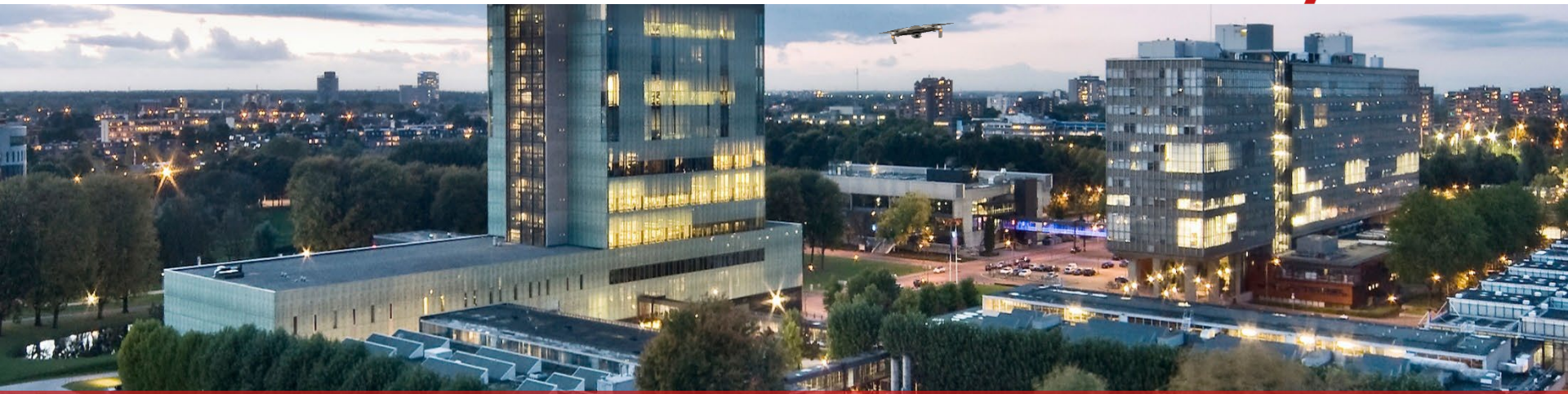
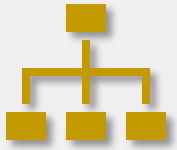


Privacy-Preserving Trajectory Matching on Autonomous Unmanned Aerial Vehicles

Savio Sciancalepore, Dominik Roy George
Eindhoven University of Technology (TU/e), Department of Mathematics and Computer Science, Netherlands

ACSAC 2022 – Austin (TX, US) – 7-9 December, 2022

Agenda



- Context and Motivation
- System Model
- PPTM Protocol
- Security Considerations
- Performance Assessment
- Conclusion and Future Work

Context

- Unmanned Aerial Vehicles (UAVs), a.k.a. drones
- Several application domains
  - Goods Delivery
  - Search & Rescue
  - Telecom services
- Autonomous or Remotely-Piloted
- Expected Proliferation (FAA, 2022)
  - 314,689 commercial drones registered in US
  - 538,172 recreational drones registered in US
  - 3,644 paper registrations in US

https://thepeak.com.my/lifestyle-travel/thai-startup-fling-to-offer-worlds-first-drone-delivery-service-in-bangkok/

Motivation

- Detecting collisions among drones in advance is critical
  - Drones Integrity
  - Business Integrity
  - People Safety
  - Path Planning Efficiency

Credit: Ingo Bartussek/Shutterstock.com.

- We need a solution for real-time collision detection on full UAVs path
- Naïve Solution: Sharing of Location and Time Data
  - Privacy Issues

Objective

- Can we design a protocol for efficient real-time privacy-preserving collision detection on autonomous UAVs?

https://physics.aps.org/articles/v14/7

Challenges

- Very large and heterogeneous trajectories
- Heterogeneous Processing Capabilities
  - From i7 CPUs to single-core @ 160 MHz
- Limited Energy Availability
  - From 7 to 30 mins autonomy
- GPS Inaccuracies

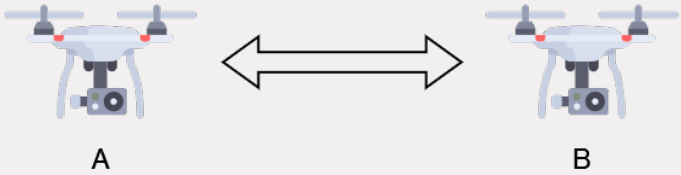
https://www.reichelt.nl/nl/nl/holybro-x500-v2-kit-drone-kit-x500-kit-v2-p324607.html?r=1

https://www.drones.nl/drones/3d-robotics-solo

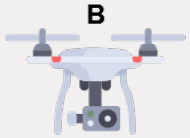
https://www.bitcraze.io/products/old-products/crazyflie-2-0/

System and Adversary Model

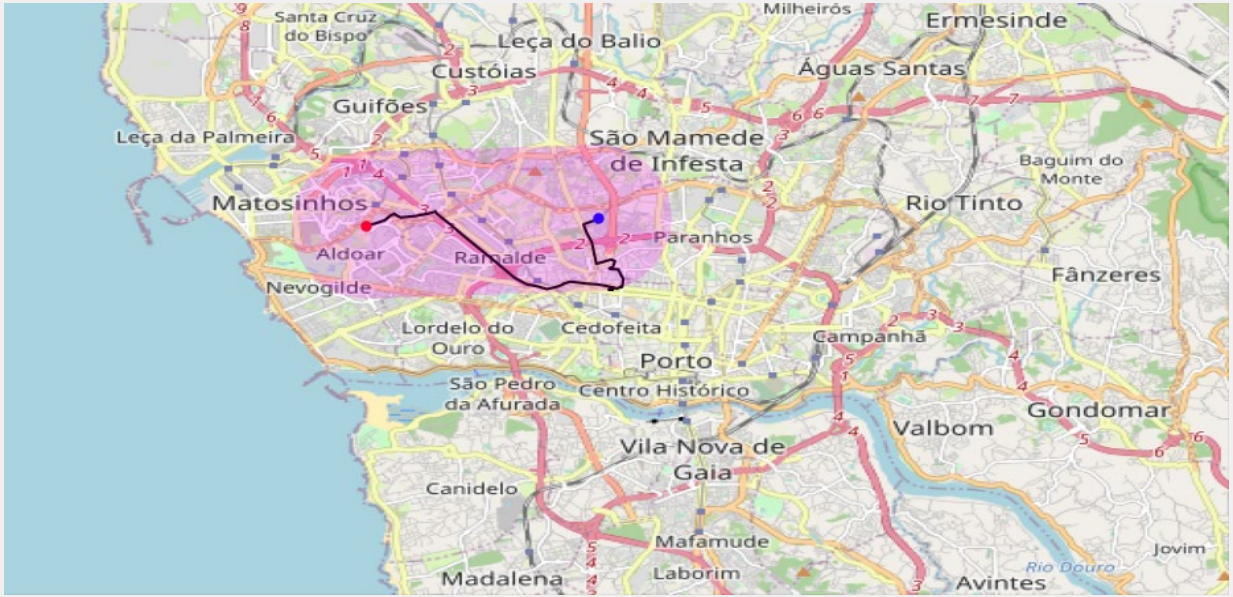
- Two Autonomous Drones
  - Pre-loaded path with time and location
  - Variable step among consecutive trajectory entries
  - Communication module available (e.g., WiFi Direct)
  - WiFi Radio Visibility
  - Traffic encryption/authentication active (e.g., TLS)
- Honest-but-Curious Adversary
  - Regular behavior (according to protocol)
  - Stealthy data mining to obtain trajectory information



PPTM - Example



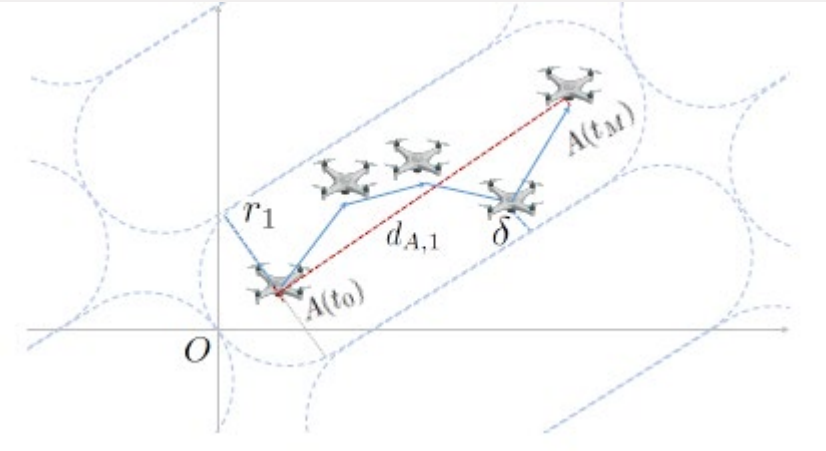
PPTM - Example



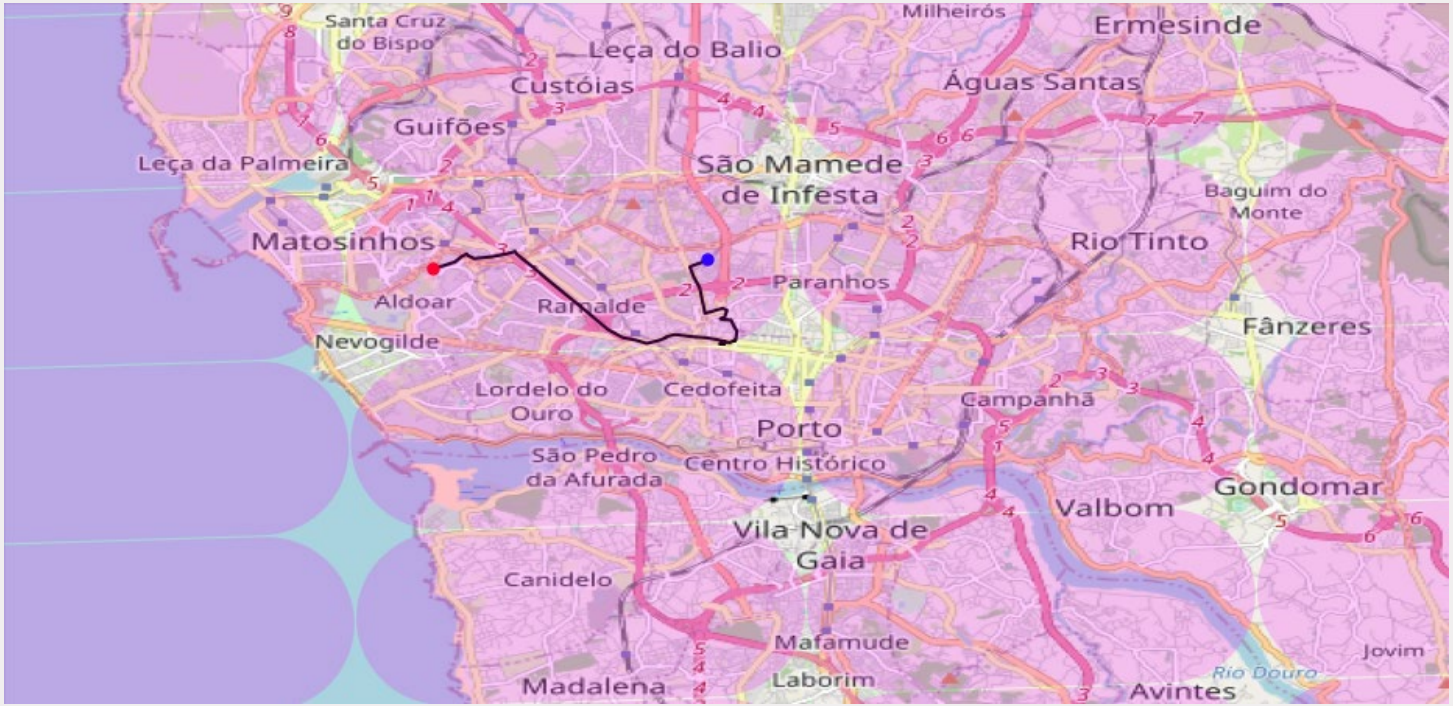
- Why a Capsule?
  - Circle around drone location
  - Multiple Circles per each point from source to destination

Space Tessellation Logic

- Line merging first and last point of trajectory
- Max distance of a point from such line d_M
- Addition of Guard Space δ (no drone can get closer than δ to a location)
- Max GPS Inaccuracy σ (location of the drone might be different than actual one)
- Radius of the capsule $r = d_M + \delta + \sigma$
- We also compute diameter and orientation of the capsule in space
- Random Origin Capsule, for capsules numbering (1,2,3,…)

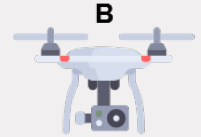


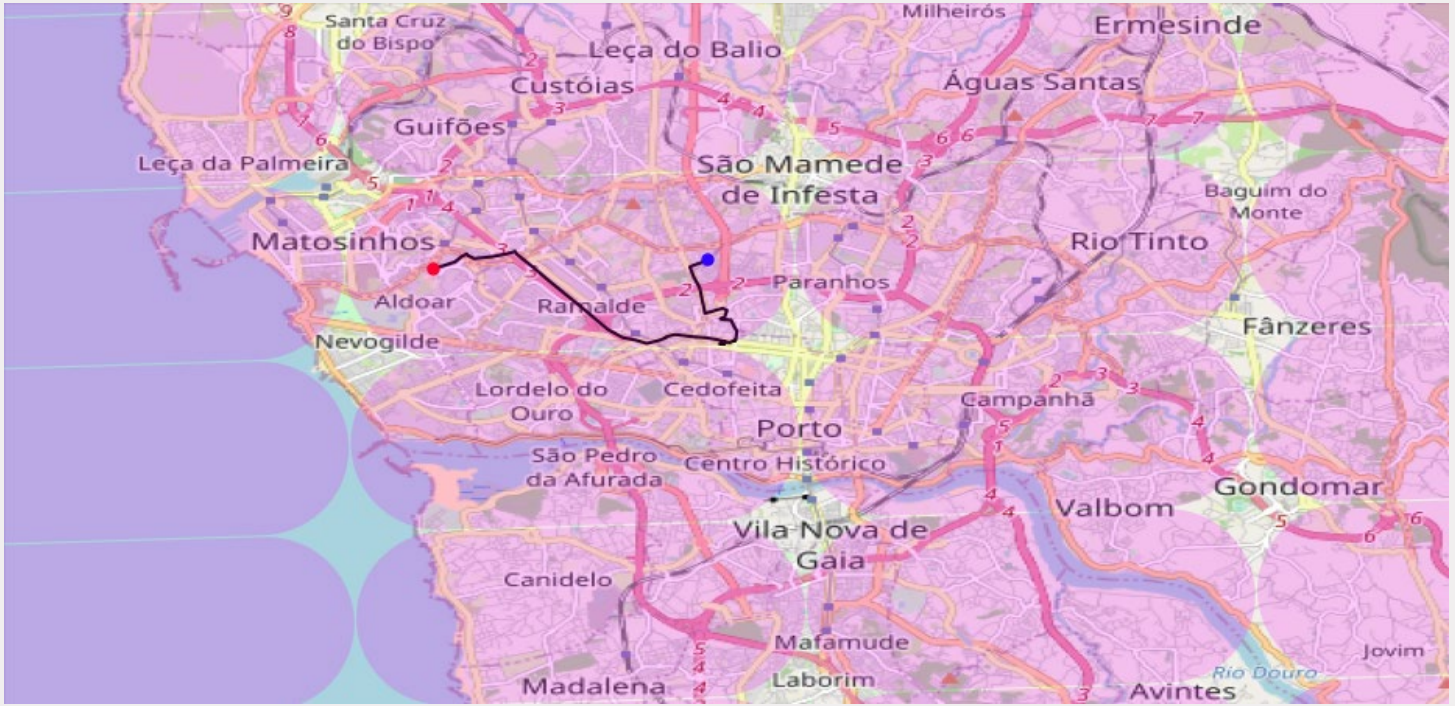
PPTM - Example



PPTM - Example

Capsule dimensions, Coordinates of 1 random capsule,

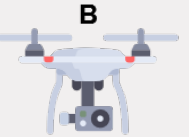


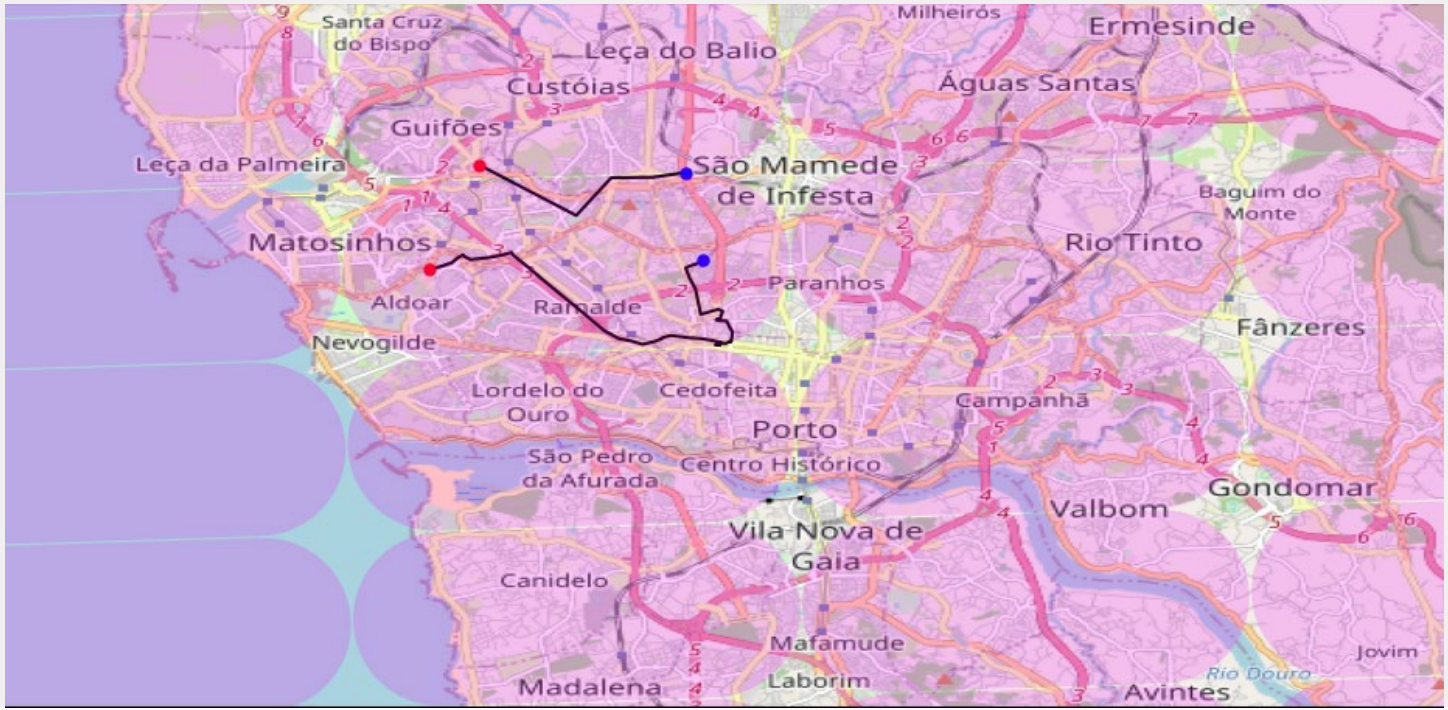


TU/e

PPTM - Example

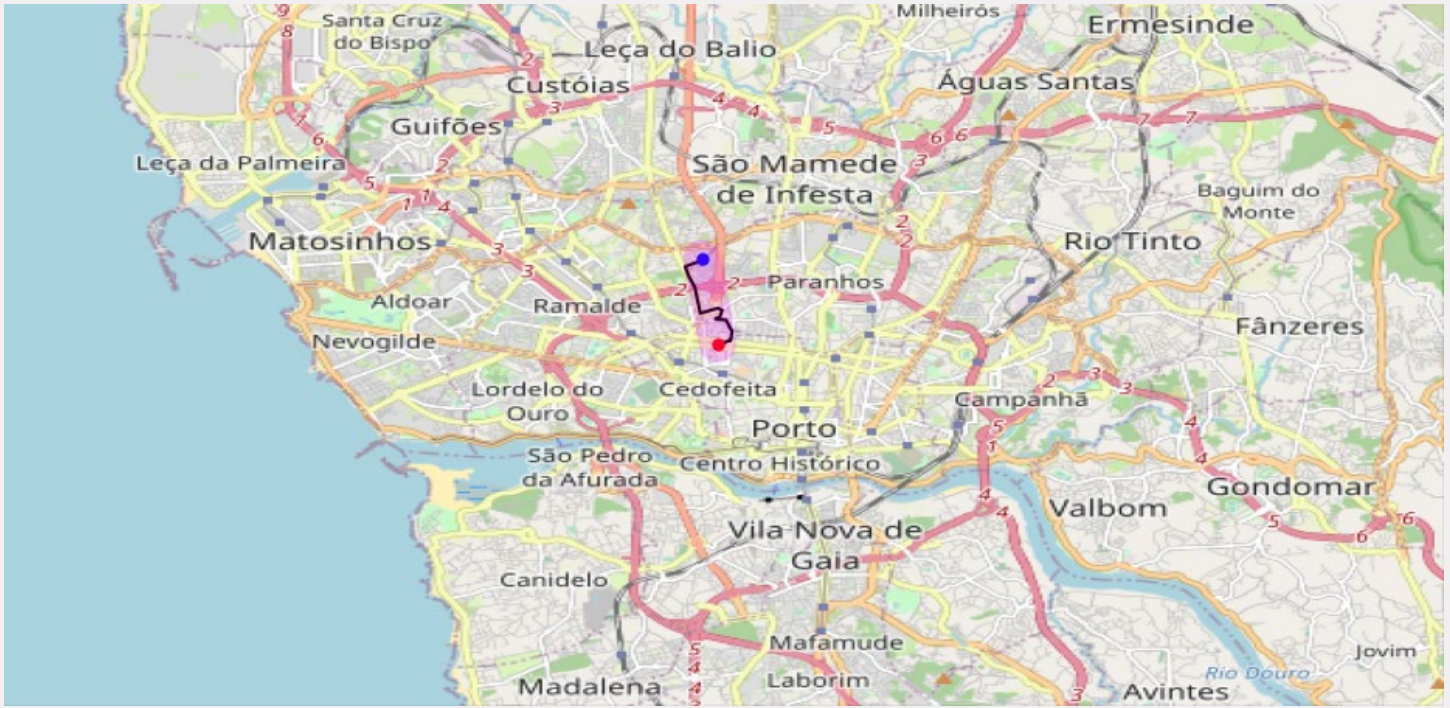
Capsules containing B's points





TU/e

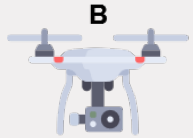
PPTM - Example



PPTM - Example

PPTM - Example

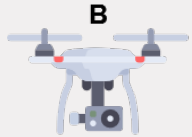
Capsule dimensions, Coordinates of 1 random capsule



TU/e

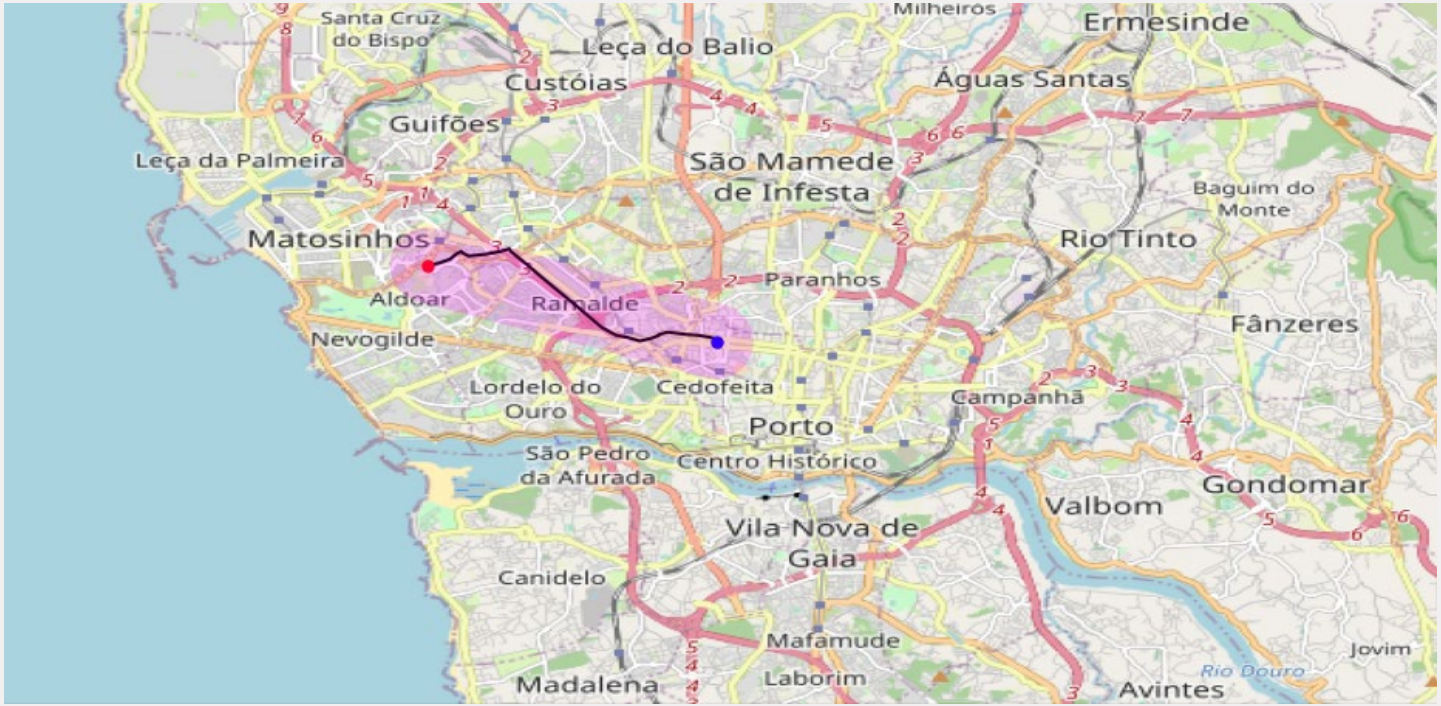
PPTM - Example

colliding capsules

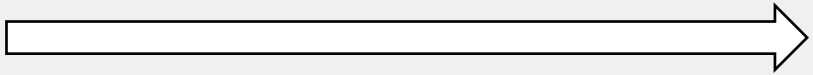


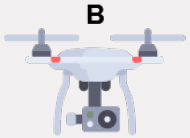
TU/e

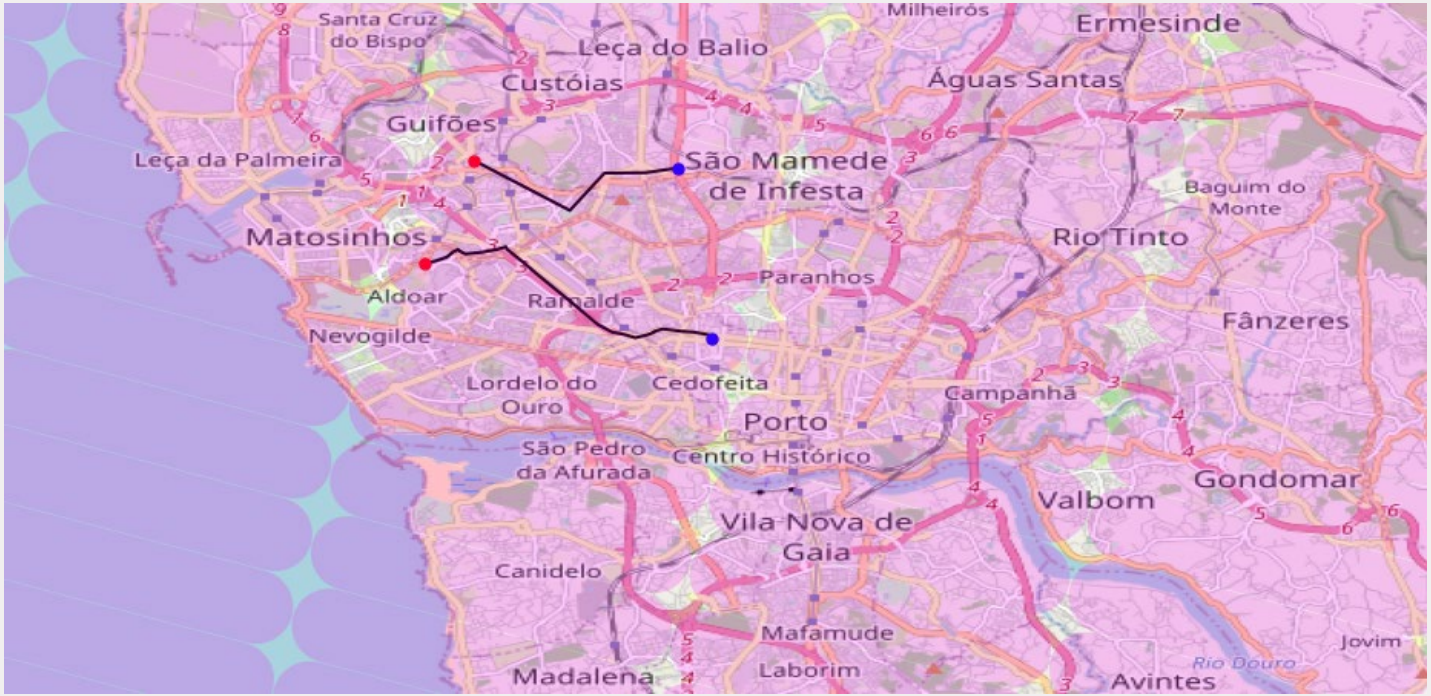
PPTM - Example



PPTM - Example



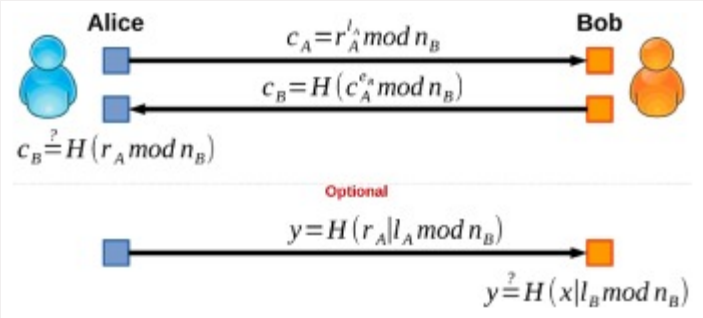




TU/e

Private Matching

- At each round, PPTM compares capsules identifiers
- If revealed, such capsules identifiers leak UAV position
- Private Set Intersection Solution (borrowed by Kotzanikolau et al.)
  - Given two private sets, we want to know the intersection, without revealing anything else
  - 1 exponentiations per comparison → more comparisons, more overhead!



https://www.sciencedirect.com/science/article/abs/pii/S0140366415002558

Truncated Mode vs Full Mode

- When do we stop halving capsules?
  - No matching among capsule identifiers → No Space Collisions → No Collision Risk
  - Capsules of A made up of 2 traj. points are colliding → Collision Risk → Truncated Mode
    - On A, no smaller capsules can be created
    - On B, smaller capsules might be created, (possibly) leading to no collision
    - Reduced overhead, but (limited) privacy leakage
  - Capsules of A and B made up of 2 traj. points are colliding → Collision Risk → Full Mode
    - Both on A and B, no smaller capsules can be created
    - More computations and communications (overhead), but no privacy leakage

- Space matching does not imply collision(A and B may travel the same traj, at different times)
- Same procedure is repeated for timestamps (Time Trajectory Match)

TU/e

Security Considerations

- Formal security analysis of single PPTM instance via ProVerif
  - Logic usage of secure crypto primitives
  - Secrecy of locations, although being weak secrets
  - Indistinguishability of the input locations

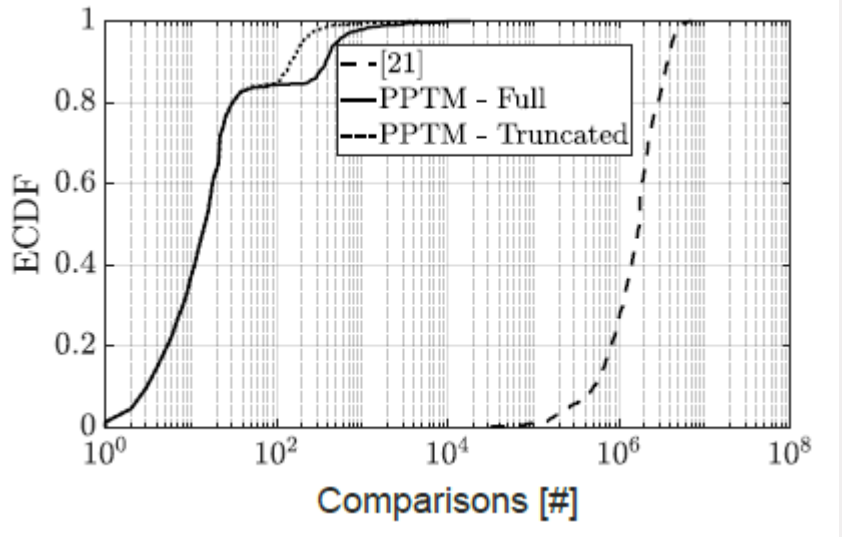
```
Verification summary:
Weak secret dA_i is true.
Weak secret dB_i_k is true.
Query not attacker(dA_i[]) is true.
Query not attacker(dB_i_k[]) is true.
Non-interference dB_i_k is true.
Non-interference dA_i is true.
```

- Code Available Open-Source: https://github.com/DominikRoy/PPTM
- Paper: Probability of correct location guessing at each step of PPTM

TU/e

Performance Assessment - Simulations

- Implementation of PPTM in MATLAB
- Evaluation of comparisons required to decide on colliding trajectories
  - Fixed no. of exps. per comparison
  - [21], point-to-point evaluation
  - 4 orders of magnitude advantage



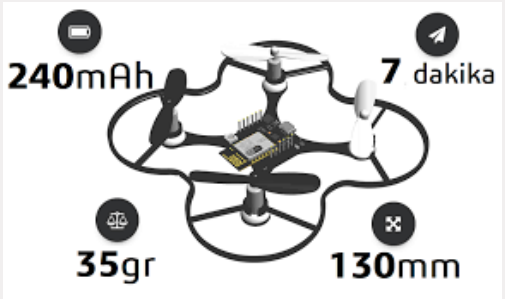
- Truncated Mode vs Full Mode
  - Faster in 20% of cases
  - Privacy Leakage (avg 0.08% of trajectory)

	Avg.	Max	Min	95% conf. int.
PPTM Trunc. Mode	0.08%	6.7%	0	0.07%-0.09%

TU/e

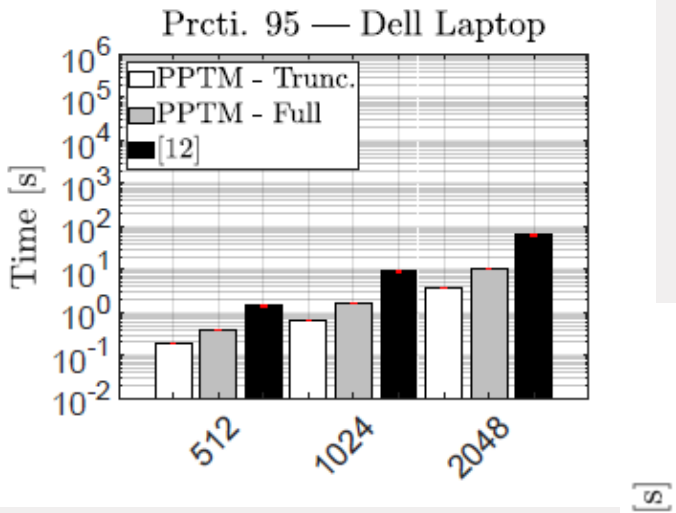
Performance Assessment on Real Devices

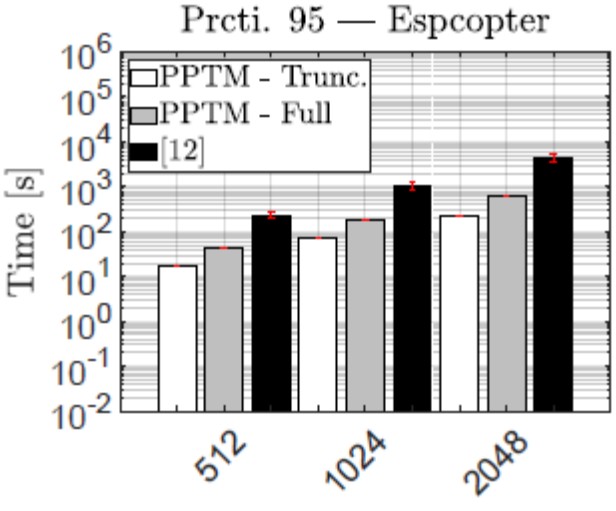
- Implementation of PPTM on real devices
  - *DELL XPS 9560*
    - *I7 CPU @ 2.8GHz (High-end UAVs)*
  - *Raspberry PI 3 Model B+*
    - *CPU @ 1.4 GHz (Commercial UAVs)*
  - *ESPCopter*
    - *ESP8266 @ 160 MHz (Constrained UAVs)*

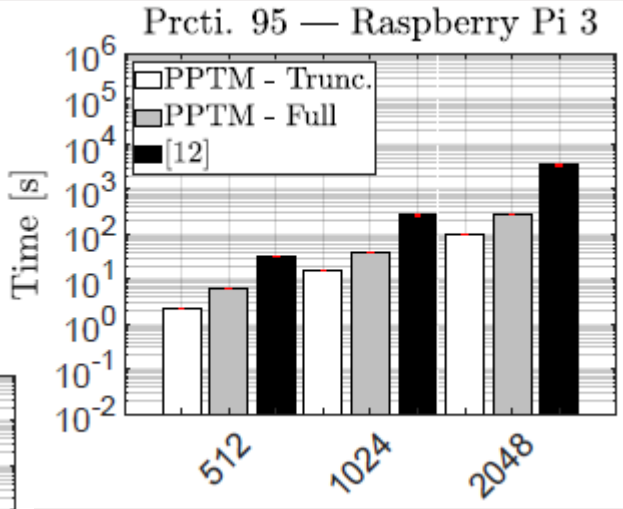


TU/e

Results and Comparison







Conclusion and Future Work

- We presented **PPTM**, an effective and efficient solution for **privacy-preserving trajectory matching on autonomous UAVs**
- Combination of a new dedicated algorithm, namely, **Incremental Capsule Matching**, with **privacy-preserving proximity testing**, to create a new solution working efficiently on spatio-temporal data sequences
- We presented two versions of PPTM, **Truncated** and **Full Mode**, the former being more lightweight at the expense of a few false-positives
- PPTM runs efficiently on very constrained devices (**98% better than closer competing solutions**)
- Future Work: Analysis with real trajectory traces, larger experimental assessment (energy)

Savio Sciancalepore, PhD

Assistant Professor
Security Group --- Faculty of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, The Netherlands
email: s.sciancalepore@tue.nl
web: sciancalepore.win.tue.nl

ACSAC 2022 – Austin (TX, US) – 7-9 December, 2022