Delivery Drones and Citizen Privacy

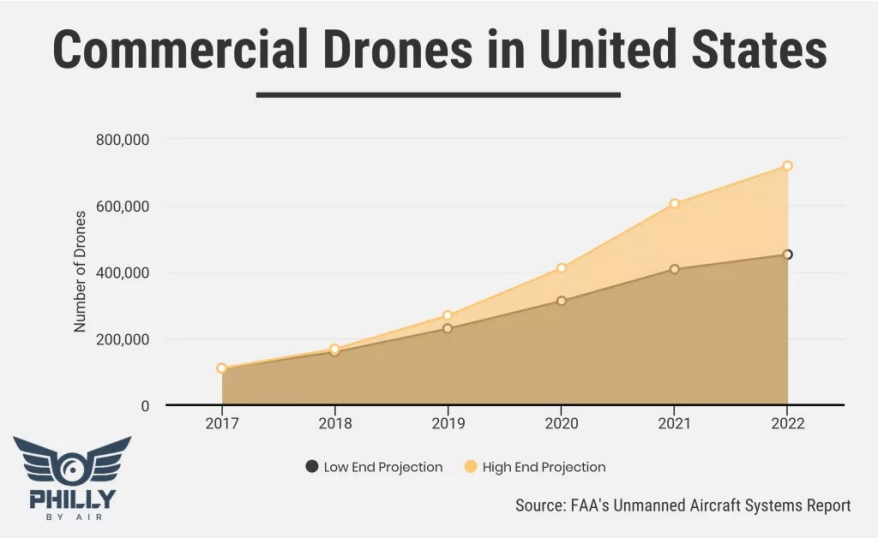
Vinod Ganapathy

vg@iisc.ac.in

Computer Systems
Security Laboratory

IISc Bangalore

Privacy in the age of drones



Predicted 2.4 million hobbyist UAVs by 2022
Predicted 450,000 commercial UAVs by 2022
[FAA Aerospace Forecast FY 2018-2038]

- End-user drones are now commonly available.
- Equipped with sensors such as cameras and GPS.
- Threat to individual privacy.
- Regulations are loose and mechanisms to enforce privacy are lacking!

Our focus: Delivery drones

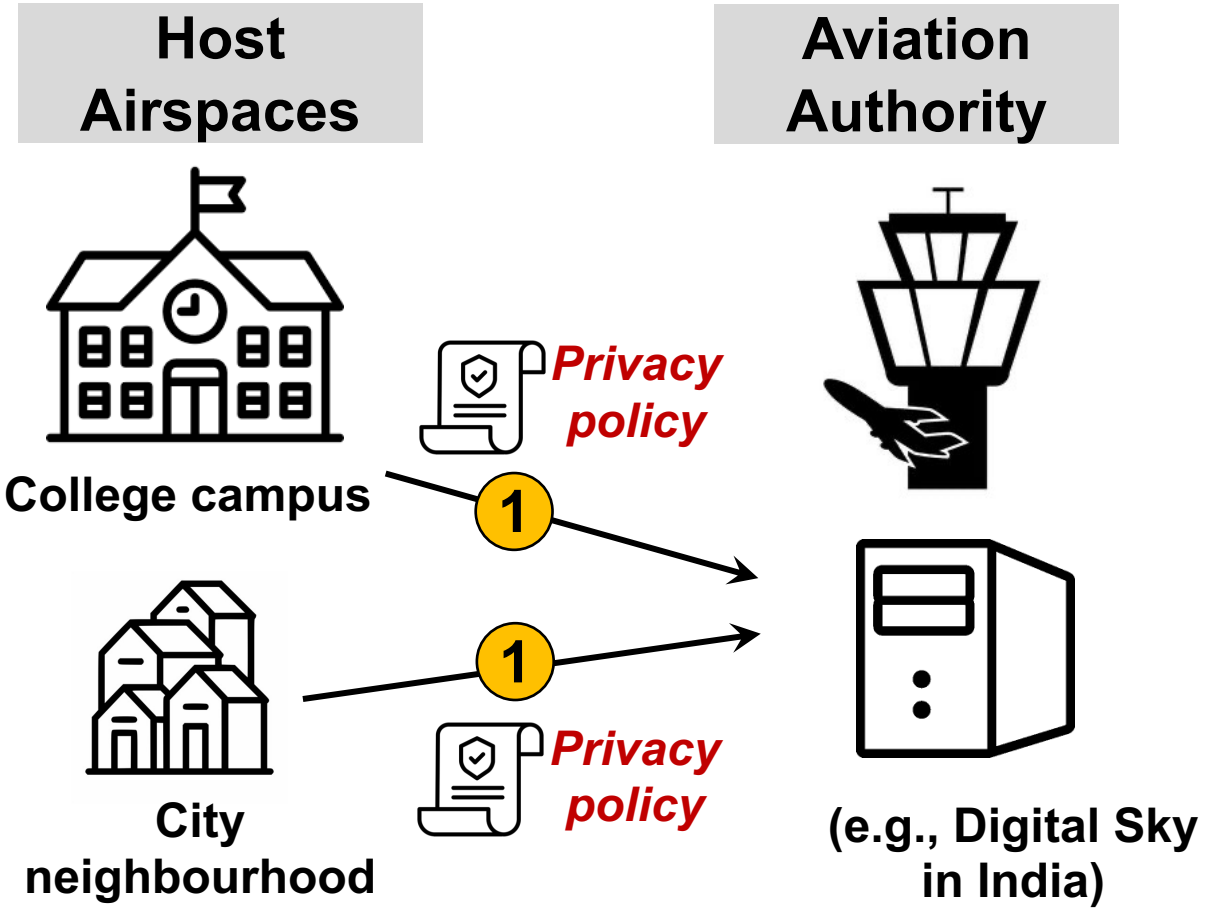
- Incentive to comply with privacy regulations?
  - E-commerce companies with reputations to protect → no overt malicious intentions → our threat model can exclude rogue drones.
  - Strong interest to comply with local regulations.
- Yet, we need to mechanisms to enforce privacy:
  - Different **host airspaces** may have different privacy needs
  - E-commerce companies may contract out drone operations to third-party fleet operators (*a.k.a*. “delivery-service partners”).
  - Host airspaces may wish to determine that these **guest drones** comply with their privacy requirements.

Enter → Privaros

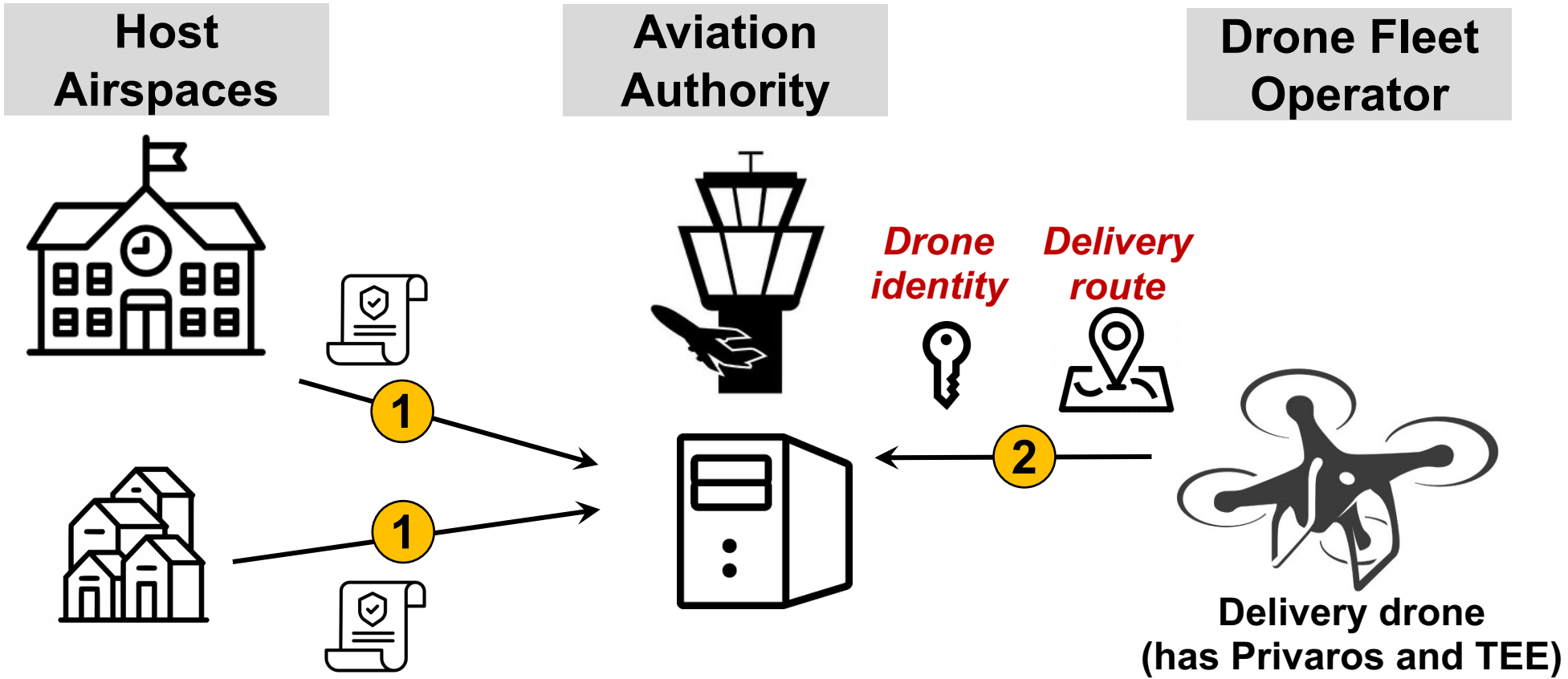
Drone software stack with mechanisms to enforce privacy policies specified by host airspaces

- Adds **mandatory access control (MAC)** based policy enforcement to the **Robot Operating System** (ROS v2).
- **Runs on the guest delivery drone** and enforces MAC policies in the OS and ROS layer.
- Uses **hardware-based attestations** from a trusted execution environment (TEE) on guest drone convince host airspace that guest drone runs Privaros.

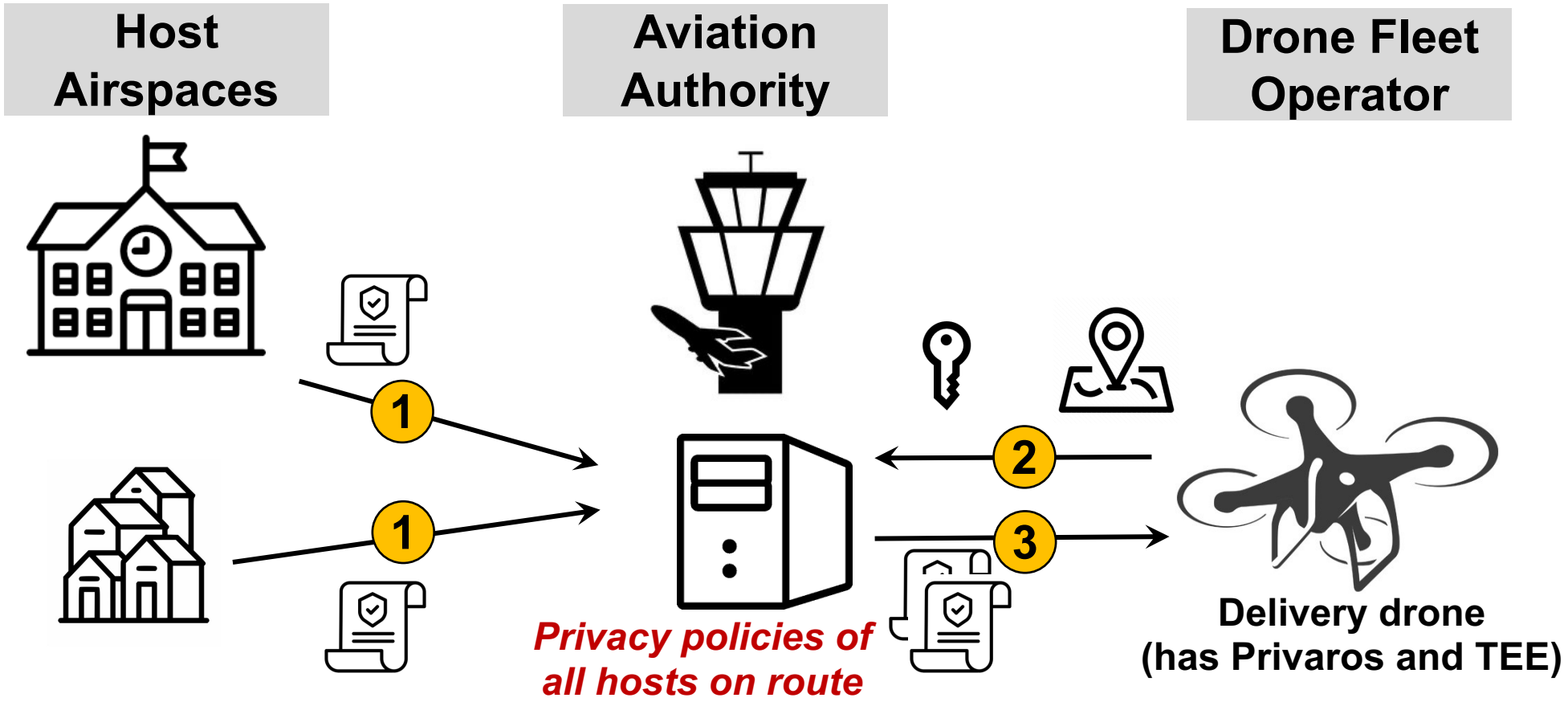
1 Host airspaces specify their privacy policies and send it to the aviation authority



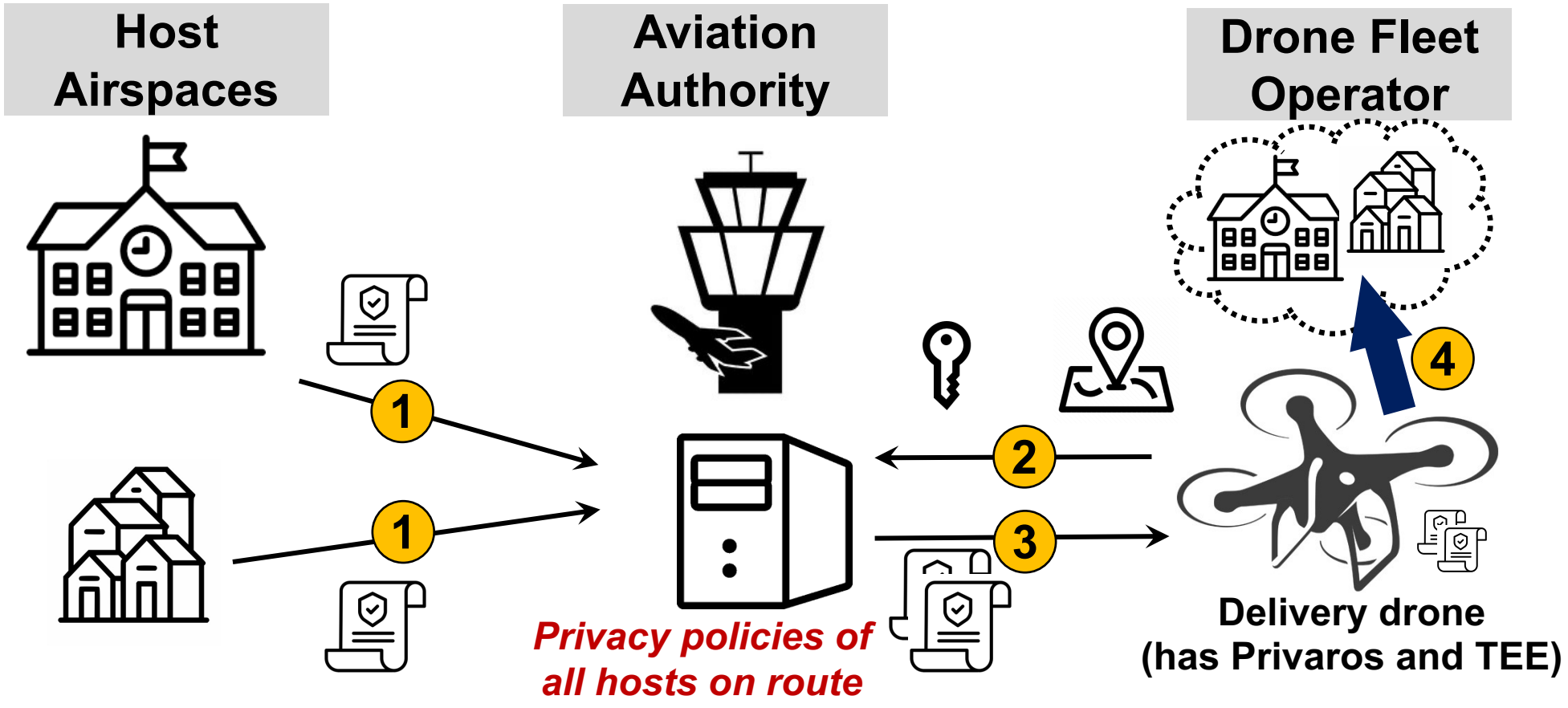
2 Drone sends its identity, attestation, and delivery route to aviation authority prior to delivery run



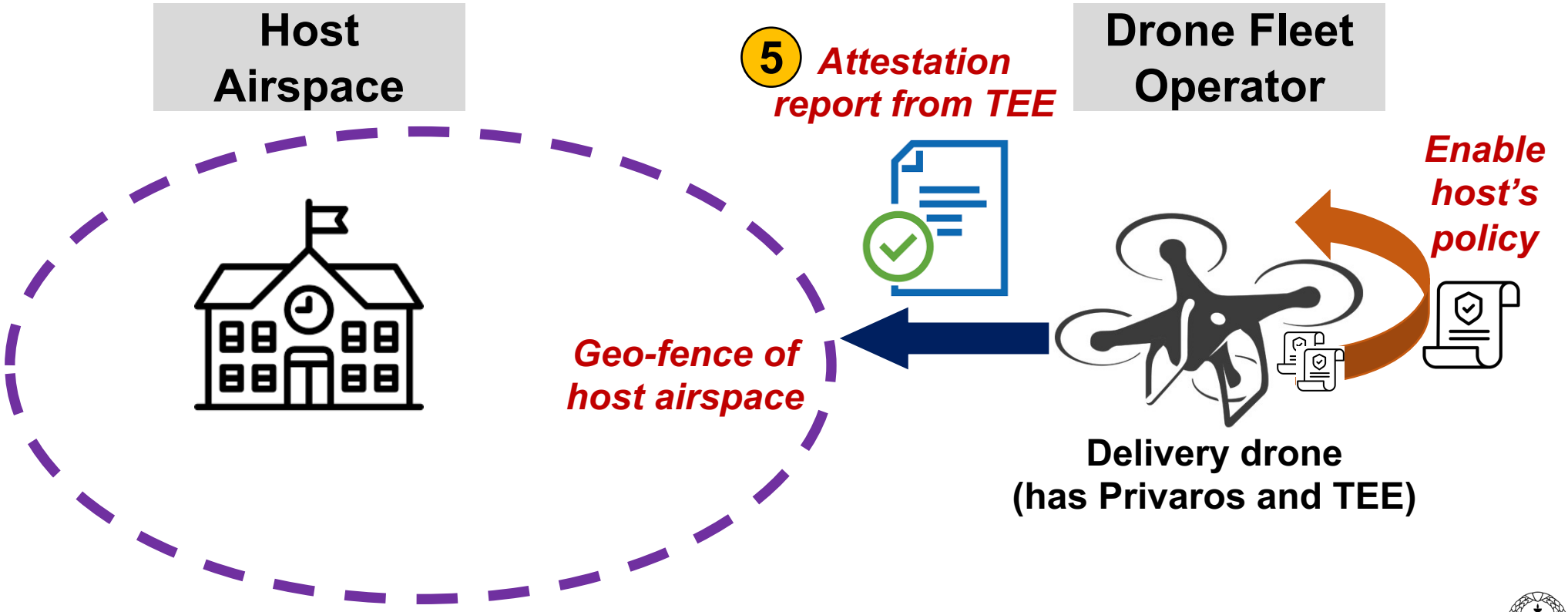
3 Aviation authority sends the drone the privacy policies of all host airspaces in its delivery run



4 Drone loads privacy policies and starts route



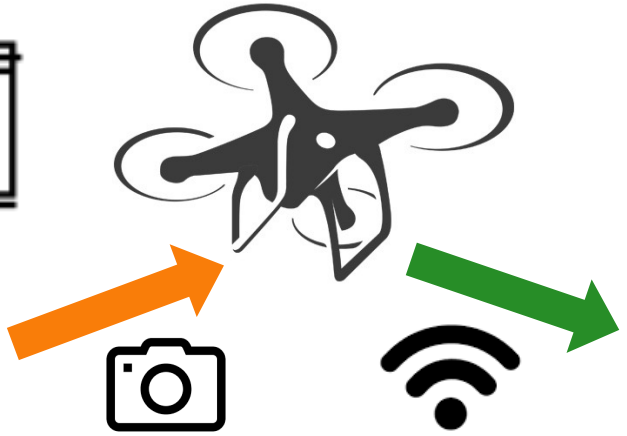
5 Drone applies host's privacy policy before entering airspace. Drone proves to host that it is equipped with Privaros and that the host's policy is applied



Role of TEE on guest drone

- Trusted application identified by a host must execute on guest drone before entering host airspace.
- Hardware-based TEE on guest drone attests that the drone runs these trusted applications atop Privaros.

Example policy: **Blur-Exported**

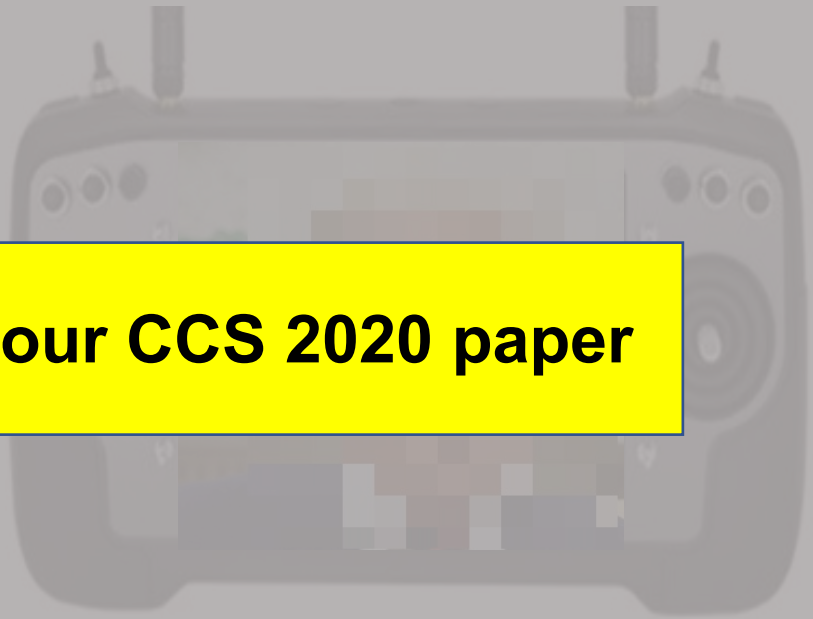


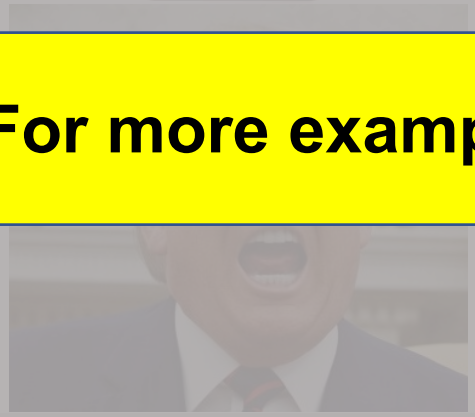
Delivery drone running **Privaros**

Host airspace → sensitive objects captured in video feed of drone

First-person view on untrusted remote control → sensitive parts hidden

Example policy: **Blur-Exported**





Host airspace → sensitive objects captured in video feed of drone

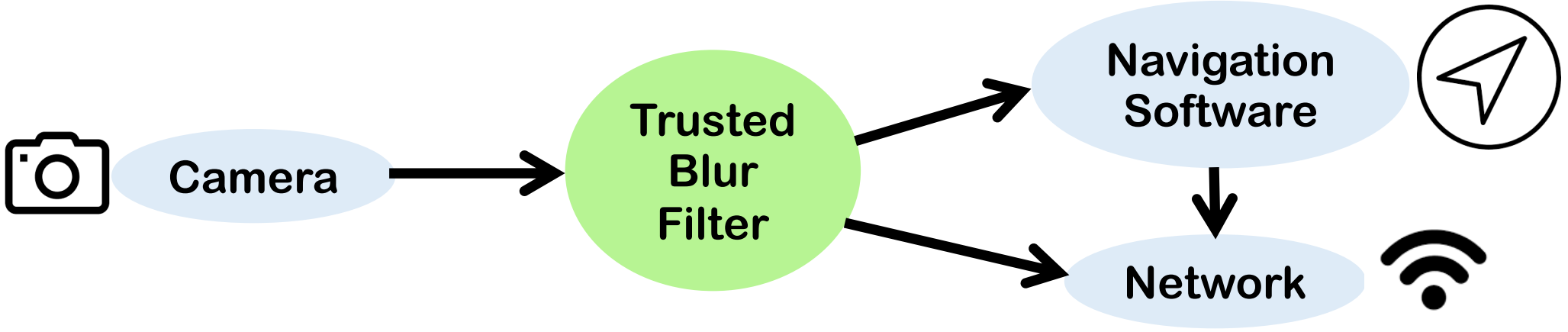
Delivery drone running **Privaros**

First-person view on untrusted remote control → sensitive parts hidden

For more examples of policies, see our CCS 2020 paper

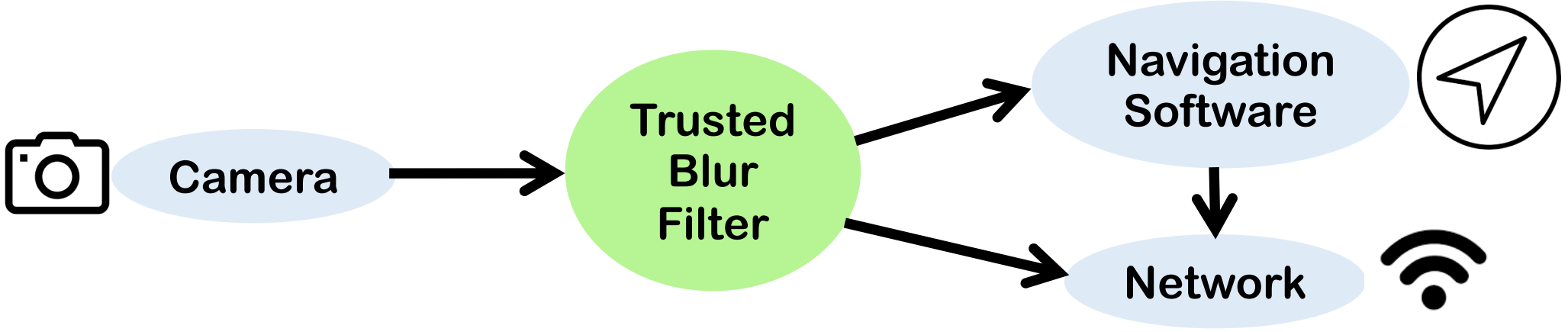
Policies as communication graphs

- Hosts use a **communication graph** to specify their policy, which restricts how applications on the drone can communicate with each other.



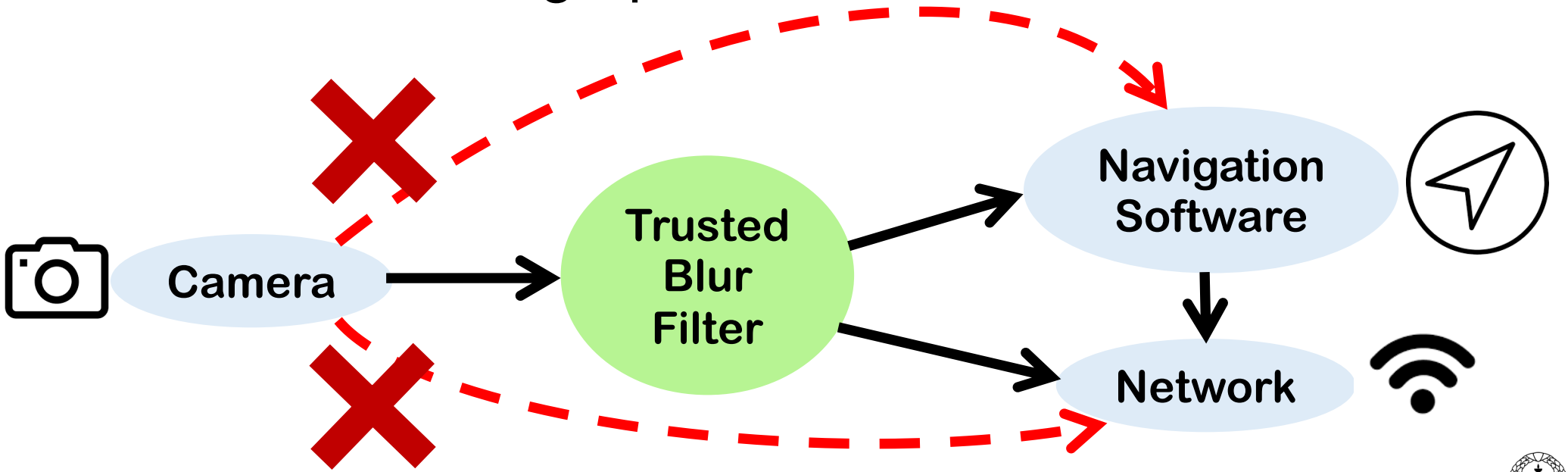
Trusted applications

- **Trusted applications** running on the drone process sensitive data before the data leaves the drone.
- Hosts identify these trusted applications that they entrust with data declassification.



Mandatory access control

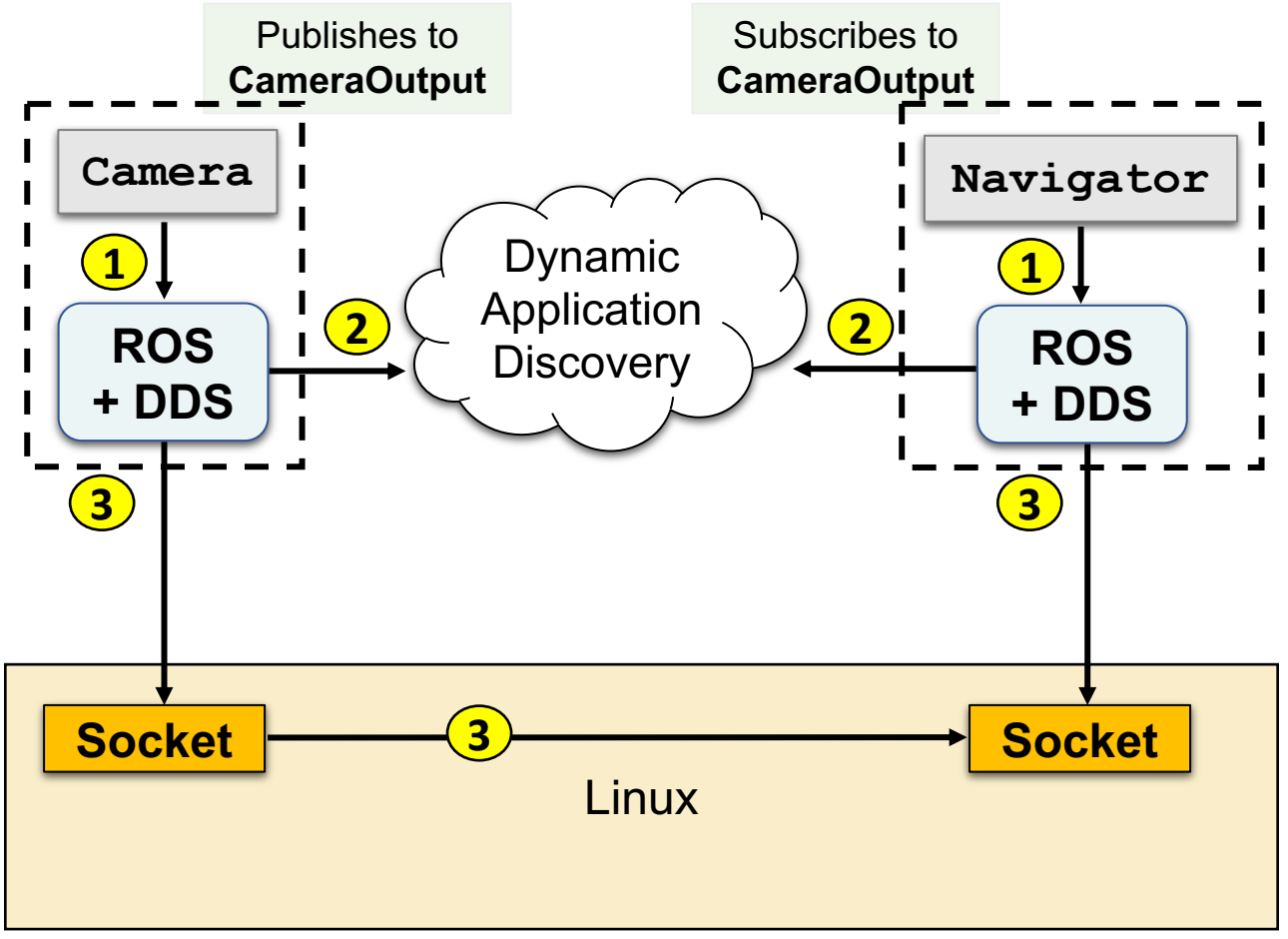
- Privaros uses mandatory access control to ensure that applications communicate as specified by the communication graph.



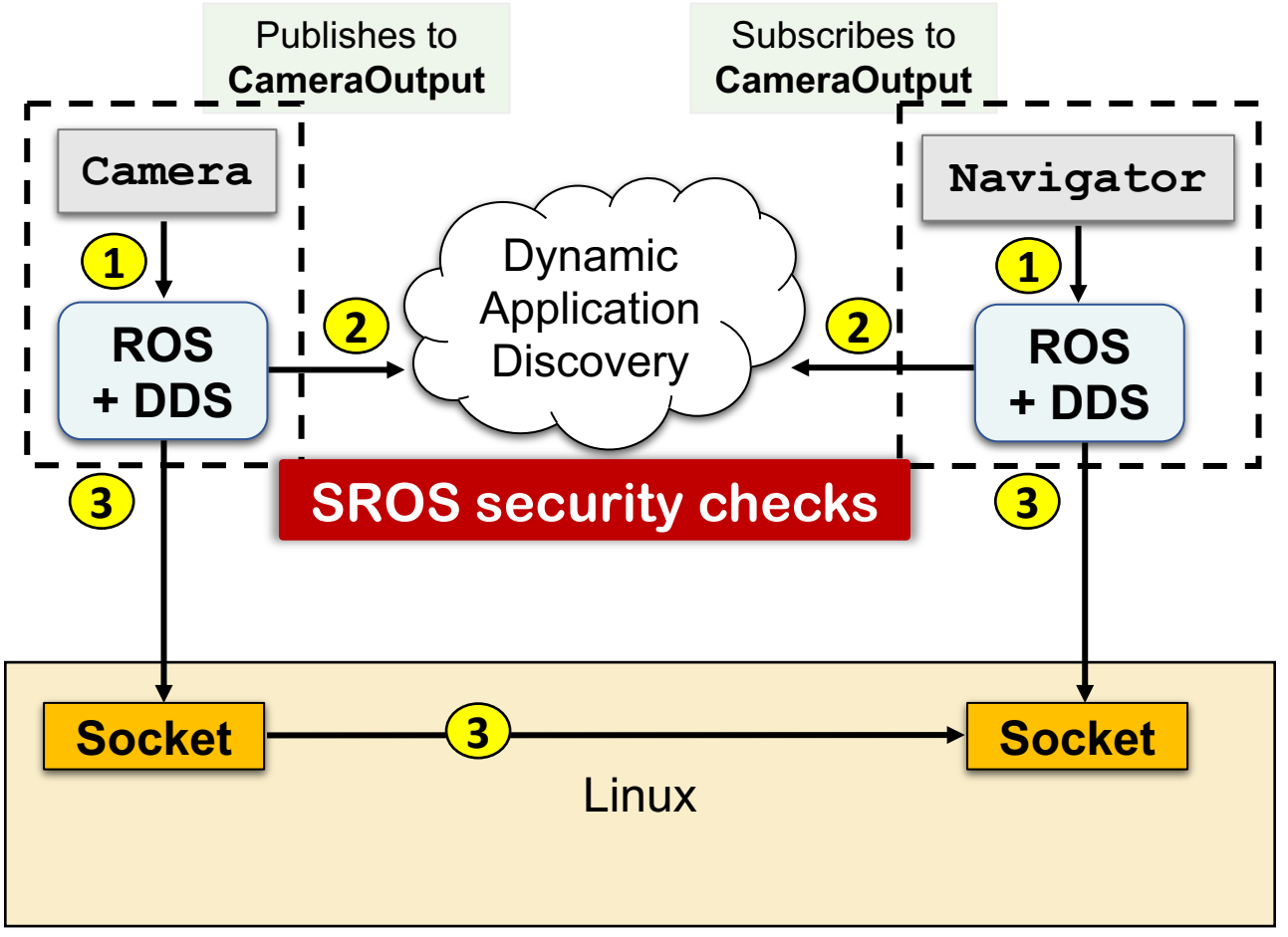
Existing solutions: Secure ROS

- The Secure ROS (SROS) project already provides some mechanisms for access control.
- Applications declare manifests and only applications with matching topics can communicate.
- Manifests are digitally signed by developers and therefore are cryptographically bound to the applications they are associated with.

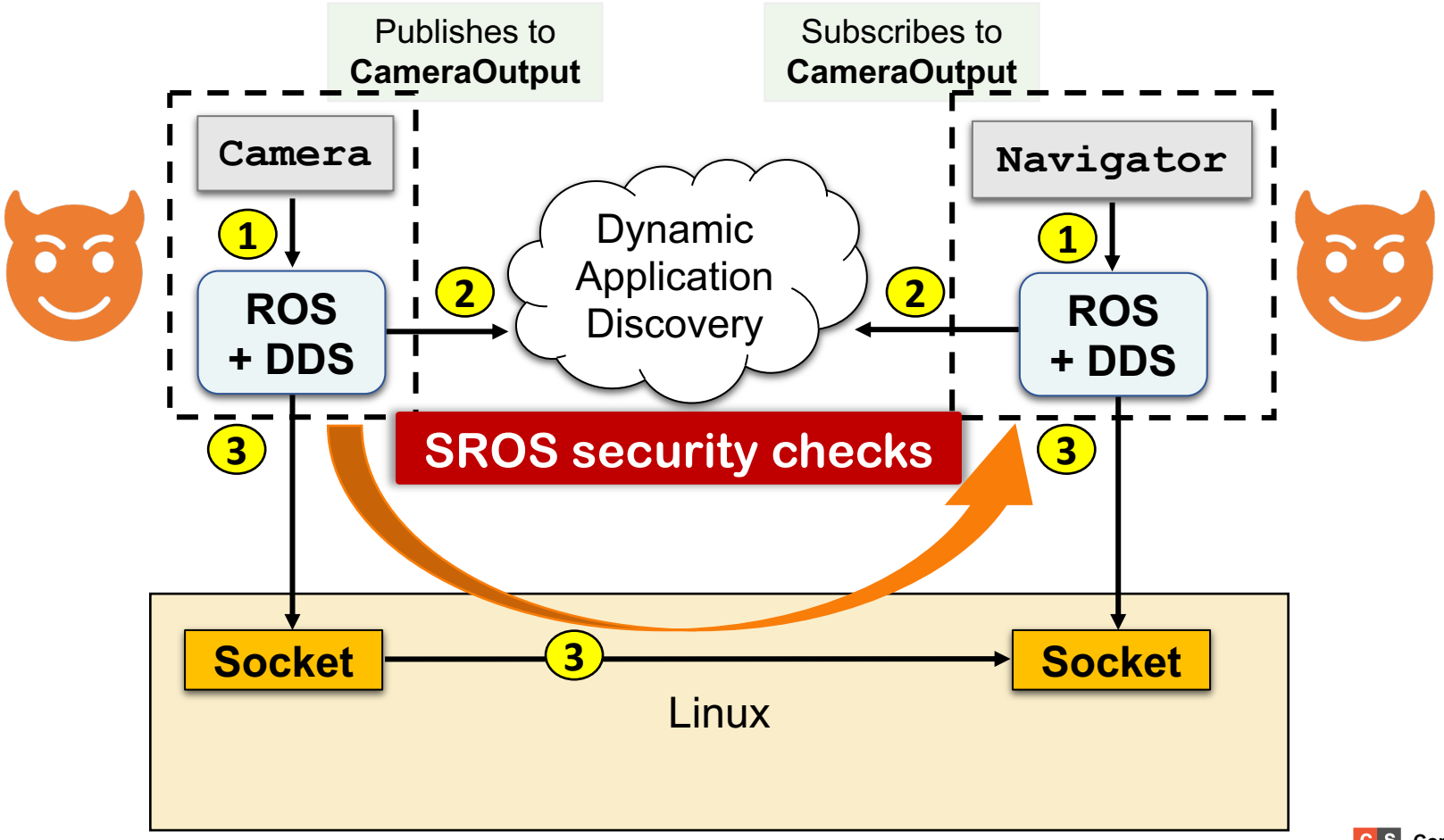
Communication in ROS



SROS mediates ROS communication



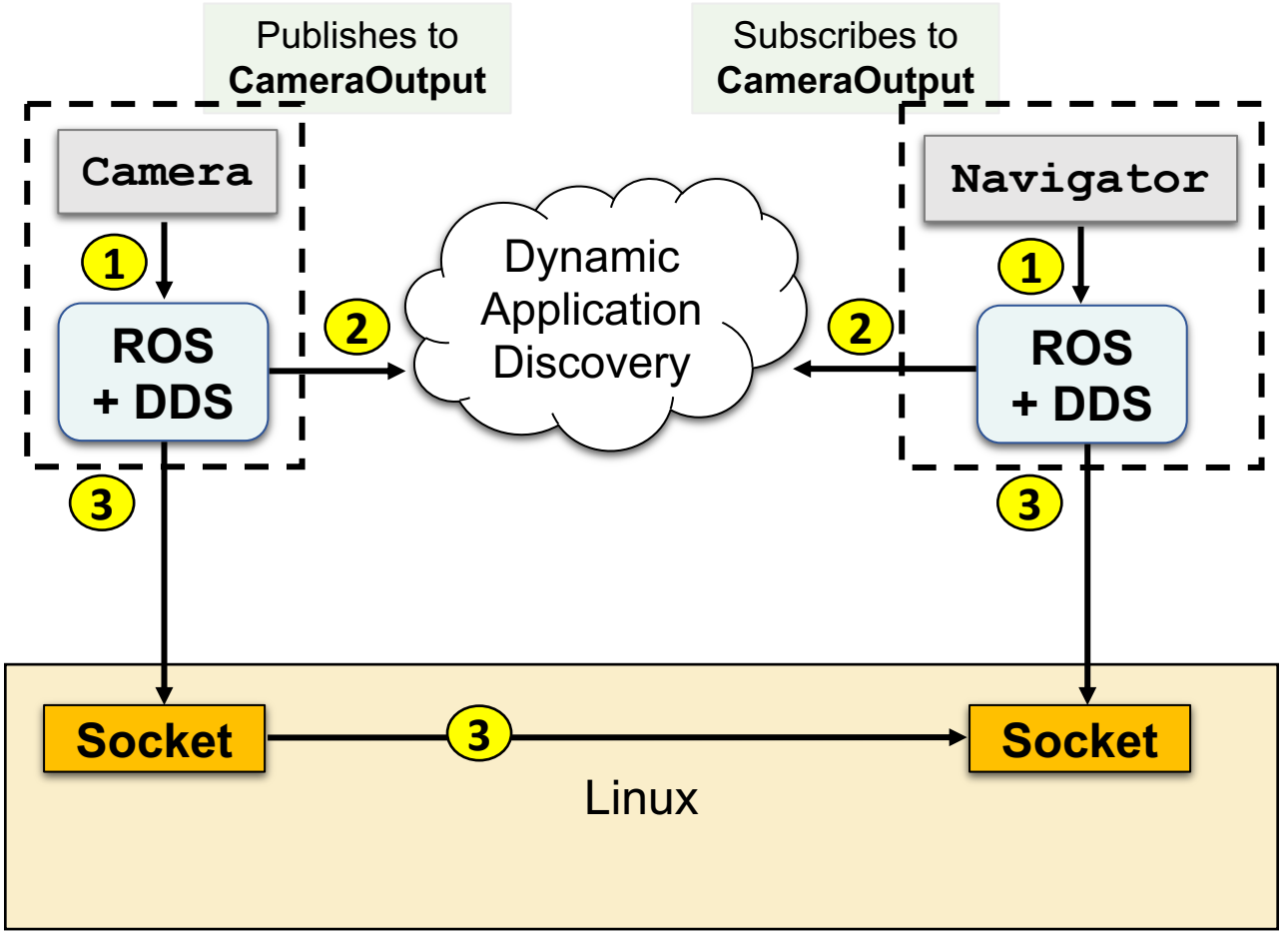
Shortcomings of SROS



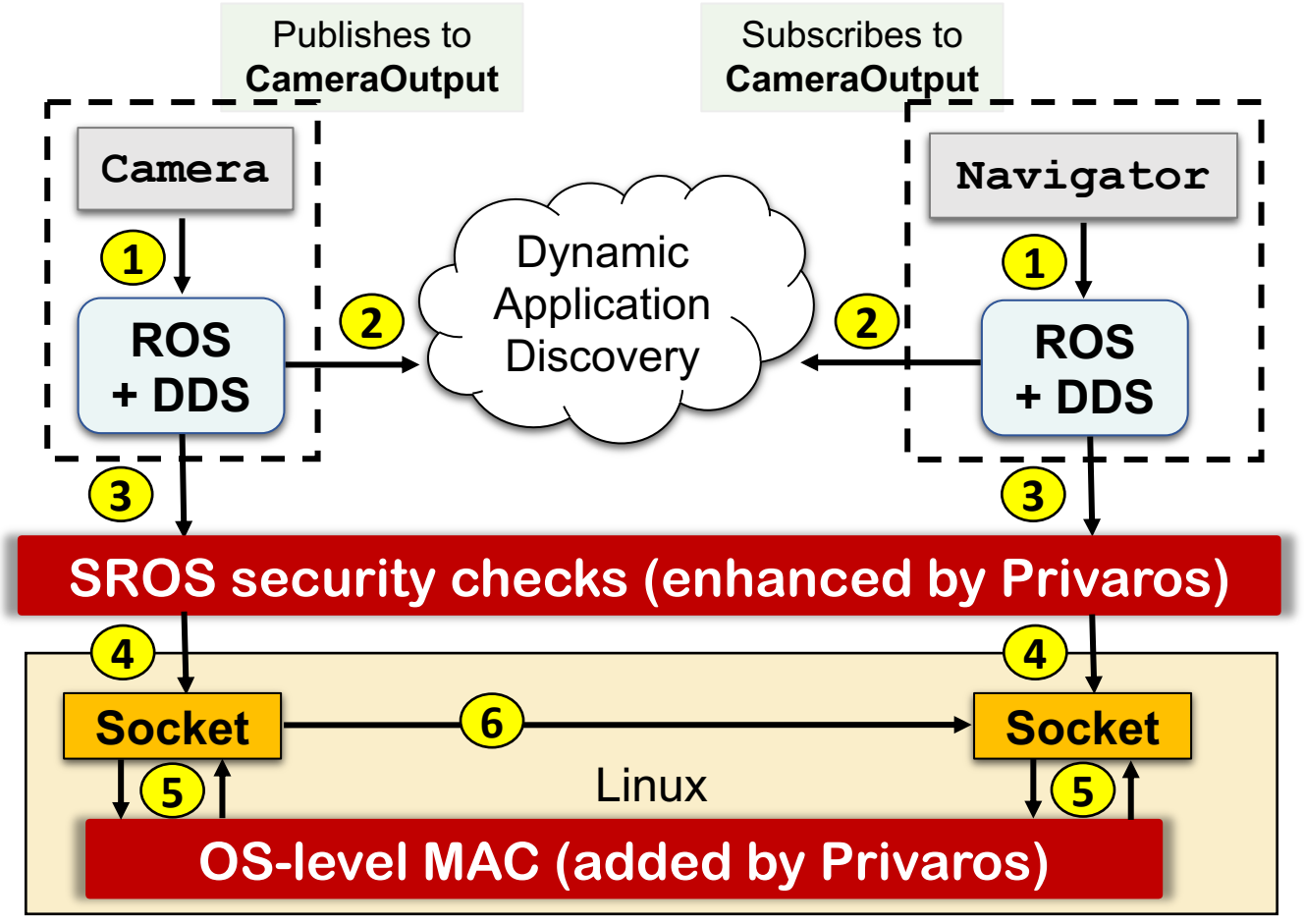
Shortcomings of SROS

- Enforcement of application manifests happens only when the communication happens within the purview of SROS (using SROS primitives)
- Easy to bypass via low-level code in the application (e.g., a system call to open a socket or shared memory)
- Manifests only determine the next hop of communication and there is no end-to-end reasoning of application data usage: MAC policy exposes end-to-end application behavior.

Mechanisms in Privaros

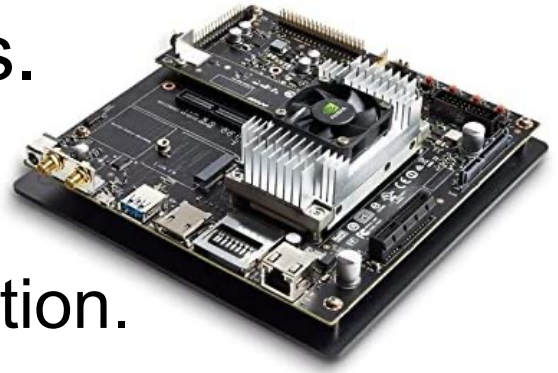


Mechanisms in Privaros



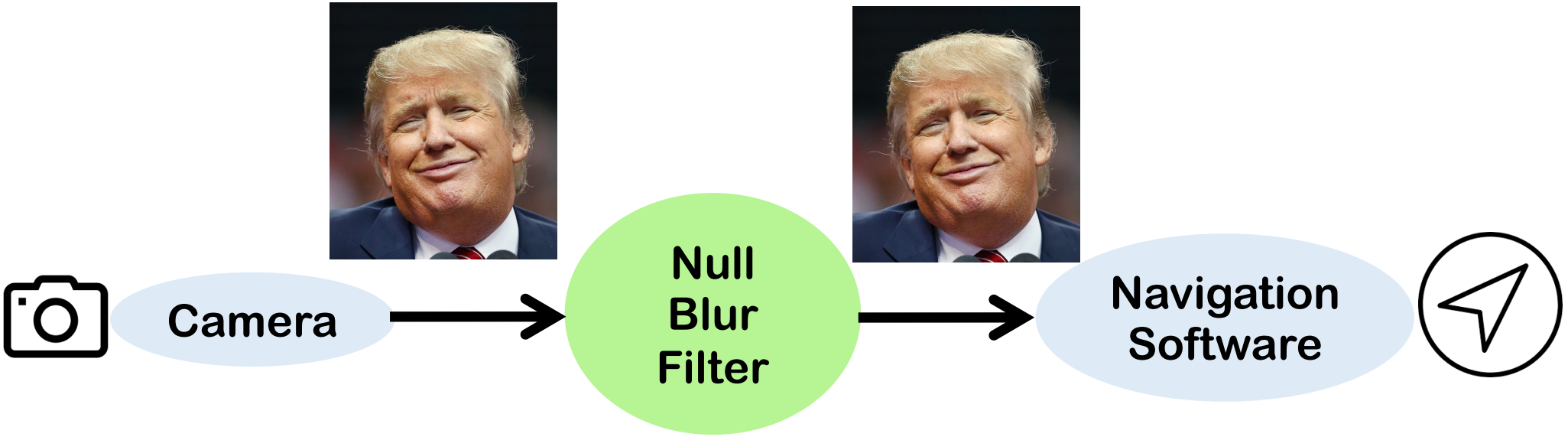
Snippet from our evaluation

- What is the **performance impact of redirecting flows** through trusted applications?
- **Experimental Platform**: **Nvidia Jetson TX2** evaluation board running Privaros.

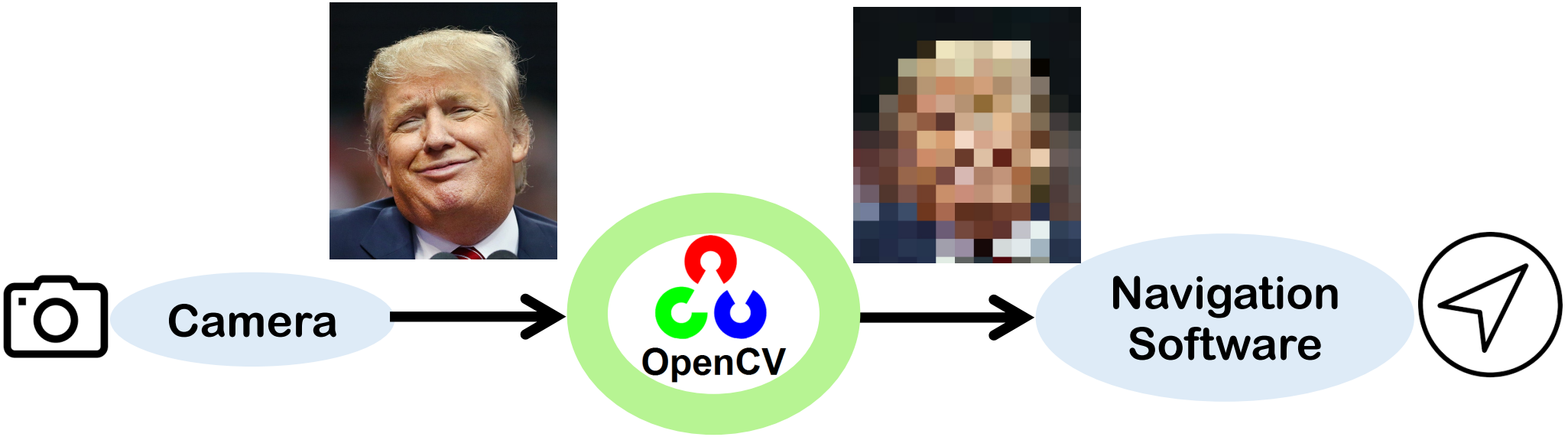


- **In the paper**:
  - **Security and robustness** evaluation.
  - Performance evaluation with **microbenchmarks**.

Scenario	Latency (ms)	Power (mW)
No redirection	8.1	4749.4

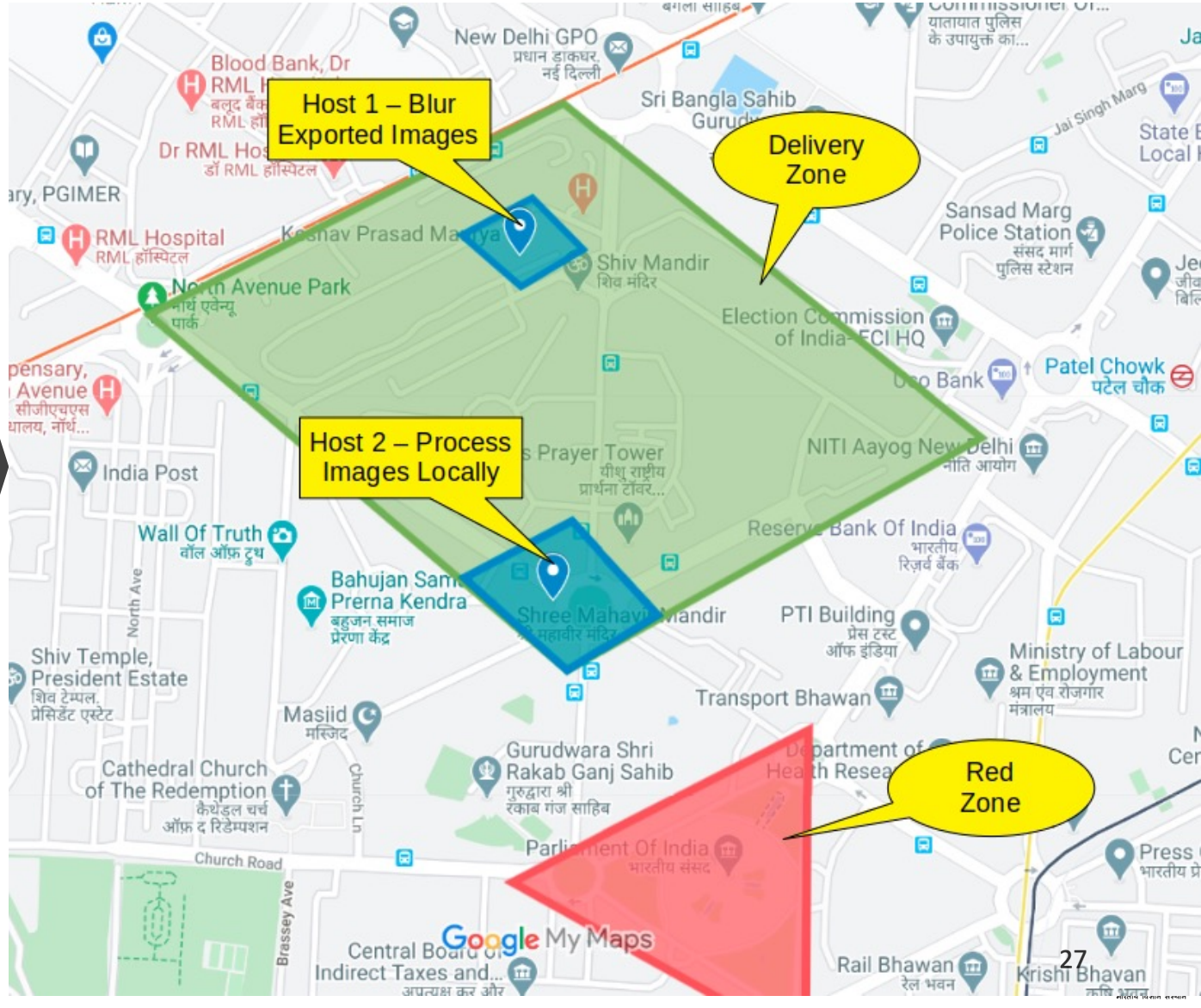


Scenario	Latency (ms)	Power (mW)
No redirection	8.1	4749.4
Null blur filter	17.5 (+115.5%)	4836.2 (+1.8%)



Scenario	Latency (ms)	Power (mW)
No redirection	8.1	4749.4
Null blur filter	17.5 (+115.5%)	4836.2 (+1.8%)
OpenCV blur filter	21.5 (+164.8%)	5132.4 (+8.1%)

Integration with Digital Sky



For more details

"***Privaros: A Framework for Privacy-Compliant Delivery Drones,***" Rakesh Rajan Beck, Abhishek Vijeev, Vinod Ganapathy.

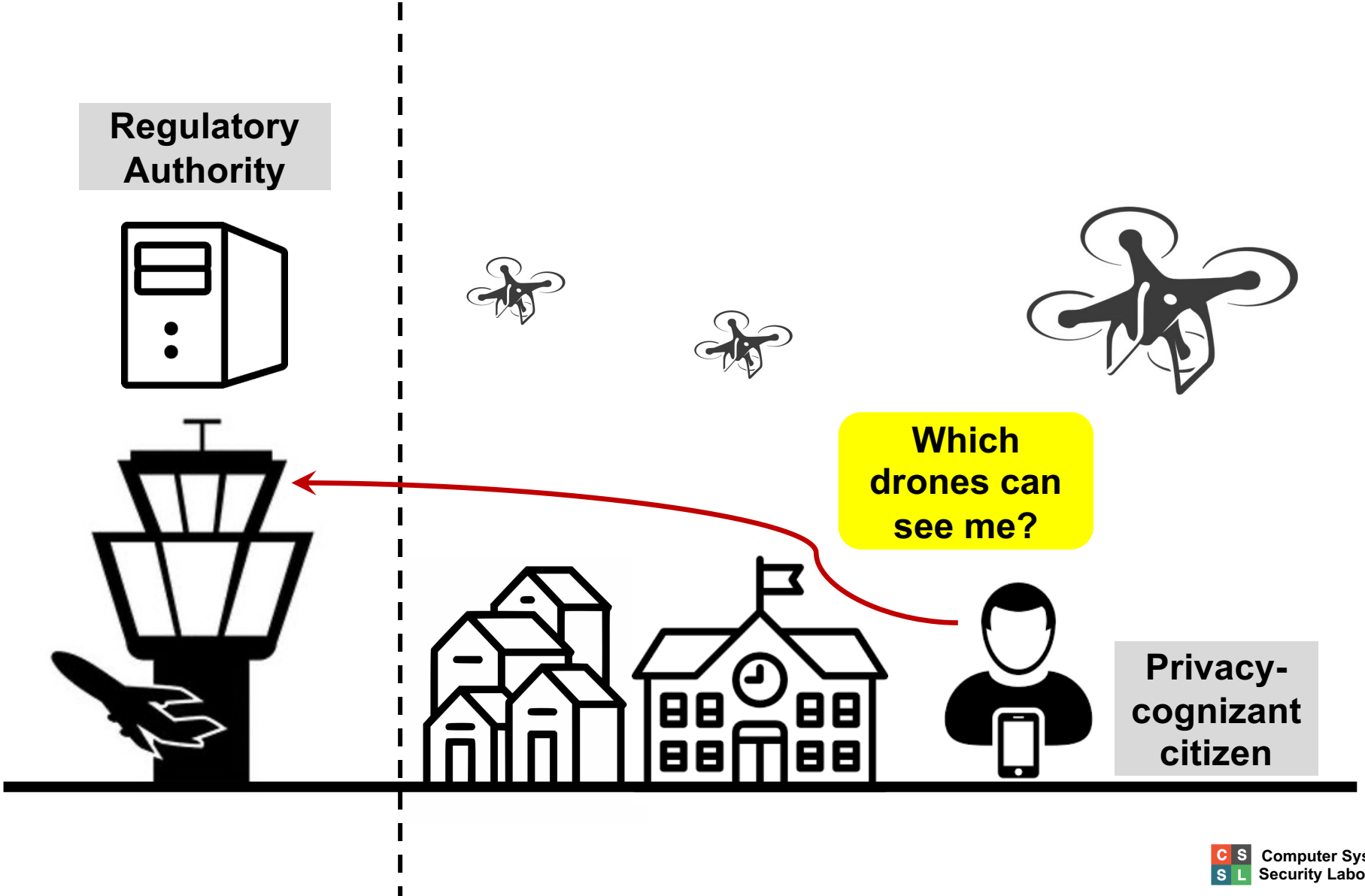
Proceedings of the *ACM Conference on Computer and Communications Security (CCS'20)*, November 2020

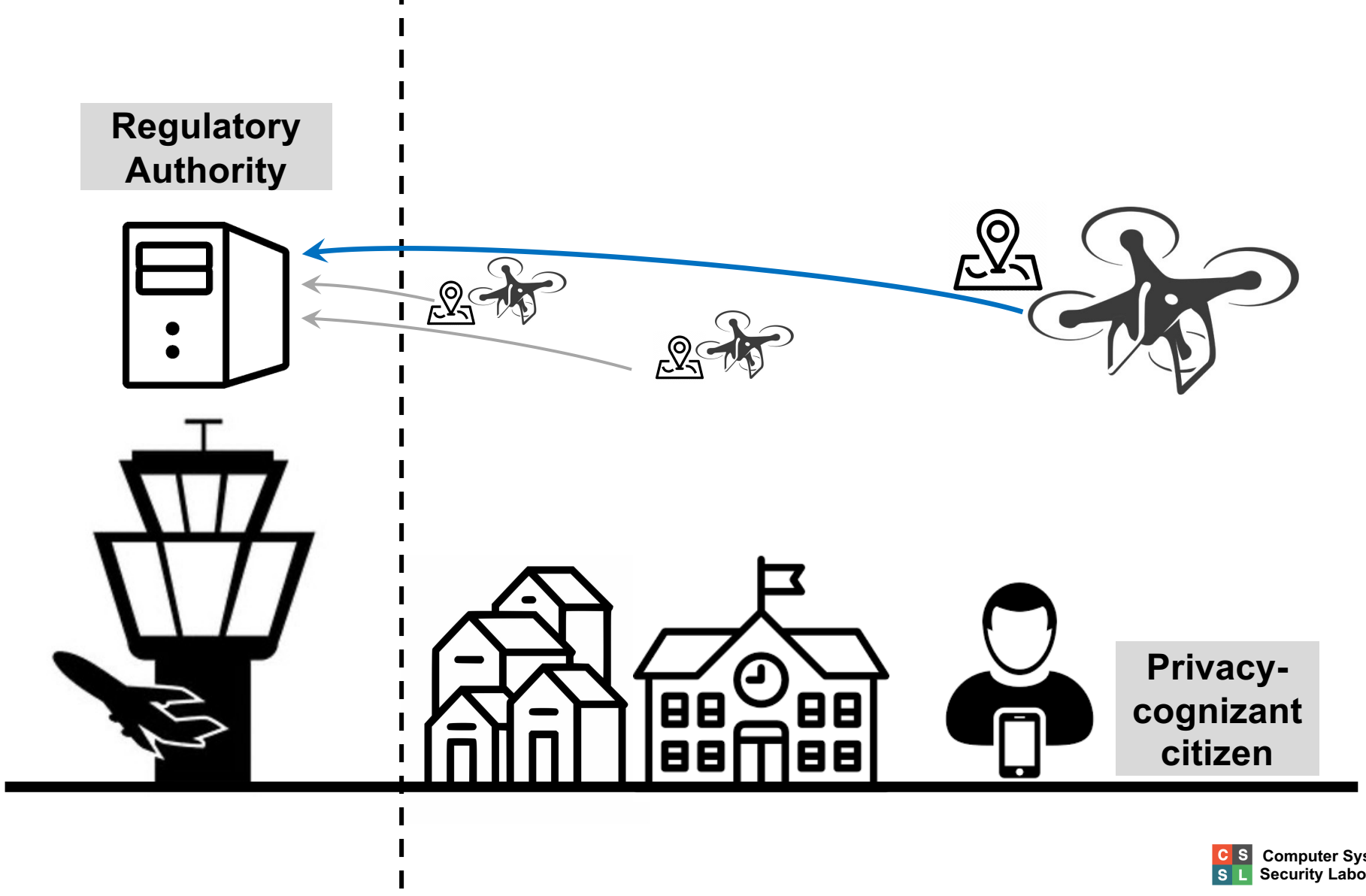
Is the problem solved?

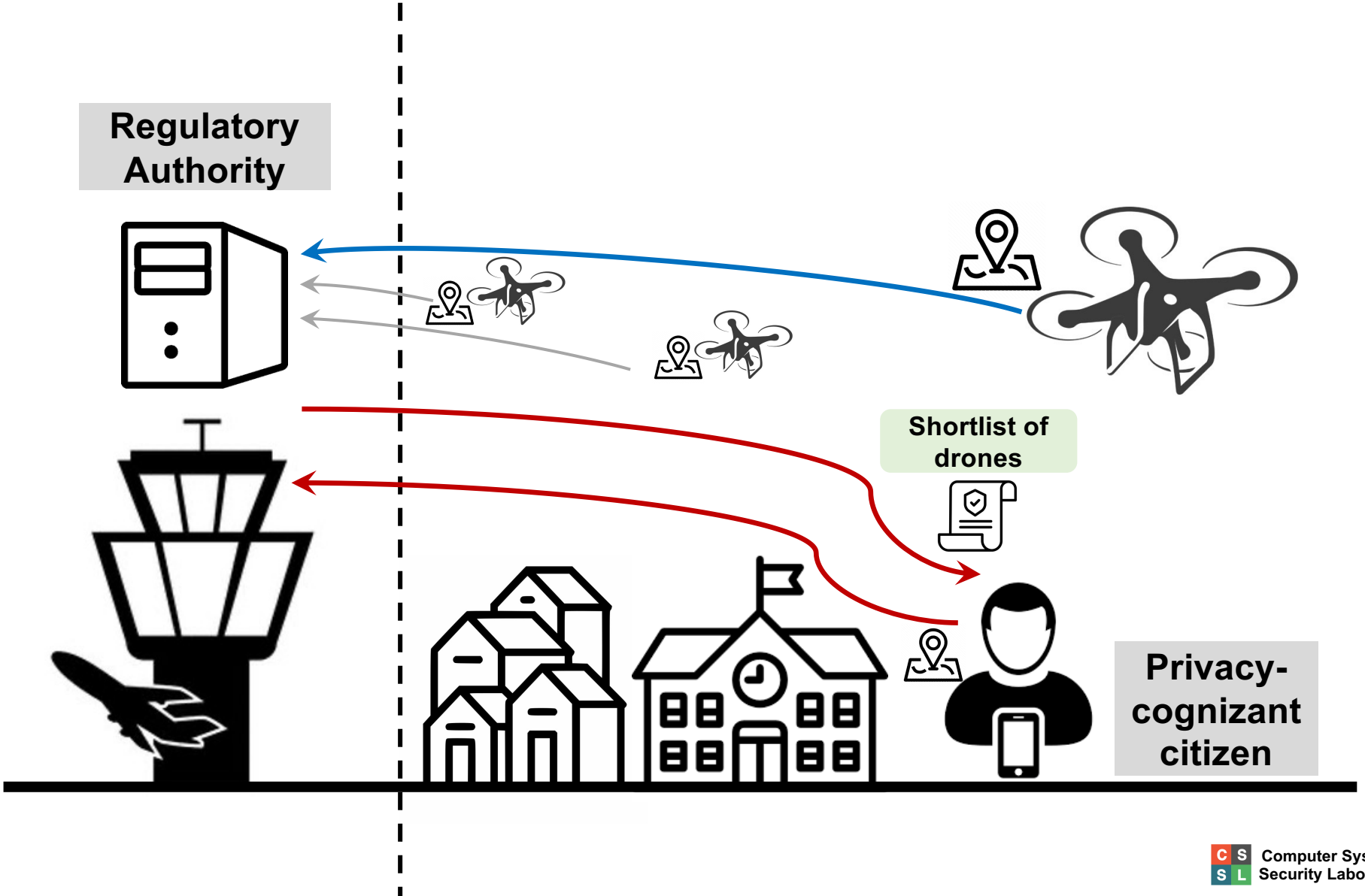
- **NO!** Our solution so far focuses on constraining drones within **host airspaces.**
- Host airspace defines the policies, which protects all citizens within that airspace
- But **what about individual citizens** that may not be located within a host airspace?

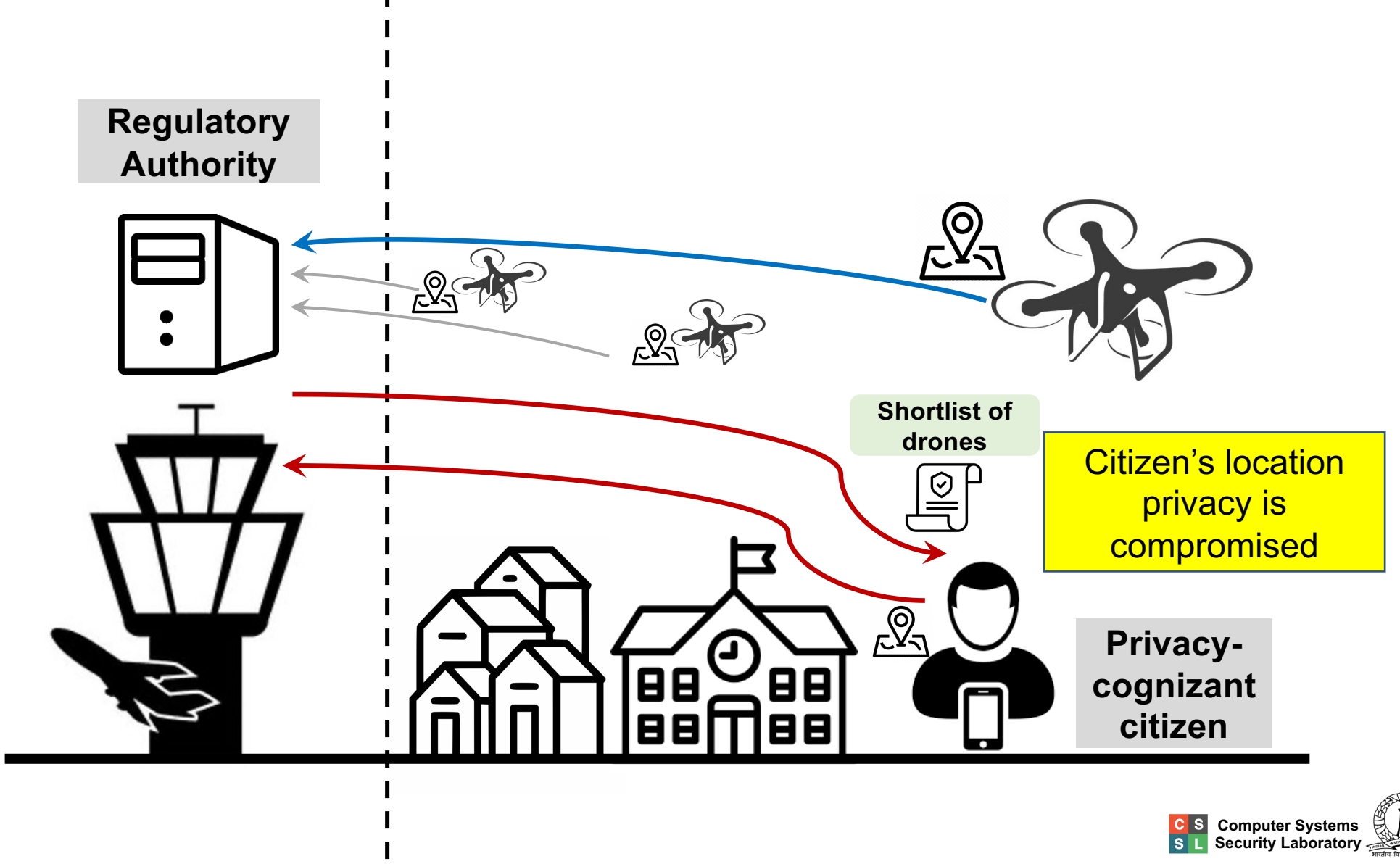
Is the problem solved?

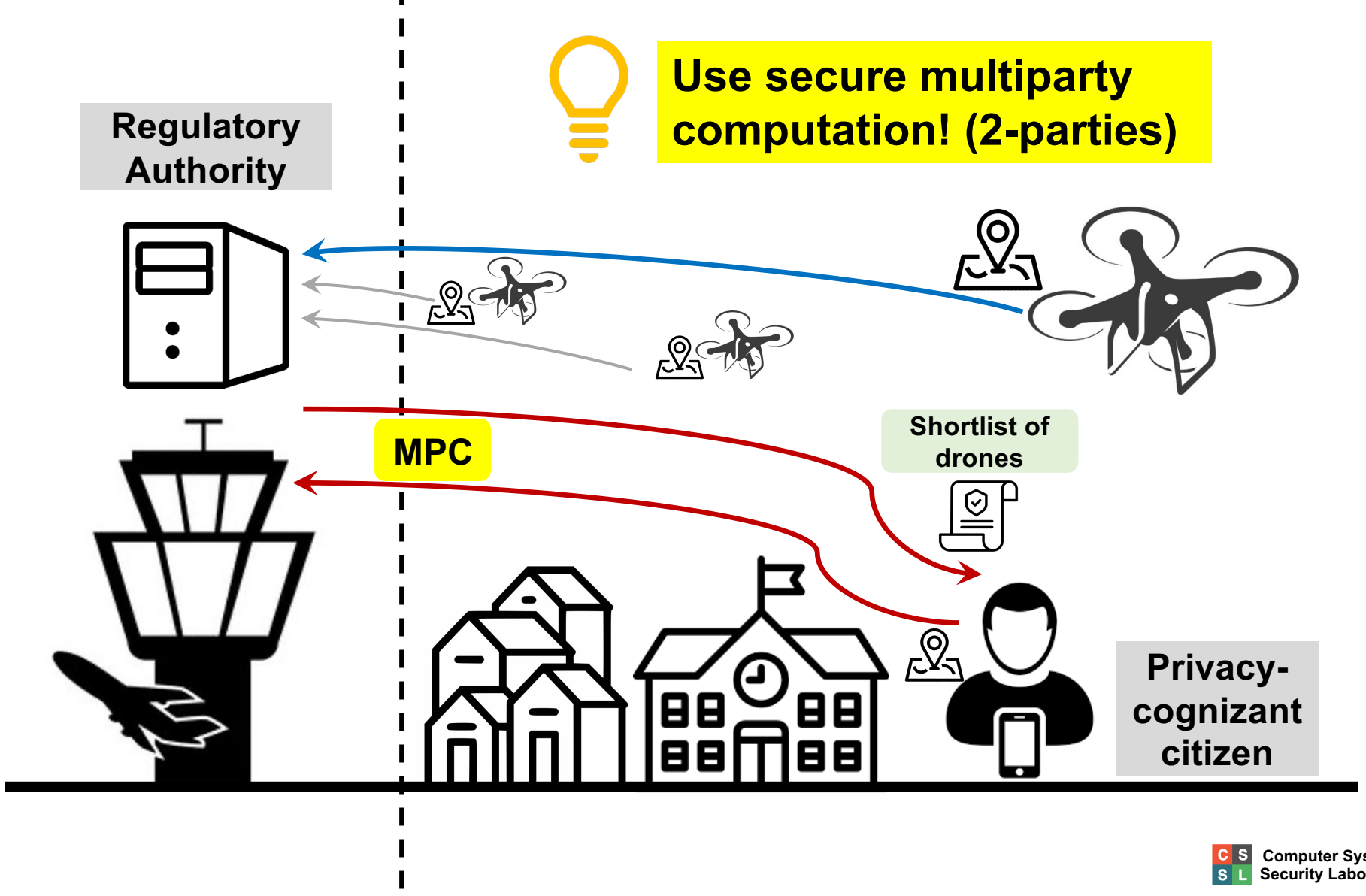
- **NO!** Our solution so far focuses on constraining drones within **host airspaces.**
- Host airspace defines the policies, which protects all citizens within that airspace
- But **what about individual citizens** that may not be located within a host airspace?
- Can we notify citizens if they are within the field of view of a drone's camera? Enter → **Privadome.**


Regulatory Authority
Which drones can see me?
Privacy-cognizant citizen

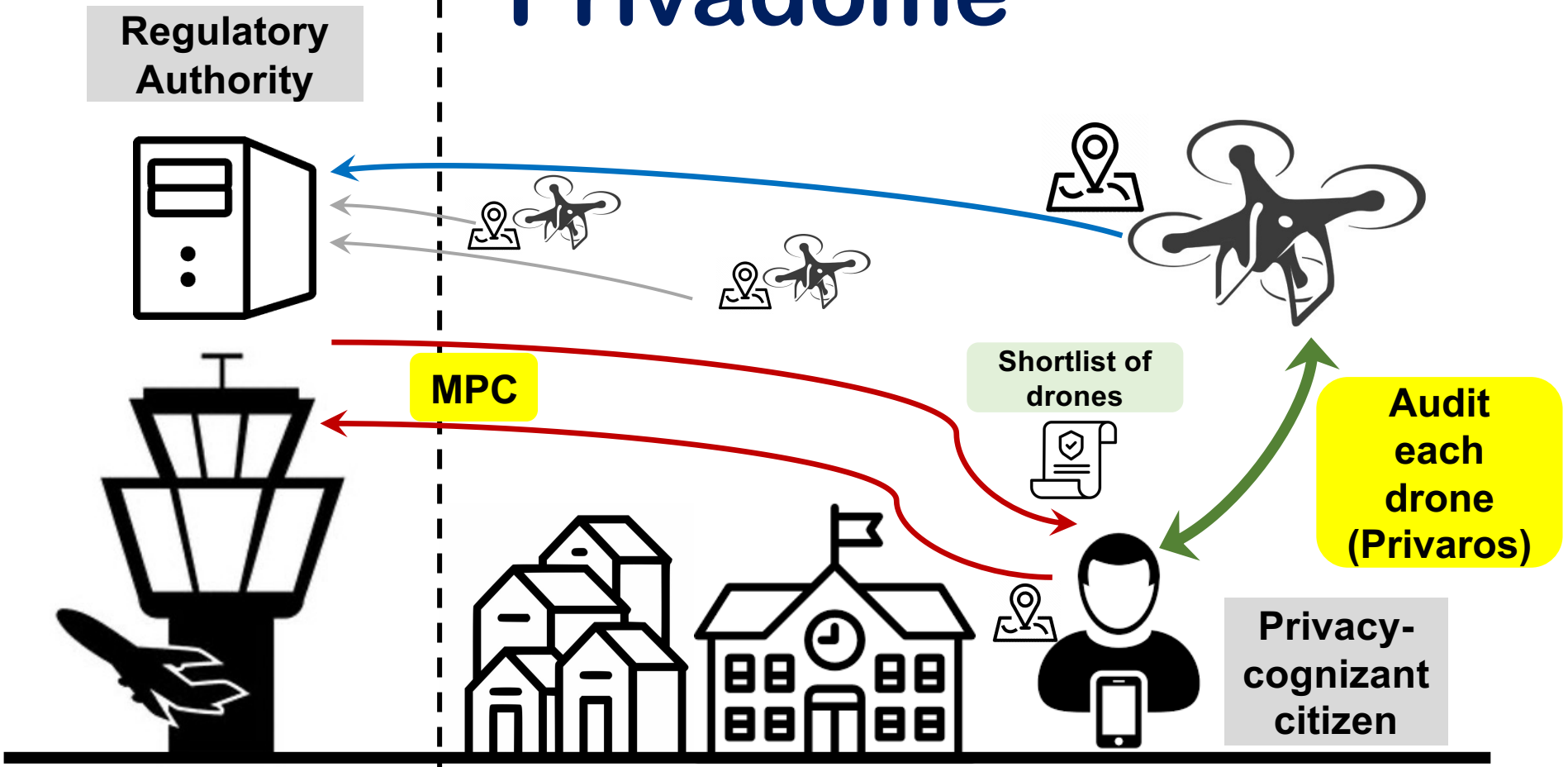

Regulatory Authority
Privacy-cognizant citizen


Regulatory Authority
Shortlist of drones
Privacy-cognizant citizen


Regulatory Authority
Shortlist of drones
Citizen's location privacy is compromised
Privacy-cognizant citizen


Use secure multiparty computation! (2-parties)
Regulatory Authority
MPC
Shortlist of drones
Privacy-cognizant citizen

Privadome


Regulatory Authority
MPC
Shortlist of drones
Audit each drone (Privaros)
Privacy-cognizant citizen

Identifying “interesting” drones?

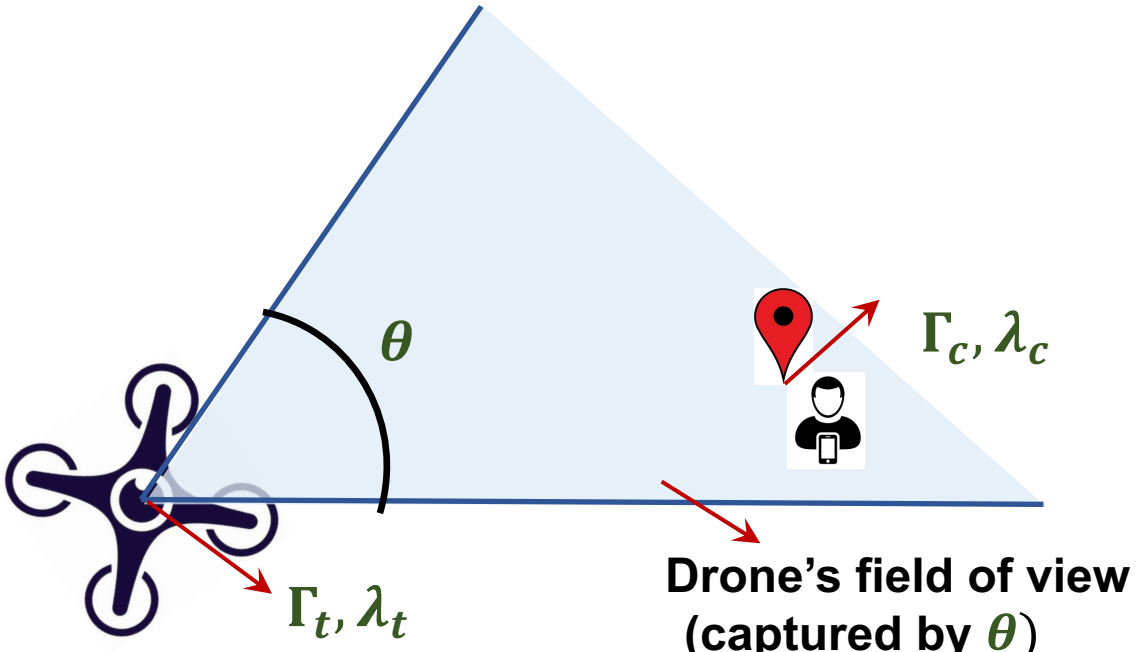
Γ_t, λ_t

Drone’s location

Citizen’s location

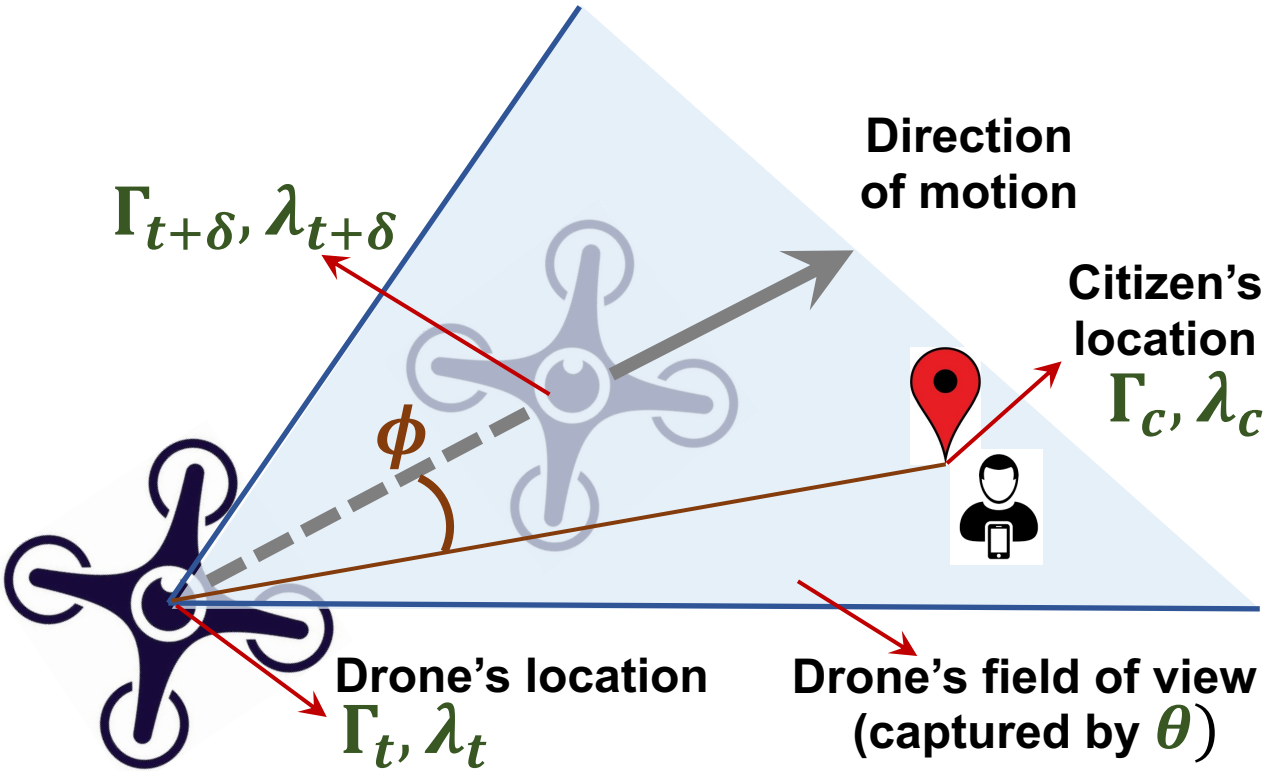
Γ_c, λ_c

Identifying “interesting” drones?

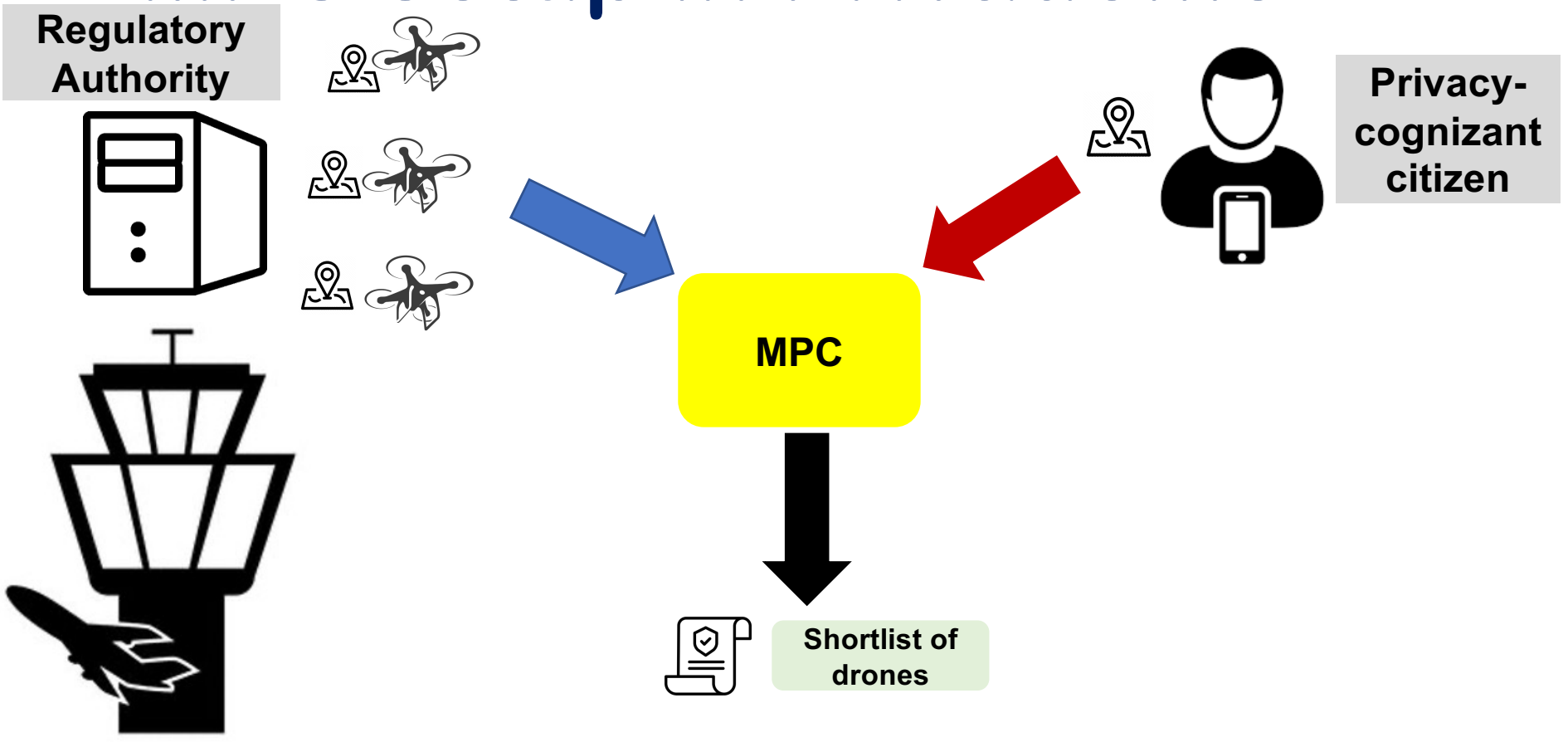


Value of θ is known to the regulatory authority

Identifying “interesting” drones?



MPC setup in Privadome



MPC setup in Privadome

Input: From citizen: Γ_c, λ_c, VicinityRadius.
Input: From regulatory authority: Γ_t, λ_t, $\Gamma_{t+\delta}$, $\lambda_{t+\delta}$, θ.
Output: True if citizen in field of view, else False.
// Each (Γ, λ) is a GPS latitude/longitude pair.

1 Dist = DISTANCE(Γ_c, λ_c, Γ_t, λ_t)
2 **if** (Dist > VicinityRadius) **then return** False
3 $\overrightarrow{D}$ = VECTORIZE(Γ_t, λ_t, $\Gamma_{t+\delta}$, $\lambda_{t+\delta}$)
4 $\overrightarrow{C}$ = VECTORIZE(Γ_t, λ_t, Γ_c, λ_c)
5 $\phi = \arccos((\overrightarrow{D} \cdot \overrightarrow{C}) / (|\overrightarrow{D}| \times |\overrightarrow{C}|))$
6 **if** ($\phi \leq \theta$) **then return** True **else return** False

Challenge 1: Side-channels

Input: From citizen: Γ_c, λ_c, VicinityRadius.
Input: From regulatory authority: Γ_t, λ_t, $\Gamma_{t+\delta}$, $\lambda_{t+\delta}$, θ.
Output: True if citizen in field of view, else False.
// Each (Γ, λ) is a GPS latitude/longitude pair.

1 Dist = DISTANCE(Γ_c, λ_c, Γ_t, λ_t)
2 **if** (Dist > VicinityRadius) **then return** False
3 $\overrightarrow{D}$ = VECTORIZE(Γ_t, λ_t, $\Gamma_{t+\delta}$, $\lambda_{t+\delta}$)
4 $\overrightarrow{C}$ = VECTORIZE(Γ_t, λ_t, Γ_c, λ_c)
5 $\phi = \arccos((\overrightarrow{D} \cdot \overrightarrow{C}) / (|\overrightarrow{D}| \times |\overrightarrow{C}|))$
6 **if** ($\phi \leq \theta$) **then return** True **else return** False

Avoiding side channels

Challenge 2: Performance

Input: From citizen: Γ_c, λ_c, VicinityRadius.
Input: From regulatory authority: Γ_t, λ_t, $\Gamma_{t+\delta}$, $\lambda_{t+\delta}$, θ.
Output: True if citizen in field of view, else False.
// Each (Γ, λ) is a GPS latitude/longitude pair.

1 Dist = DISTANCE(Γ_c, λ_c, Γ_t, λ_t)
2 **if** (Dist > VicinityRadius) **then return** False
3 $\overrightarrow{D}$ = VECTORIZE(Γ_t, λ_t, $\Gamma_{t+\delta}$, $\lambda_{t+\delta}$)
4 $\overrightarrow{C}$ = VECTORIZE(Γ_t, λ_t, Γ_c, λ_c)
5 $\phi = \arccos((\overrightarrow{D} \cdot \overrightarrow{C}) / (|\overrightarrow{D}| \times |\overrightarrow{C}|))$
6 **if** ($\phi \leq \theta$) **then return** True **else return** False

Costly operations in MPC

Practicality of Privadome at city-scale

Amount of data consumed on the citizen's mobile device per query

Number of drones in city	Data consumed (MBs)
100	0.972
200	1.910
500	4.723
1000	9.411
2000	18.788
10,000	93.800

Practicality of Privadome at city-scale

Amount of data consumed on the citizen's mobile device per query

Number of drones in city	Data consumed (MBs)
100	0.972
200	1.910
500	4.723
1000	9.411
2000	18.788
10,000	93.800

Practicality of Privadome at city-scale

↓ Number of drones in city	Query latency at citizen's device	
	LAN (milliseconds)	WAN (seconds)
100	6.029±1.231	4.023±0.680
200	12.513±1.057	6.378±0.834
500	31.196±3.700	10.791±1.837
1000	293.494±82.340	21.091±2.013
2000	830.492±133.611	34.757±3.143
10,000	5161.938±1162.962	282.508±52.479

Practicality of Privadome at city-scale

↓ Number of drones in city	Query latency at citizen's device	
	LAN (milliseconds)	WAN (seconds)
100	6.029±1.231	4.023±0.680
200	12.513±1.057	6.378±0.834
500	31.196±3.700	10.791±1.837
1000	293.494±82.340	21.091±2.013
2000	830.492±133.611	34.757±3.143
10,000	5161.938±1162.962	282.508±52.479

For more details

"***Privadome: Protecting Citizen Privacy from Delivery Drones***", Gokulnath Pillai, Eikansh Gupta, Ajith Suresh, Vinod Ganapathy, and Arpita Patra.

Please email me if you're interested in reading a draft!

Future opportunities

- Airbus study indicates a drone density of 16,667 drones per hour over a city the size of Paris by 2035 → MPC practical for short to medium term?
- Our threat model considers a semi-trusted model, targeting primarily delivery drones. How to deal with malicious operators?
  - Evil operators who attach a Go-Pro camera to the drone?
  - Non-regulated sector -- rogue drone operators?

Thank you

Vinod Ganapathy

vg@iisc.ac.in

http://www.csa.iisc.ac.in/~vg

Computer Systems Security Laboratory

IISc Bangalore