necessary context information, as his location is contained in the shared area. The size of this area influences the degree of privacy obtained by the vehicle but also influences the performance of filter-operations used to select information matching the vehicle's context: A large context-area protects the privacy of the user, while it significantly reduces the share of received *relevant messages*, i. e., the messages required for the vehicle's future planning. That is, as more (partly irrelevant) messages need to be transmitted to guarantee the recipience of all relevant messages.

We consider this additional load induced by the imprecise context in our heterogeneous communication approach by reducing the effective assigned bandwidth by a factor reflecting the imprecision of context. This factor corresponds to the expected increase in the number of messages based on the size of the context-area. Thus, vehicles with privacy-sensitive occupants can only share an imprecise description of their context, which leads to these vehicles only receiving messages of high importance.

3.2 Influence of Privacy on the Performance of a Heterogeneous Network

While privacy-awareness generally leads to a reduction of received relevant messages if the bandwidth is fixed, vehicles in proximity may be less privacy-sensitive, i. e., can share received information with the privacy-sensitive vehicles, which reduces the negative impact of privacy-sensitivity.

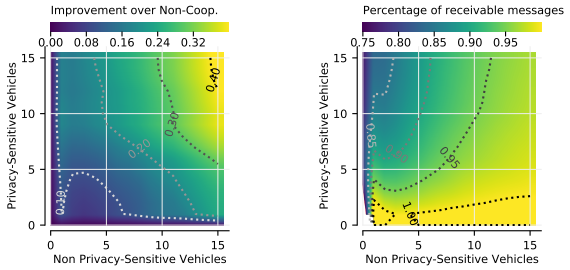
To consider privacy awareness in our model, we need to consider differing assigned bandwidths for vehicles in proximity. However, our previous approach assumed that the assigned bandwidth of each vehicle is similar. Thus, our model ignores the potential influences of other assigned bandwidths of vehicles in proximity. This deviation in expected and actual bandwidth may lead to a loss of messages.

To approach this issue, we exchange information about the currently available bandwidth with vehicles in proximity via the local Wifi channel. That way, the network can alleviate the issues induced by privacy-sensitive vehicles. However, these poses additional challenges, which we describe in the following section.

4 PRELIMINARY RESULTS

In this section, we describe the preliminary results we obtained by a numerical analysis of one example use case. In this use case, the number of different impact levels is limited to three to keep the required computational complexity low. That is, as we do find a solution to the cooperating privacy-sensitive and non-privacy-sensitive vehicles using brute force. For this purpose, we set the available bandwidth of the non-privacy-sensitive vehicles to 10% of the required bandwidth, while we assigned 2.5% of the required bandwidth for the privacy-sensitive vehicles.

To showcase the potential improvement of our approach to consider the privacy-sensitive vehicles in the optimization process, we use the improvement compared to a separate optimization of privacy-sensitive and non-privacy-sensitive vehicles. As an upper baseline, we use the maximum achieved impact (27.5) of an optimal



(a) Improvement by considering the existence of privacy-sensitive vehicles in the optimization.

(b) Percentage of the received messages compared to a setup with non-privacy-sensitive vehicles.

Figure 1: Impact of privacy on the communication quality.

setup, in which all privacy-sensitive vehicles become non-privacy-sensitive. This metric is shown in Figure 1a. It can be observed that the gained improvement in quality is neglectable for few vehicles, but increases with increasing number of vehicles (both privacy-sensitive and non-privacy-sensitive) up to a quality gain of 40%.

As an additional metric, we can observe that the percentage of received messages for our approach remains above 80% as shown in Figure 1b. Additionally, the negative impacts of privacy-sensitive vehicles decreases with increasing number of non-privacy-sensitive vehicles, as the improvement per vehicle in [3] decreases with increasing number of vehicles. That is, the relative share of received messages decrease for a higher number of privacy-sensitive vehicles, as these vehicles contribute less to the network compared to the optimal setup. However, the performance of our approach seems to be comparable to the optimal setup, which encourages us to have a more in-depth look into this modeling of privacy in the future.

5 CONCLUSION

In this work, we proposed a system of adaptable location privacy. A high privacy-sensitivity generally leads to a reduction in performance but using similar methods as in [3], we can reduce these effects drastically to match the performance of a non-privacy-sensitive network. For that purpose, non-privacy-sensitive vehicles provide FCD to the privacy-sensitive vehicles. As future work, we aim to model this behavior for multiple privacy-levels and impact-levels to make this approach applicable for large-scale scenarios.

ACKNOWLEDGEMENTS

This work has been funded by the DFG as part of projects B1 and C2 within the CRC 1053 - MAKI.

REFERENCES

[1] Chi-Yin Chow, Mohamed F Mokbel, and Walid G Aref. 2009. Casper*: Query processing for location services without compromising privacy. *Transactions on Database Systems* 34, 4 (2009).
[2] Matt Duckham and Lars Kulik. 2006. Location privacy and location-aware computing. In *Dynamic and Mobile GIS*. CRC press.
[3] T. Meuser, D. Bischoff, B. Richerzhagen, and R. Steinmetz. 2019. Cooperative Offloading in Context-Aware Networks: A Game-Theoretic Approach. In *Proc. of DEBS*.
[4] Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li. 2014. Achieving k-anonymity in privacy-aware location-based services. *Proc. of INFOCOM* (2014).