Geocaching-inspired Resilient Path Planning for Drone Swarms

Michel Barbeau[1], Joaquin Garcia-Alfaro[2], and Evangelos Kranakis[1]

[1]Carleton University, Ottawa, Canada
[2]Institut Polytechnique de Paris, Telecom SudParis, France

IEEE MiSARN
April 29th, 2019

Introduction

- Path planning algorithm for drone swarms
  - None of the drones knows the path and final destination
  - Collectively determine and uncover step-by-step the path and final destination
  - Resolve a localization problem at each step
- Geocaching inspired
  - Collectively hide and seek objects while at the same time navigating a waypoint trajectory
- Shared-information and is fault-tolerant
  - Correctly navigate provided that the number of faulty drones is less than $\frac{n-d}{2}$, where n is number of drones and d is the dimension $(d = 2, 3)$

Shared-information Path Planning - Localization Problem

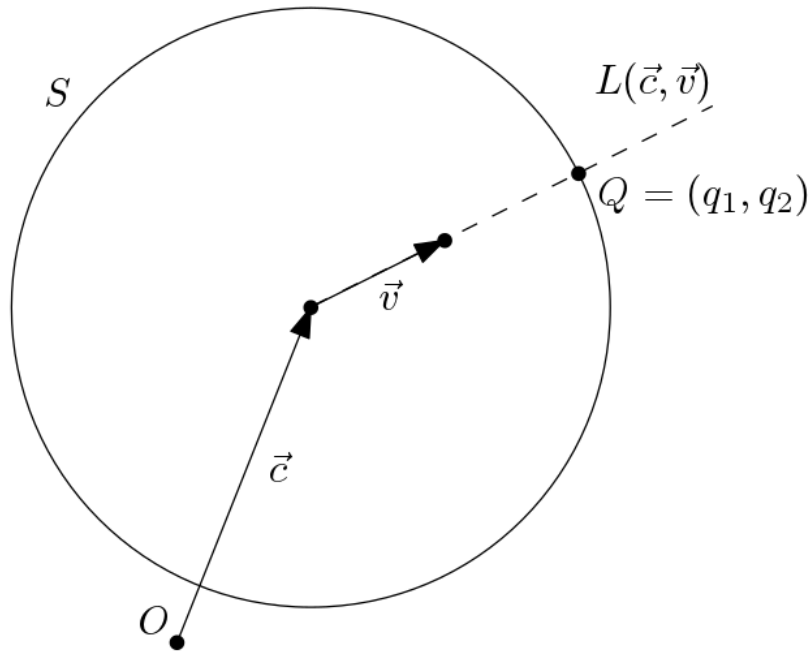


Figure: In Euclidean space with origin O, the point Q is on the intersection of the line of action of vector $\vec{v}$, i.e., $L(\vec{c}, \vec{v})$ & perimeter of the circle S

Shared-information Path Planning - Representing Waypoints

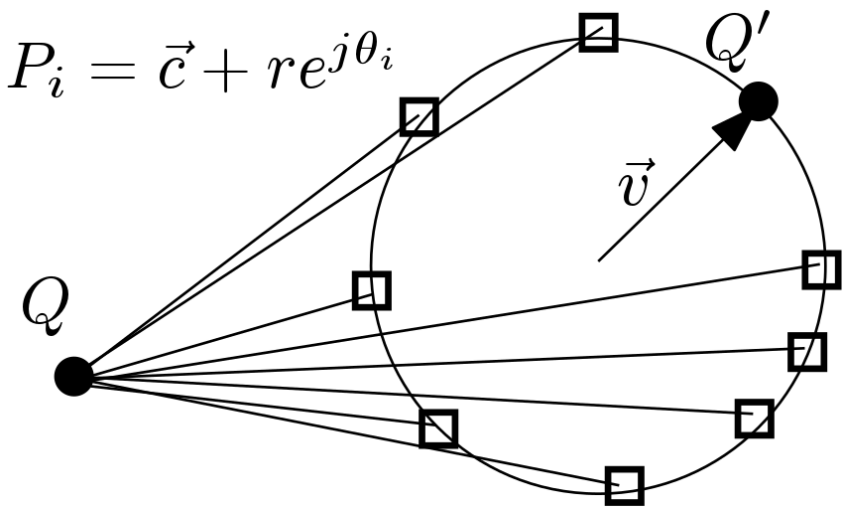


Figure: Given points Q, Q' a unique circle can be determined. It is formed by the new positions of the drones (depicted as squares) in such a way that the point Q' lies on its perimeter.

Shared-information Path Planning - Representing Paths

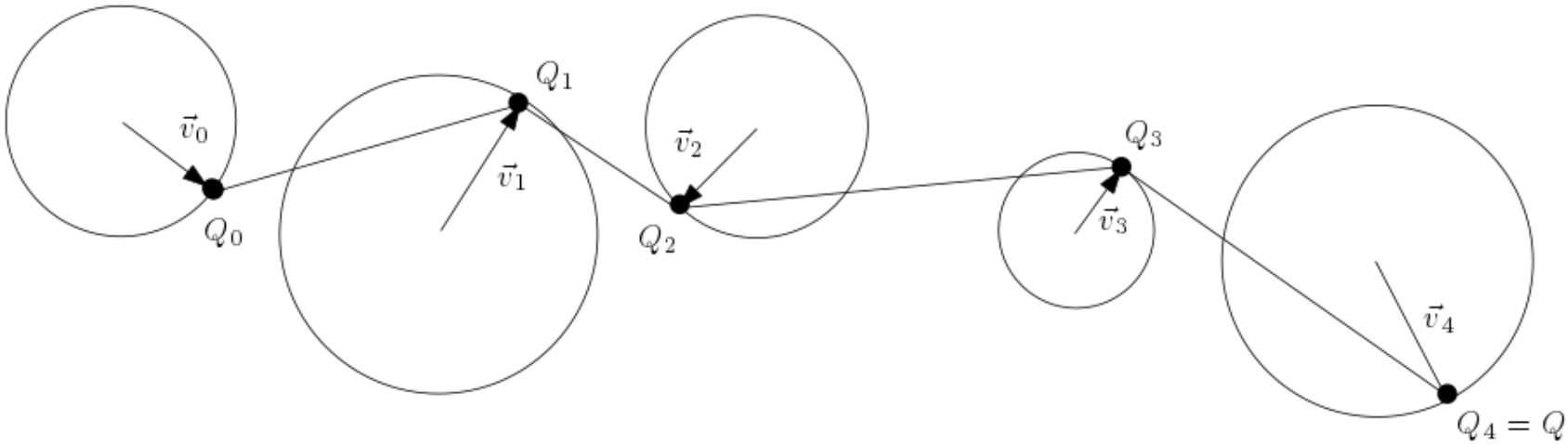


Figure: A path consisting of four hops, as traversed by the drones. The drones start from point Q_0. In each instance, they use a direction vector $\vec{v}$ to compute an intermediate destination point Q_i on the perimeter of a circle. They determine their new positions and again compute the next intermediate destination using the next destination vector. This is repeated until the final destination point Q is reached.

Fault Tolerance and Resilience to Attacks

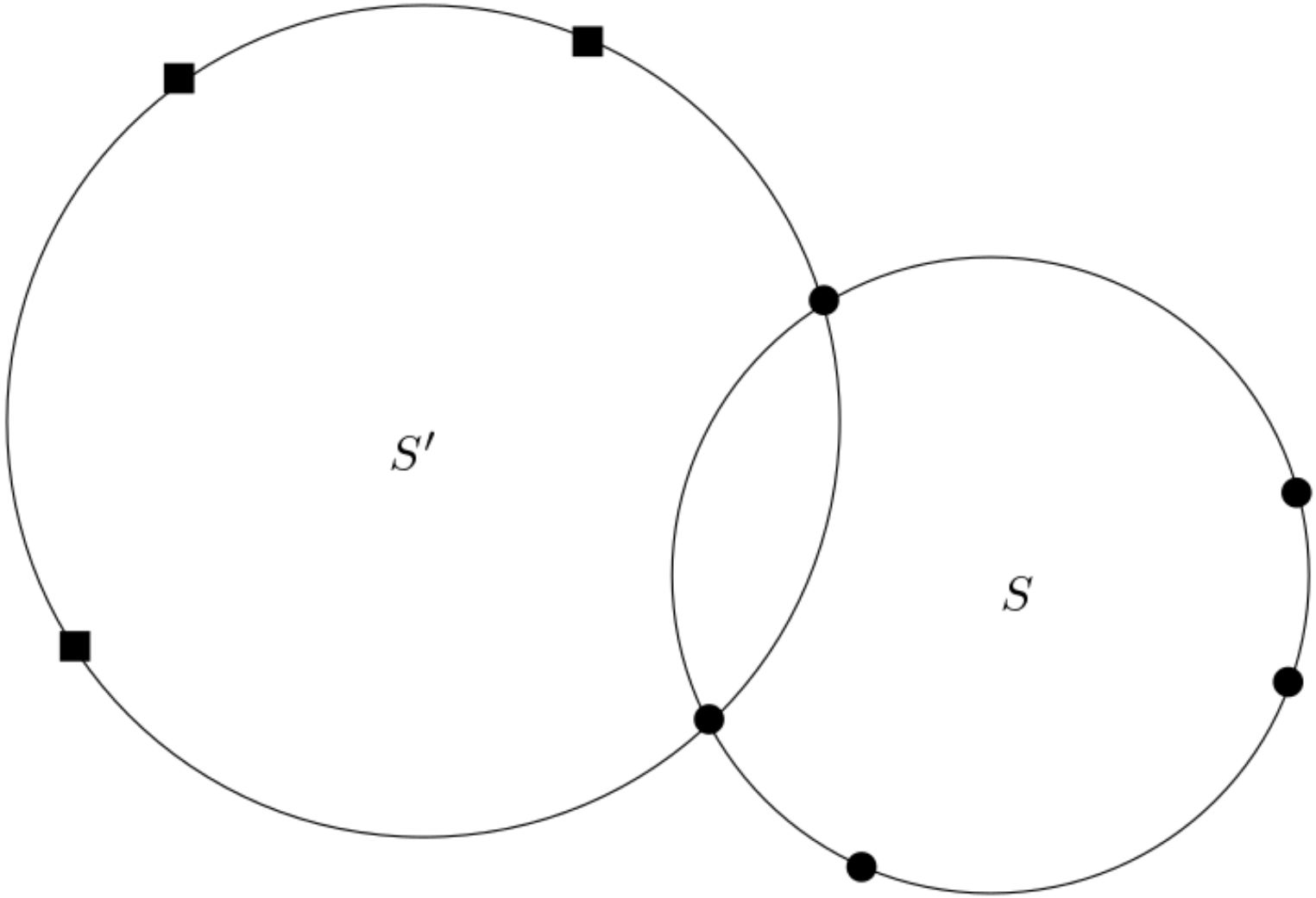


Figure: An arrangement of $n = 8$ drones with $f = 3$ faulty. Black dots represent reliable drones and black squares faulty drones.

Fault Tolerance and Resilience to Attacks

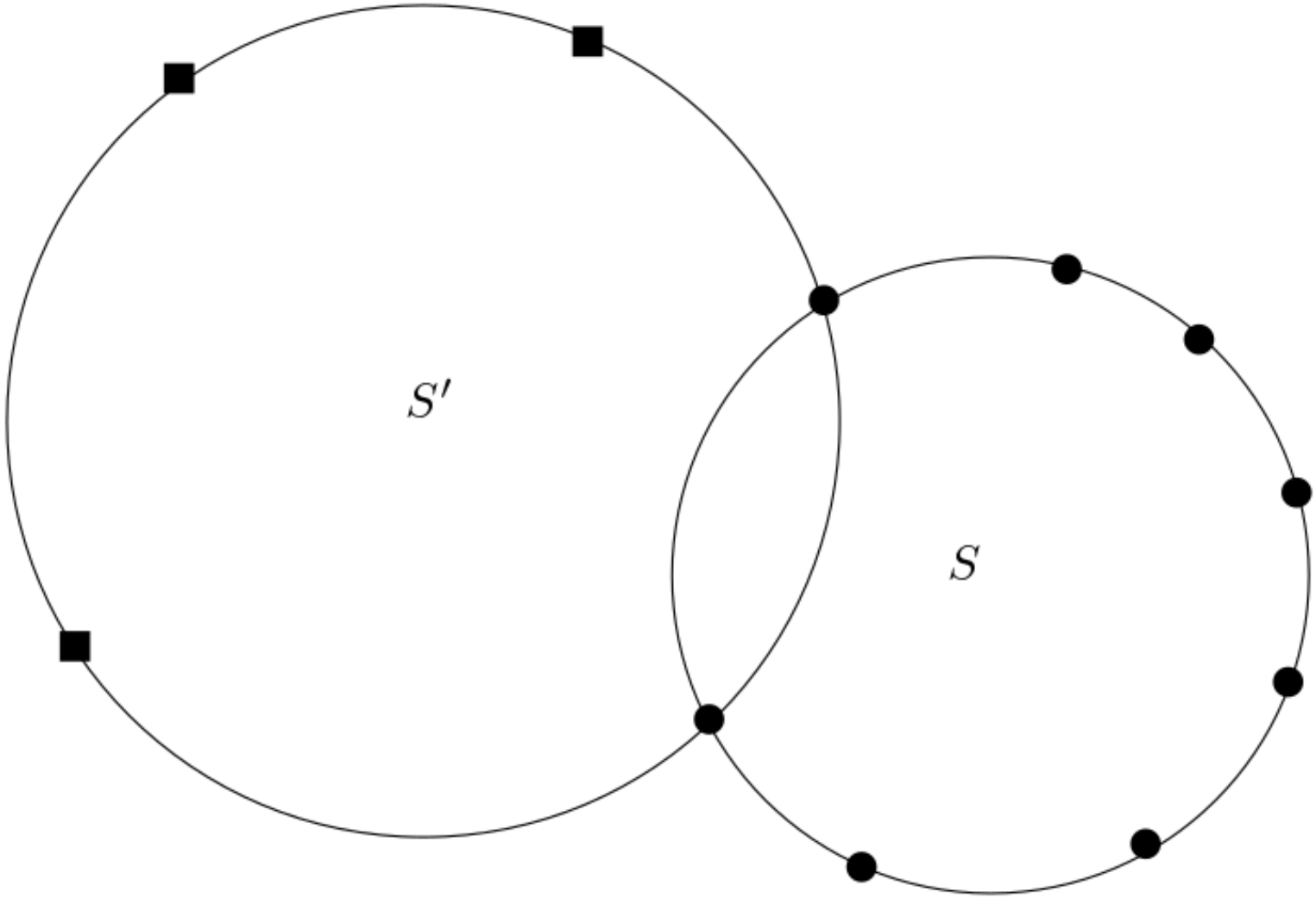
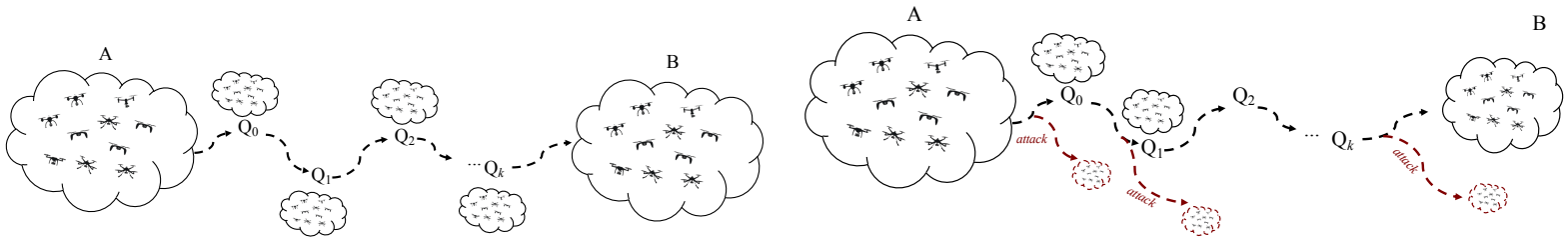


Figure: An arrangement of $n = 11$ drones with $f = 3$ faulty. Black dots represent reliable drones and black squares unreliable drones.

Simulations & Early Results

Simulation Scenarios

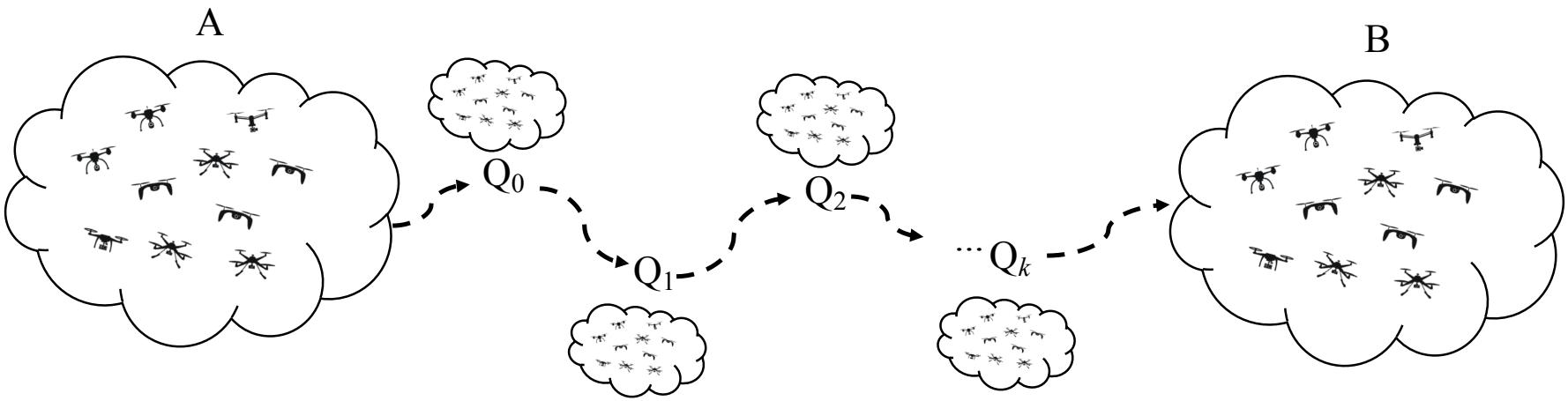


(a) Baseline (prior attacks)

(b) Defense strategy (under GPS jamming and spoofing attacks)

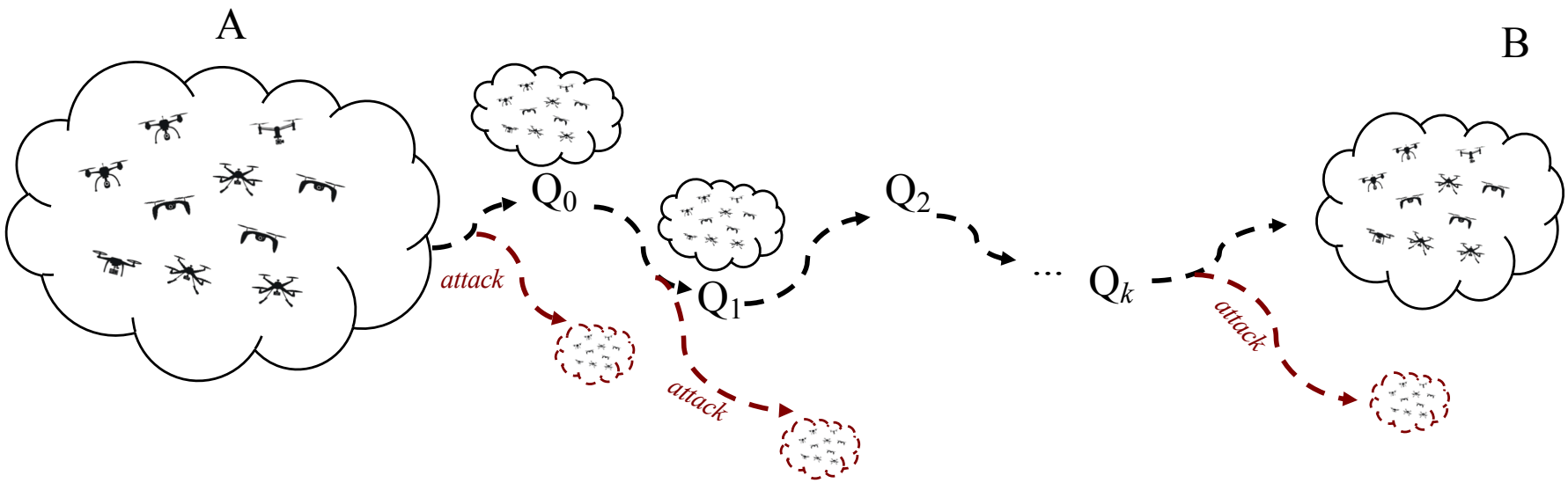
Figure: Simulation scenario. (a) depicts a swarm of n drones, starting at point A and **cooperating to reach point** B, after visiting k intermediate waypoints (i.e., $Q_0, Q_1, Q_2, \ldots, Q_k$). (b) depicts a series of **zombie** drones (under the control of the **remote adversary**) & **captured** drones (**disrupted** by GPS **jamming & spoofing** attacks perpetrated by the zombie drones). Both victim types in **(b) fail at reaching the waypoints of the path & get lost forever**. Only a few survivor drones from the original swarm succeed at reaching the final destination.

Simulation Scenarios [zoom 1/2]



(a) Baseline (prior attacks)

Simulation Scenarios [zoom 2/2]



(b) Defense strategy (under GPS jamming and spoofing attacks)

Real World GPS Spoofing[1] [1/2]

[http://www.dailymail.co.uk, Dec 2011]:

- US drone lost over Iranian airspace
- Drone shown on Iranian TV (intact?)
- Iranian engineers claimed GPS spoofing to *trick* the drone into landing in Iran
- http://dailym.ai/2GD0wiO

[Inside GNSS, http://j.mp/IGNSSJul13]:

- Research team from Texas University successfully spoofed a ship's GPS-based navigation system sending the 213-foot yacht hundreds of yards off course
- The ship actually turned while the chart display & the crew saw only a straight line

[1] [Shepard et al. 2012] Evaluation of Civilian UAV Vulnerability to GPS Spoofing Attacks. ION GNSS Conference Nashville, TN, September 1921, 2012

Real World GPS Spoofing [2/2]

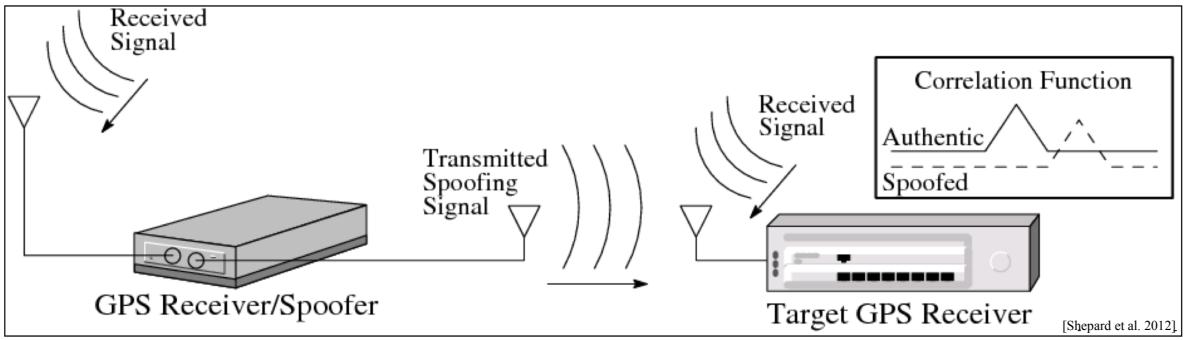


Figure: Texas University Civilian GPS spoofing testbed. Spoofing involves **broadcasting realistic**, though inaccurate, **GPS signals** (e.g., start out sending valid signals in synch with real signals, **gradually** up the bogus signals strength while **altering the location data**).

OMNeT++ Simulation Testbed [1/3]

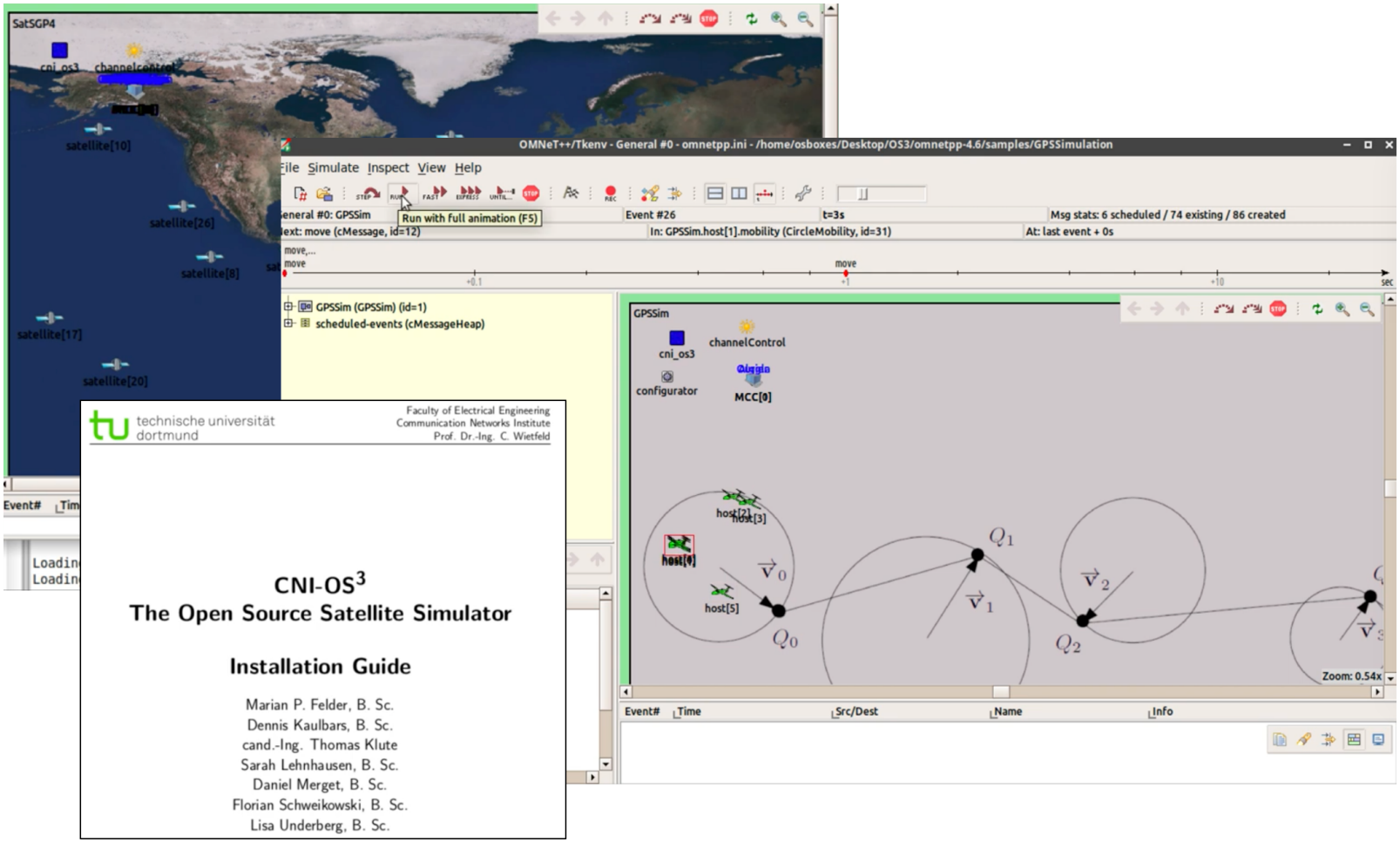
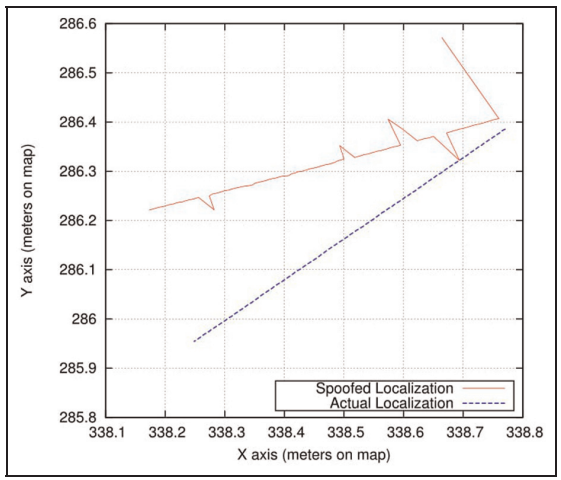


Figure: Sample visualization captures of our ongoing simulation testbed using OMNeT++, OS3 and GNSSim [Javaid *et al.* 2017]. Some additional information available at **http://j.mp/gnssimuav**.

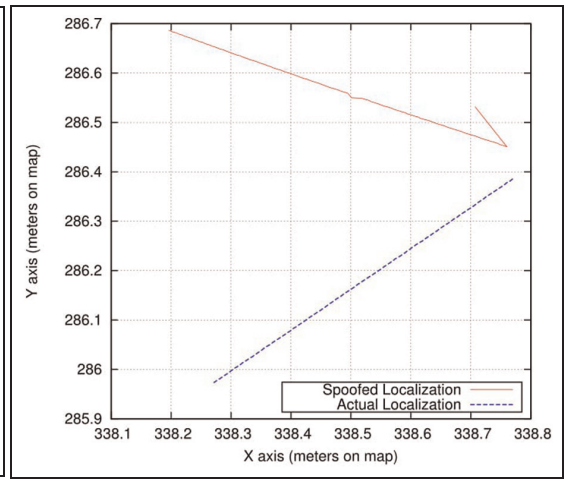
OMNeT++ Simulation Testbed [2/3]

`https://github.com/ayjavaid/OMNET_OS3_UAVSim` [Javaid *et al.* 2017]

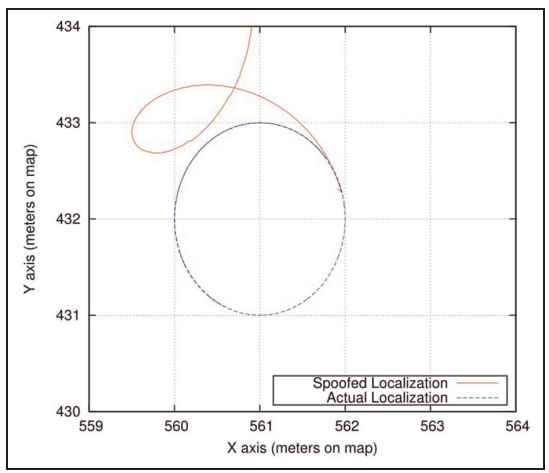
Effect of discrepancy. (a,b) Linear path. (c,d) Circular paths.

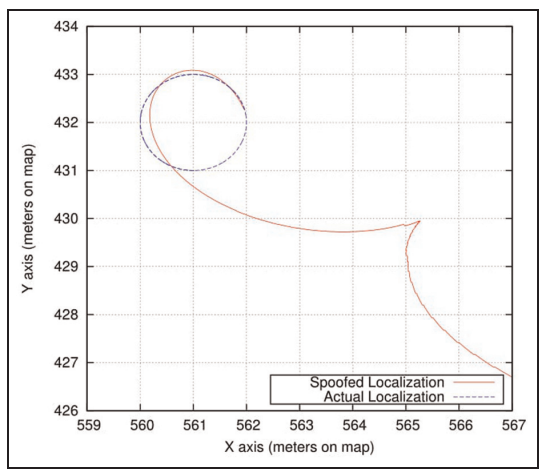


(a) Spoofed X-values



(b) Spoofed Y-values





(c,d) Spoofed X- & Y-values

OMNeT++ Simulation Testbed [3/3]

Parameter	Value
Mobility type of satellites	*SarSGP4Mobility*
Mobility type of drones	*PathPlanningMobility*
Transmitter power	*500 watts*
Packet interval	*0.5 seconds*
Burst duration	*10 seconds*
Sleep duration	*0 seconds*
Position update interval	*1 second*
GPS Jamming attack range	*100 km*
GPS Spoofing attack range	*100 km*
Drone communication range	*80 km*

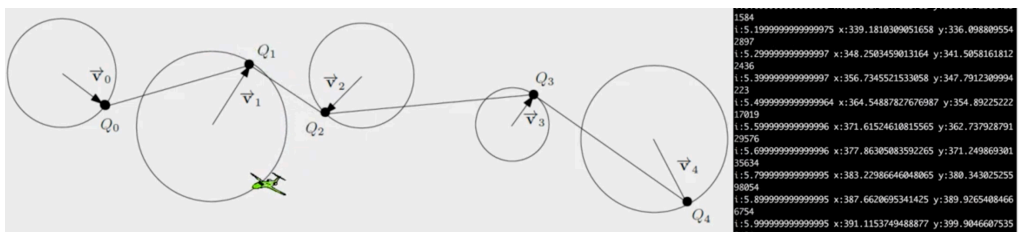


Figure: Parameters used in our simulations. Further details, available at the companion Website, see **http://j.mp/gnssimuav**

Simulation scenario and early results

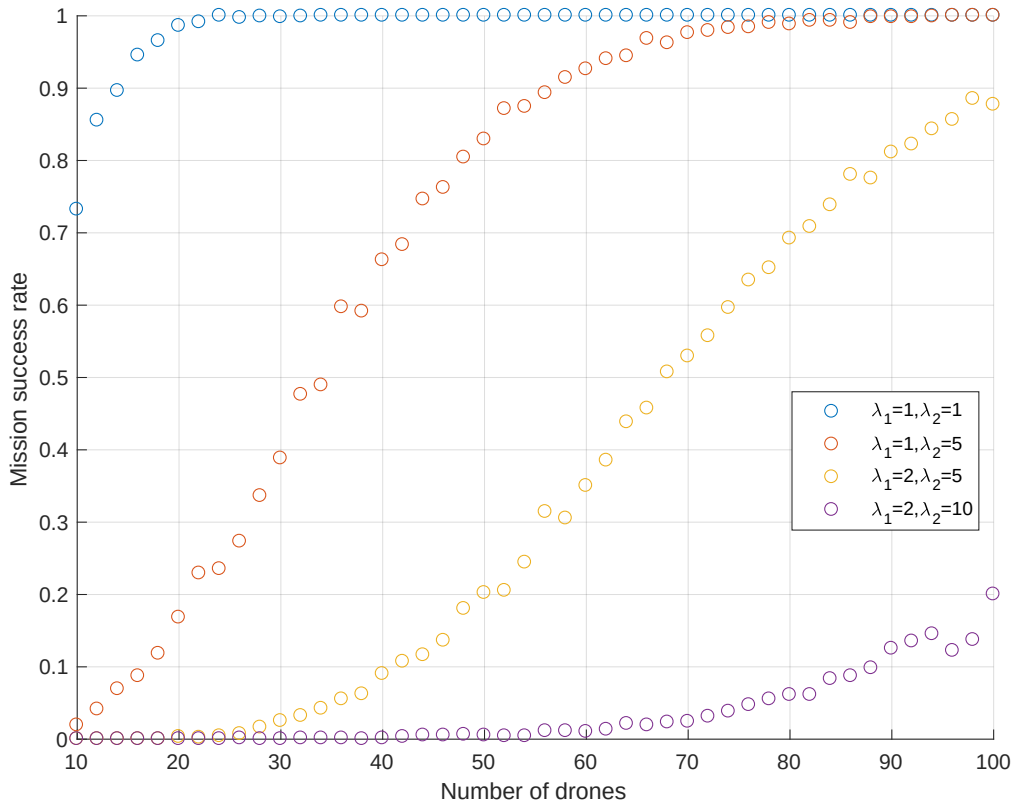


Figure: Number of zombies per attack follow a Poisson distribution (λ_1), as well as number of victims per zombie (λ_2). **Mission succeeds** if, at least, **one drone** reaches the final destination. **Success rate grows** consistently with the number of drones (i.e., more **collective work**); while **greater values for the parameters λ_1 and λ_2** translate in higher impact of the attack & **less chances of mission success**.

Conclusion

- **Vulnerability to GPS spoofing attacks** must be handled with alternative solutions & **robust localization techniques**
- **Collective work** to determine & uncover path steps using secret sharing leads to fault-tolerant navigation systems
- Further work includes **visual odometry** (e.g., use of downward facing cameras and inertial sensors, to identify and follow **visual landmarks**)

Thank you. Questions?

References

- **Kleinberg** *E Pluribus Unum*, in "This Will Make You Smarter: New Scientific Concepts to Improve Your Thinking" (J. Brockman, editor). Harper Perennial, 2012.
- **Mackenzie and Duell** *We hacked US drone*, Dailymail, December 2011, `https://dailym.ai/2GD0wiO`
- **IG Inside GNSS** *GPS Spoofing Experiment Knocks Ship off Course*, July 2013, `http://j.mp/IGNSSJul13`
- **Shepard et al.** Evaluation of Civilian UAV Vulnerability to GPS Spoofing Attacks. ION GNSS Conference Nashville, TN, September 1921, 2012.
- **Jahan et al.** GNSSim: An Open Source GNSS/ GPS Framework for Unmanned Aerial Vehicular Network Simulation. EAI Endorsed Transactions on Mobile Communications and Applications, 2(6), 2015.
- **Javaid et al.** Analysis of Global Positioning System-based attacks and a novel Global Positioning System spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation, Transactions of the Society for Modeling and Simulation International, DOI: 10.1177/0037549716685874, 2017.