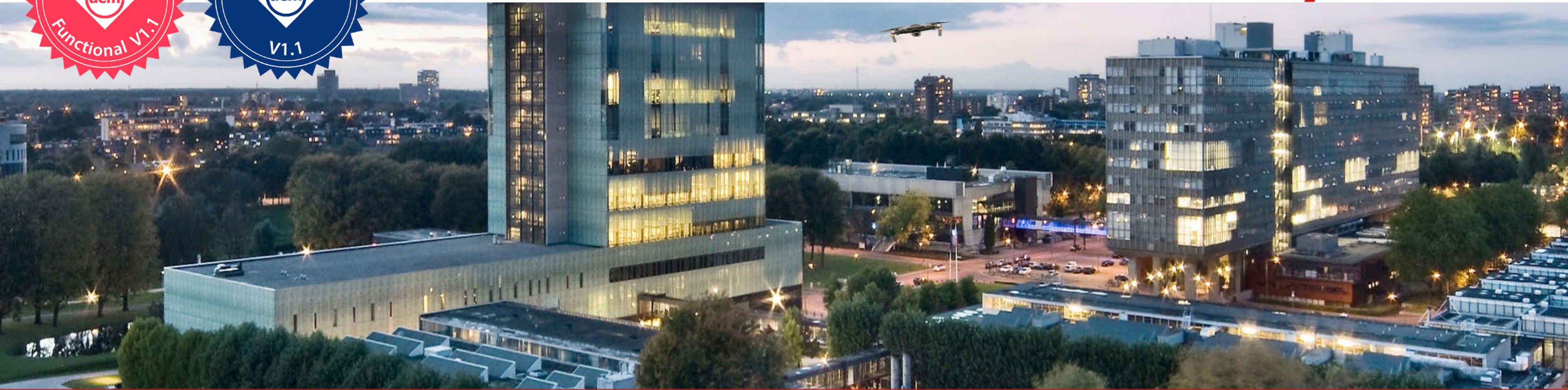
EINDHOVEN UNIVERSITY OF TECHNOLOGY



Lightweight Privacy-Preserving Proximity Discovery for Remotely-Controlled Drones

[1] Pietro Tedeschi, [2] **Savio Sciancalepore**, [3] Roberto Di Pietro
[1] Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi, United Arab Emirates
[2] Eindhoven University of Technology (TU/e), Department of Mathematics and Computer Science, Netherlands
[3] King Abdullah University of Science and Technology - CEMSE - RC3 Thuwal, Saudi Arabia

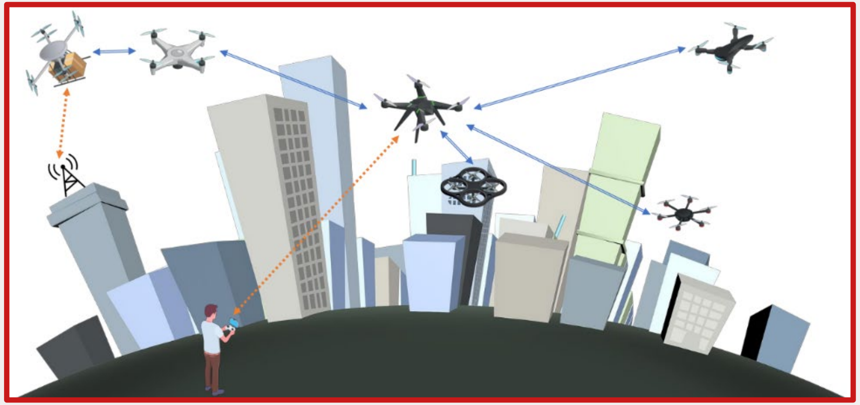
ACSAC 2023 – Austin (TX, US) – 6 December 2023

Agenda

- Context and Motivation
- System Model
- LPPD 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



Motivation

- Proximity discovery for RPAS is critical
  - UAVs Safety
  - Business Integrity
  - People Safety
  - Mission Efficiency

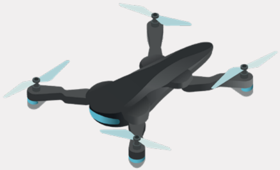
- We need a solution for real-time proximity detection between UAVs
- Naïve Solution: Sharing of Location and Time Data
  - Privacy Issues

Objective

- Can we discover proximity between remotely-piloted UAVs without disclosing precise location data?

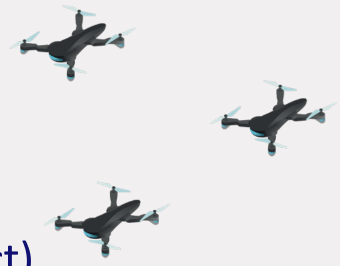
Challenges

- UAVs Heterogeneous Processing Capabilities
- Time constraints
  - Proximity should be detected before collisions occur
- Limited Energy Availability
  - From 7 to 30 mins autonomy
- GPS Inaccuracies

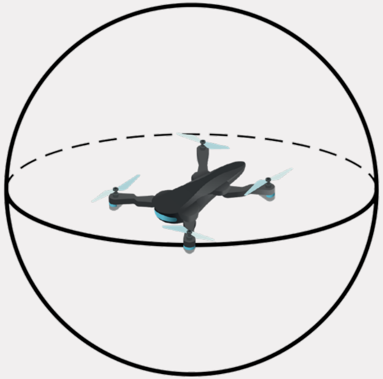


System and Adversary Model

- 2 Remotely-Piloted Drones
  - Drones occupy a given location
  - Drones can move anytime based on pilot input
  - Communication module available onboard (e.g., Wi-Fi Direct)
  - Wi-Fi Radio Visibility between the drones
  - Traffic encryption/authentication active (e.g., TLS)
- Adversary features both passive and active features
  - Objective: knowledge of the location of the drones
  - Disrupt the flight of the drone, e.g., via jamming or spoofing
  - Capture the drone

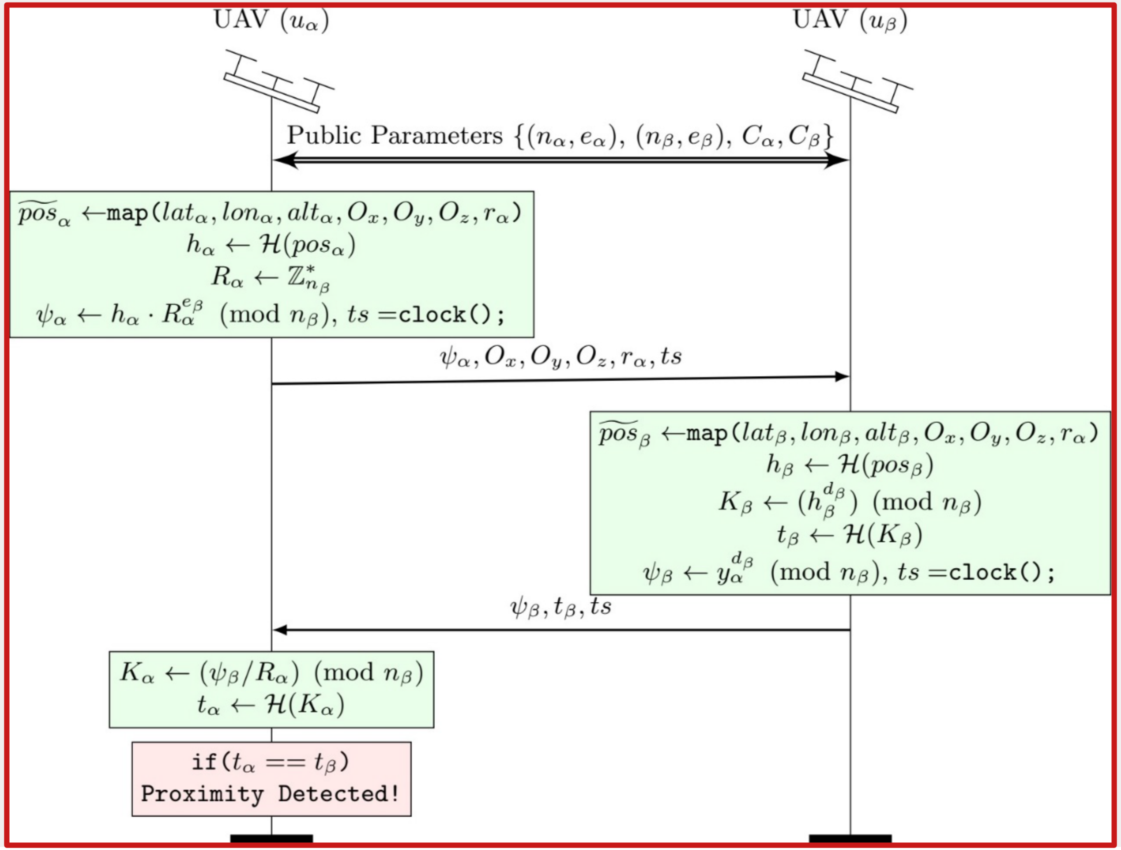


Space Tessellation Logic



- LPPD is rooted in a specific division of the Earth's surface in multiple dynamic three-dimensional spheres
- Sphere centered at the drone A location with radius r_A:
  $r_A = T_A + \delta + V_{MAX} \cdot t_p$
  - T_A Guard space, δ GNSS inaccuracy, V_{MAX} maximum speed, t_p execution time
- Random displacement of drone's location to be used for proximity detection (i.e., usage a random nonce $\boldsymbol{s} = (s_x, s_y, s_z)$). Origin **O** = **o** + $\boldsymbol{s}$
- Actual location of UAV is still at the center of a sphere, but the specific identifier of the sphere is moved according to the nonce
- The comparison among the identifiers occurs in the encrypted domain, using *private-set intersection*

Private Set Intersection



Considerations

- We only detect proximity: evasion maneuvers follow (out of scope)
- LPPD needs to be run for every couple of communicating drones (scalability is a concern)
- Security and Privacy
  - Only assumption: trust on public key/certificate of remote party
  - Location is never disclosed (difficulty: breaking RSA)
  - Spoofing protection thanks to TLS
  - Wireless Localization Attacks
    - Tackled in another paper (CCNC 2024)
    - Not so easy to achieve (requires infrastructure of multiple sensors)
    - Not so accurate depending on environmental factors (noise)

Security Considerations

- Formal security analysis of single LPPD instance via ProVerif
  - Logic usage of secure crypto primitives
  - Secrecy of locations, although being weak secrets
  - Resistance of the protocol to offline guessing attacks on the locations
  - Authenticity of the messages

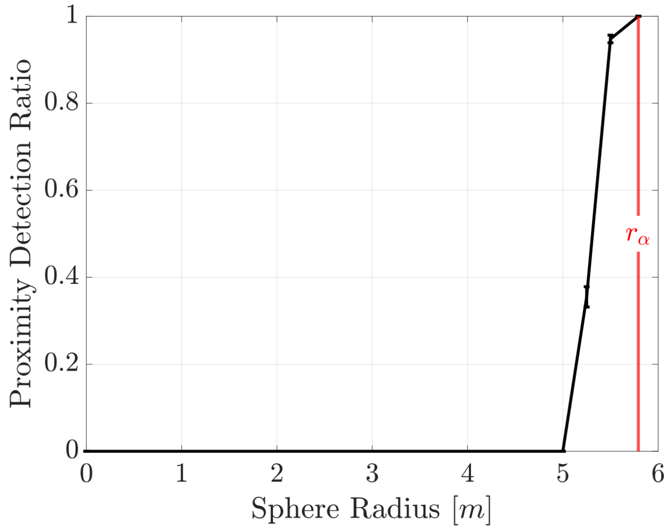
Verification summary:
Weak secret posA is **true**.
Weak secret posB is **true**.
Query inj-event(termUAVa(x, y)) ⟹ inj-event(acceptUAVb(x, y)) is **true**.
Query inj-event(termUAVb(x, y)) ⟹ inj-event(acceptUAVa(x, y)) is **true**.
Query not attacker(**posA**[]) is **true**.
Query not attacker(**posB**[]) is **true**.

- Code Available Open-Source: https://github.com/pietrotedeschi/lppd/

TU/e

Accuracy Assessment - Simulations

- Simulation Analysis via MATLAB
- 50 UAVs to move randomly in a geographical area of $50 \times 50 \times 120\ m^3$, at a random speed $[0 - 20.88]\frac{m}{s}$
- GPS Error $\delta = 0.375m$
- Common guard space of $5m$
- Guard Radius: $\delta + T + VMAX \cdot tp = 0.375 + 5 + 20.88 \cdot 0.02 = 5.793m$
- Increasing the sphere radius increases the capability of LPPD to detect co-locations



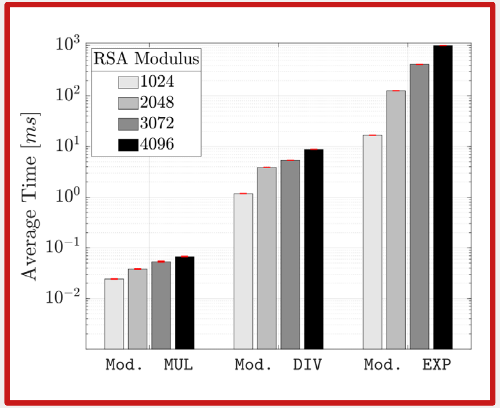
TU/e

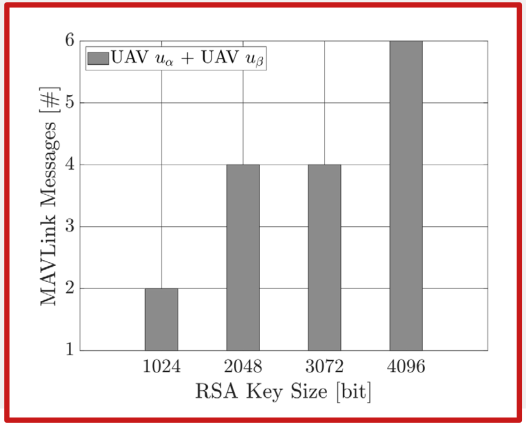
Performance Assessment on 3DR-Solo Drone

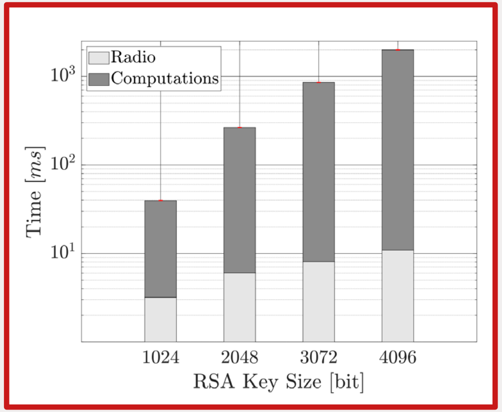
- Implementation of LPPD on a real drone
  - *Hardware*
    - *3DR-Solo Drone*
      - ARM Cortex A9 1.00 GHz
      - 7, 948 MB (ROM)
      - 512 MB (RAM)
  - *Software*
    - 3DR Poky Linux (Yocto)
    - C Programming Language
    - Micro Air Vehicle Message Marshalling Library
    - OpenSSL
    - 1,545.324 KB of Flash Memory and 90.179 KB of RAM

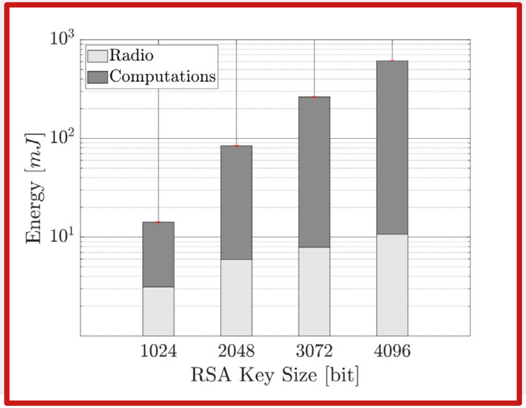
TU/e

Performance Evaluation









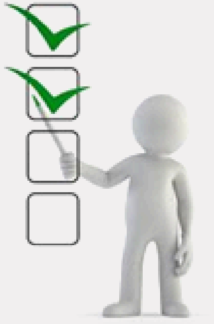
- Time consumption

With RSA Key Size of 3072 or less, always less than 1 second

- Energy Consumption

14.15mJ of energy, i.e., the $5 \cdot 10^{-6}\%$ of the 3DR-Solo battery

Conclusion and Future Work



- We presented **LPPD**, the first solution for lightweight privacy-preserving proximity discovery for remotely-piloted Unmanned Aerial Vehicle
- Combination of a novel space tessellation logic based on randomized spheres with a lightweight solution for private-set intersection
- Security of LPPD has been formally verified
- LPPD consumes only $14.15mJ$ of energy, i.e., the $5 \cdot 10^{-6}\%$ of the 3DR-Solo battery
- Future Work: Extension of **LPPD** in a broadcast scenario (compliance with Remote ID)

Savio Sciancalepore, PhD

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