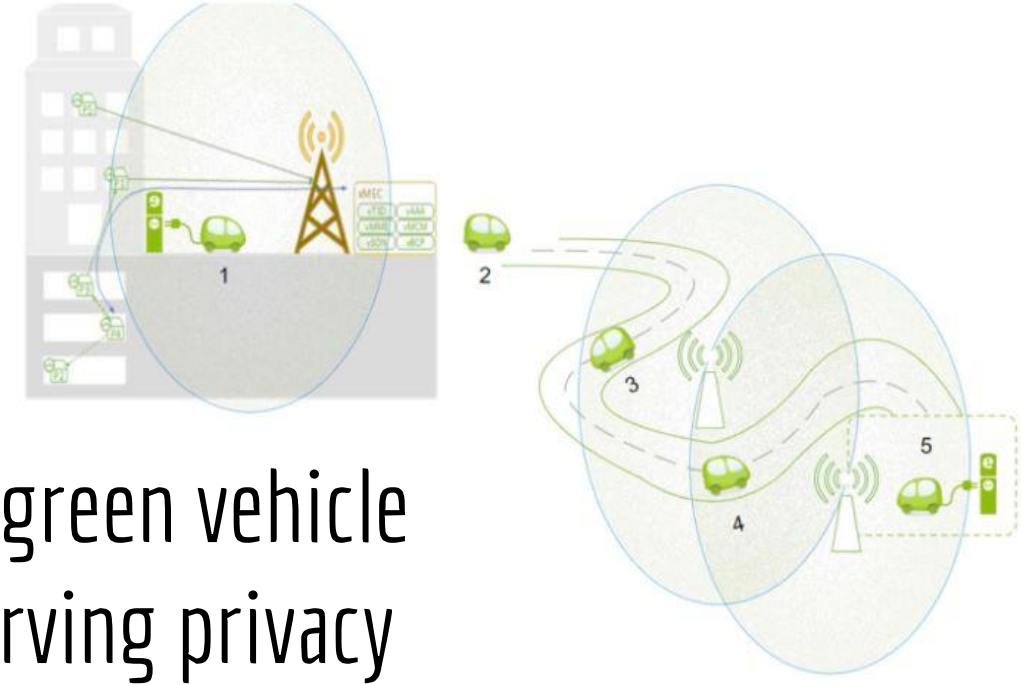


Enjoy green vehicle preserving privacy in the age of 5G

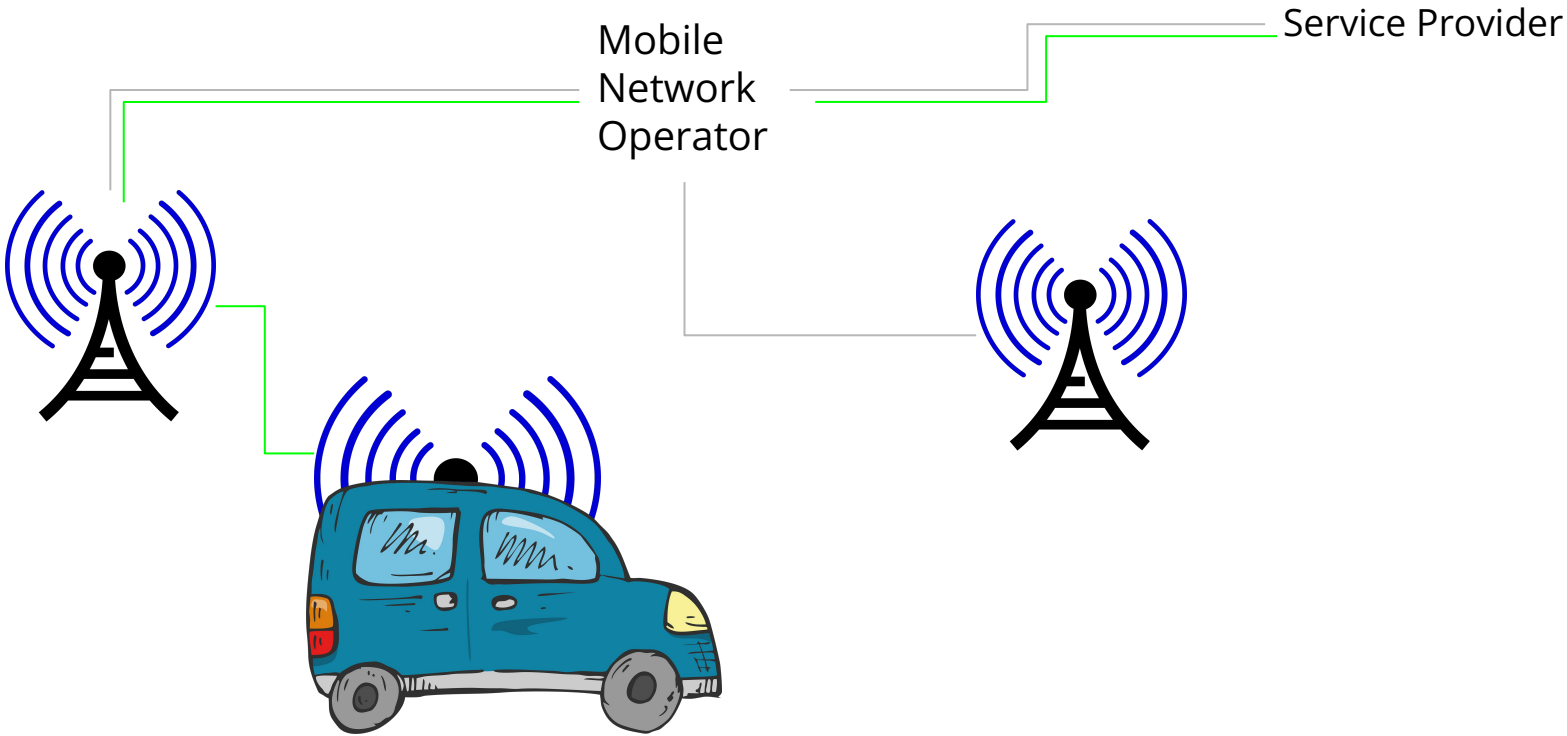
Alexandru-Nicolae Milcu
Giuseppe Lamantea
Gloria Balducci
Iulia Vasilica
Mario Gancarski
Niklas Beierl
Radu-Florin Tudorache
Yohan Meyer

In a perfect world, I would like to use **location-based services** without service providers being able to **tie my location to my identity**

Alice goes for a drive...

Alice is a proud **e-vehicle** owner. Her car's connectivity is enabled by the **5G technology**. Her first long trip approaches: she will find out if her shiny new car is really **trustworthy** when it comes to her **privacy**.

Alice loves to travel, but does her data like to travel too?



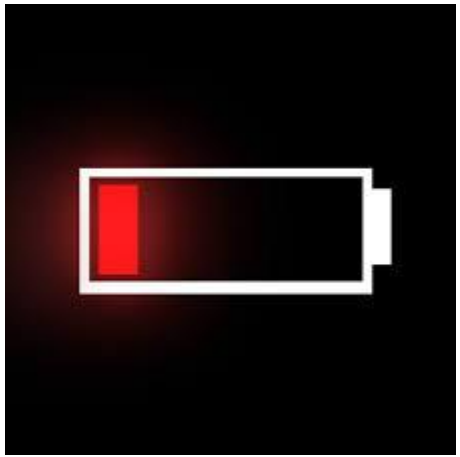
Alice enters Germany...

- ... and loses her 5G connectivity immediately.

- But is her location private now? For how long ?

Moving on

- She arrives in Munich and reconnects to the 5G network
- It has been 500km → She needs to recharge the car
- She asks her car for the nearest charging station…

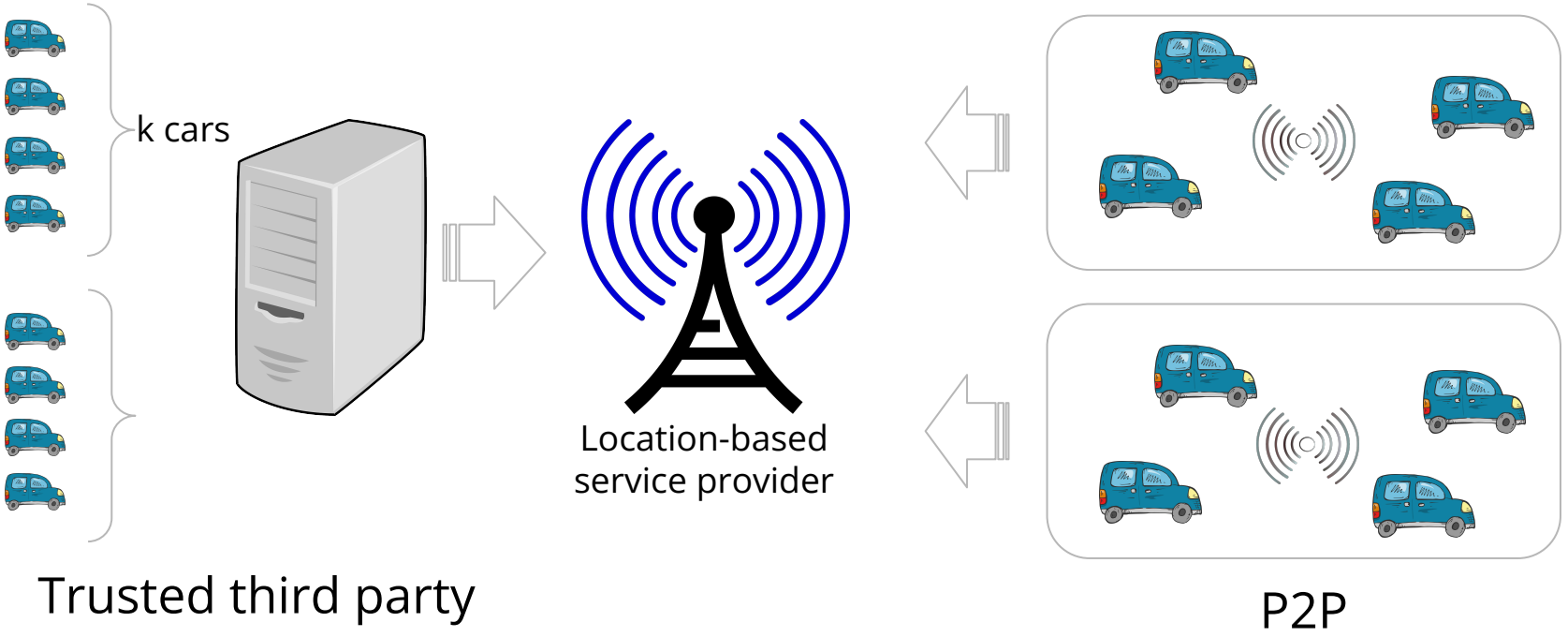


How can we protect Alice's location data?

The service Alice relies on is offered on the cloud by an external vendor.
→ She has to share her location data with the service provider, but she likes to maintain her privacy.

How can we protect Alice's location data?

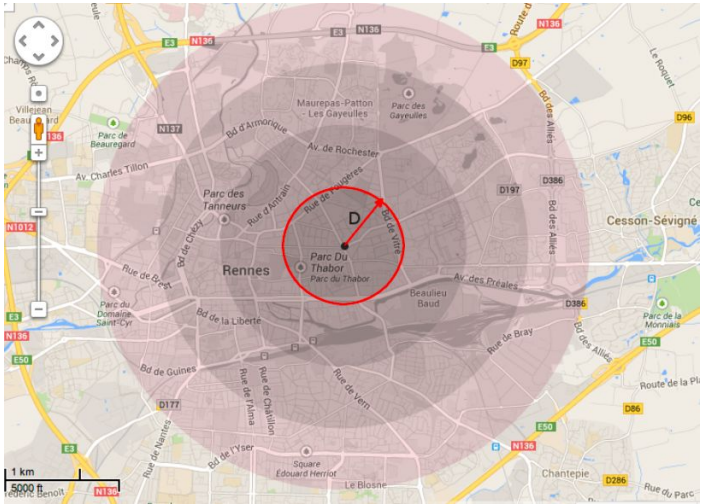
Generalization of location data based on *k-anonymity*



How can we protect Alice's location data?

Location data perturbation

- based on ε-differential privacy and geo-indistinguishability
- works without the need of other cars nearby
- can be run locally, no need for P2P or Trusted Third Part



How can we protect Alice's location data?

Deception / Dummy data

- "Confuse" the LBS provider with "dummy data"
- Flexible implementation
  - Proxy adding "dummy requests" (TTP)
  - Generate additional requests locally
- **Challenge**: Making "dummy data" indistinguishable from real data
- Drawbacks:
  - Sensitive to re-identification attacks
  - "Waste" of resources

How can we protect Alice's location data?

Protocol based? Not really...

- a **paradox**, showcasing the **trade-off** between privacy and utility
- **homomorphic encryption** and strong guarantees regarding privacy
- **specific** use cases, sometimes **too** specific
- **practically** unusable
- **PIR** protocol

But Alice doesn't want to "just" charge her car

She wants a "charging experience" with a nice cup of coffee.

A nice cup of coffee that *she* will like!

Can we reconcile
Privacy and ***Personalization***?

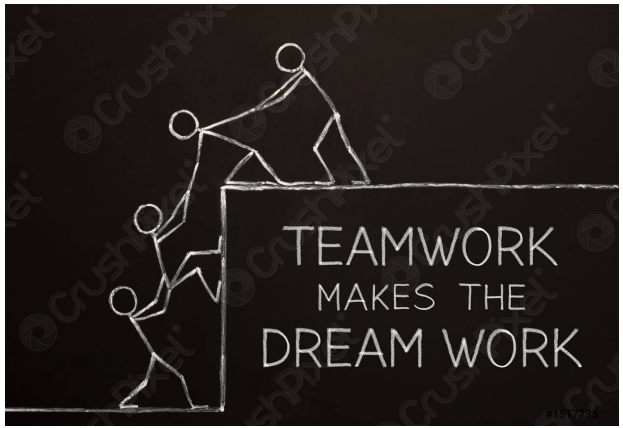
Local recommenders

- Federated Learning enabled cars allow the users to benefit from AI technology without entirely compromising their privacy
- The edge network distributes the most recent recommendation models to the cars using 5G
- Each car runs the model locally: the actual inputs are not sent over the internet!

To be continued...

There is no such thing as free lunch, so eventually Alice has to pay for charging her car and the delicious coffee.

Here, we put our trust in our colleagues from the orange team to maintain the privacy standard that we proposed for the car related features.



Conclusion

- **No silver bullet** for Location Privacy Protection Mechanisms
  →Hybrid, context-sensitive approaches
  New Challenges: Configuration, Automation, Communication
- Edge computing offers new possibilities for privacy, but…
  - More computation → More energy consumption → Less range
  - More capabilities → More hardware → Higher costs
- Balancing *Service Quality*, *Personalisation* and *Privacy* is tricky
  But we can achieve much more than current implementations!

Before ending...

A few questions never hurt anybody :

- Does technical progress always mean social progress ?
- Is it really necessary ?
- Do the (economical) benefits outweigh the environmental costs ?

Thank you for your attention,
let's hear questions !

Bibliography

- R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage
  A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions
- Besma Khalfoun, Sonia Ben Mokhtar, Sara Bouchenak, and Vlad Nitu
  EDEN: Enforcing Location Privacy through Re-identification Risk Assessment: A Federated Learning Approach.
- J. Cui, J. Wen, S. Han and H. Zhong
  Efficient Privacy-Preserving Scheme for Real-Time Location Data in Vehicular Ad-Hoc Network"
- V. Primault, A. Boutet, S. B. Mokhtar and L. Brunie
  "The Long Road to Computational Location Privacy: A Survey," in *IEEE Communications Surveys & Tutorials*